ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Γεώργιος Μαρινάκης

Τίτλος : **Μέθοδοι Αξιολόγησης Κρυπτογραφικών Συστημάτων**

Αθήνα, Δεκέμβριος 2017

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης Πληροφορίας
και Τεχνολογίας Υλικών

Μέθοδοι Αξιολόγησης Κρυπτογραφικών Συστημάτων

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Γιώργος Μαρινάκης

Συμβουλευτική Επιτροπή: Νικόλαος Ουζούνογλου
Ιάκωβος Βενιέρης
Δήμητρα Κακλαμάνη

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την η Δεκεμβρίου 2017.

.....	.....	.....
Νικόλαος Ουζούνογλου Καθηγητής ΕΜΠ	Ιάκωβος Βενιέρης Καθηγητής ΕΜΠ	Δήμητρα Κακλαμάνη Καθηγήτρια ΕΜΠ
.....	.....	.....
Δέσποινα Πολέμη Καθηγήτρια Παν.Πειραιά	Νικόλαος Δάρας Καθηγητής ΣΣΕ	Κων/νος Παπαοδυσσεύς Καθηγητής ΕΜΠ

.....
Παναγιώτης Τσανάκας
Καθηγητής ΕΜΠ

Αθήνα , Δεκέμβριος 2017

……
Γιώργος Μαρινάκης
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών ΕΜΠ

Περίληψη

Καθώς αυξάνουν τα κρυπτογραφικά συστήματα τα οποία κυκλοφορούν στο εμπόριο, αυξάνεται και η ανάγκη των χρηστών να αναπτύξουν δική τους τεχνογνωσία για να ελέγχουν, να αξιολογούν, να συγκρίνουν και τελικά να επιλέγουν τα ασφαλέστερα κρυπτοσυστήματα για τις ανάγκες τους. Ωστόσο, η ολοκληρωμένη αξιολόγηση των κρυπτοσυστημάτων είναι ένα εξαιρετικά εξειδικευμένο και ευαίσθητο έργο για το οποίο υπάρχουν ελάχιστες αναφορές στη διεθνή βιβλιογραφία. Ο στόχος λοιπόν της παρούσας διατριβής είναι να σχεδιάσει μια επιστημονική μεθοδολογία για την αξιολόγηση της συνολικής ασφάλειας που προσφέρει ένα κρυπτογραφικό σύστημα.

Στην πρώτη φάση της διατριβής μελετώνται οι ευπάθειες και οι τρωτότητες των κρυπτογραφικών συστημάτων, καθώς και οι τρόποι με τους οποίους αυτές μπορούν να εντοπιστούν, ώστε να αποφευχθούν οι εναντίον τους κρυπταναλυτικές επιθέσεις. Στη δεύτερη και κύρια φάση, μελετώνται οι τεχνικές παράμετροι και τα διάφορα προβλήματα κατά την αξιολόγηση των κρυπτοσυστημάτων και προτείνονται μέθοδοι και τεχνικές διαδικασίες, με στόχο την όσο το δυνατόν πιο αξιόπιστη αξιολόγηση της ασφάλειάς τους.

Η αξιολόγηση ενός κρυπτοσυστήματος είναι μία πολυσύνθετη εργασία, η οποία περιλαμβάνει πολλά στάδια, διότι αποτελείται από πολλές αλληλοεπιδρούσες μονάδες, οι οποίες πρέπει να εξεταστούν. Η πιο σημαντική μονάδα είναι αυτή του κρυπτογραφικού αλγορίθμου, για αυτό εξετάζεται στο πρώτο στάδιο. Κατ'αρχήν αξιολογείται το μήκος της κλείδας, ως προς την αντοχή του στην εξαντλητική έρευνα. Για το σκοπό αυτό, συγκρίνουμε το μήκος της αξιολογούμενης κλείδας με το ελάχιστο ασφαλές μήκος κλείδας, το οποίο υπολογίζουμε βάσει της σημερινής και της μέλλουσας τεχνολογίας. Κατόπιν αξιολογείται η τυχαιότητα των αλγοριθμικών εξόδων με ειδικούς στατιστικούς ελέγχους, χρησιμοποιώντας ένα συνδυασμό τυχαίας και στρωματοποιημένης δειγματοληψίας. Με κατάλληλο συνδυασμό των αποτελεσμάτων των δύο ανωτέρω αξιολογήσεων, εκτιμούμε την ασφάλεια του αλγορίθμου έναντι κρυπταναλυτικών επιθέσεων.

Μετά την αξιολόγηση του κρυπτογραφικού αλγορίθμου, είναι απαραίτητο να διεξαχθούν και έλεγχοι στους υπόλοιπους μηχανισμούς ασφαλείας του κρυπτοσυστήματος. Αυτοί αφορούν τον τρόπο υλοποίησης και ενσωμάτωσης του κρυπταλγορίθμου εντός του συστήματος, τον τρόπο παραγωγής και διαχείρισης των κλειδών, καθώς και τον τρόπο υλοποίησης των περιφερειακών μηχανισμών ασφαλείας (πρόσβαση χρηστών, ασφάλεια παραβίασης, αυτοέλεγχοι, ασφάλεια ηλεκτρομαγνητικών ακτινοβολιών κλπ.).

Στο τελικό στάδιο, γίνεται μία συνδυαστική επεξεργασία των αποτελεσμάτων της αξιολόγησης του κρυπτογραφικού αλγορίθμου και των υπόλοιπων μηχανισμών ασφαλείας, ώστε να εκτιμήσουμε την συνολική ασφάλεια του κρυπτογραφικού συστήματος.

..... * .....

Λέξεις κλειδιά : Ασφάλεια Πληροφοριών , Κρυπτογραφία

Abstract

As the cryptographic systems that are commercially available are increasing, there is also an increasing need of the users to develop their own know how in order to evaluate, compare and select the most secure cryptographic system for their own needs. However the complete and thorough evaluation of a cryptographic system is an extremely specialized and sensitive work, for which there are very few references in the international literature. Therefore, the aim of this dissertation is to design a scientific methodology in order to evaluate the overall security which offers a cryptographic system.

At the first phase of this dissertation we study the vulnerabilities of the various cryptographic systems, as well as the methods with which we can detect them, in order to avoid cryptanalytic attacks. At the second and most important phase, we study the technical parameters and the various problems of cryptographic systems evaluation and we propose methods and technical procedures in order to achieve the most reliable evaluation of their security.

Cryptographic systems are consisted of many interacted units, therefore their evaluation is a very complicate work with many stages, because we must evaluate the security of all their units. The most important unit is the cryptographic algorithm and therefore we examine it at the first stage. We start with the evaluation of the key length, against the exhaustive key search (Brute Force Attack). For this reason, we compare the key length of the algorithm under evaluation, with the minimum safe key length which we have calculated according to the current and future technology. And then we evaluate the randomness of the algorithm outputs, applying to them specific statistical tests, using a combination of random and stratified sampling. With the proper combination of the results of the above two evaluations, we estimate the strength of the algorithm against cryptanalytic attacks.

After the evaluation of the cryptographic algorithm, it is necessary to test the function of the rest security mechanisms of the cryptographic system. These mechanisms include the implementation and embodiment of the cryptographic algorithm into the system, the production and management of the keys, as well as the implementation of the peripheral security mechanisms (users access control, tamper protection, functional self tests, protection from electromagnetic radiations etc.).

At the final stage, we make a combinational process of the evaluation results of the cryptographic algorithm and the other security mechanisms, in order to estimate the overall security of the cryptographic system.

..... * .....

Key words : Information Security , Cryptography.

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΜΕΘΟΔΟΙ ΑΞΙΟΛΟΓΗΣΗΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Γεώργιος Μαρινάκης

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΘΟΔΟΙ ΑΞΙΟΛΟΓΗΣΗΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1. Ιστορικό

Μέχρι και πριν από τριάντα περίπου χρόνια (έως την δεκαετία του 1980), τα κρυπτογραφικά συστήματα χρησιμοποιούνταν σχεδόν αποκλειστικά από τις διάφορες κρατικές υπηρεσίες οι οποίες διαχειρίζονται διαβαθμισμένες πληροφορίες (ένοπλες δυνάμεις, υπηρεσίες ασφαλείας, υπουργεία κλπ.). Σκοπός τους ήταν η διασφάλιση των εμπιστευτικών και απόρρητων εθνικών πληροφοριών, ώστε να αποτρέψουν τη διαρροή τους σε μη εξουσιοδοτημένα άτομα ή σε εχθρικές χώρες. Αυτό είχε και ως αναπόφευκτο αποτέλεσμα ότι την τεχνογνωσία για την ανάπτυξη και αξιολόγηση των κρυπτογραφικών συστημάτων την κατείχαν αποκλειστικά οι υπηρεσίες ασφαλείας και ολίγες εξειδικευμένες εταιρείες.

Όμως, με την πάροδο του χρόνου και τον εκσυγχρονισμό των ηλεκτρονικών υπολογιστών και των δικτύων τους, πολλοί μη κρατικοί οργανισμοί (τράπεζες, βιομηχανίες κλπ.) αλλά και ιδιώτες, άρχισαν να ανταλλάσουν εμπιστευτικές πληροφορίες μέσω των διαφόρων τηλεπικοινωνιακών δικτύων. Οι πληροφορίες αυτές μπορεί να είναι κάποια εμπιστευτικά οικονομικά στοιχεία (π.χ. αριθμοί λογαριασμών), βιομηχανικά απόρρητα (π.χ. πατέντες προϊόντων), προσωπικά στοιχεία (π.χ. κωδικοί πιστωτικών καρτών). Έτσι, εκτός από την προστασία των εθνικών πληροφοριών, προέκυψε σταδιακά και η ανάγκη για την προστασία των «ιδιωτικών» πληροφοριών. Και εκτός από τον κίνδυνο διαρροής της πληροφορίας κατά την διάρκεια της επικοινωνίας (ενσύρματης ή ασύρματης), υπάρχει πλέον και ο κίνδυνος διαρροής της κατά την διάρκεια της παραγωγής, επεξεργασίας και αποθήκευσης της. Διότι, σήμερα διακινείται μέσω κινητών αποθηκευτικών μέσων (CD's, DVD's, USB memory sticks κλπ.), αλλά και μέσω του Ίντερνετ, ένας τεράστιος όγκος εμπιστευτικών στοιχείων, τα οποία αναπόφευκτα έχουν γίνει στόχος των κάθε είδους οικονομικών εγκληματιών.

Λόγω των ανωτέρω, σταδιακά άρχισαν να κυκλοφορούν στο εμπόριο πολλά κρυπτογραφικά συστήματα, για να προστατεύσουν τις εμπιστευτικές πληροφορίες κατά την διαβίβαση και αποθήκευση τους μέσω των Η/Υ, καθώς και την ασφάλεια των συναλλαγών μέσω του Διαδικτύου. Είναι όμως όλα αυτά τα κρυπτοσυστήματα τόσο ασφαλή όσο ισχυρίζονται οι κατασκευαστές τους; Μήπως κάποια από αυτά έχουν διασπαστεί από κάποιους έμπειρους ερευνητές ή από μυστικές υπηρεσίες; Μήπως οι εταιρείες που τα κατασκευάζουν ή κάποιες υπηρεσίες ασφαλείας έχουν ενσωματώσει σε αυτά κάποιες κρυφές κερκόπορτες, μέσω των οποίων μπορούν να διαρρεύσουν οι εμπιστευτικές πληροφορίες; Και πως τελικά ένας χρήστης, μία επιχείρηση ή μία αρμόδια κρατική υπηρεσία μπορεί να αξιολογήσει και να πιστοποιήσει την ασφάλειά τους;

1.2. Στόχος της διατριβής

Από όσα αναφέραμε είναι φανερό ότι, εκτός από την ανάγκη για μία ευρύτερη χρήση των κρυπτογραφικών συστημάτων, προκύπτει και η ανάγκη για την αξιολόγηση της ασφάλειας που αυτά παρέχουν, με βάσει κάποια αντικειμενικά κριτήρια που θα βασίζονται σε διεθνώς εγκεκριμένα πρότυπα και επιστημονικά τεκμηριωμένες διαδικασίες και μεθόδους. Έτσι, οι χρήστες θα αποκτήσουν μεγαλύτερη εμπιστοσύνη στην ασφάλεια των κρυπτογραφικών συστημάτων, αλλά θα μπορούν να επιλέγουν και το καταλληλότερο από αυτά, για την προστασία των πληροφοριών τους.

Ο στόχος λοιπόν της παρούσας διατριβής είναι σε πρώτη φάση να μελετήσει τις ευπάθειες και τις τρωτότητες των διαφόρων κρυπτοσυστημάτων, καθώς και τους τρόπους με τους οποίους αυτές μπορούν να εντοπιστούν, ώστε να αποφευχθεί η εκμετάλλευσή τους για επιθέσεις κρυπτανάλυσης. Και σε δεύτερη και κύρια φάση, ο στόχος της διατριβής είναι να μελετήσει τις βασικές παραμέτρους οι οποίες υπεισέρχονται, καθώς και τα διάφορα προβλήματα που ανακύπτουν, κατά τις αξιολογήσεις της ασφάλειας των κρυπτογραφικών συστημάτων. Το τελικό παραδοτέο της διατριβής θα είναι η πρόταση συγκεκριμένων μεθόδων, κριτηρίων και τεχνικών διαδικασιών, οι οποίες θα είναι βασισμένες σε επιστημονικά δεδομένα, με στόχο την όσο το δυνατόν πιο αξιόπιστη αξιολόγηση της ασφάλειας την οποία παρέχουν τα διάφορα κρυπτοσυστήματα. Έτσι θα μπορέσει να δημιουργηθεί ένα εφαρμοσμένο τεχνικό πρότυπο, το οποίο θα καλύψει τα πολλά και σημαντικά κενά που υπάρχουν διεθνώς στον επιστημονικό αυτό τομέα.

1.3. Απαιτήσεις Ασφάλειας Πληροφοριών

Σε σχέση με το επιστημονικό πεδίο στο οποίο εντάσσεται η παρούσα διατριβή, είναι σκόπιμο να κάνουμε τις εξής παρατηρήσεις:

α. Σε ότι αφορά τα διάφορα συστήματα επεξεργασίας, η ασφάλεια των πληροφοριών μπορεί να διαχωριστεί σε δύο κυρίως κατηγορίες, την Ασφάλεια Επικοινωνιών (Communications Security - COMSEC) και την Ασφάλεια Ηλεκτρονικών Υπολογιστών (Computer Security - COMPUSEC). Ωστόσο, σήμερα είναι πλέον δύσκολο να διαχωρίσουμε τα συστήματα των Επικοινωνιών από αυτά των Ηλεκτρονικών Υπολογιστών και για αυτό έχει επικρατήσει ο γενικός όρος Ασφάλειας Πληροφοριών (Information Security - INFOSEC).

β. Οι απαιτήσεις της Ασφάλειας Πληροφοριών (INFOSEC) αφορούν όλα τα στάδια της επεξεργασίας, διακίνησης και αποθήκευσής τους και κατατάσσονται στις παρακάτω τέσσερεις ενότητες:

Εμπιστευτικότητα (Confidentiality) : Προστασία έναντι της διάθεσης ή αποκάλυψης διαβαθμισμένων πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα.

Ακεραιότητα (Integrity) : Προστασία έναντι της τροποποίησης ή αλλοίωσης των πληροφοριών.

Αυθεντικότητα (Authentication) : Προστασία έναντι παραπλανητικών πληροφοριών, καθώς και επιβεβαίωση της ταυτότητας των χρηστών.

Διαθεσιμότητα (Availability) : Εξασφάλιση της απρόσκοπτης διάθεσης των πληροφοριών.

Μη απάρνηση (Non repudiation) : Προστασία έναντι της άρνησης παροχής πληροφοριών.

Τα κρυπτογραφικά συστήματα εντάσσονται και στις δύο προαναφερθείσες κατηγορίες συστημάτων (Επικοινωνιών και Η/Υ), διότι δεν χρησιμοποιούνται μόνο για την προστασία των πληροφοριών κατά την επικοινωνία-διαβίβαση, αλλά και για την προστασία τους σε όλα τα στάδια επεξεργασίας-αποθήκευσης. Σε ότι αφορά τις απαιτήσεις ασφαλείας, ενώ παλαιότερα τα κρυπτογραφικά συστήματα χρησιμοποιούνταν κυρίως για την εξασφάλιση της εμπιστευτικότητας, σήμερα χρησιμοποιούνται πλέον και για την εξασφάλιση της ακεραιότητας και αυθεντικότητας (π.χ. χρήση ασύμμετρων κρυπταλγόριθμων για ψηφιακές υπογραφές).

1.4. Αξιολόγηση - Πιστοποίηση – Διαπίστευση

Προτού προχωρήσουμε στις τεχνικές λεπτομέρειες, είναι σκόπιμο να διευκρινίσουμε τους τρεις βασικούς όρους που αφορούν τις διαδικασίες για τον έλεγχο της ασφάλειας των πληροφοριακών συστημάτων:

Αξιολόγηση είναι ο λεπτομερής τεχνικός έλεγχος των μηχανισμών ασφαλείας ενός μεμονωμένου συστήματος ή ενός προϊόντος τεχνολογίας πληροφορικής (Ι.Τ.), με σκοπό να διερευνηθούν τα τυχόν προβλήματα και οι τρωτότητες του.

Πιστοποίηση είναι η έκδοση ενός επίσημου πορίσματος, το οποίο στηρίζεται στα αποτελέσματα μίας αξιολόγησης και το οποίο δηλώνει τον βαθμό στον οποίο ένα σύστημα ή προϊόν τεχνολογίας πληροφορικής (Ι.Τ.) ανταποκρίνεται σε συγκεκριμένες απαιτήσεις ασφαλείας, δηλαδή δηλώνει το επίπεδο ασφαλείας που αυτό παρέχει.

Διαπίστευση είναι η έγκριση λειτουργίας που δίδεται σε ένα σύνθετο σύστημα ή δίκτυο Αυτόματης Επεξεργασίας Δεδομένων (ΑΕΔ), ώστε να επεξεργάζεται διαβαθμισμένες πληροφορίες μέσα στο ιδιαίτερο επιχειρησιακό του περιβάλλον (το οποίο μπορεί να περιλαμβάνει πολλά διαφορετικά συστήματα, πολλούς χρήστες, διαφορετικά είδη πληροφοριών, διαφορετικά επίπεδα ασφαλείας, διαφορετικούς χώρους εγκατάστασης κλπ.).

Στην παρούσα εργασία θα ασχοληθούμε κυρίως με το κομμάτι της τεχνικής αξιολόγησης των κρυπτογραφικών συστημάτων, η οποία είναι η περισσότερο τεχνικά πολύπλοκη διαδικασία ασφαλείας, δημιουργεί τα περισσότερα προβλήματα στην πράξη, αλλά παρουσιάζει και το σημαντικότερο επιστημονικό ενδιαφέρον.

1.5. Βασικά στοιχεία Κρυπτολογίας

Πολύ συνοπτικά, αναφέρουμε τις βασικότερες έννοιες της επιστήμης της Κρυπτολογίας, τις οποίες χρησιμοποιούμε στην παρούσα διατριβή :

Κρυπτογράφηση (encryption) είναι ο μετασχηματισμός μιας πληροφορίας σε ακατανόητη μορφή, με την χρήση ενός κρυπτογραφικού αλγορίθμου και ενός κλειδιού, ώστε αυτή να μπορεί να αποκωδικοποιηθεί μόνο από το νόμιμο παραλήπτη, ο οποίος κατέχει και το κλειδί. Η αντίστροφη διαδικασία όπου από την κρυπτογραφημένη πληροφορία παράγεται η αρχική, ονομάζεται **αποκρυπτογράφηση (decryption)**.

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Κλειδί (key) είναι μία παράμετρος πολύ μεγάλου μήκους, η οποία είναι απαραίτητη για την ενεργοποίηση και την ασφαλή λειτουργία του κρυπτογραφικού αλγορίθμου. Στους σύγχρονους ψηφιακούς κρυπταλγόριθμους, το μέγεθος του κλειδιού μετριέται σε αριθμό bits.

Ανοικτό ή Αρχικό κείμενο (plaintext) είναι η πληροφορία (δεδομένα, κείμενο, φωνή κλπ.) η οποία αποτελεί την είσοδο σε μία διαδικασία κρυπτογράφησης.

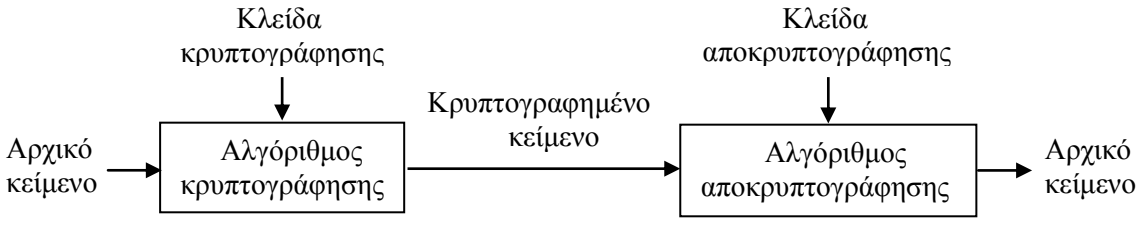
Κρυπτογραφημένο κείμενο (ciphertext) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο ανοικτό κείμενο.

Οι μαθηματικές εκφράσεις της κρυπτογράφησης /αποκρυπτογράφησης είναι :

$$\mathbf{C = E_K(P)} \quad \text{και} \quad \mathbf{P = D_K(C)}$$

όπου **C** = κρυπτογραφημένο κείμενο, **P** = ανοικτό κείμενο, **K** = κλειδί,
E = συνάρτηση κρυπτογράφησης, **D** = συνάρτηση αποκρυπτογράφησης.

Η πολυπλοκότητα του κρυπταλγορίθμου, το μέγεθος της κλείδας, καθώς και η συχνή αλλαγή της κλείδας, αποτελούν βασικές προϋποθέσεις για την ασφάλεια ενός κρυπτοσυστήματος. Η τυπική διαδικασία της κρυπτογράφησης φαίνεται στο Σχήμα 1. Ο αλγόριθμος αποκρυπτογράφησης συνήθως είναι ίδιος με τον αλγόριθμο κρυπτογράφησης, ο οποίος εκτελεί την αντίστροφη διαδικασία.



Σχήμα 1. Τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης

Κρυπτανάλυση (cryptanalysis) είναι η επιστήμη που ασχολείται με τη «διάσπαση» της κρυπτογραφικής τεχνικής, ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, να μπορεί να αποκωδικοποιηθεί το αρχικό κείμενο. Γενικά, όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να διασπασθεί το κρυπτογραφημένο μήνυμα.

Κρυπταξιολόγηση (cryptographic evaluation) είναι η διαδικασία ανεύρεσης των ευπαθειών και των τρωτοτήτων ενός κρυπτογραφικού συστήματος και η κατάταξή του σε ένα αντίστοιχο επίπεδο ασφαλείας (πιστοποίηση). Η κρυπταξιολόγηση και η κρυπτανάλυση χρησιμοποιούν κάποιες κοινές μεθόδους και οπωσδήποτε πριν από κάθε κρυπτανάλυση ενός συστήματος, πάντα προηγείται η κρυπταξιολόγησή του.

Απόλυτα ασφαλές (unconditionally secure) ονομάζεται ένα κρυπτογραφικό σύστημα, όταν δεν μπορεί να διασπασθεί ακόμα και αν διατεθεί για το σκοπό αυτό απεριόριστη υπολογιστική ισχύς. **Υπολογιστικά ασφαλές (computationally secure)** ονομάζεται ένα κρυπτογραφικό σύστημα, όταν δεν είναι πρακτικά εφικτό να διατεθεί η αναγκαία υπολογιστική ισχύς για την διάσπασή του.

Είδη κρυπτογραφικών αλγορίθμων:

α. Αμφίδρομοι κρυπτογραφικοί αλγόριθμοι : Ορίζουν την ευθεία και την ανάστροφη κρυπτογραφική διαδικασία. Χωρίζονται σε δυο κατηγορίες :

(1). Συμμετρικοί κρυπτογραφικοί αλγόριθμοι : Χρησιμοποιούν ένα και μοναδικό κλειδί, τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Η διαρροή του κλειδιού θέτει σε σοβαρό κίνδυνο την ασφάλεια του συστήματος, για τον λόγο αυτό θα πρέπει το κλειδί να παραμένει αυστηρά μυστικό. Οι συμμετρικοί κρυπταλγόριθμοι χωρίζονται σε κώδικες ροής (stream ciphers) και σε κώδικες ομάδας (block ciphers).

(2). Ασύμμετροι κρυπτογραφικοί αλγόριθμοι : Χρησιμοποιούν διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Το ένα από τα δύο κλειδιά παραμένει μυστικό (Private Key), ενώ το άλλο δημοσιοποιείται (Public Key). Οι ασύμμετροι κρυπταλγόριθμοι χρησιμοποιούνται σε συνδυασμό με τους συμμετρικούς στα συστήματα υποδομής δημόσιας κλείδας (PKI), για την εξασφάλιση της εμπιστευτικότητας, αυθεντικότητας και ακεραιότητας των πληροφοριών.

β. Μη αμφίδρομοι κρυπτογραφικοί αλγόριθμοι ή μονόδρομοι (one way) : Ορίζουν μόνο την ευθεία κρυπτογραφική διαδικασία. Είναι γνωστοί και ως hash functions και χρησιμοποιούνται σε συστήματα ψηφιακών υπογραφών (digital signatures) για την εξασφάλιση της ακεραιότητας της πληροφορίας (integrity).

Διαχείριση Κλειδών (Key Management):

Η καθοιονδήποτε τρόπο αποκάλυψη των κλειδών σε μη εξουσιοδοτημένα άτομα, καταργεί την ασφάλεια των κρυπτοσυστημάτων. Για τον λόγο αυτό, θα πρέπει τα κλειδιά να προστατεύονται σε όλη τη διάρκεια της παραγωγής, διαβίβασης και αποθήκευσή τους και να αλλάζουν όσο το δυνατόν συχνότερα. (πολύ συχνή κρυπτοπερίοδος - cryptoperiod). Επίσης, η ανταλλαγή των κλειδιών (key exchange), θα πρέπει να γίνεται μέσω ασφαλών καναλιών επικοινωνίας, είτε δια φυσικής διανομής (crypto custodians), είτε με ηλεκτρονικό τρόπο μέσω ειδικού δικτύου (Electronic Key Distribution). Στη περίπτωση της ηλεκτρονικής διανομής, οι κλείδες πρέπει να διαβιβάζονται κρυπτογραφημένες, μέσω ενός ασφαλούς κρυπτοσυστήματος.

1.6. Βασικά στοιχεία Κρυπτανάλυσης

1.6.1. Γενικά

Έως τα μέσα του 20ου αιώνα, η κρυπτανάλυση βασιζόταν αποκλειστικά στην επιτηδειότητα, τη διαίσθηση και την κοπιαστική εργασία. Αλλά με την εξέλιξη των ηλεκτρονικών υπολογιστών, άρχισαν σταδιακά να διασπώνται τα παραδοσιακά κρυπτοσυστήματα (χειρογραφικές μέθοδοι πολυαλφαβητικών αντικαταστάσεων και μεταθέσεων), με σχετικά απλές μεθόδους.

Τα παραδοσιακά κρυπτοσυστήματα τα διαδέχθηκαν τα αναλογικά ηλεκτρονικά κρυπτοσυστήματα (π.χ. κρυπτοφωνικά scrambler). Σε αυτά, ο κρυπταναλυτης εκμεταλλευόμενος τις ασυνέχειες του σήματος και τη φασματική δομή της φωνής, με τον υπολογιστή δοκιμάζει πολλούς συνδυασμούς ανασύνθεσης, με ταυτόχρονη ακρόαση για να ελέγχει την κατανοητότητα του αποτελέσματος. Και επειδή οι συνδυασμοί της κλείδας είναι λίγοι (φασματικές και χρονικές ανακατατάξεις της φωνής), σήμερα αυτά τα κρυπτοσυστήματα διασπώνται σε μικρό χρόνο.

Όταν όμως το κρυπτοσύστημα είναι ψηφιακό (π.χ. κρυπτοφωνικό vocoder ή κρυπτογράφησης δεδομένων), ο χρόνος για τη διάσπασή του είναι πάρα πολύ μεγάλος. Όσο ισχυρό υπολογιστή και να διαθέτουμε, οι συνδυασμοί της κλείδας είναι τόσοι πολλοί, που μπορεί να χρειαστούν πολλά χρόνια συνεχούς λειτουργίας του υπολογιστή για να διασπαστεί το σύστημα.

Γενικά, τα σημεία στα οποία στηρίζεται η κρυπτανάλυση είναι τα εξής:

α) Η εμπειρία του κρυπταναλυτή.

β) Σφάλματα των χειριστών κατά την κρυπτογράφηση.

γ) Μη σωστή λειτουργία των κρυπτοσυσκευών.

δ)Μεγάλο πλήθος σημάτων κωδικοποιημένων με την ίδια κρυπτοσυσκευή (και ενδεχομένως την ίδια κλείδα).

ε) Σφάλματα κατά τον συγχρονισμό των συσκευών.

Ειδικότερα σήμερα, με τις σύγχρονες μεθόδους τηλεπικοινωνιών και κρυπτογράφησης, η υποκλοπή και εν συνεχεία η διάσπαση ενός κρυπτογραφημένου μηνύματος παρουσιάζει τις εξής κατά σειρά δυσκολίες:

α) Άγνωστες τεχνικές επικοινωνίας (διαμόρφωση, πρωτόκολλο κλπ.).

β) Άγνωστη γλώσσα του ανοικτού κειμένου (plaintext).

γ) Άγνωστος κρυπτογραφικός αλγόριθμος.

δ) Άγνωστο κρυπτογραφικό κλειδί.

Το επικοινωνιακό σύστημα και η γλώσσα που χρησιμοποιήθηκε είναι σχετικά εύκολο να ευρεθούν, διότι κατά κανόνα δεν είναι μυστικά. Όμως ο κρυπταλγόριθμος και κυρίως το κλειδί, είναι στοιχεία μυστικά και επομένως πολύ δύσκολο να βρεθούν. Όταν ο κρυπταναλυτής δεν γνωρίζει ούτε τον αλγόριθμο ούτε και το κλειδί, έχει να αντιμετωπίσει ένα εξαιρετικά δύσκολο έργο. Με την εξαίρεση της περίπτωσης να έχει χρησιμοποιηθεί ένας πολύ απλός κώδικας, είναι σχεδόν αδύνατο να αποκαλυφθεί με τεχνικά μέσα ο αλγόριθμος που χρησιμοποιήθηκε, γνωρίζοντας μόνο το κρυπτογραφημένο μήνυμα. Όταν ο αλγόριθμος είναι γνωστός, απομένει να βρεθεί μόνο το κλειδί για την αποκρυπτογράφηση. Όμως για τα σύγχρονα κρυπτοσυστήματα η εύρεση του

κλειδιού είναι ένα φοβερά χρονοβόρο έργο, γιατί ο αριθμός των πιθανών τιμών της κλείδας είναι τεράστιος. Έτσι, η δοκιμή όλων των δυνατών τιμών του κλειδιού, είναι χαρακτηρισμένη ως μέθοδος εξαντλητικής έρευνας (**exhaustive search**) ή ως επίθεση βάναυσης δύναμης (**brute force attack**).

Στην κρυπτανάλυση κατ'αρχήν ερευνούμε τα ενδεχόμενα τρωτά σημεία του κρυπταλγόριθμου, τα οποία μπορούμε να εκμεταλλευτούμε ώστε να παρακάμψουμε την κλείδα ή να μειώσουμε τις πιθανές τιμές της. Με αυτό τον τρόπο μειώνουμε το χρόνο έρευνας της κλείδας, καθώς και την απαιτούμενη υπολογιστική ισχύ. Όταν όμως δεν μπορούμε να βρούμε τρωτό σημείο στον αλγόριθμο, τότε αναγκαστικά χρησιμοποιούμε τη μέθοδο της εξαντλητικής έρευνας η οποία είναι πολύ χρονοβόρος και απαιτεί μεγάλη υπολογιστική ισχύ.

Ορισμένες φορές (ιδιαίτερα στα παλαιά κρυπτοσυστήματα) είναι εφικτό να αποκρυπτογραφηθεί ένα μήνυμα χωρίς να βρεθεί το κλειδί (π.χ. με γλωσσολογική ή στατιστική ανάλυση). Όμως, είναι πολύ πιο σημαντική η ανεύρεση του κλειδιού, διότι με την γνώση ενός κλειδιού είναι πιθανόν να αποκαλυφθούν πολλά μηνύματα τα οποία κρυπτογραφήθηκαν με αυτό.

Για να επιβεβαιώσουμε την δύναμη ενός κώδικα, πρέπει να προβαίνουμε στις χειρότερες υποθέσεις σχετικά με τις πληροφορίες που διαθέτει ο αντίπαλος. Έτσι, θεωρούμε ότι ο αλγόριθμος είναι γνωστός στον κρυπταναλυτή και ότι η προσπάθεια να σπάσει το μήνυμα συνίσταται στο να βρει μόνο το κλειδί. Αυτή η υπόθεση είναι συμβατή και με την γνωστή «αρχή του Kerchoff», βάσει της οποίας για να θεωρηθεί ένα κρυπτοσύστημα ασφαλές, πρέπει η ασφάλειά του να στηρίζεται κυρίως στο μεγάλο πλήθος των κλειδών του και όχι στην πολυπλοκότητα του αλγορίθμου.

1.6.2. Είδη κρυπταναλυτικής επίθεσης

Εκτός από τη γνώση του αλγορίθμου, ο κρυπταναλυτής πρέπει να έχει στη διάθεσή του ένα μεγάλο πλήθος από ανοικτά και αντίστοιχα κρυπτογραφημένα σήματα. Έτσι, διακρίνουμε τις εξής περιπτώσεις:

α. Γνωστό κρυπτογραφημένο κείμενο: Το έργο του κρυπταναλυτή είναι πιο δύσκολο, όταν εκτός από τον αλγόριθμο γνωρίζει μόνο το κρυπτογραφημένο κείμενο (cipher text only attack). Στην περίπτωση αυτή, εάν δεν υπάρχει μεγάλος αριθμός πλεονασμών στο ανοικτό κείμενο, είναι σχεδόν αδύνατον να βρεθεί το κλειδί. Κάποια γνωστά τμήματα του ανοικτού κειμένου θα μπορούσαν να βοηθήσουν, για παράδειγμα αν το μήνυμα έχει μία τυποποιημένη εισαγωγή. Τα κλειδιά μπορούν να ελεγχθούν μέχρι τη στιγμή που ένα σημείο της τυποποιημένης εισαγωγής εμφανίζεται αποκωδικοποιημένο. Και αν η εισαγωγή είναι αρκετά μεγάλη, τότε μπορούμε να είμαστε σίγουροι ότι βρήκαμε το κλειδί, αφού η εισαγωγή θα αποκαλυφθεί μόνο για μια τιμή κλειδιού. Επίσης, η γνώση ενός αντιπροσωπευτικού κώδικα του ανοικτού κειμένου, π.χ. η ισοτιμία ελέγχου (parity), μπορεί να δώσει στον κρυπταναλυτή κάποιο στοιχείο για να προχωρήσει. Διαφορετικά, θα πρέπει να ερευνηθεί ένα τεράστιο πλήθος από πιθανά κλειδιά.

β. Γνωστό ανοικτό κείμενο: Περισσότερο εφικτή για τον κρυπταναλυτή, είναι η έρευνα κατά την οποία εκτός από κρυπτογραφημένο, είναι γνωστό και το ανοικτό κείμενο. Η περίπτωση αυτή είναι γνωστή ως επίθεση με γνωστό ανοικτό κείμενο (known plaintext attack).

Το έργο εν συνεχεία είναι να βρεθεί ένα κλειδί που ανταποκρίνεται σε αυτή την αντιστοιχία. Εάν το μήκος του διαθέσιμου κειμένου είναι αρκετό, τότε το κλειδί μπορεί να αποκαλυφθεί με μεγάλη βεβαιότητα. Περιπτώσεις όπου το ζεύγος plaintext-ciphertext είναι γνωστό, είναι περισσότερο συνήθεις από όσο μπορεί κάποιος να υποθέσει. Για παράδειγμα, οι αλλαγές της αγοράς μπορούν να οδηγήσουν στην πρόβλεψη των οδηγιών που στέλνονται στους τραπεζίτες ή στους χρηματιστές. Μία άλλη περίπτωση είναι τα κρυπτογραφημένα κείμενα του τύπου, τα οποία στέλνονται από μια πρεσβεία στην χώρα της. Αυτό βέβαια είναι ένα δύσκολο έργο για τον κρυπταναλυτή, εξαιτίας του μεγάλου όγκου του υλικού που διαβιβάζεται μέσω ενός διπλωματικού κρυπτοσυστήματος. Η προστασία έναντι αυτής της περίπτωσης είναι ότι, οι πληροφορίες του τύπου πρέπει να είναι παραφρασμένες πριν διαβιβαστούν.

γ. Επιλεγμένο ανοικτό κείμενο : Η πιο αποδοτική κρυπταναλυτική επίθεση είναι με επιλεγμένο ανοικτό κείμενο (chosen plaintext attack). Εδώ ο κρυπταναλυτής κατορθώνει κατά κάποιο τρόπο να εισάγει ένα δικό του ανοιχτό κείμενο στην διαδικασία κρυπτογράφησης, το οποίο μπορεί να επιλέξει έτσι ώστε να διευκολυνθεί η ανεύρεση του κλειδιού. Για παράδειγμα, ίσως είναι χρήσιμο αν το επιλεχθέν ανοικτό κείμενο μπορεί να είναι "όλα μηδενικά".

Η "πιθανή λέξη" είναι ένα παράδειγμα γνωστού ανοικτού κειμένου, χωρίς ο κρυπταναλυτής να γνωρίζει τη θέση της στο κείμενο. Μερικές φορές η πιθανή λέξη είναι στην ουσία ένα "επιλεχθέν ανοικτό κείμενο". Παράδειγμα εξαναγκασμένης εισόδου μιας λέξης σε ένα κρυπτοσύστημα, είχαμε κατά την διάσπαση της Γερμανικής κρυπτοσυσκευής ENIGMA (Β' Παγκόσμιος πόλεμος), όπου έγινε ένας φαινομενικά «άσκοπος» βομβαρδισμός ενός πλωτού σημαντήρα, με την βεβαιότητα ότι η σπάνια γερμανική λέξη "leuchttonne" θα υπήρχε μέσα στα κωδικοποιημένα Γερμανικά μηνύματα.

Ένα παρόμοιο κριτήριο, ίσως λίγο εξεζητημένο αλλά άξιο μνημόνευσης, είναι αυτό του επιλεγμένου κρυπτογραφημένου κειμένου. Θα μπορούσε για παράδειγμα ο αντίπαλος να εισαγάγει το δικό του κρυπτογραφημένο κείμενο στην γραμμή και κατά κάποιο τρόπο να έχει πρόσβαση στο ανοικτό κείμενο.

1.6.3. Απαιτούμενος χρόνος εξαντλητικής έρευνας

Στην περίπτωση της κρυπτανάλυσης με **εξαντλητική έρευνα** (exhaustive key search ή brute force attack), με γνωστό τον αλγόριθμο και ορισμένα κρυπτογραφημένα κείμενα, μπορούμε να υπολογίσουμε τον μέσο χρόνο που θα χρειαστεί για να βρεθεί το κλειδί με την χρήση Η/Υ. Αυτός είναι ο χρόνος που απαιτείται για την δοκιμή ενός κλειδιού, επί τον αριθμό όλων των πιθανών κλειδιών, έως ότου αποκαλυφθεί το ανοικτό κείμενο.

Στο παρακάτω παράδειγμα, κατ'αρχήν υποθέτουμε ότι ο χρόνος που απαιτείται από ένα Η/Υ για την δοκιμή ενός κλειδιού βρίσκεται στην περιοχή μεταξύ 1ms και 1μs. Αυτοί οι χρόνοι μπορούν να επιτευχθούν με ένα σύστημα μικροεπεξεργαστού ή με ένα hardware ειδικού σκοπού και μεγάλης κλίμακας ολοκλήρωσης (τύπου FPGA ή ASIC) αντίστοιχα. Επίσης, υποθέτουμε ότι κατά μέσο όρο το σωστό κλειδί βρίσκεται κατόπιν έρευνας του μισού συνολικού αριθμού των κλειδών. Για λόγους καθαρά ενδεικτικούς, εξετάζονται μεγέθη κλειδών των 32, 40, 48, 56, 64 και 128 bits.

α. Απλή έρευνα : Με την υπόθεση ότι ο κρυπταναλυτής μπορεί να ελέγξει με ένα κοινό Η/Υ κάθε φορά μόνο ένα κλειδί, υπολογίσαμε τους χρόνους για την εύρεση του κλειδιού, όπως φαίνεται στις δύο πρώτες στήλες του Πίνακα 1. Οι χρόνοι που εκφράζονται σε μέρες (d), αντιστοιχούν σε κλείδες που πρέπει να αποφεύγονται για την προστασία σημαντικών πληροφοριών, ενώ οι χρόνοι που εκφράζονται σε έτη (y), αντιστοιχούν σε κλείδες οι οποίες είναι αρκετά ισχυρές. Τα αποτελέσματα για χρόνους μεγαλύτερους των 100 ετών δεν φαίνονται, διότι βρίσκονται πάνω από τα όρια του ανθρώπινου βίου.

β. Παράλληλη έρευνα : Υποθέτουμε ότι ο κρυπταναλυτής μπορεί να δοκιμάσει πολλά κλειδιά ταυτόχρονα, με ένα υπερυπολογιστή. Αυτός περιέχει μία κεντρική μονάδα, η οποία ελέγχει πολλούς ανεξάρτητους και παράλληλα συνδεδεμένους υπολογιστές (transputers), κάθε ένας από τις οποίους προγραμματίζεται για να ερευνά ένα συγκεκριμένο τμήμα από το πλήθος των κλειδιών. Όταν ένας από τους Η/Υ αναγνωρίσει το κλειδί, ειδοποιεί αυτόματα την κεντρική μονάδα και σταματάει η περαιτέρω έρευνα. Ένας τέτοιος υπερυπολογιστής μπορεί σήμερα να κατασκευαστεί για να ελέγχει τουλάχιστον 1.000.000 κλειδιά ταυτόχρονα, οπότε οι χρόνοι έρευνας μειώνονται θεαματικά.

Οι δύο τελευταίες στήλες του Πίνακα 1, δείχνουν τους χρόνους για την ανεύρεση του κλειδιού μέσω εξαντλητικής παράλληλης έρευνας. Όπως φαίνεται, χρησιμοποιώντας ένα τέτοιο υπερυπολογιστή για κρυπτανάλυση, ακόμα και ένα κλειδί 64 bit δεν είναι αρκετά μεγάλο για να παράσχει επαρκή ασφάλεια (διασπάται σε 107 ημέρες), ενώ όταν το κλειδί είναι 128 bits παρέχει πολύ μεγάλη ασφάλεια (μέσος χρόνος διάσπασης $1{,}079 * 10^{19}$ έτη).

Μέγεθος κλειδιού (bits)	**Απλή έρευνα**		**Παράλληλη έρευνα (10^6)**	
	Χρόνος δοκιμής κλείδας		**Χρόνος δοκιμής κλείδας**	
	1 ms	**1 μs**	**1 ms**	**1 μs**
32	24.9 d	35.8 m	2.15 s	2.15 ms
40	17.4 y	6.4 d	9.2 m	550 ms
48	>100 y	4.46 y	1.63 d	2.35 m
56		>100 y	1.14 y	10.0 h
64			>100 y	107 d
70				18,7 y
128				$1{,}079 * 10^{19}$ y

Πίνακας 1. Χρόνος κρυπτανάλυσης με εξαντλητική έρευνα

1.6.4. Μέτρα προστασίας έναντι της κρυπτανάλυσης

α. Μήκος της κλείδας : Δεδομένου ότι η ισχύς των Η/Υ συνεχώς αυξάνει, είναι προφανές ότι θα αυξάνουν και οι δυνατότητες των κρυπταναλυτών. Από την άλλη μεριά όμως, αυξάνει και η πολυπλοκότητα των κρυπτογραφικών αλγορίθμων και κυρίως το μέγεθος του κλειδιού. Πόσο μεγάλη όμως πρέπει να είναι μια κλείδα; Δυστυχώς δεν υπάρχει μια απλή απάντηση, διότι πάντοτε εξαρτάται από το είδος και τη σημαντικότητα της πληροφορίας που θέλουμε να προστατεύσουμε. Γενικά, για να καθορίσουμε

πόση ασφάλεια χρειαζόμαστε από ένα κρυπτοσύστημα, πρέπει να απαντήσουμε στις εξής βασικές ερωτήσεις:

(1) Πόσο αξίζουν οι πληροφορίες που θέλουμε να προστατέψουμε;

(2) Πόσο καιρό πρέπει να είναι ασφαλείς;

(3) Τι δυνατότητες διαθέτει ο αντίπαλος;

Παρακάτω δίδεται ένας καθαρά ενδεικτικός πίνακας με τα ελάχιστα μήκη κλειδών για την προστασία ορισμένων χαρακτηριστικών ειδών πληροφοριών.

ΤΥΠΟΣ ΠΛΗΡΟΦΟΡΙΑΣ	ΔΙΑΡΚΕΙΑ ΖΩΗΣ	ΕΛΑΧΙΣΤΟ ΜΗΚΟΣ ΚΛΕΙΔΑΣ
Στρατιωτικές / Τακτικές	Λεπτά/Ώρες	56 bits
Αναγγελίες Εμπορικών Προϊόντων	Ημέρες/Εβδομάδες	64 bits
Εμπορικά Σχέδια	Χρόνια	64 bits
Εμπορικά Μυστικά (πατέντες κλπ.)	Δεκαετίες	112 bits
Πυρηνικά Μυστικά	50 χρόνια	128 bits
Ταυτότητες Κατασκόπων	50 χρόνια	128 bits
Προσωπικά – Ιδιωτικά Θέματα	50 χρόνια	128 bits
Διπλωματικά/Κρατικά Μυστικά	65 χρόνια	>>128 bits

Πίνακας 2. Ελάχιστο μήκος κλείδας ανάλογα με τη σημαντικότητα της πληροφορίας

Στο Κεφάλαιο 5 κάνουμε ένα αναλυτικό υπολογισμό του ελάχιστου μήκους της κλείδας, βασιζόμενοι στη σημερινή τεχνολογία και εν συνεχεία στην αναμενόμενη τεχνολογική πρόοδο, σε ότι αφορά την κατασκευή των ολοκληρωμένων κυκλωμάτων και την ταχύτητα των Η.Υ.

β. Συχνή αλλαγή της κλείδας : Το βασικότερο μέτρο έναντι της κρυπτανάλυσης είναι η όσο το δυνατόν συχνότερη αλλαγή των κλειδών (μικρή κρυπτοπερίοδος). Η διατήρηση μιας κλείδας για μεγάλο διάστημα εισάγει τους εξής σοβαρούς κινδύνους:

-Κίνδυνος διαρροής της κλείδας.

-Συγκέντρωση από τους αντίπαλους κρυπταναλυτές πολλών κρυπτογραφημάτων τα οποία έχουν την ίδια κλείδα.

-Αποκάλυψη μεγάλου όγκου διαβαθμισμένων πληροφοριών σε περίπτωση διάσπασης του κρυπταλγορίθμου.

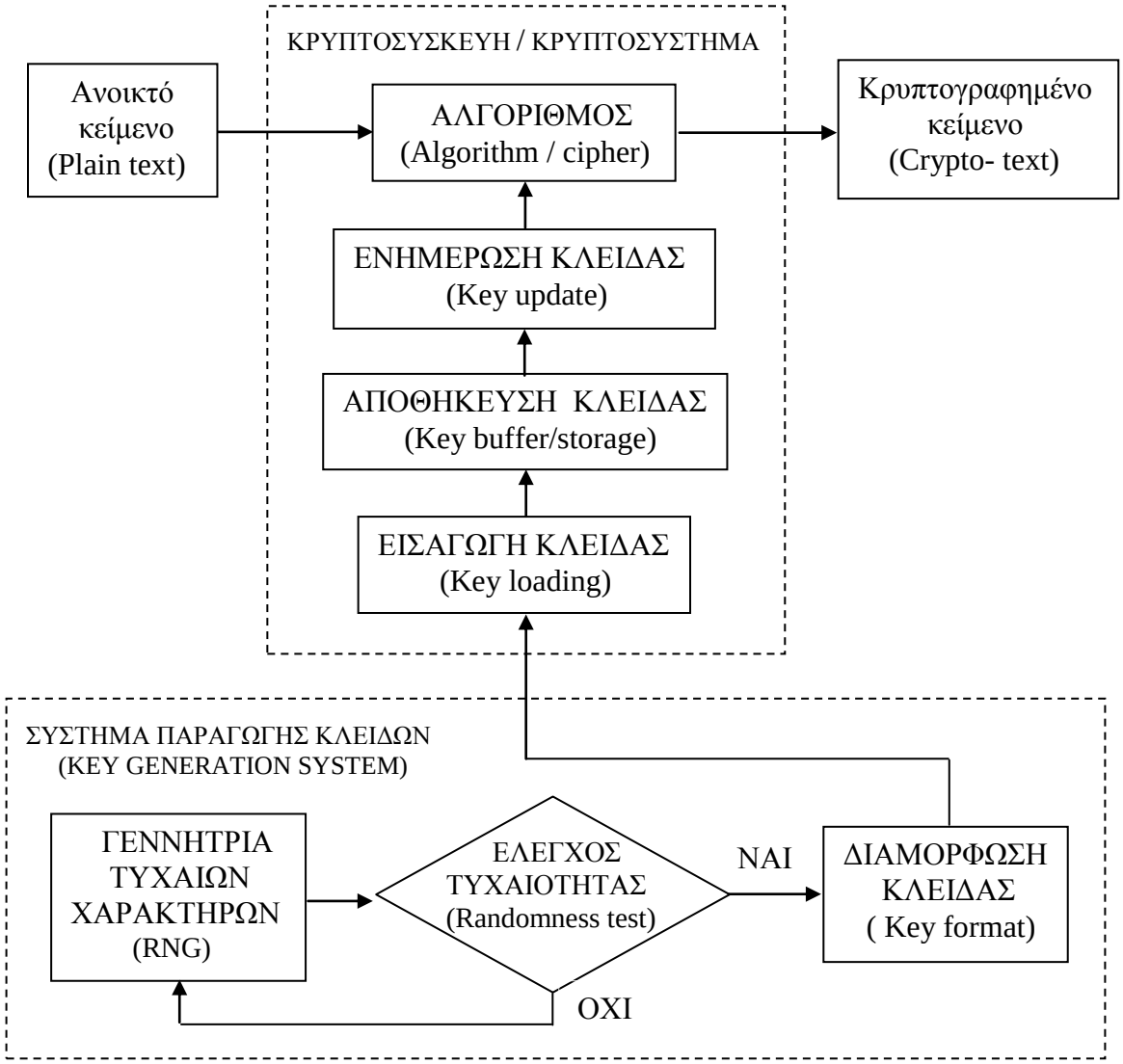
γ. Ανανέωση του κρυπτοσυστήματος : Ένα επίσης πολύ σημαντικό μέτρο είναι ότι, τα κρυπτοσυστήματα πρέπει να έχουν ένα περιορισμένο χρόνο ζωής και πρέπει να ανανεώνονται ή να αντικαθίστανται από νέα περισσότερο εξελιγμένα, κυρίως στον τομέα του κρυπταλγορίθμου αλλά και των υπολοίπων μηχανισμών ασφαλείας. Έτσι μπορούμε να προλάβουμε έγκαιρα τυχόν επιθέσεις εναντίον τους λόγω της τεχνολογικής εξέλιξης. Ένας γενικός κανόνας είναι ότι, ο χρόνος ζωής ενός κρυπτοσυστήματος πρέπει να είναι ανάλογος του βαθμού ασφαλείας του.

ΚΕΦΑΛΑΙΟ 2

ΑΞΙΟΛΟΓΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

2.1. Γενικά

Η αξιολόγηση ενός κρυπτογραφικού συστήματος είναι μία εξαιρετικά σύνθετη και πολύπλοκη εργασία, η οποία περιλαμβάνει πολλές φάσεις. Όπως φαίνεται στο Σχήμα 2, ένα ολοκληρωμένο κρυπτογραφικό σύστημα αποτελείται από πολλές μονάδες, η λειτουργία των οποίων θα πρέπει να εξεταστεί, διότι υπάρχει μεταξύ τους σημαντική αλληλεπίδραση η οποία έχει επιπτώσεις στην συνολική ασφάλεια του κρυπτοσυστήματος. Είναι προφανές λοιπόν ότι για να διεξαχθεί μία εμπεριστατωμένη και ασφαλής αξιολόγηση, είναι απαραίτητο ο κατασκευαστής του κρυπτοσυστήματος να διαθέσει πολύ λεπτομερή και τεκμηριωμένα στοιχεία.



Σχήμα 2. Μονάδες ενός ολοκληρωμένου κρυπτογραφικού συστήματος

Τα στοιχεία τα οποία πρέπει να διαθέσει ο κατασκευαστής αφορούν κυρίως τον θεωρητικό σχεδιασμό και την αναλυτική περιγραφή του συστήματος, τον τρόπο υλοποίησης του αλγορίθμου και των μηχανισμών ασφαλείας, καθώς και τα ηλεκτρομηχανικά κατασκευαστικά στοιχεία του

συστήματος. Στις επόμενες παραγράφους γίνεται μια αναλυτική περιγραφή όλων των απαιτούμενων στοιχείων τα οποία πρέπει να προσκομίσει ο κατασκευαστής. Τα κυριότερα εξ αυτών είναι εν συντομία τα παρακάτω :

α. Ένα ζεύγος των κρυπτοσυσκευών μαζί με τις αναλυτικές οδηγίες χρήσης και προγραμματισμού των συσκευών.

β. Καλώδια σύνδεσης και λοιπά παρελκόμενα υλικά, όπως συσκευή ανάγνωσης/φόρτισης κλειδών (key loader ή key gun) κλπ.

γ. Τεχνικά χαρακτηριστικά των κρυπτοσυσκευών.

δ. Αναλυτική περιγραφή της δομής του κρυπταλγορίθμου με τη συνοδεία διαγραμμάτων ροής (flow charts) σε έντυπη μορφή και ηλεκτρονική μορφή. Επίσης, περιγραφή όλων των λεπτομερειών της υλοποίησης του αλγορίθμου σε υλικό ή λογισμικό (hardware/ software), όπως τα ηλεκτρονικά κυκλωματικά διαγράμματα, ο πηγαίος κώδικας του λογισμικού (source code), η μέθοδος συγχρονισμού κλπ.

ε. Εξομοίωση του κρυπταλγορίθμου σε εκτελέσιμο πρόγραμμα Η/Υ (.exe), το οποίο θα έχει την δυνατότητα να παράγει διαφορετικές ακολουθίες εξόδου (keystreams) με την εισαγωγή διαφορετικών κλειδών. Το μήκος των ακολουθιών εξόδου θα πρέπει να είναι της τάξεως του 1 Mbit και να καταγράφεται σε αρχείο με δυαδική μορφή (binary unformatted form). Επίσης, το πρόγραμμα θα πρέπει να έχει την δυνατότητα επιλογής συγκεκριμένου μήκους ακολουθιών εξόδου.

2.2. Αξιολόγηση κρυπτογραφικού συστήματος

Από όλες τις μονάδες του κρυπτογραφικού συστήματος, η πιο σημαντική είναι η «καρδιά» του, δηλαδή ο κρυπτογραφικός αλγόριθμος, για αυτό και εξετάζεται στην πρώτη φάση της αξιολόγησης. Κατά την φάση αυτή ουσιαστικά εξετάζεται η κρυπταναλυτική αντοχή του αλγορίθμου, δηλαδή η αντοχή του στις προσπάθειες να διασπαστεί η κρυπτογραφημένη πληροφορία για την αποκάλυψη της αρχικής πληροφορίας (ανοιχτό κείμενο).

Μετά όμως από τη φάση εξέτασης του κρυπταλγορίθμου, είναι απαραίτητο να διεξαχθούν και κάποιοι σημαντικοί περαιτέρω έλεγχοι. Οι έλεγχοι αυτοί αφορούν τον τρόπο υλοποίησης και ενσωμάτωσης του κρυπταλγορίθμου εντός του συστήματος, τον τρόπο που διαχειρίζεται το σύστημα τις κρυπτογραφικές παραμέτρους, καθώς και τον τρόπο υλοποίησης των περιφερειακών μηχανισμών ασφαλείας. Έτσι, η αξιολόγηση περιλαμβάνει δύο βασικά στάδια, την αξιολόγηση του κρυπταλγορίθμου και την αξιολόγηση των μηχανισμών ασφαλείας, τα οποία περιγράφονται παρακάτω.

2.2.1. Αξιολόγηση κρυπτογραφικού αλγορίθμου

α. Δομή του αλγόριθμου: Εξετάζεται η δομή και η πολυπλοκότητα του αλγορίθμου και οι τυχόν αδυναμίες του, κυρίως στα τμήματα μη γραμμικής λογικής. Κατά τη φάση αυτή, πρέπει να γίνεται σύγκριση του υπό εξέταση αλγορίθμου με όλους τους γνωστούς (δημοσιευμένους) αλγορίθμους και ιδιαίτερα με όσους έχουν δεχθεί κρυπταναλυτικές επιθέσεις.

β. Κλείδες: Αρχικά εξετάζεται το μήκος των κλειδών, καθώς και η πολλαπλότητά τους (master key, auxiliary key, session key κλπ.). Κατόπιν, εξετάζεται ο τρόπος παραγωγής των κλειδών και ιδιαίτερα οι τυχόν ενσωματωμένες ή εξωτερικές γεννήτριες τυχαίων ή ψευδοτυχαίων χαρακτήρων (RNG). Τέλος, εξετάζεται ο τρόπος εισαγωγής των κλειδών (key loaders, fill guns, USB tokens κλπ.), καθώς και ο τρόπος διαχείρισης και διανομής τους (crypto custodians, Electronic Key Distribution κλπ).

γ. Στατιστικοί / Κρυπταναλυτικοί έλεγχοι : Οι έλεγχοι αυτοί ουσιαστικά εξετάζουν την τυχαιότητα των χαρακτήρων εξόδου του κρυπταλγορίθμου (keystream), βάσει ειδικών στατιστικών μεθόδων υλοποιημένων σε λογισμικό Η/Υ. Για τον σκοπό αυτό απαιτείται να δοθεί από τον κατασκευαστή εξομοιωμένη μορφή του αλγορίθμου σε εκτελέσιμο πρόγραμμα Η/Υ. Λόγω του τεράστιου πλήθους των κλειδών (της τάξεως του 2^{128} έως 2^{256} για συμμετρικούς αλγορίθμους), οι έλεγχοι αυτοί γίνονται δειγματοληπτικά. Το πλήθος των δειγμάτων εξόδου, το μέγεθός τους, καθώς και ο τρόπος επιλογής των κλειδών με τις οποίες θα παραχθούν τα δείγματα, αποτελούν αντικείμενα ευρείας μελέτης. Κατά τη φάση αυτή πρέπει να υπάρχει και ειδική μεθοδολογία για να ευρεθούν οι τυχόν «ισοδύναμες» ή «αδύναμες» κλείδες. Τέλος, επειδή οι ανωτέρω έλεγχοι είναι εξαιρετικά χρονοβόροι, η υλοποίηση τους είναι αποτελεσματική μόνο μέσω συστημάτων Η/Υ υψηλής ταχύτητας και με τεχνικές παράλληλης επεξεργασίας. Αυτή η φάση της αξιολόγησης είναι η πλέον σημαντική, διότι αποκαλύπτει την κρυπταναλυτική αντοχή του κρυπταλγορίθμου.

δ. Προσαρμοστικότητα αλγορίθμου (customization) : Εξετάζεται η δυνατότητα τροποποίησης της δομής του αλγορίθμου από το χρήστη, καθώς και ο τρόπος με τον οποίο μπορεί να γίνει αυτή (εύρος της τροποποίησης, απαιτούμενα εργαλεία σε υλικό/λογισμικό κλπ.). Η δυνατότητα αυτή είναι πολύ χρήσιμη και μπορεί να προσφέρει μία περαιτέρω ασφάλεια. Ωστόσο, παρουσιάζει πολλές ιδιαιτερότητες, διότι η δυσκολία, ο χρόνος υλοποίησης, καθώς και το κόστος της προσαρμογής, ποικίλουν ανάλογα με το μέθοδο που θα επιλεχθεί.

ε. Υλοποίηση - Ενσωμάτωση: Στην τελική φάση της αξιολόγησης του κρυπταλγορίθμου, πρέπει να διεξάγεται μια εργαστηριακή ταυτοποίηση της λογισμικής εξομοίωσης που έχει δοθεί για έλεγχο από τον κατασκευαστή (σε software), σε σχέση με την πραγματική υλοποίηση του κρυπταλγορίθμου (η οποία μπορεί να είναι σε hardware, firmware ή software). Η διαδικασία αυτή είναι απαραίτητη, διότι πιστοποιεί τη σωστή υλοποίηση του κρυπταλγορίθμου σε σχέση με το θεωρητικό του μοντέλο, πιστοποιεί την ενσωμάτωση του στο κρυπτογραφικό σύστημα, αλλά και διερευνάται εάν υπάρχει κάποια εκούσια ή ακούσια ενσωματωμένη κερκόπορτα (trap door, back door κλπ.). Η φάση αυτή είναι καθαρά τεχνική και διεξάγεται σε συνεργασία με τον κατασκευαστή του κρυπτοσυστήματος, διότι εμπλέκονται τα διάφορα πρωτόκολλα επικοινωνίας καθώς και τα ειδικά interfaces του κάθε συστήματος. Θα πρέπει να υπάρχει μία γενική μεθοδολογία ελέγχου και κατόπιν για κάθε αξιολογούμενο σύστημα να καθορίζεται ο απαιτούμενος ειδικός εξοπλισμός και οι διαδικασίες.

2.2.2. Αξιολόγηση μηχανισμών ασφαλείας

α. Λειτουργικότητα : Εξετάζονται οι τυχόν λειτουργικές αδυναμίες του κρυπτοσυστήματος οι οποίες έχουν επιπτώσεις επί της ασφάλειάς του, καθώς και ο τρόπος υλοποίησης των μηχανισμών ασφαλείας. Αυτές οι λειτουργίες και μηχανισμοί αφορούν κυρίως την διαχείριση των κρυπτογραφικών παραμέτρων (αλγόριθμος, κλείδες κλπ.), την ασφάλεια πρόσβασης (κωδικοί, smart cards, βιομετρία κλπ.), τεχνικές αντι-παραβίασης (tamper proof), τα αντίμετρα ανάλυσης κίνησης (traffic flow security), καθώς και την προστασία έναντι λανθασμένων χειρισμών του χρήστη (user interface security).

β. Ηλεκτρομαγνητικές ακτινοβολίες: Θα πρέπει να διεξάγονται μακροσκοπικοί καθώς και εργαστηριακοί έλεγχοι του τρόπου της εσωτερικής κατασκευής και της ειδικής θωράκισης των διαφόρων ηλεκτρονικών βαθμίδων του κρυπτοσυστήματος, για να διαπιστωθεί εάν υπάρχει διαφυγή ανεπιθύμητων ακτινοβολιών (compromising emanations). Επίσης εξετάζονται οι μετρήσεις και οι τυχόν πιστοποιήσεις έναντι ηλεκτρομαγνητικών ακτινοβολιών που προσκομίζει ο κατασκευαστής (EMI/RFI, TEMPEST).

Κάθε ένα από τα στάδια της αξιολόγησης τα οποία περιγράφτηκαν περιληπτικά, ουσιαστικά αποτελεί ένα ξεχωριστό ερευνητικό έργο. Η παρούσα διδακτορική διατριβή θα επικεντρωθεί πιο αναλυτικά στα προβλήματα τα οποία ανακύπτουν κατά την αξιολόγηση του κρυπτογραφικού αλγορίθμου. Ωστόσο, θα αναλυθούν επαρκώς και θα προταθούν λύσεις και στα προβλήματα που αντιμετωπίζονται και στα άλλα στάδια της αξιολόγησης (σε επίπεδο κρυπτοσυστήματος), ώστε αυτά να αποτελέσουν ενδεχομένως αντικείμενα κάποιων περαιτέρω ερευνητικών εργασιών.

ΚΕΦΑΛΑΙΟ 3

ΑΞΙΟΛΟΓΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ

3.1. Γενικά

Βασικός στόχος του παρόντος κεφαλαίου είναι η διερεύνηση των απαιτήσεων και προϋποθέσεων κάτω από τις οποίες θα πρέπει να διεξάγονται οι έλεγχοι κρυπταναλυτικής αντοχής των κρυπτογραφικών αλγορίθμων, ώστε να επιτύχουμε πιο ολοκληρωμένες, πιο σωστές και επομένως πιο ασφαλείς αξιολογήσεις. Κατ'αρχήν θα εξετάσουμε τις επιπτώσεις του δειγματοληπτικού ελέγχου, ο οποίος επιλέγεται αναγκαστικά αντί του εξαντλητικού ελέγχου, λόγω του τεραστίου μήκους της κρυπτογραφικής κλείδας. Εν συνεχεία, θα εξετάσουμε το πλήθος και το μέγεθος των δειγμάτων τα οποία θα πρέπει να επιλέγουμε, ανάλογα με το είδος και τον όγκο της κρυπτογραφημένης πληροφορίας και της ταχύτητας του καναλιού επικοινωνίας. Κατόπιν, θα υπολογίσουμε τον απαιτούμενο χρόνο των ελέγχων, συναρτήσει της διατιθέμενης υπολογιστικής ισχύος. Και στο Κεφάλαιο 4, θα εξετάσουμε τη βέλτιστη μεθοδολογία για τη δειγματοληπτική επιλογή των κλειδών με τις οποίες θα πραγματοποιηθούν οι έλεγχοι.

Το παρόν κεφάλαιο εστιάζεται σε κρυπταλγορίθμους τύπου ροής (stream ciphers), όμως τα αποτελέσματα του είναι ανάλογα και για τους κρυπταλγορίθμους τύπου ομάδας (block ciphers).

3.2. Έλεγχοι των κρυπτογραφικών αλγορίθμων

Κατά τους ελέγχους των κρυπτογραφικών αλγορίθμων, ουσιαστικά εξετάζεται η πολυπλοκότητα και η μη γραμμικότητα της δομής τους και κατά συνέπεια η κρυπταναλυτική αντοχή τους.

Οι έλεγχοι των αλγορίθμων γίνονται επί των ακολουθιών εξόδου του αλγορίθμου (keystreams), καθώς και επί των κρυπτογραφημένων κειμένων, βάσει ειδικών προγραμμάτων στατιστικής ανάλυσης. Όπως αναφέραμε στην παράγραφο 2.1.ε, για να παράγουμε τις ακολουθίες εξόδου (δείγματα), χρησιμοποιούμε μία λογισμική εξομοίωση του εξεταζόμενου αλγορίθμου, η οποία θα πρέπει να έχει την δυνατότητα να παράγει εξόδους για όλους τους δυνατούς συνδυασμούς της κρυπτογραφικής κλείδας. Το λογισμικό εξομοίωσης θα πρέπει να το εκπονήσει ο κατασκευαστής του αλγορίθμου και θα πρέπει να δίνει την δυνατότητα στον χρήστη να επιλέγει και να τροποποιεί την κλείδα, καθώς και να επιλέγει το μήκος της παραγόμενης ακολουθίας. Κατόπιν, τα παραγόμενα δείγματα εξόδου υποβάλλονται σε ειδικούς στατιστικούς ελέγχους τυχαιότητας, σε ελέγχους ανεξαρτησίας μεταξύ ανοικτού-κλειστού κειμένου, σε ελέγχους ομοιοτήτων μεταξύ των αλγοριθμικών εξόδων και εν γένει σε ελέγχους ανθεκτικότητας έναντι κρυπτανάλυσης.

3.3. Έλεγχοι τυχαιότητας

Σε μία απόλυτα τυχαία ψηφιακή ακολουθία από bits, ο αριθμός των 0 και των 1 θα πρέπει να είναι ίσος. Δηλαδή η πιθανότητα εμφάνισης των 0 και των 1 θα πρέπει να είναι ίση με το 1/2. Επί πλέον, τα bits θα πρέπει να είναι ανεξάρτητα μεταξύ τους, καθώς και μη προβλέψιμα. Δηλαδή το κάθε bit της ακολουθίας δεν θα πρέπει να εξαρτάται από οποιονδήποτε δυνατό συνδυασμό των προηγούμενων του. Αυτό σημαίνει ότι εάν κάποιος γνωρίζει κάποια bits της ψηφιακής ακολουθίας, να μην μπορεί να προβλέψει αυτά που θα ακολουθήσουν, αλλά ούτε και αυτά που έχουν προηγηθεί. Σε ένα κρυπτογραφικό αλγόριθμο, τα bits της εξόδου του θα πρέπει να ακολουθούν τις ανωτέρω τρεις ιδιότητες, δηλαδή της τυχαιότητας (randomness), ανεξαρτησίας (independency) και μη προβλεψιμότητας (unpredictability). Εάν υπάρχει οποιαδήποτε απόκλιση από αυτές τις τρεις ιδιότητες (π.χ. από κάποια bits της εξόδου να μπορεί να προβλεφθεί το κλειδί) τότε ο κρυπταλγόριθμος θα έχει μια πολύ σοβαρή αδυναμία. Οι ανωτέρω ιδιότητες μπορούν να επαναδιατυπωθούν και να επεκταθούν με τα εξής τρία χαρακτηριστικά:

Ομοιομορφία (uniformity): Σε οποιαδήποτε περιοχή μιας τυχαίας ακολουθίας, η κατανομή των 0 και των 1 πρέπει να είναι ομοιόμορφη, δηλαδή η πιθανότητα εμφάνισης τους πρέπει να είναι ίση με το 1/2.

Κλιμάκωση (scalability): Εάν μια ακολουθία είναι τυχαία, τότε και κάθε υποσύνολό της (δηλαδή μια μικρότερη ακολουθία που έχει εξαχθεί από αυτή), πρέπει να είναι και αυτό τυχαίο.

Συνέπεια (consistency): Η συμπεριφορά του αλγορίθμου σε ότι αφορά την τυχαιότητα των εξόδων του, πρέπει να είναι ίδια για όλες τις κλείδες οι οποίες παράγουν τις εξόδους.

Για την αξιολόγηση της τυχαιότητας των bits της ακολουθίας εξόδου του αλγορίθμου (keystreams), υπάρχουν στη διεθνή βιβλιογραφία πολλών ειδών στατιστικοί έλεγχοι, οι οποίοι μπορούν να ανιχνεύσουν μη κανονικότητες στην κατανομή των bits και να δώσουν ενδείξεις για αδυναμίες ασφαλείας και πιθανούς κινδύνους για κρυπταναλυτικές επιθέσεις. Οι σημαντικότεροι από αυτούς είναι οι εξής:

α). Στο βιβλίο «**The Art of Computer Programming, Seminumerical Algorithms, Volume 2»,** του Donald Knuth, καθηγητή του Πανεπιστημίου του Στάνφορντ (βιβλιογραφία **[4]**), περιγράφονται πολλοί εμπειρικοί έλεγχοι τυχαιότητας, οι οποίοι περιλαμβάνουν τους εξής : *frequency, serial , gap , poker , coupon collector's , permutation , run , maximum-of-t , collision , birthday spacings , serial correlation.* Αναλυτικές λεπτομέρειες υπάρχουν στην ιστοσελίδα: http://www-cs-faculty.stanford.edu/~knuth/taocp.html.

β). Ο καθηγητής του Πανεπιστημίου της Florida, George Marsaglia, ανέπτυξε τη σουίτα στατιστικών ελέγχων τυχαιότητας **DIEHARD** (βιβλιογραφία **[5]**), η οποία περιλαμβάνει τους εξής δεκαπέντε ελέγχους : *birthday spacings , overlapping permutations , ranks of 31x31 and 32x32 matrices , ranks of 6x8 matrices , monkey tests on 20-bit Words , monkey tests OPSO , OQSO , DNA , count the 1's in a stream of bytes , count the 1's in specific bytes , parking lot , minimum distance , random spheres , squeeze,*

overlapping sums , runs , craps. Αναλυτικές λεπτομέρειες υπάρχουν στην ιστοσελίδα: http://stat.fsu.edu/~geo\diehard.html.

γ). Το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας των ΗΠΑ (NIST), εξέδωσε την σουίτα στατιστικών ελέγχων **NIST 800-22** (βιβλιογραφία **[6]**), για τις τυχαίες και ψευδοτυχαίες γεννήτριες χαρακτήρων σε κρυπτογραφικές εφαρμογές. Η σουίτα αυτή, προϊόν συνεργασίας μεταξύ του Computer Security Division και του Statistical Engineering Division του NIST, περιλαμβάνει τους ελέγχους : *frequency , block frequency , cumulative sums , runs , long runs , rank (του G.Marsaglia) , spectral (βασισμένος στον Discrete Fourier Transform) , nonoverlapping template matchings , overlapping template matchings , universal statistical (του Maurer) , approximate entropy (βασισμένος στην εργασία των Pincus, Singer και Kalman) , random excursions (των Baron και Rukhin) , Lempel-Ziv complexity , linear complexity , serial.* Αναλυτικές λεπτομέρειες υπάρχουν στην ιστοσελίδα: http://www.itl.nist.gov/div893/staff/soto/jshome.html.

δ). Οι ερευνητές Κέντρου Ερευνών Ασφαλείας Πληροφοριών του Πανεπιστημίου Queensland University of Technology της Αυστραλίας, ανέπτυξαν τη σουίτα στατιστικών ελέγχων **Crypt-XS** (βιβλιογραφία **[7]**), για κρυπτογραφικούς τύπου stream και block. Το Crypt- XS περιλαμβάνει μεταξύ άλλων τους ελέγχους: frequency , binary derivative , change point , runs , sequence complexity , linear complexity. Αναλυτικές λεπτομέρειες υπάρχουν στην ιστοσελίδα: http://www.isrc.qut.edu.au/cryptx/index.html.

Τα (β), (γ) και (δ) από τα ανωτέρω πακέτα στατιστικών ελέγχων τυχαιότητας διατίθενται και σε λογισμικό και οι έλεγχοι που περιλαμβάνουν φαίνονται συνοπτικά στον Πίνακα 3. Αναλυτικές λεπτομέρειες για αυτά υπάρχουν στα **[5]**, **[6]** και **[7]** της βιβλιογραφίας.

Σε πολύ γενικές γραμμές, η διαδικασία με την οποία διεξάγονται οι προαναφερθέντες στατιστικοί έλεγχοι τυχαιότητας, σύμφωνα με το [6] είναι η εξής: Σε κάθε στατιστικό έλεγχο, καθορίζεται μία κρίσιμη τιμή (critical value), ανάλογα με το μαθηματικό υπόβαθρο στο οποίο βασίζεται ο έλεγχος. Στη συνέχεια διεξάγεται ο έλεγχος επί του δείγματος και εάν η στατιστική τιμή του ελέγχου δεν υπερβεί την κρίσιμη τιμή, τότε το δείγμα είναι τυχαίο, ενώ αν υπερβεί την κρίσιμη τιμή το δείγμα δεν είναι τυχαίο. Σε κάθε έλεγχο, έχει μεγάλη σημασία η ελαχιστοποίηση της πιθανότητας για λάθος Τύπου 1 (βγαίνει μη τυχαίο ένα δείγμα που είναι τυχαίο) και για λάθος Τύπου 2 (βγαίνει τυχαίο ένα δείγμα το οποίο δεν είναι τυχαίο).

Από όσα αναφέρθηκαν παραπάνω, και δεδομένου του πλήθους των στατιστικών ελέγχων οι οποίοι αναφέρθηκαν, υπάρχει ένας προβληματισμός σε ότι αφορά την αλληλοεπικάλυψη ορισμένων από αυτούς. Και γεννάται το εύλογο ερώτημα, πόσοι διαφορετικοί έλεγχοι απαιτούνται για να αξιολογήσουν επαρκώς την τυχαιότητα ενός συνόλου χαρακτήρων. Για το θέμα αυτό υπάρχει σε εξέλιξη ειδική επιστημονική μελέτη από το NIST, στην οποία χρησιμοποιείται η μεθοδολογία Ανάλυσης Κύριων Συστατικών (Principal Component Analysis) και για την οποία υπάρχει μια εισαγωγική αναφορά στο **[8]** της βιβλιογραφίας.

NIST SP 800-22 (για RNG και PRNG)	**DIEHARD (Marsaglia)** (για RNG)	**CRYPT-X** (Stream και Block Ciphers)
1) Frequency 2) Cumulative Sum 3) Runs 4) Rank 5) Spectral 6) Templates Matching 7) Universal Statistical 8) Approximate Entropy 9) Random Excursions 10) Moving Averages 11) Lempel-Ziv Compression 12) Linear Complexity 13) Bayes	1) Birthday Spacings 2) Overlapping 5-permutation 3) Binary Rank (6x8 Matrices) 4) Binary Rank (31x31& 32x32 Matrices) 5) Monkey tests (20-bit words) 6) Monkey tests (OPSO, OQSO, DNA) 7) Number of 1's in stream of bytes 8) Number of 1's in specific bytes 9) Parking Lot 10) Overlapping Sums 11) Squeeze 12) Minimum Distance 13) Random Sphere's 14) Runs 15) Craps	STREAM CIPHERS 1) Frequency 2) Binary derivatives 3) Change points 4) Runs 5) Sequence complexity 6) Linear complexity BLOCK CIPHERS (1) Frequency (2) Binary Derivative (3) Linear (4) Affine (5) Avalanche (Plaintext) (6) Complementation

Πίνακας 3. Τρία πακέτα στατιστικών ελέγχων τυχαιότητας (διατιθέμενα σε λογισμικό)

Στα Κεφάλαια 3 και 4 περιγράφουμε τις προϋποθέσεις και την διαδικασία εκτέλεσης των στατιστικών ελέγχων, ενώ στο Κεφάλαιο 12 περιγράφουμε τη μεθοδολογία εκτίμησης της ισχύος του κρυπτογραφικού αλγορίθμου βάσει των αποτελεσμάτων των ελέγχων.

3.4. Έλεγχοι ομοιότητας

Εκτός από τους ελέγχους τυχαιότητας, οι οποίοι εξετάζουν «εσωτερικά» τα δείγματα του αλγορίθμου, πρέπει να διεξαχθούν και «εξωτερικοί» έλεγχοι μεταξύ των δειγμάτων. Αυτό σημαίνει ότι, εκτός από τους ελέγχους τυχαιότητας στα bits των εξόδων του κρυπταλγορίθμου (οι οποίοι περιγράφηκαν στην προηγούμενη παράγραφο), είναι απαραίτητο να διεξάγονται και έλεγχοι για την εύρεση ομοιοτήτων μεταξύ των διαφορετικών εξόδων (οι οποίες παράχθηκαν με διαφορετική κλείδα). Στην περίπτωση αυτή, ερευνούμε εάν υπάρχουν κάποιες σημαντικού μεγέθους όμοιες ομάδες από bits σε δύο ή περισσότερα δείγματα. Εάν συμβαίνει αυτό, σημαίνει ότι ο αλγόριθμος έχει κάποιες «ισοδύναμες» κλείδες οι οποίες μειώνουν την αλγοριθμική του πολυπλοκότητα (όπως εξηγούμε στην παράγραφο 3.5).

Κατά τους ελέγχους αυτούς, πρέπει να εξετάζονται με προσοχή, ο αριθμός των τυχόν όμοιων ομάδων από bits, το μέγεθος τους, καθώς και η θέση τους εντός των κρυπτογραφικών εξόδων. Ο στόχος είναι να διερευνηθεί εάν αυτές οι ομοιότητες μπορούν να προκαλέσουν σημαντική μείωση της ισχύος του κρυπταλγορίθμου και να οδηγήσουν σε μια επιτυχή κρυπτανάλυση. Σε μια τέτοια περίπτωση, ο κρυπταναλυτής μπορεί να εφαρμόσει την επίθεση με γνωστό ανοικτό κείμενο (όπως αναφέραμε στην παράγραφο 1.5.2). Στην συνέχεια, αναζητάει συγκεκριμένα κρυπτογραφημένα κείμενα, τα οποία παρουσιάζουν τις ομοιότητες, τα στοιχεία των οποίων γνωρίζει εκ των προτέρων από την έρευνα που έχει κάνει στον αλγόριθμο (αριθμός, μέγεθος, θέση των ομοιοτήτων και κλείδα με την οποία αυτές εμφανίζονται). Από τις ομοιότητες βρίσκει τις αντίστοιχες κλείδες και φυσικά στην συνέχεια μπορεί να αποκρυπτογραφήσει όλα τα κείμενα τα οποία παρήχθησαν με αυτές.

Στη συνέχεια, δίνουμε δύο ενδεικτικά και απλά παραδείγματα ομοιοτήτων μέσα σε δύο δυαδικά αρχεία:

Παράδειγμα 1: Στο παρακάτω παράδειγμα φαίνονται δύο όμοια τμήματα από 20 συνεχόμενα bits σε δύο διαφορετικές αλγοριθμικές εξόδους που παρήγαγαν οι κλείδες K_1 και K_2 (σημειωμένα με κόκκινο).

Έξοδος με την κλείδα K_1: 10110110011100010111001110111011100100 11
Έξοδος με την κλείδα K_2: 00101010111010011110001011100111011110 10

Στην περίπτωση αυτή, τα 20 ίδια συνεχόμενα bits είναι αρκετά για να μην θεωρηθούν αμελητέα, οπότε η περίπτωση αυτή χρήζει περαιτέρω εξέτασης.

Παράδειγμα 2: Στο παρακάτω παράδειγμα όπου φαίνονται οι αλγοριθμικές έξοδοι με τις κλείδες K_3 και K_4 , έχουμε αρκετές όμοιες ομάδες από 2 συνεχόμενα bits (που δεν σημειώνονται), καθώς και από 3 συνεχόμενα bits (σημειωμένες με κόκκινο).

Έξοδος με την κλείδα K_3: 10010110010101101010101001011100111011 10
Έξοδος με την κλείδα K_4: 10101010010101111001011110000110100110 10

Στην περίπτωση αυτή, τα 2 ή 3 όμοια συνεχόμενα bits είναι πολύ λίγα για να θεωρηθεί ότι αποτελούν μια σημαντικού μεγέθους ομοιότητα στις αλγοριθμικές εξόδους.

3.4.1 Αριθμός ελέγχων ομοιότητας

Είναι προφανές ότι για την εύρεση των ομοιοτήτων μεταξύ των δειγμάτων του αλγορίθμου, τα δείγματα πρέπει να εξεταστούν ανά ζεύγη. Από τη θεωρία της συνδυαστικής **[10]** έχουμε ότι ο αριθμός των συνδυασμών των n δειγμάτων ανά 2 , δίδεται από τον τύπο:

$$\binom{n}{2} = \frac{n!}{2!\,(n-2)!}$$

Όπως έχουμε αναφέρει, λόγω του τεράστιου πλήθους των κλειδών των κρυπτογραφικών αλγορίθμων, οι έλεγχοι τυχαιότητας και ομοιότητας γίνονται δειγματοληπτικά. Π.χ. για ένα αλγόριθμο με κλείδα 128 bits, αντί να παράγουμε και να εξετάσουμε ένα δείγμα για κάθε του κλείδα (δηλαδή συνολικά 2^{128} δείγματα!), στην πράξη εξετάζουμε πολύ λιγότερα δείγματα με τη μέθοδο της δειγματοληψίας (η οποία εξετάζεται διεξοδικά στην παράγραφο 3.8). Έτσι, αν υποθέσουμε ότι αντί των 2^{128} δειγμάτων, αποφασίσουμε ότι για ένα αποδεκτό σφάλμα δειγματοληψίας θα εξετάσουμε μόνο 1000 δείγματα, από τον ανωτέρω τύπο για n=1000 προκύπτει ότι πρέπει να εξεταστούν 499.500 ζευγάρια δειγμάτων για έλεγχο ομοιότητας. Επειδή όμως και αυτός είναι ένας τεράστιος αριθμός ελέγχων, αλλά και επειδή κάθε έλεγχος ομοιότητας είναι πολύ χρονοβόρος, στην πράξη θα πρέπει να εξετάσουμε ένα πολύ μικρότερο αριθμό ζευγαριών, χρησιμοποιώντας πάλι τη μέθοδο της δειγματοληψίας.

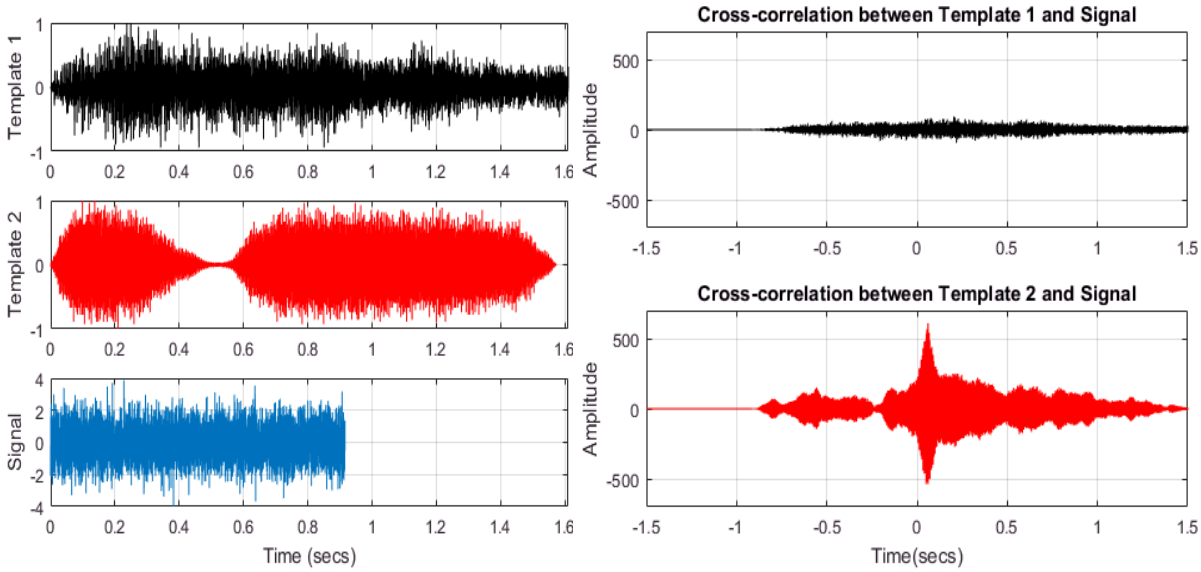
3.4.2 Μέθοδοι ελέγχου ομοιότητας

Από όσα αναφέρθηκαν, συμπεραίνεται ότι για την εύρεση των ομοιοτήτων μεταξύ των ψηφιακών εξόδων του αλγορίθμου, πρέπει να χρησιμοποιηθεί μία μέθοδος η οποία να αναλύει κάθε φορά δύο δείγματα εξόδου του αλγορίθμου και να εντοπίζει τον αριθμό, το μέγεθος και τη θέση των όμοιων ομάδων από bits μέσα σε αυτά. Τα διάφορα διαθέσιμα λογισμικά του εμπορίου δεν είναι κατάλληλα για να κάνουν μια αναλυτική έρευνα για την ανεύρεση ομοιοτήτων. Τα μεν προγράμματα ανάλυσης δυαδικών αρχείων (hex editors) δίνουν κυρίως μία οπτική εμφάνιση των bits για έλεγχο και διορθώσεις, χωρίς περαιτέρω ανάλυση. Ενώ τα προγράμματα σύγκρισης αρχείων (π.χ. το file comparison στο MATLAB, το πρόγραμμα Beyond Compare, η εντολή FC των Windows κλπ,), έχουν στόχο να βρουν εάν δύο αρχεία είναι όμοια ή ανόμοια στο σύνολό τους, χωρίς να δίνουν τις απαιτούμενες για την έρευνά μας αναλυτικές πληροφορίες.

Ένας τρόπος για να γίνει η σύγκριση ομοιότητας, είναι να εφαρμόσουμε τη μέθοδο της ετεροσυσχέτισης (cross correlation). Η ετεροσυσχέτιση μεταξύ δύο σημάτων ουσιαστικά εφαρμόζει μία βαθμιαία μετατόπιση (χρονική καθυστέρηση) του ενός σήματος μέσα στο άλλο, και μετά από κάθε μετατόπιση διαπιστώνει τις τυχόν ομοιότητες μεταξύ τους (βιβλ. **[11]** και **[12]**). Για τις ψηφιακές ακολουθίες (όπως στην περίπτωσή μας) η μετατόπιση υλοποιείται με βαθμιαία ολίσθηση των bits της μίας ακολουθίας μέσα στην άλλη.

Στην Εικόνα 1 (δεξιό τμήμα) φαίνονται οι γραφικές παραστάσεις των ετεροσυσχετίσεων μεταξύ ενός σήματος (signal) και δύο σημάτων αναφοράς Template 1 και Template 2 (που φαίνονται στο αριστερό τμήμα της εικόνας).

Βλέπουμε ότι η ετεροσυσχέτιση του σήματος με το Template 1 είναι σχεδόν μηδενική, που σημαίνει ότι δεν υπάρχει ομοιότητα μεταξύ τους. Όμως η ετεροσυσχέτιση του σήματος με το Template 2 δεν είναι μηδενική και δείχνει μία έξαρση λίγο μετά το χρόνο 0 (μέγιστο σημείο ομοιότητας), που σημαίνει ότι το σήμα ενυπάρχει μέσα στο Template 2 (βιβλ. **[13]**).

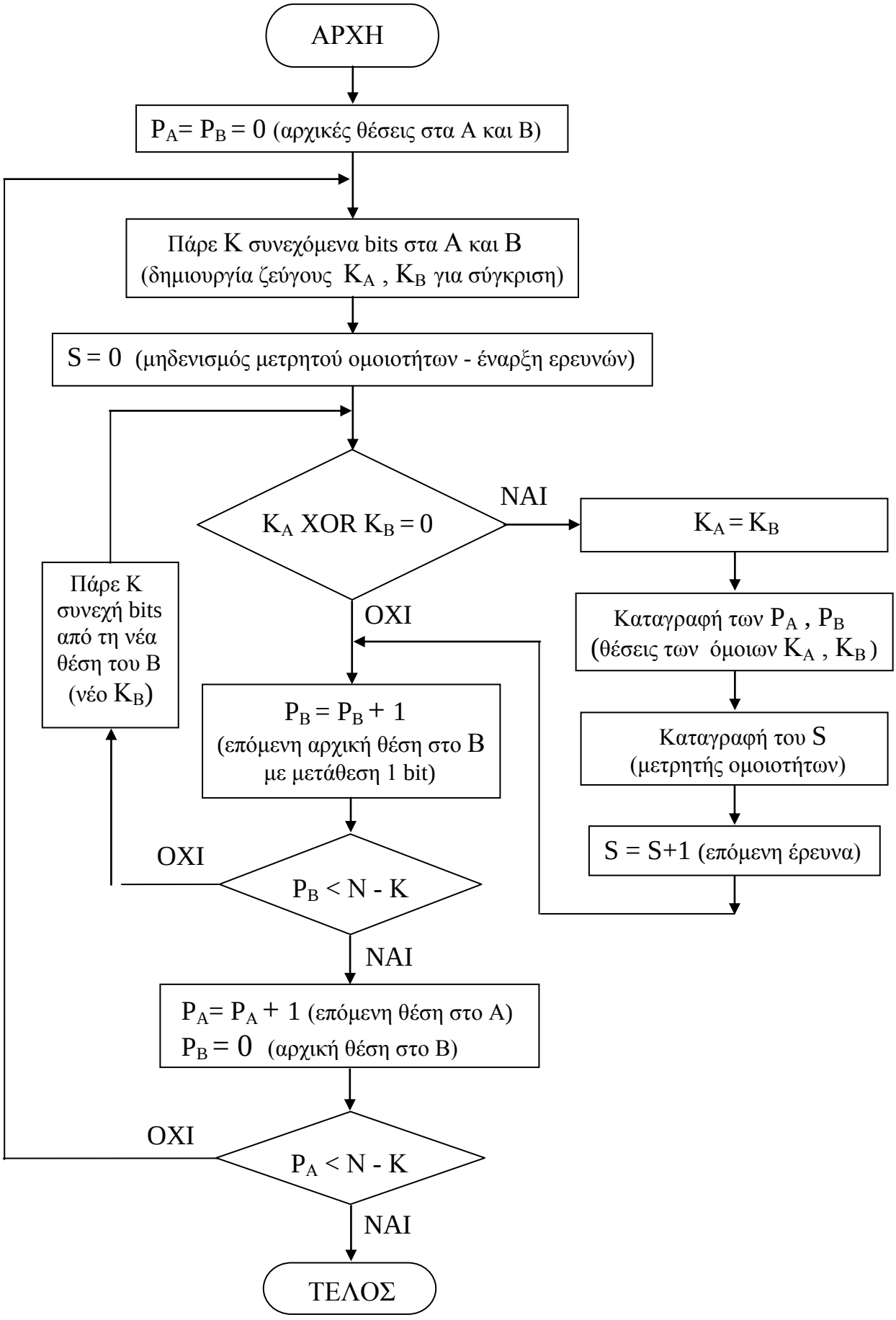


Εικόνα 1. Ετεροσυσχετίσεις μεταξύ ενός σήματος (signal) και δύο σημάτων αναφοράς Template 1 και Template 2 (από το λογισμικό MATLAB).

Καμία όμως από τις μεθόδους σύγκρισης ψηφιακών αρχείων οι οποίες περιγράφηκαν, δεν είναι τόσο αναλυτική, ώστε να εντοπίζει το πλήθος, το μέγεθος και την ακριβή θέση των όμοιων ομάδων από bits μέσα σε αυτά. Για το λόγο αυτό σχεδιάσαμε μία αναλυτική μέθοδο εντοπισμού των ομοιοτήτων εντός δύο δυαδικών ακολουθιών, η διαδικασία της οποίας παρουσιάζεται στο διάγραμμα ροής του Σχήματος 3. Η μέθοδος σε γενικές γραμμές ανιχνεύει και καταγράφει όμοιες ομάδες από K bits, μέσα σε δύο αρχεία A και B τα οποία έχουν ίσο μήκος από N bits το κάθε ένα (έξοδοι κρυπταλγορίθμου). Η γενική ιδέα είναι να παίρνουμε κάθε φορά ένα τμήμα από K bits στο αρχείο A (τμήμα K_A) και να το συγκρίνουμε με διαδοχικά τμήματα από K bits του αρχείου B (τμήματα K_B). Τα διαδοχικά τμήματα K_B του αρχείου B σχηματίζονται εάν κάθε φορά μεταθέτουμε κατά ένα bit το σημείο εκκίνησης στο B και δημιουργούμε ένα νέο αρχείο από K bits το οποίο και συγκρίνουμε με το K_A.

Η έρευνα για την ομοιότητα των K_A και K_B γίνεται με δυαδική πράξη XOR. Εάν το αποτέλεσμα της XOR είναι μηδέν, τότε σημειώνουμε την ανευρεθείσα ομοιότητα και τα στοιχεία της, δηλαδή τις θέσεις P_A και P_B στις οποίες βρίσκονται τα K_A και K_B αντίστοιχα, καθώς και την τιμή του μετρητή του αριθμού ομοιοτήτων S. Εάν το αποτέλεσμα της XOR δεν είναι μηδέν, τότε όπως είπαμε προηγουμένως, μεταθέτουμε την προηγούμενη θέση του K_B κατά 1 bit, σχηματίζουμε ένα νέο K_B και επαναλαμβάνουμε την ίδια διαδικασία για να διαπιστώσουμε εάν είναι όμοιο με το K_A.

Αφού τελειώσουμε τις συγκρίσεις για το πρώτο K_A , μεταθέτουμε κατά ένα bit το σημείο εκκίνησης στο A, και δημιουργούμε το δεύτερο K_A από K bits, το οποίο συγκρίνουμε και αυτό με όλα τα K_B του αρχείου B, με τον ίδιο τρόπο που αναφέραμε προηγουμένως. Η διαδικασία αυτή επαναλαμβάνεται έως ότου φθάσουμε στο τέλος του αρχείου A.



<u>Σχήμα 3.</u> Διάγραμμα ροής, για την ανεύρεση όμοιων ομάδων από Κ bits, μέσα σε δύο αρχεία Α και Β μήκους Ν bits (έξοδοι κρυπταλγορίθμου).
Το S είναι ο αριθμός των K_B που είναι όμοια με το εκάστοτε K_A .

Η διαδικασία η οποία περιγράφηκε στο διάγραμμα ροής του Σχήματος 3, θα έχει ως τελικό αποτέλεσμα τον Πίνακα 4 , στον οποίο φαίνονται όλα τα όμοια K_A και K_B που εντοπίσαμε, μαζί με τα στοιχεία τους, δηλαδή τις θέσεις που βρίσκονται (P_A και P_B αντίστοιχα) και την τιμή του μετρητή των αριθμών ομοιότητας S.

Όσο μεγαλύτερο είναι το πλήθος και το μέγεθος των όμοιων ομάδων bits, τόσο πιο «επικίνδυνη» είναι η ομοιότητα των δύο εξεταζόμενων εξόδων του αλγορίθμου. Και προφανώς όσο περισσότερα είναι αυτά τα «επικίνδυνα» ζεύγη των εξόδων του, τόσο πιο «ύποπτος» για μη τυχαιότητα είναι ο αλγόριθμος.

ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΛΕΓΧΟΥ ΟΜΟΙΟΤΗΤΑΣ		
ΒΗΜΑ ΕΡΕΥΝΑΣ	ΘΕΣΕΙΣ ΕΜΦΑΝΙΣΗΣ ΤΩΝ ΟΜΟΙΩΝ K_A , K_B	ΑΡΙΘΜΟΣ ΟΜΟΙΩΝ K_B ΜΕ ΤΟ ΤΡΕΧΟΝ K_A
1	$P_{A(1)}$, ($P_{B(1)}$, $P_{B(2)}$, $P_{B(3)}$, ...)	S_1
2	$P_{A(2)}$, ($P_{B(1)}$, $P_{B(2)}$, $P_{B(3)}$, ...)	S_2
3	$P_{A(3)}$, ($P_{B(1)}$, $P_{B(2)}$, $P_{B(3)}$, ...)	S_3
.....	……	…..
.....	……	…..
N-K	$P_{A(N-K)}$,($P_{B(1)}$, $P_{B(2)}$, $P_{B(3)}$, ...)	S_{N-K}

Πίνακας 4. Αποτελέσματα των ελέγχων ομοιότητας του Σχήματος 3

Σημείωση 1: Αν στο διάγραμμα του Σχήματος 3 βάλουμε K=N, τότε προφανώς θα ερευνηθεί μόνο η ομοιότητα ολόκληρων των αρχείων Α και Β.

Σημείωση 2: Αν θέλουμε να αναζητήσουμε την τυχόν ύπαρξη μίας εκ των προτέρων γνωστής ακολουθίας από bits μέσα στο αρχείο Β, τότε καταργείται ο εξωτερικός βρόχος επανάληψης στο διάγραμμα του Σχήματος 3 και στη θέση του K_A θα βάλουμε τη γνωστή ακολουθία από bits. Η περίπτωση αυτή μπορεί να εφαρμοστεί όταν ψάχνουμε για κάποιο κακόβουλο λογισμικό (malware) ή κάποια κερκόπορτα (back door) στον αλγόριθμο. Απαραίτητη βέβαια προϋπόθεση για αυτό, είναι να γνωρίζουμε κάποιο pattern από bits το οποίο περιέχεται στο ζητούμενο κακόβουλο λογισμικό.

3.5. Αδύναμες και ισοδύναμες κλείδες

Στη βιβλιογραφία της κρυπτολογίας, αδύναμες κλείδες (weak keys) ονομάζονται αυτές για τις οποίες η επανακρυπτογράφηση του κρυπτογραφήματος με την ίδια κλείδα, δίνει το ανοικτό κείμενο:

$$\underline{\text{Αδύναμη κλείδα K}} \rightarrow E_K [\, E_K (x) \,] = x$$

Επίσης, ζεύγος αδύναμων κλειδών (weak key pair) ονομάζεται ένα ζευγάρι κλειδών για το οποίο, η κρυπτογράφηση με την πρώτη κλείδα του κρυπτογραφήματος της δεύτερης κλείδας, δίνει το ανοικτό κείμενο:

$$\underline{\text{Ζεύγος αδύναμων κλειδών } K_1 , K_2} \rightarrow E_{K1} [\, E_{K2} (x) \,] = x$$

Ενδεικτικά αναφέρουμε ότι ο αλγόριθμος DES έχει 4 αδύναμες κλείδες και 6 ζεύγη αδύναμων κλειδών.

Στα πλαίσια της παρούσας εργασίας, εισάγουμε μια διαφοροποίηση του ορισμού των αδύναμων κλειδών και επίσης εισάγουμε τον νέο ορισμό των ισοδύναμων κλειδών, ως εξής:

Αδύναμη κλείδα (weak key), ονομάζεται κάθε κλείδα για την οποία η έξοδος του κρυπταλγορίθμου δεν είναι τυχαία.

Ισοδύναμη κλείδα (equivalent key), ονομάζεται κάθε κλείδα η οποία δίνει όμοια (ή παρόμοια) αλγοριθμική έξοδο με αυτή που δίνει κάποια άλλη κλείδα.

Είναι ευνόητο ότι η ύπαρξη αδύναμων και ισοδύναμων κλειδών μειώνει το ονομαστικό πλήθος N των κλειδών ενός κρυπτογραφικού αλγορίθμου, το οποίο είναι $N = 2^L$, όπου L = μήκος του κλειδιού (σε bits). Στην περίπτωση αυτή, ο ενεργός (ουσιαστικός) αριθμός των κλειδών N_A είναι :

$$N_A = N - N_W - N_E$$

όπου N_W είναι ο αριθμός των αδύναμων κλειδών και N_E ο αριθμός των ισοδύναμων κλειδών.

Από όσα αναφέρθηκαν στην παρούσα παράγραφο, ουσιαστικά προκύπτει ότι οι έλεγχοι τυχαιότητας στο περιεχόμενο κάθε αλγοριθμικής εξόδου έχουν σκοπό να αναδείξουν τις αδύναμες κλείδες, ενώ οι έλεγχοι ομοιότητας μεταξύ των αλγοριθμικών εξόδων έχουν σκοπό να αναδείξουν τις ισοδύναμες κλείδες.

3.6. Διαδικασία των ελέγχων

Από το συνολικό πλήθος N των κρυπτογραφικών κλειδών, επιλέγουμε ένα μικρότερο πλήθος από n κλείδες με τη μέθοδο της δειγματοληψίας (η οποία περιγράφεται στην παράγραφο 3.8). Με την διαδικασία που περιγράψαμε στην παράγραφο 3.2., για κάθε μία από αυτές τις n κλείδες παράγουμε ένα δείγμα εξόδου του αλγορίθμου και αποθηκεύουμε τα n δείγματα σε αντίστοιχα αρχεία. Κατόπιν, υποβάλουμε όλα τα δείγματα στους στατιστικούς ελέγχους και αποθηκεύουμε τα αποτελέσματα των ελέγχων. Η τελική απόφαση για το επίπεδο της τυχαιότητας, ανεξαρτησίας και μη προβλεψιμότητας των εξόδων του υπό εξέταση αλγορίθμου, γίνεται βάσει του συνολικού ποσοστού επιτυχίας που έχουν οι στατιστικοί έλεγχοι στα εξετασμένα δείγματα. Τα βασικά προβλήματα που προκύπτουν εάν θέλουμε να έχουμε μια αξιόπιστη αλλά και πρακτικά εφικτή διενέργεια των ελέγχων, είναι τα εξής:

α. Πόσα δείγματα εξόδου του αλγορίθμου θα πρέπει να ελέγξουμε;

β. Πόσο πρέπει να είναι το μέγεθος κάθε δείγματος;

γ. Πως μπορούμε να μειώσουμε τον χρόνο των ελέγχων;

δ. Με ποια μέθοδο πρέπει να επιλέξουμε τις δειγματοληπτικές κλείδες;

ε. Πως βαθμολογούμε την ασφάλεια των αλγορίθμων με βάση τα αποτελεσμάτων των ελέγχων;

Στις επόμενες παραγράφους θα αναλύσουμε τα προβλήματα (α), (β), (γ) και θα προτείνουμε τρόπους επίλυσής τους. Το πρόβλημα (δ) εξετάζεται στο Κεφάλαιο 4 και το πρόβλημα (ε) εξετάζεται στο Κεφάλαιο 12.

3.7. Πλήθος δειγμάτων

Από θεωρητικής άποψης, για να διενεργήσουμε μία ολοκληρωμένη και εξαντλητική αξιολόγηση, θα πρέπει για κάθε κλείδα να κατασκευάσουμε και ένα δείγμα του κρυπταλγορίθμου. Στον Πίνακα 5 φαίνεται το πλήθος των συνδυασμών της κλείδας ενός τυπικού συμμετρικού κρυπταλγορίθμου για τέσσερεις ενδεικτικές τιμές (64, 128, 256 και 512 bits).

Μέγεθος κλείδας (σε bits)	Πλήθος συνδυασμών κρυπτογραφικής κλείδας	
	Δυαδικό σύστημα	Δεκαδικό σύστημα
64	2^{64}	$1{,}8 \cdot 10^{19}$ (18 πεντάκις εκατομμύρια)
128	2^{128}	$3{,}4 \cdot 10^{38}$ (340 εντεκάκις εκατομμύρια)
256	2^{256}	$1{,}2 \cdot 10^{77}$ (120 εικοσιτετράκις εκατομμύρια)
512	2^{512}	$1{,}3 \cdot 10^{154}$ (13 πενηντάκις εκατομμύρια)

Πίνακας 5. Πλήθος συνδυασμών της κρυπτογραφικής κλείδας

Όπως φαίνεται από τον Πίνακα 5, το πλήθος των συνδυασμών της κλείδας είναι ένας αστρονομικά μεγάλος αριθμός. Στον Πίνακα 1 της παραγράφου 1.5.3 έχουμε ήδη παρουσιάσει για κάποια ενδεικτικά μεγέθη κλειδών, τις τιμές του χρόνου που απαιτείται για να γίνει μία εξαντλητική κρυπταναλυτική έρευνα για όλους τους συνδυασμούς της κλείδας (exhaustive

search). Είναι φανερό ότι είναι αδύνατο να εξετάσουμε όλο αυτό το πλήθος των συνδυασμών σε ένα πρακτικά εκμεταλλεύσιμο χρόνο, ακόμα και με την παράλληλη χρήση ενός εκατομμυρίου γρήγορων υπολογιστών (τύπου PC) ή ειδικών ολοκληρωμένων κυκλωμάτων που θα εξομοιώνουν τον αλγόριθμο (τύπου FPGA ή ASIC). Από τα παραπάνω, είναι φανερό ότι κατά τους κρυπτογραφικούς ελέγχους θα πρέπει να εφαρμόσουμε την μέθοδο της δειγματοληψίας, η οποία περιγράφεται παρακάτω.

3.8. Δειγματοληπτικοί έλεγχοι

Όταν επιθυμούμε να μετρήσουμε την ύπαρξη κάποιου συγκεκριμένου χαρακτηριστικού πάνω σε ένα πολύ μεγάλο πλήθος *N* στοιχείων, είναι πολύ δύσκολο και χρονοβόρο να εξετάσουμε ένα προς ένα τα μεμονωμένα *N* στοιχεία. Για να αποφύγουμε αυτή τη δυσκολία, χρησιμοποιούμε τη μέθοδο της δειγματοληψίας. Κατά τη δειγματοληψία εξετάζουμε μόνο ένα μικρό δείγμα *n* από το συνολικό πλήθος *N* και κατόπιν αποφασίζουμε για το γενικό σύνολο, με κάποιο προκαθορισμένο εκ των προτέρων ποσοστό σφάλματος. Βάσει της βιβλιογραφίας **[14]**, **[15]** και **[16]**, ο αριθμός των απαιτούμενων δειγμάτων *n* προκύπτει από τον τύπο (1) :

$$n = \frac{\frac{z^2 pq}{e^2}}{1 + \frac{1}{N}\left\{\frac{z^2 pq}{e^2} - 1\right\}} \quad \textbf{(1)}$$

όπου:

N = συνολικό πλήθος (υπερσύνολο του *n*).

z = 1.96 (η τιμή από την καμπύλη της κανονικής κατανομής για επίπεδο εμπιστοσύνης 95%).

p = 1- q το ποσοστό του ζητούμενου χαρακτηριστικού των δειγμάτων .

p = *q* = 0,5 = 50% οι οριακές εκτιμήσεις των p, q , για τη «χειρότερη εκδοχή» της μέγιστης μεταβλητότητας τους (και επομένως για μέγιστο n).

e = το περιθώριο σφάλματος του εκτιμώμενου ποσοστού.

Σημείωση : Στη περίπτωσή μας θεωρητικά ισχύει η διωνυμική κατανομή, διότι τα ενδεχόμενα είναι δύο (τυχαίο και μη τυχαίο δείγμα). Όμως για διευκόλυνση των υπολογισμών επιλέξαμε την κανονική κατανομή, την οποία προσεγγίζει κατά πολύ η διωνυμική για n >100 (σύμφωνα με τα [6] και [14]).

Για τους κρυπτογραφικούς ελέγχους, το ***n*** είναι ο αριθμός των εξεταζόμενων δειγμάτων εξόδου του αλγορίθμου, δηλαδή ισούται με τον αριθμό των εξεταζόμενων κλειδών. Οπότε, το ***N*** είναι το συνολικό πλήθος των κλειδών και το ***p*** είναι το ποσοστό τυχαιότητας των δειγμάτων. Και επειδή το ***N*** είναι ένας πάρα πολύ μεγάλος αριθμός (συνήθως μεταξύ 2^{128} έως 2^{256}) το οποίο πρακτικά τείνει στο άπειρο, ο τύπος (1) απλοποιείται στον (2) :

$$n = \frac{z^2 pq}{e^2} \quad \textbf{(2)}$$

Εφαρμόζοντας τον τύπο (2) μπορούμε να υπολογίσουμε τον απαιτούμενο αριθμό των δειγμάτων του κρυπταλγορίθμου για ορισμένες χαρακτηριστικές τιμές του περιθωρίου σφάλματος. Από τον τύπο φαίνεται ότι εάν θέλουμε να μειώσουμε το περιθώριο σφάλματος ***e*** , θα πρέπει να αυξήσουμε κατά πολύ τον αριθμό των δειγμάτων ***n*** . Όμως, κατά τους κρυπτογραφικούς ελέγχους εκτός από το πλήθος των δειγμάτων, παίζει σημαντικό ρόλο και το μέγεθος του κάθε δείγματος, το οποίο εξετάζουμε στην επόμενη παράγραφο.

3.9. Μέγεθος δειγμάτων

Αν πάρουμε ως παράδειγμα τους κρυπταλγόριθμους ροής (stream ciphers), αυτοί παράγουν ψηφιακές ακολουθίες, με τις οποίες αναμιγνύουν την ανοικτή πληροφορία (με XOR) για να παράγουν το κρυπτογραφημένο κείμενο. Αυτές οι ακολουθίες (key streams) πρέπει να είναι όσο το δυνατόν πιο πολύπλοκες, για να μην μπορούν να υπολογιστούν και να αναπαραχθούν από κάποιον υποκλοπέα (δηλαδή πρέπει να πλησιάζουν την τυχαιότητα). Όμως στην πράξη οι κρυπτογραφικές ακολουθίες των stream ciphers οι οποίοι χρησιμοποιούν γραμμικούς καταχωρητές ανάδρασης (LFSR), δεν είναι απόλυτα τυχαίες, αλλά ψευδοτυχαίες με μία πολύ μεγάλη περίοδο επανάληψης.

Από θεωρητική άποψη λοιπόν, θα λέγαμε ότι πρέπει να εξετάζουμε δείγματα των stream cipher, μεγέθους ίσου ή μεγαλύτερου της ελάχιστης περιόδου επανάληψής τους, ώστε να ερευνήσουμε την τυχαιότητα καθ'όλο το μήκος της παραγόμενης ακολουθίας. Στον Πίνακα 6 φαίνονται ενδεικτικά οι ελάχιστοι περίοδοι επανάληψης ορισμένων stream ciphers. Για απλοποίηση των υπολογισμών, υποθέσαμε ότι οι stream ciphers αποτελούνται από 1 έως 4 όμοιους LFSR μεγίστου μήκους (στήλες του πίνακα). Για κάθε stream cipher βάλαμε ως εναλλακτικά μήκη των LFSR, τα 40, 48, 56 bits (γραμμές του πίνακα). Αν L είναι το μήκος (σε bits) ενός LFSR, τότε η ελάχιστη περίοδος του είναι 2^L -1, ενώ όταν έχουμε συνδυασμό περισσότερων του ενός, η συνολική περίοδος ισούται με το γινόμενο των περιόδων τους (βιβλ. **[1]**). Επομένως, στον Πίνακα 6 η ελάχιστη περίοδος επανάληψης είναι $(2^{L1}-1)(2^{L2}-1)(2^{L3}-1)(2^{L4}-1)$, όπου L_1 , L_2 , L_3 , L_4 είναι τα μήκη των LFSR και $L_1=L_2=L_3=L_4$.

Μήκος L του LFSR (bits)	ΕΛΑΧΙΣΤΗ ΠΕΡΙΟΔΟΣ ΤΟΥ STREAM CIPHER (σε bits και σε χρόνο μετάδοσης με ταχύτητα 2 Mbits/s)			
	Με 1 LFSR	Με 2 LFSR	Με 3 LFSR	Με 4 LFSR
40	$1,1*10^{12}$ bits	$1,2*10^{24}$ bits	$1,32*10^{36}$ bits	$1,46*10^{48}$ bits
	6,4 μέρες	$1,9*10^{10}$ χρόνια	$2*10^{22}$ χρόνια	$2,24*10^{34}$ χρόνια
48	$2,8*10^{14}$ bits	$8*10^{28}$ bits	$2,23*10^{43}$ bits	$6,27*10^{57}$ bits
	4,4 χρόνια	$1,24*10^{15}$ χρόνια	$3,52*10^{29}$ χρόνια	$9,9*10^{43}$ χρόνια
56	$7,2*10^{16}$ bits	$5,2*10^{33}$ bits	$3,74*10^{50}$ bits	$2,7*10^{67}$ bits
	1142 χρόνια	$8,4*10^{19}$ χρόνια	$5,9*10^{36}$ χρόνια	$2,16*10^{53}$ χρόνια

Πίνακας 6. Ελάχιστη περίοδος επανάληψης της ακολουθίας (keystream) ενός stream cipher

Στον Πίνακα 6 για κάθε L, εκτός από την περίοδο υπολογίσαμε και τον απαιτούμενο χρόνο μετάδοσης των bits σε ένα επικοινωνιακό κανάλι με ταχύτητα 2 Mbits/s (γραμμές με κίτρινο χρώμα). Αυτός είναι ο απαιτούμενος χρόνος από ένα υποκλοπέα, ώστε να λάβει όλα τα περιοδικά επαναλαμβανόμενα bits και να αναλύσει τον αλγόριθμο. Όπως φαίνεται από τον Πίνακα 6, αυτό είναι ανέφικτο λόγω του τεραστίου απαιτούμενου χρόνου. Επομένως δεν θεωρούμε αναγκαίο κατά την αξιολόγηση να εξετάζουμε ακολουθίες τόσο μεγάλου μήκους

Μία περισσότερο εφικτή αλλά και ουσιαστική προσέγγιση, είναι να επιλέξουμε το μέγεθος των ελεγχόμενων δειγμάτων ανάλογα με τον όγκο των πληροφοριών. Ειδικότερα, μας ενδιαφέρει ο όγκος των πληροφοριών οι οποίες κρυπτογραφούνται με την ίδια κλείδα, ώστε να εξετάσουμε την αντοχή του κρυπτοσυστήματος σε πρακτικές συνθήκες κρυπτανάλυσης. Στα περισσότερα κρυπτοσυστήματα η κλείδα αλλάζει κάθε ημέρα, οπότε μας ενδιαφέρει ο όγκος των πληροφοριών οι οποίες κρυπτογραφούνται κατά την διάρκεια μίας ημέρας. Ορισμένα όμως κρυπτοσυστήματα (όπως τα κρυπτοφωνικά), αλλάζουν κλείδα σε κάθε νέα επικοινωνία (session key), οπότε στην περίπτωση αυτή μας ενδιαφέρει ο όγκος των πληροφοριών οι οποίες κρυπτογραφούνται κατά την διάρκεια μίας επικοινωνιακής σύνδεσης (session).

Όπως φαίνεται από τον Πίνακα 7, το ψηφιακό μέγεθος της πληροφορίας, διαφέρει κατά πολύ ανάλογα με το είδος και την διάρκειά της. Οπότε, στην περίπτωση που αξιολογούμε ένα κρυπταλγόριθμο τύπου stream, το μέγεθος της ακολουθίας του (key stream) το οποίο θα εξετάσουμε, σύμφωνα με την ανωτέρω λογική πρέπει να είναι τουλάχιστον αντίστοιχο του μεγέθους της κρυπτογραφημένης πληροφορίας. Π.χ. στην περίπτωση που έχουμε κρυπτογράφηση 10 σελίδων κειμένου, χρειαζόμαστε μόνο 100 Kbyte ακολουθίας, ενώ για τα 10 λεπτά βίντεο, χρειαζόμαστε να παράγουμε 800.000 Kbyte ακολουθίας. Επειδή στις εργαστηριακές μας δοκιμές τα περισσότερα κρυπτοσυστήματα αφορούσαν κείμενο ή φωνή και επειδή είχαμε χρονικό περιορισμό λόγω της μικρής υπολογιστικής ισχύος, επιλέγαμε ένα μέγεθος δείγματος της τάξης των 132 Kbyte (δηλαδή 1 Mbit σε binary unformatted μορφή). Το μέγεθος του 1Mbit είναι αρκετό για απλά κείμενα έως 12 σελίδες και για ψηφιοποιημένη φωνή έως 3,5 λεπτά. Όταν όμως έχουμε μεγαλύτερη διάρκεια τηλεφωνικής επικοινωνίας ή αποστολή φωτογραφίας ή βίντεο, το μέγεθος δείγματος του 1Mbit είναι πολύ μικρό, οπότε ενδέχεται να μην ανακαλύψουμε κάποιες υπαρκτές τρωτότητες του κρυπταλγορίθμου.

Είδος πληροφορίας	Διάρκεια / Ανάλυση	Μέγεθος (Kbytes)	Παρατηρήσεις
Απλό κείμενο	10 σελίδες	100	Με το MS Word
Φωνή	5 λεπτά	1.440	Με ψηφιοποίηση vocoder (4800 bits/s)
Φωτογραφία ή σχέδιο	5 Mpixels	3.00	Με συμπίεση JPEG
Βίντεο	10 λεπτά	800.000	Με συμπίεση MPEG

Πίνακας 7. Ενδεικτικά μεγέθη ψηφιοποιημένης πληροφορίας

3.10. Απαιτούμενος χρόνος

Βάσει των όσων αναπτύχθηκαν προηγουμένως, για να υπολογίσουμε τον απαιτούμενο χρόνο των κρυπτογραφικών ελέγχων, κατ'αρχήν εφαρμόζουμε τον τύπο (2) της παραγράφου 3.8 και υπολογίζουμε τον απαιτούμενο αριθμό των δειγμάτων για ορισμένες χαρακτηριστικές τιμές του περιθωρίου σφάλματος δειγματοληψίας. Από τα αποτελέσματα τα οποία καταγράφονται στις δύο πρώτες στήλες του συγκριτικού Πίνακα 8, φαίνεται ότι εάν θέλουμε να μειώσουμε το περιθώριο σφάλματος θα πρέπει να αυξήσουμε κατά πολύ τον αριθμό των δειγμάτων. Ο μεγαλύτερος όμως αριθμός δειγμάτων του αλγορίθμου σημαίνει και πολύ μεγαλύτερο χρόνο για την παραγωγή και την επεξεργασία τους.

Ο συνολικός χρόνος ο οποίος απαιτείται για τον έλεγχο ενός δείγματος αλγορίθμου, ισούται με το άθροισμα του απαιτούμενου χρόνου για την παραγωγή του δείγματος, συν τον χρόνο που απαιτείται για τους στατιστικούς ελέγχους τυχαιότητας και κρυπταναλυτικής αντοχής του. Στην πράξη, μετρήσαμε ότι για ένα δείγμα αλγορίθμου μεγέθους 1Mbit ο συνολικός αυτός χρόνος είναι περίπου 2 ώρες, χρησιμοποιώντας τους στατιστικούς ελέγχους τυχαιότητας του λογισμικού Crypt-X (βλέπε παρ. 3.3), το οποίο «έτρεχε» σε Η/Υ τύπου PC του εμπορίου (ταχύτητας 3,6 GHz, με μνήμη RAM 4 GB). Με βάση αυτό το δεδομένο, δημιουργήσαμε το δεύτερο μέρος του συγκριτικού Πίνακα 8, όπου φαίνεται ο συνολικά απαιτούμενος χρόνος για την εξέταση των n δειγμάτων, εάν ο έλεγχος καταμεριστεί σε 1, 2, 3, 4, 5 και 6 αντίστοιχα Η/Υ.

ΣΦΑΛΜΑ ΔΕΙΓΜΑΤΟ-ΛΗΨΙΑΣ (*e*)	**ΑΡΙΘΜΟΣ ΔΕΙΓΜΑΤΩΝ (*n*)**	**ΑΠΑΙΤΟΥΜΕΝΕΣ ΗΜΕΡΕΣ (8 ώρες/ημέρα)**					
		1 PC	**2 PC**	**3 PC**	**4 PC**	**5 PC**	**6 PC**
10 %	96	24	12	8	6	5	4
9 %	119	30	15	10	8	6	5
8 %	150	38	19	13	10	8	6
7 %	196	49	25	17	12	10	8
6 %	267	67	34	23	17	13	11
5 %	384	96	48	32	24	19	16
4 %	600	150	75	50	38	30	25
3 %	1067	267	134	89	67	53	45
2 %	2401	600	300	200	150	120	100
1 %	9604	2401	1200	800	600	480	400

Πίνακας 8. Απαιτούμενος χρόνος των κρυπτογραφικών ελέγχων με βάση το περιθώριο σφάλματος της δειγματοληψίας

Από τον Πίνακα 8 φαίνεται, αφ'ενός το πόσο χρονοβόρα είναι η αξιολόγηση ενός κρυπτογραφικού αλγορίθμου αλλά και αφ'ετέρου το πόσο δραστικά μπορεί να μειωθεί ο χρόνος της αξιολόγησης εάν έχουμε την δυνατότητα να χρησιμοποιήσουμε πολλούς ηλεκτρονικούς υπολογιστές ταυτόχρονα. Διότι στην περίπτωση αυτή, θα μοιράζουμε τα δείγματα στους υπολογιστές και οι έλεγχοι τους θα εκτελούνται παράλληλα, μειώνοντας έτσι τον συνολικό χρόνο.

Στην πράξη, για να κάνουμε μία αναλυτικότερη και ασφαλέστερη αξιολόγηση, θα πρέπει το σφάλμα δειγματοληψίας να είναι μικρότερο του 3%. Στην περίπτωση σφάλματος 3%, από τον Πίνακα 8 φαίνεται ότι για να ολοκληρωθεί η αξιολόγηση σε ένα πρακτικά εκμεταλλεύσιμο χρόνο 45 ημερών (1.5 μήνας), θα πρέπει να διαθέτουμε έξη υπολογιστές. Αν επιθυμούμε μικρότερο σφάλμα δειγματοληψίας ή λιγότερες ημέρες για την αξιολόγηση, τότε είναι προφανές ότι πρέπει να διαθέσουμε περισσότερους υπολογιστές.

Είναι προφανές λοιπόν ότι με τη χρήση περισσότερων και ισχυρότερων υπολογιστών, μας δίνεται η δυνατότητα να χρησιμοποιήσουμε πολύ μεγαλύτερο αριθμό και μέγεθος δειγμάτων ελέγχου, και έτσι να ελαχιστοποιήσουμε και το περιθώριο του σφάλματος δειγματοληψίας. Και το τελικό συμπέρασμα, είναι ότι όσο πιο διεξοδικός και επομένως πιο ασφαλής επιθυμούμε να είναι ο έλεγχος των κρυπτογραφικών αλγορίθμων, τόσο μεγαλύτερη πρέπει να είναι η διατιθέμενη υπολογιστική ισχύς.

3.11. Μείωση του χρόνου των ελέγχων

Υπάρχουν πολλές μέθοδοι για την μείωση του εξαιρετικά μεγάλου χρόνου των κρυπτογραφικών ελέγχων οι οποίοι αναφέρθηκαν στην προηγούμενη παράγραφο. Οι πιο σημαντικές είναι οι εξής:

α. Αυτοματισμός και παραλληλισμός διαδικασιών : Μία πολύ σημαντική μείωση του χρόνου των ελέγχων μπορεί να επιτευχθεί εάν με τη χρήση κατάλληλου λογισμικού αυτοματοποιηθούν οι κυριότερες χρονοβόρες διαδικασίες, όπως είναι η παραγωγή των δειγμάτων, η εκτέλεση των στατιστικών ελέγχων, καθώς και η ταξινόμηση των αποτελεσμάτων. Επί πλέον πολύ σημαντική μείωση του χρόνου μπορεί να επιτευχθεί, εάν γίνει καταμερισμός σε πολλούς υπολογιστές. Οι υπολογιστές αυτοί θα είναι παράλληλα συνδεδεμένοι, μέσω ενός τοπικού δικτύου LAN (Local Area Network) και θα ελέγχονται μέσω ενός προγράμματος παράλληλης επεξεργασίας, ώστε να αυτοματοποιούνται οι διαδικασίες των ελέγχων και έτσι να γίνει περαιτέρω μείωση του χρόνου.

Αρχικά θα γίνεται ένας ισομερής καταμερισμός των n διαφορετικών δειγμάτων στους υπολογιστές, και κατόπιν κάθε ένας τους θα λειτουργεί παράλληλα με τους υπόλοιπους, ώστε να παράγει τα δείγματα που του αντιστοιχούν και για να εφαρμόσει σε αυτά τους στατιστικούς ελέγχους. Έτσι, εάν έχουμε K παράλληλα συνδεδεμένους υπολογιστές, ο συνολικός χρόνος T_P για την παραγωγή και τον έλεγχο των δειγμάτων θα είναι:

$T_P = T_1 / K$ (όπου είναι T_1 είναι ο απαιτούμενος χρόνος με ένα υπολογιστή).

Αυτό σημαίνει ότι ο χρόνος που αντιστοιχεί στη χρήση ενός μόνο υπολογιστή στον Πίνακα 8 της παραγράφου 3.10, μπορεί να μειωθεί στο ένα δέκατο με την χρήση δέκα «παράλληλων» υπολογιστών.

β. Χρήση της Μονάδας Επεξεργασίας Γραφικών (GPU) : Στους σύγχρονους υπολογιστές η Μονάδα Επεξεργασίας Γραφικών GPU (Graphics Processing Unit) έχει μεγάλες δυνατότητες παράλληλης επεξεργασίας (η οποία είναι απαραίτητη για την διαχείριση των pixel της οθόνης). Έτσι, πολλοί κατασκευαστές GPU δίνουν στους χρήστες την δυνατότητα μέσω ειδικού λογισμικού να προγραμματίσουν την GPU και για δικές τους ειδικές εφαρμογές. Μία τέτοια ειδική εφαρμογή της GPU μπορεί να είναι και ο προγραμματισμός της για την επιτάχυνση των κρυπτογραφικών ελέγχων, στα πλαίσια των όσων αναφέρθηκαν στην προηγούμενη παράγραφο.

γ. Χρήση προγραμματιζόμενου υλικού (FPGA ή ASIC) : Η υλοποίηση του κρυπταλγορίθμου είναι πιο εύκολη όταν γίνει με τη χρήση μίας ανώτερης γλώσσας προγραμματισμού (high level language). Όμως, όπως αναφέρθηκε και στην παράγραφο 1.5.3 για την κρυπτανάλυση, μπορεί να επιταχυνθεί δραματικά ο χρόνος εκτέλεσης της κρυπτογράφησης, εάν η υλοποίηση του κρυπταλγορίθμου γίνει σε ένα ειδικά προγραμματιζόμενο υλικό FPGA (Field Programmable Gate Array) ή ASIC (Application Specific Integrated Circuit). Το ίδιο ακριβώς ισχύει και όταν η υλοποίηση των στατιστικών ελέγχων γίνει σε ένα FPGA ή ASIC.

δ. Υπεροδήγηση του υπολογιστή (Overclocking) : Η τεχνική της «υπεροδήγησης» (overclocking), αφορά την αύξηση της ονομαστικής συχνότητας του ρολογιού του υπολογιστή η οποία έχει καθοριστεί από τον κατασκευαστή, ώστε αυτός να λειτουργήσει πιο γρήγορα από τις προδιαγραφές του. Ωστόσο, αυτή η τεχνική είναι αμφιλεγόμενη και δεν την προτείνουμε, διότι μπορεί να προκαλέσει υπερβολική θέρμανση, αστάθεια, αλλά και πλήρη καταστροφή της CPU.

ΚΕΦΑΛΑΙΟ 4

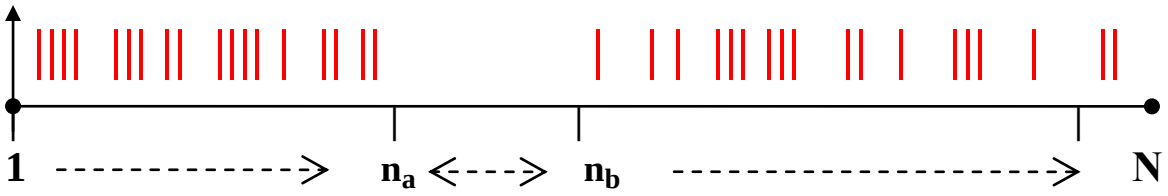
ΔΕΙΓΜΑΤΟΛΗΨΙΑ ΚΛΕΙΔΩΝ

4.1. Μεθοδολογία επιλογής των κλειδών

Για τη διεξαγωγή των ελέγχων του προηγούμενου κεφαλαίου, ένα σημαντικό πρόβλημα είναι ο τρόπος επιλογής των κλειδών, ώστε να έχουμε μία σωστή δειγματοληψία, η οποία να ανταποκρίνεται στην πραγματική εικόνα του αλγορίθμου. Το βασικό ερώτημα είναι εάν η επιλογή των κλειδών πρέπει να είναι τυχαία ή πρέπει να ακολουθεί κάποιους κανόνες. Εάν η επιλογή είναι τελείως τυχαία, τότε ενδεχομένως να μην ανιχνεύσουμε κάποιες «αδύναμες» ή «ισοδύναμες» κλείδες, οι οποίες δίνουν παρόμοια αποτελέσματα και επομένως μειώνουν το συνολικό πλήθος των ενεργών κλειδών. Εάν όμως επιλέξουμε τις κλείδες με κάποια συγκεκριμένα κριτήρια, τότε υπάρχει πολύ μεγαλύτερη πιθανότητα να ανιχνεύσουμε τις τυχόν αδύναμες ή ισοδύναμες κλείδες. Σε αυτό το κεφάλαιο προτείνουμε την βέλτιστη μεθοδολογία επιλογής των κλειδών, η οποία συνδυάζει την τυχαία και την «εξαναγκασμένη» επιλογή.

4.2. Τυχαία επιλογή κλειδών

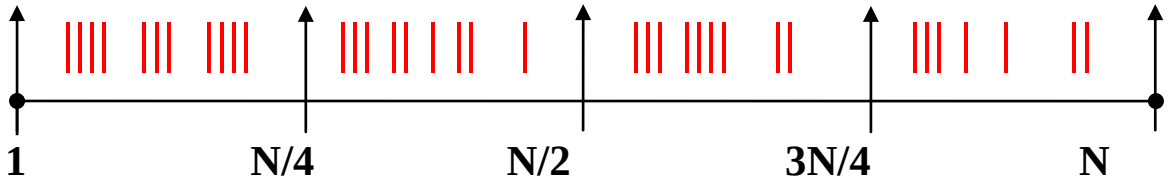
Όταν η επιλογή των **n** δειγματοληπτικών κλειδών είναι τελείως τυχαία, υπάρχει ενδεχόμενο να μη εξεταστούν κάποια μεγάλα διαστήματα τιμών της κλείδας, μέσα στο συνολικό διάστημα από 1 έως N (όπου $N = 2^L$, ο συνολικός αριθμός κλειδών και L = μήκος κλειδιού). Στο Σχήμα 4, φαίνεται μία τέτοια περίπτωση, όπου οι **n** εξετασθείσες τιμές της κλείδας (με κόκκινο) αφήνουν μία μεγάλη περιοχή τιμών (από $\mathbf{n_a}$ έως $\mathbf{n_b}$) οι οποίες δεν εξετάστηκαν.



Σχήμα 4. Τυχαία επιλογή των κλειδών **n**

4.3. Μικτή επιλογή κλειδών

Για να αποφύγουμε την προηγούμενη περίπτωση, διεξάγουμε μία μικτή μεικτή επιλογή των κλειδών (τυχαία και καθορισμένη). Δηλαδή, διαιρούμε το διάστημα των τιμών της κλείδας σε ίσες περιοχές και εντός κάθε μίας από αυτές διεξάγουμε την τυχαία δειγματοληψία. Η μέθοδος αυτή στη θεωρία της δειγματοληψίας καλείται στρωματοποίηση (stratified sampling). Στο Σχήμα 5, φαίνεται ένα τέτοιο παράδειγμα, όπου οι **n** εξετασθείσες τιμές της κλείδας (με κόκκινο) έχουν στρωματοποιηθεί (μοιραστεί) σε τέσσερεις περιοχές τιμών (1 έως N/4, N/4 έως N/2, N/2 έως 3N/4 και 3N/4 έως N).

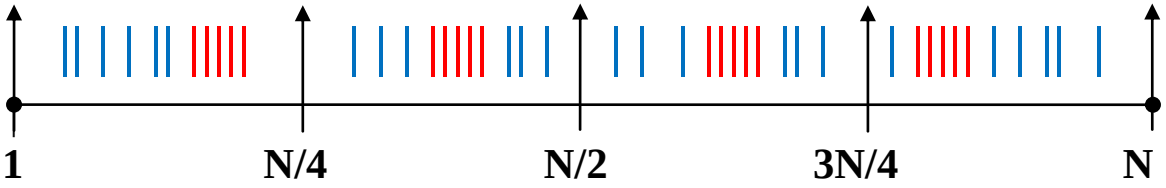


Σχήμα 5. Μικτή επιλογή κλειδών (τυχαία, εντός τεσσάρων ίσων περιοχών)

4.3.1. Επιλογή συνεχόμενων κλειδών

Στα πλαίσια της μικτής επιλογής κλειδών, είναι επιθυμητό να εξετάσουμε τη συμπεριφορά της εξόδου του αλγορίθμου και σε ορισμένες ειδικές περιπτώσεις. Μια τέτοια ειδική περίπτωση, είναι όταν εισάγουμε στον αλγόριθμο κλείδες με συνεχόμενες τιμές. Και τούτο διότι ένα κρυπτογραφικός αλγόριθμος πρέπει να είναι πολύ «ευαίσθητος» στις αλλαγές της κλείδας. Δηλαδή, για μικρές αλλαγές στην τιμή της κλείδας, πρέπει όχι μόνο να εξακολουθεί να διατηρεί την τυχαιότητα της εξόδου του, αλλά και να μην υπάρχουν ομοιότητες μεταξύ των διαφορετικών εξόδων του.

Στο Σχήμα 6, φαίνεται μία μικτή επιλογή κλειδών, όπου σε κάθε μία από τις τέσσερεις ίσες περιοχές τιμών, εκτός από τις τυχαίες κλείδες (μπλε) επιλέγουμε και μία ομάδα κλειδών οι οποίες έχουν συνεχόμενες τιμές (κόκκινες). Στην περίπτωση αυτή (όπως αναφέραμε στην παράγραφο 8), πρέπει πάντα να εξετάζουμε τις αλγοριθμικές εξόδους που προκύπτουν από τις συνεχόμενες κλείδες για τυχόν ομοιότητες μεταξύ τους (ισοδύναμες κλείδες).



Σχήμα 6. Μικτή επιλογή κλειδών **n** **(n = n1 + n2)**
(όπου **n1** οι τυχαίες κλείδες και **n2** οι συνεχείς κλείδες)

Στο Σχήμα 7 φαίνεται ένα παράδειγμα επιλογής τεσσάρων συνεχόμενων κλειδών, όπου από μία αρχική κλείδα με τιμή K_1 (η οποία μπορεί να είναι τυχαία ή συγκεκριμένη), κατασκευάζουμε άλλες τρεις κλείδες με τιμές $K_2 = K_1+1$, $K_3 = K_2+1$, και $K_4 = K_3 +1$ (με κίτρινο χρώμα).

	MSB ……..……..…… LSB							
K_1	……	0	1	1	0	1	0	0	1
K_2	……	0	1	1	0	1	0	1	0
K_3	……	0	1	1	0	1	0	1	1
K_4	……	0	1	1	0	1	1	0	0

Σχήμα 7. Επιλογή τεσσάρων συνεχόμενων κλειδών K_1, K_2, K_3, K_4

4.3.2. Επιλογή κλειδών με διαφορά ενός bit

Μία ακόμα σημαντική ειδική περίπτωση, είναι η επιλογή κλειδών οι οποίες έχουν διαφορά ενός μόνο bit μεταξύ τους. Η επιλογή αυτή μπορεί να αναδείξει κάποιες ισοδύναμες κλείδες και στηρίζεται σε τρεις ιδιότητες τις οποίες πρέπει να πληρούν οι κρυπτογραφικοί αλγόριθμοι:

α. Πληρότητα (Completeness property):

Κάθε bit του κρυπτογραφημένου κειμένου πρέπει να εξαρτάται από όλα τα bits της κλείδας. Αυτή η ιδιότητα διατυπώθηκε πρώτα από τον Claude Shanon το 1949, ως ιδιότητα της σύγχυσης (confusion property).

β. Ιδιότητα χιονοστιβάδας (Avalanche effect):

Η αλλαγή ενός bit της εισόδου πρέπει να επηρεάσει όσο το δυνατόν περισσότερα bits της εξόδου. Ο C.Shanon ονόμασε αυτή την ιδιότητα ως διάχυση (diffusion property), υπό την έννοια ότι οι στατιστικές ιδιομορφίες του ανοικτού κειμένου θα πρέπει «πολλαπλασιάζονται» μέσα στο κρυπτογραφημένο κείμενο.

γ. Αυστηρό κριτήριο χιονοστιβάδας (Strict Avalanche Criterion-SAC):

Όταν αλλάζει ένα bit του ανοικτού κειμένου, κάθε bit του κρυπτογραφημένου κειμένου πρέπει να αλλάζει με πιθανότητα 1/2 (δηλαδή τα μισά από τα bits του πρέπει να αλλάζουν).

Σημειώνουμε ότι η ιδιότητα (α) ισχύει όταν ως είσοδο του κρυπταλγορίθμου θεωρούμε την κλείδα, ενώ στις (β) και (γ) ως είσοδος του θεωρείται το ανοικτό κείμενο. Όμως οι ιδιότητες (β) και (γ) πρέπει να ισχύουν και όταν ως είσοδο θεωρήσουμε την κλείδα, διότι η κλείδα οφείλει να επηρεάζει εξίσου (αν όχι περισσότερο) την έξοδο του κρυπταλγορίθμου (και κατ'επέκταση το κρυπτογραφημένο κείμενο).

Στο Σχήμα 8 φαίνεται ένα παράδειγμα επιλογής τεσσάρων κλειδών, όπου από μία αρχική κλείδα K_1 (η οποία μπορεί να είναι τυχαία ή συγκεκριμένη), κατασκευάζουμε άλλες τρεις κλείδες K_2, K_3, K_4 , αλλάζοντάς κάθε φορά το πρώτο, δεύτερο και τρίτο bit της αρχική κλείδας (με κίτρινο χρώμα).

	MSB …….							LSB
K_1	……	0	1	1	0	0	1	0	1
K_2	……	0	1	1	0	0	1	0	0
K_3	……	0	1	1	0	0	1	1	1
K_4	……	0	1	1	0	0	0	0	1

Σχήμα 8. Επιλογή τεσσάρων κλειδών K_1, K_2, K_3, K_4 με διαφορά ενός bit

ΚΕΦΑΛΑΙΟ 5

ΜΗΚΟΣ ΤΗΣ ΚΛΕΙΔΑΣ

5.1. Γενικά

Η ασφάλεια ενός συμμετρικού κρυπτογραφικού αλγόριθμου βασίζεται στην εσωτερική του πολυπλοκότητα και το μήκος της κρυπτογραφικής του κλείδας. Όταν όμως ο αλγόριθμος δεν έχει κάποιο γνωστό και εκμεταλλεύσιμο ελάττωμα στην εσωτερική δομή του, τότε η μόνη κρυπταναλυτική επίθεση που μπορεί να εφαρμοστεί σε αυτόν είναι η μέθοδος της Εξαντλητικής Έρευνας της Κλείδας (Exhaustive Key Search) ή όπως αλλιώς ονομάζεται Επίθεση Βάναυσης Δύναμης (Brute Force Attack). Αυτή η διαδικασία επίθεσης είναι εξαιρετικά χρονοβόρα και εάν η κρυπτογραφική κλείδα έχει επαρκές μήκος, τότε η Εξαντλητική Έρευνα Κλείδας είναι πρακτικά ανεφάρμοστη και συνεπώς λέμε ότι ο αλγόριθμος είναι πρακτικά ασφαλής.

Το 1996, μια μελέτη από μια ομάδα κρυπτογράφων υπολόγισε ότι το ελάχιστο μήκος κλείδας πρέπει να είναι 75 bits για να είναι ασφαλείς οι κρυπτογραφικοί αλγόριθμοι από την Εξαντλητική Έρευνα της Κλείδας για εκείνη την περίοδο (1996), ενώ πρέπει να είναι 90 bits για να είναι ασφαλείς τα επόμενα 20 χρόνια (βιβλιογραφία **[17]**). Από τότε, εκδόθηκαν πολλοί νέοι κρυπταλγόριθμοι με μεγαλύτερη πολυπλοκότητα και μεγαλύτερο μήκος κλείδας, αλλά και οι τεχνολογίες της υλοποίησής τους εξελίχθηκαν σε ταχύτητα και απόδοση. Επομένως, λόγω των νέων τεχνολογικών εξελίξεων, σήμερα υπάρχει ανάγκη για μια νέα αξιολόγηση του ελάχιστου μήκους κλείδας, ώστε οι κρυπταλγόριθμοι να είναι ασφαλείς ενάντια στην Εξαντλητική Έρευνα της Κλείδας (την οποία θα ονομάζουμε Brute Force Attack ή συντομογραφικά BFA στις επόμενες παραγράφους).

5.2. Εισαγωγή

Σε αυτή τη μελέτη, εξετάζουμε τις διάφορες παραμέτρους οι οποίες επηρεάζουν το χρόνο για την Εξαντλητική Έρευνα της Κλείδας (Brute Force Attack) και βασιζόμενοι σε αυτές, υπολογίζουμε το ελάχιστο μήκος κλείδας ενός συμμετρικού κρυπτογραφικού αλγόριθμου για να είναι ασφαλής ενάντια στις κρυπταναλυτικές επιθέσεις οι οποίες χρησιμοποιούν υπολογιστές σύγχρονης τεχνολογίας (σε λογισμικό και υλικό). Στη συνέχεια, υπολογίζουμε το ελάχιστο μήκος κλείδας για τα μελλοντικά έτη, σύμφωνα με την προσδοκώμενη τεχνολογική εξέλιξη.

Στην αρχή της μελέτης, παρέχουμε τις θεωρητικές εξισώσεις και στη συνέχεια διενεργούμε τον πρακτικό υπολογισμό του χρόνου Brute Force Attack (BFA) για διάφορες κρυπτογραφικές κλείδες σύγχρονων αλγόριθμων. Και για να είμαστε όσο το δυνατό περισσότερο πρακτικοί, στους υπολογισμούς χρησιμοποιούμε τους χρόνους εκτέλεσης των υπαρχόντων και δημοσιευμένων υλοποιήσεων αλγόριθμων σε λογισμικό και υλικό.

Καθόλη τη διάρκεια της μελέτης, δεν υπολογίζουμε το κόστος των διαφόρων υλοποιήσεων της Brute Force Attack, αλλά θεωρούμε ότι ο αντίπαλος έχει το κίνητρο να κάνει τις απαραίτητες επενδύσεις στην σύγχρονη τεχνολογία της Πληροφορικής, ώστε να αναλύσει την κρυπτογραφημένη

πληροφορία. Φυσικά, μερικές μεγάλες επενδύσεις (ειδικά αυτές που χρειάζονται μαζικό παραλληλισμό συγκεκριμένου υλικού) δεν δύνανται να πραγματοποιηθούν από έναν μεμονωμένο hacker, αλλά έχουν ένα οικονομικό κόστος που μπορεί να αναληφθεί μόνο από μια μεγάλη εταιρεία ή μια Υπηρεσία Πληροφοριών. Μερικά χαρακτηριστικά παραδείγματα όσον αφορά το υπολογισμένο κόστος των διαφορετικών μεθόδων Brute Force Attack καθώς επίσης και του υπολογισμού της αξίας των κρυπτογραφημένων πληροφοριών (βάσει του είδους και του κινήτρου του αντιπάλου) δίνονται στο **[2].**

5.3. Απλή Έρευνα

Η πιο απλή περίπτωση Brute Force Attack (BFA) είναι η Απλή Έρευνα, κατά την οποία χρησιμοποιούμε μόνο μία υλοποίηση του αλγόριθμου τη φορά (σε λογισμικό ή υλικό). Σε αυτήν την περίπτωση, ο απαραίτητος χρόνος TBFA για μια Brute Force Attack είναι:

$$T_{BFA} = T_{MDL} \cdot N = T_{MDL} \cdot 2^{L} \qquad (1)$$

όπου T_{BFA} είναι ο χρόνος Brute Force Attack, T_{MDL} είναι ο χρόνος που απαιτείται από την εφαρμογή για να εκτελεστεί ένας Βρόγχος Κύριας Αποκρυπτογράφησης (Main Decryption Loop) του αλγόριθμου, N είναι το σύνολο των κλειδών και L είναι το μήκος της κλείδας (σε bits).

Σημείωση: Στην πράξη, όταν χρησιμοποιούμε την Brute Force Attack είναι πιθανό να βρούμε την κλείδα πριν εξαντλήσουμε το συνολικό εύρος κλείδας. Αλλά σε αυτή τη μελέτη, υπολογίζουμε την χειρότερη περίπτωση, κατά την οποία πρέπει να εξετάσουμε όλους τους συνδυασμούς της κλείδας μέχρι να αποκωδικοποιήσουμε το μήνυμα.

5.3.1. Υλοποίηση σε λογισμικό

Όταν η υλοποίηση του αλγόριθμου πραγματοποιείται σε λογισμικό, ο απαραίτητος χρόνος για έναν υπολογιστή γενικής χρήσης να εκτελέσει ένα Βρόγχος Κύριας Αποκρυπτογράφησης (MDL) του αλγόριθμου είναι:

$$T_{MDL} = C_{MDL} \cdot T_C = \frac{C_{MDL}}{F_{MAX}} \qquad (2)$$

όπου C_{MDL} είναι οι απαραίτητοι CPU κύκλοι για ένα MDL, T_C είναι η διάρκεια για κάθε κύκλο CPU (T=1/F) και F_{MAX} είναι η τωρινή μέγιστη ταχύτητα του χρόνου των υπολογιστών γενικών καθηκόντων. Λόγω της εξίσωσης (2), η εξίσωση (1) γίνεται:

$$T_{BFA} = \frac{C_{MDL} \cdot 2^{L}}{F_{MAX}} \qquad (3)$$

Τα σύγχρονα εργαλεία και μέθοδοι της εξέλιξης του λογισμικού οδήγησαν σε σημαντική μείωση του χρόνου εκτέλεσης των κρυπτογραφικών αλγόριθμων. Σύμφωνα με το **[18]**, η γρηγορότερη εφαρμογή λογισμικού του αλγόριθμου AES-128 μέχρι το έτος 2008, ήταν 193 κύκλοι CPU για την αποκρυπτογράφηση μιας ομάδας δεδομένων.

Όσο αφορά την ταχύτητα του υπολογιστή, στις μέρες μας η μέγιστη συχνότητα της CPU των εμπορικών υπολογιστών είναι 3 GHZ (Σεπτέμβριος 2012). Επομένως, εάν βάλουμε C_{MDL} = 193 cycles/block και $F_{MAX} = 3 \cdot 10^9$ Hz στην εξίσωση (3), μπορούμε να υπολογίσουμε τον χρόνο Brute Force Attack (T_{BFA}) όταν ο αλγόριθμος εφαρμόζεται σε λογισμικό για διαφορετικές τιμές της κλείδας L. Με αυτές τις τιμές της T_{BFA} δημιουργήσαμε την πρώτη στήλη του Πίνακα 9 (Απλή Έρευνα/Λογισμικό).

Σημείωση 1: Για την απλούστευση των υπολογισμών, υποθέτουμε ότι οι απαραίτητοι CPU κύκλοι είναι οι ίδιοι για τα διαφορετικά μήκη κλειδών. Στην πράξη, όταν η κλείδα αυξάνεται, ο χρόνος που χρειάζεται ο αλγόριθμος για να "τρέξει" επίσης αυξάνεται. Ωστόσο, αυτές οι διαφορές στο χρόνο, είναι σχετικά μικρές και δεν επηρεάζουν τα γενικά συμπεράσματα αυτής της μελέτης.

Σημείωση 2: Για ενδεικτικούς λόγους, οι υπολογισμοί του Πίνακα 1 γίνονται για block ciphers, οι οποίοι είναι περισσότερο γνωστοί. Αλλά οι υπολογισθείσες τιμές είναι ανάλογες με τις αντίστοιχες τιμές των stream ciphers για το ίδιο μήκος κλείδας.

5.3.2. Υλοποίηση σε υλικό

Οι κρυπτογραφικοί αλγόριθμοι μπορούν να εφαρμοστούν είτε σε FPGA (Field Programmable Gate Arrays) είτε σε ASIC (Application Specific Integrated Circuits). Μια σύντομη περιγραφή της τεχνολογίας των ανωτέρω ολοκληρωμένων κυκλωμάτων, καθώς και σύγκριση μεταξύ των, δίνεται στο **[19]**. Για να συνοψίσουμε τη σύγκριση, μπορούμε να πούμε ότι τα FPGA είναι επαναπρογραμματιζόμενα και φθηνότερα, ενώ τα ASIC δεν μπορούν να επαναπρογραμματιστούν και είναι περισσότερο δαπανηρά. Από την άλλη μεριά, τα ASIC είναι πολύ πιο γρήγορα από τα FPGA.

Όταν υλοποιούμε αλγόριθμους σε υλικό, ο χρόνος T_{MDL} που χρειάζεται ο υπολογιστής να εκτελέσει ένα Βρόγχο Κύριας Αποκρυπτογράφησης (MDL) του αλγόριθμου ονομάζεται καθυστέρηση (Latency) και σύμφωνα με το **[19]**, ορίζεται από την ακόλουθη εξίσωση:

$$L_{atency} = \frac{B_{lock\_size} \cdot S_{imultaneus\_blocks}}{T_{hroughput}} \qquad (4)$$

όπου: Block_ size = μέγεθος του block εισόδου του αλγορίθμου σε bits
Simultaneous_ blocks = αριθμός των blocks τα οποία επεξεργάζονται ταυτόχρονα , Throughput = αριθμός των bits τα οποία κρυπτογραφούνται ή αποκρυπτογραφούνται / second.

Εάν θεωρήσουμε ότι επεξεργαζόμαστε μόνο ένα block κάθε φορά (Simultaneous_ blocks=1), η (1) λόγω της (4) θα γίνει :

$$T_{BFA} = L_{atency} \cdot 2^L = \frac{B_{lock\_size} \cdot 2^L}{T_{hroughput}} \qquad (5)$$

Σήμερα έχουν επιτευχθεί πολύ γρήγορες υλοποιήσεις αλγορίθμων σε FPGA και ASIC, όπου ο αριθμός των bits τα οποία κρυπτογραφούνται/ αποκρυπτογραφούνται στη μονάδα του χρόνου είναι πάρα πολύ υψηλός. Ένα τέτοιο παράδειγμα είναι η υλοποίηση του αλγορίθμου AES-128 σε ASIC η οποία αναφέρεται στο **[20]**, επιτυγχάνοντας ένα Throughput της τάξης των 40 Gbps. Εάν λοιπόν στη σχέση (5) βάλουμε ως ενδεικτικές τιμές : Block_ size = 128 bits και Throughput = $40 \cdot 10^9$ bits/sec , μπορούμε να υπολογίσουμε τον απαιτούμενο χρόνο των εξαντλητικών δοκιμών T_{BFA} όταν ο αλγόριθμος υλοποιείται σε υλικό, για διάφορα μεγέθη L της κρυπτογραφικής κλείδας L. Με αυτές τις τιμές, δημιουργήθηκε η δεύτερη στήλη του Πίνακα 9 (Απλή Έρευνα/Hardware).

Σημείωση: Στην πράξη, το μέγεθος του block δεν είναι ίδιο για όλους τους block ciphers. Για παράδειγμα, οι αλγόριθμοι 3DES και IDEA έχουν μέγεθος block 64 bits, αλλά οι πιο σύγχρονοι block ciphers όπως οι τρεις τελικοί υποψήφιοι για τον AES, Rijndael, Serpent και Twofish έχουν μέγεθος block 128 bits. Για λόγους απλοποίησης, χρησιμοποιούμε το μέγεθος block των 128 bits για όλους τους διαφορετικούς υπολογισμούς κλειδών στις σειρές του Πίνακα 1. Αυτή η απλοποίηση δεν επιφέρει σημαντική διαφορά στις τιμές των πινάκων, ούτε μεταβάλλει τα γενικά συμπεράσματα αυτής της μελέτης.

5.4. Παράλληλη Έρευνα

Ο χρόνος Brute Force Attack μπορεί να μειωθεί σημαντικά εάν χρησιμοποιήσουμε παραλληλοποίηση (parallelization). Αυτό σημαίνει ότι χρησιμοποιούμε ταυτόχρονα πολλά συστήματα τα οποία υλοποιούν τον αλγόριθμο και διανέμουμε τον συνολικό αριθμό των κλειδών με το να δίνουμε στην κάθε υλοποίηση διαφορετικές τιμές κλειδών. Με αυτό τον τρόπο, ο συνολικός χρόνος αναζήτησης διαιρείται με το n, που είναι ο αριθμός των παράλληλων υλοποιήσεων που χρησιμοποιούμε. Σήμερα, είναι εφικτό να χρησιμοποιούμε ένα εκατομμύριο υπολογιστές γενικής χρήσης, ή FPGA, ή ASIC, για να διεξάγουμε μια παραλληλισμένη Brute Force Attack.

5.4.1. Υλοποίηση σε λογισμικό

Εάν κάνουμε παράλληλη BFA έρευνα (parallel search), χρησιμοποιώντας ταυτόχρονα n υπολογιστές του εμπορίου οι οποίοι θα μοιράζονται το πλήθος των κλειδών, τότε η (3) θα γίνει :

$$T_{BFA} = \frac{C_{MDL} \cdot 2^L}{n \cdot F_{MAX}} \qquad (6)$$

Εάν στη σχέση (6) βάλουμε τις ακόλουθες τιμές :

C_{MDL}= 193 cycles/block , $F_{MAX} = 3 \cdot 10^9$ Hz , n = 1.000.000

μπορούμε να υπολογίσουμε τον απαιτούμενο χρόνο των εξαντλητικών δοκιμών T_{BFA} για διάφορα μεγέθη L της κρυπτογραφικής κλείδας, όταν χρησιμοποιούμε

παράλληλα 1.000.000 υπολογιστές οι οποίοι υλοποιούν τον αλγόριθμο σε λογισμικό. Με αυτές τις τιμές, δημιουργήθηκε η τρίτη στήλη του Πίνακα 9 (Παράλληλη έρευνα /Software).

5.4.2. Υλοποίηση σε υλικό

Εάν κάνουμε παράλληλη BFA έρευνα (parallel search), με την ταυτόχρονη χρήση n ολοκληρωμένων κυκλωμάτων FPGA ή ASIC , τα οποία θα μοιράζονται το πλήθος των κλειδών, τότε η (5) θα γίνει :

$$T_{BFA} = \frac{B_{lock\ \_\ size} \cdot 2^{L}}{n \cdot T_{hroughput}} \qquad (7)$$

Εάν στη σχέση (7) βάλουμε τις τιμές : Block_ size = 128 bits
και Throughput = $40 \bullet 10^9$ bits/sec , n = 10^6 , υπολογίζουμε το χρόνο εξαντλητικών δοκιμών T_{BFA} για διάφορα μεγέθη L της κλείδας, όταν χρησιμοποιούμε παράλληλα 1.000.000 ολοκληρωμένα κυκλώματα FPGA ή ASIC τα οποία υλοποιούν τον αλγόριθμο. Με αυτές τις τιμές, δημιουργήθηκε η τέταρτη στήλη του Πίνακα 9 (Παράλληλη έρευνα /Hardware).

Κλείδα (bits)	Ελάχιστος χρόνος BFA σε χρόνια (y)			
	Απλή έρευνα		Παράλληλη έρευνα (10^6)	
	Software	Hardware	Software	Hardware
75	77068788 y	3833475.3 y	77.068 y	3.833 y
90	$2.525 \cdot 10^{12}$ y	$1.256 \cdot 10^{11}$ y	$2.525 \cdot 10^{6}$ y	$1.256 \cdot 10^{5}$ y
128	$6.941 \cdot 10^{23}$ y	$3.452 \cdot 10^{22}$ y	$6.941 \cdot 10^{17}$ y	$3.452 \cdot 10^{16}$ y
192	$1.280 \cdot 10^{43}$ y	$6.369 \cdot 10^{41}$ y	$1.280 \cdot 10^{37}$ y	$6.369 \cdot 10^{35}$ y
256	$2.362 \cdot 10^{62}$ y	$1.174 \cdot 10^{61}$ y	$2.362 \cdot 10^{56}$ y	$1.174 \cdot 10^{55}$ y

Πίνακας 9. Ελάχιστος χρόνος BFA χρησιμοποιώντας σημερινή τεχνολογία

5.5. Μελλοντική Εξέλιξη

Οι σχέσεις (6) και (7) εκφράζουν το TBFA με τη σημερινή μέγιστη ταχύτητα των υπολογιστών. Όμως, η ταχύτητα των Η/Υ δεν μένει σταθερή αλλά αυξάνεται με τα χρόνια, διότι βελτιώνεται η τεχνολογία κατασκευής των ολοκληρωμένων κυκλωμάτων. Ο «νόμος του Moore» ο οποίος διατυπώθηκε το 1965 **[21]**), έλεγε ότι ο αριθμός των τρανζίστορ στα ολοκληρωμένα κυκλώματα διπλασιάζεται κάθε χρόνο. Το 1975 ο Moore τον διασκεύασε λέγοντας ότι η πυκνότητα των τρανζίστορ διπλασιάζεται κάθε δύο χρόνια. Στα επόμενα χρόνια αποδείχτηκε ότι ο χρόνος διπλασιασμού ποικίλλει από 18 μήνες έως τρία χρόνια. Σύμφωνα με πολλές δημοσιεύσεις, όπως η **[22]** και η **[23]**, ο Νόμος του Moore σχετικά με τον διπλασιασμό κάθε δύο χρόνια κατά μέσο όρο, ακόμα ισχύει σήμερα και θα συνεχίσει να ισχύει για πολλές ακόμα δεκαετίες. Αυτό το γεγονός δεν προκύπτει μόνο από την αναμενόμενη αύξηση στον αριθμό των

transistors στα ολοκληρωμένα κυκλώματα, αλλά και εξαιτίας της ενσωμάτωσης νέων υλικών, διαδικασιών και δομικών στοιχείων που θα συνδυαστούν με τις μονάδες των τρανζίστορ CMOS. Και εάν ο αριθμός των τρανζίστορ στα ολοκληρωμένα κυκλώματα διπλασιάζεται κάθε δύο χρόνια, αυτό θα έχει ως αποτέλεσμα ότι στον ίδιο χρόνο η απόδοση τους να διπλασιάζεται και αυτή (και αυτό έχει αποδειχθεί και πρακτικά). Επομένως, μετά το πέρασμα d ετών, η ταχύτητα / απόδοση των υπολογιστών θα έχει διπλασιαστεί για d/2 φορές ακολουθώντας μία γεωμετρική πρόοδο η οποία θα καθορίζεται από την παρακάτω σχέση:

$$F_d = F_{2017} \cdot 2^{d/2} \qquad (8)$$

όπου F_d είναι η μέγιστη ταχύτητα ενός υπολογιστή γενικής χρήσης μετά από d χρόνια και F_{2017} είναι η μέγιστη ταχύτητα σήμερα (2017).

Για τους ίδιους λόγους, το Throughput στις μελλοντικές υλοποιήσεις σε υλικό θα είναι:

$$Throughput_{-d} = Throughput_{-2017} \cdot 2^{d/2} \qquad (9)$$

όπου $Throughput_{-d}$ είναι η μέγιστη Throughput μετά από d χρόνια και $Throughput_{-2017}$ είναι η μέγιστη Throughput σήμερα (2017).

Τελικά, εξαιτίας του Νόμου του Moore, πρέπει να αναμένουμε ότι ο αριθμός n των παράλληλων υλοποιήσεων επίσης θα αυξηθεί. Αυτό προκύπτει από το γεγονός ότι λόγω της αυξημένης πυκνότητας των τρανζίστορ, τα ολοκληρωμένα κυκλώματα, εκτός του ότι γίνονται γρηγορότερα θα γίνουν και μικρότερα σε μέγεθος και φτηνότερα σε τιμή. Επιπλέον, αναμένεται ότι στο μέλλον θα υπάρξουν σημαντικές εξελίξεις στις τεχνικές παραλληλοποίησης και στη δικτύωση των υπολογιστών. Επομένως, για να θεωρήσουμε μια μεγαλύτερη τεχνολογική εξέλιξη (και συνεπώς ένα μεγαλύτερο κίνδυνο κρυπταναλυτικής επίθεσης), μπορούμε να υποθέσουμε ότι το n επίσης θα αυξηθεί με τον ίδιο ρυθμό όπως το F_d και το $Throughput_{-d}$ και θα γίνει :

$$n_d = n_{2017} \cdot 2^{d/2} \qquad (10)$$

όπου n_d είναι ο μέγιστος αριθμός παράλληλων υλοποιήσεων μετά από d έτη και n_{2017} είναι ο μέγιστος αριθμός n σήμερα (2017).

Βάσει των εξισώσεων (8) και (10), η (6) μετατρέπεται στην (11). Και βάσει των εξισώσεων (9) και (10), η (7) μετατρέπεται στην (12):

$$T_{BFA} = \frac{C_{MDL} \cdot 2^L}{n_{2017} \cdot F_{2017} \cdot 2^d} \qquad (11)$$

$$T_{BFA} = \frac{B_{lock\_size} \cdot 2^L}{n_{2017} \cdot T_{hroughput} \cdot 2^d} \qquad (12)$$

Βάζοντας στην εξίσωση (11) τις τιμές C_{MDL}=193 cycles/block, F_{2017} =3 · 109 Hz και n_{2017} = 1000000, υπολογίσαμε το χρόνο της Brute Force Attack T_{BFA} με παράλληλη χρήση n_d υπολογιστών γενικής χρήσης, για διάφορα μήκη L της κρυπτογραφικής κλείδας, χρησιμοποιώντας διαφορετικές χρονικές

αποστάσεις από σήμερα (d = 30, 50, 70, 90 έτη) και χρησιμοποιώντας την αντίστοιχη τεχνολογία εκείνης της εποχής. Με τις ανωτέρω τιμές των T_{BFA}, δημιουργήθηκε ο Πίνακας 10 (όπου y=έτη, d=μέρες, h=ώρες, m=λεπτά, s=δευτερόλεπτα).

Παρομοίως, βάζοντας στην εξίσωση (12) τις τιμές: Block size = 128 bits , Throughput = 40 · 109 bits/sec και n_{2017} = 1000000, υπολογίσαμε το χρόνο της Brute Force Attack T_{BFA} με την παράλληλη χρήση n_d FPGA ή ASIC, για διάφορα μήκη L της κρυπτογραφικής κλείδας, χρησιμοποιώντας διαφορετικές χρονικές αποστάσεις από σήμερα (d = 30, 50, 70, 90 έτη) και χρησιμοποιώντας την αντίστοιχη τεχνολογία εκείνης της εποχής. Με τις ανωτέρω τιμές των TBFA, δημιουργήθηκε ο Πίνακας 11.

Παρατηρώντας τις εξισώσεις (11) και (12), βλέπουμε ότι εξαιτίας του Νόμου του Moore, κάθε χρόνο ο παρανομαστής τους πολλαπλασιάζεται επί 2, γεγονός που σημαίνει ότι το TBFA διαιρείται δια δύο. Για να εξισορροπήσουμε αυτή τη μείωση του TBFA , ο αριθμητής των εξισώσεων πρέπει επίσης να πολλαπλασιάζεται επί 2. Αυτό σημαίνει ότι το μήκος κλείδας L πρέπει να αυξάνεται κατά ένα bit κάθε χρόνο (12 μήνες). Αυτό το συμπέρασμα είναι λίγο πιο αυστηρό από αυτό της βιβλιογραφίας **[17]**, σύμφωνα με το οποίο το μήκος κλείδας πρέπει να αυξάνεται κατά ένα bit κάθε 18 μήνες.

Κλείδα (bits)	Ελάχιστος χρόνος BFA με n_d παράλληλους Η/Υ			
	d=30	d=50	d=70	d=90
75	2.263 s	$2.158 \cdot 10^{-6}$ s	$2.058 \cdot 10^{-12}$ s	$1.963 \cdot 10^{-18}$ s
90	20.6 h	0.07 s	$6.745 \cdot 10^{-8}$ s	$6.433 \cdot 10^{-14}$ s
128	$6.465 \cdot 10^{8}$ y	616.55 y	5.15 h	0.017 s
192	$1.192 \cdot 10^{28}$ y	$1.137 \cdot 10^{22}$ y	$1.084 \cdot 10^{16}$ y	$1.034 \cdot 10^{10}$ y
256	$2.199 \cdot 10^{47}$ y	$2.098 \cdot 10^{41}$ y	$2 \cdot 10^{35}$ y	$1.908 \cdot 10^{29}$ y

Πίνακας 10. Ελάχιστος χρόνος BFA καθώς εξελίσσεται η τεχνολογία λογισμικού

Κλείδα (bits)	Ελάχιστος χρόνος BFA με n_d παράλληλα FPGA ή ASIC			
	d=30	d=50	d=70	d=90
75	0.112 s	$1.073 \cdot 10^{-7}$ s	$1.024 \cdot 10^{-13}$ s	$9.765 \cdot 10^{-20}$ s
90	61.489 m	$3.518 \cdot 10^{-3}$ s	$3.355 \cdot 10^{-9}$ s	$3.2 \cdot 10^{-15}$ s
128	$3.215 \cdot 10^{7}$ y	30.667 y	15.372 m	$8.796 \cdot 10^{-4}$ s
192	$5.932 \cdot 10^{26}$ y	$5.657 \cdot 10^{20}$ y	$5.395 \cdot 10^{14}$ y	$5.145 \cdot 10^{8}$ y
256	$1.094 \cdot 10^{46}$ y	$1.043 \cdot 10^{40}$ y	$9.952 \cdot 10^{33}$ y	$9.491 \cdot 10^{27}$ y

Πίνακας 11. Ελάχιστος χρόνος BFA καθώς εξελίσσεται η τεχνολογία υλικού

5.6. Συμπεράσματα

Από τον Πίνακα 9 της παραγράφου 5.4.2, διαπιστώνουμε ότι ακόμα και εάν χρησιμοποιούμε 10^6 παράλληλες υλοποιήσεις σε υλικό σύγχρονης τεχνολογίας, μία κλείδα των 90 bits είναι αρκετή για την προστασία έναντι μίας Brute Force Attack σήμερα, γιατί θα χρειαστεί $1.25 \cdot 10^5$ έτη για να διασπαστεί η κλείδα. Όμως, από τους Πίνακες 10 και 11 της παραγράφου 5.5, είναι φανερό ότι εξαιτίας του Νόμου του Moore και λόγω της τεράστιας παραλληλοποίησης λογισμικού και ιδιαίτερα υλικού (massive parallelization), ο χρόνος της Brute Force Attack μπορεί στο μέλλον να μειωθεί σημαντικά. Από τον Πίνακα 3, βλέπουμε ότι εάν αρχίσουμε μια Brute Force Attack σε 50 χρόνια από τώρα, θα είναι εφικτό να σπάσουμε μια κλείδα των 128 bits σε σχεδόν 30 χρόνια. Επίσης εάν διεξάγουμε μια BFA σε 70 χρόνια από τώρα, θα είναι εφικτό να σπάσουμε μια κλείδα των 128 bits σε σχεδόν 15 λεπτά, ενώ μετά από 90 χρόνια από τώρα, θα είναι εφικτό να σπάσουμε μια κλείδα των 128 bits σε 0.87 ms. Επομένως, εάν θέλουμε να κρατήσουμε μυστικές τις κωδικοποιημένες πληροφορίες μας για 10, 20 ή 30 χρόνια, τα 128 bits θα είναι αρκετά. Αλλά εάν θέλουμε να τις κρατήσουμε μυστικές για περισσότερο από 30 χρόνια, ένα κλειδί 128 bits ίσως να μην είναι αρκετό.

Όπως είδαμε στην παράγραφο 5.5, ένας πρακτικός κανόνας για να προστατέψουμε τους κρυπτογραφικούς αλγόριθμους από την τεχνολογική εξέλιξη εξαιτίας του Νόμου του Moore, είναι να αυξάνουμε το μήκος κλείδας τους κατά ένα bit κάθε έτος. Αυτό σημαίνει ότι εάν σήμερα (2017) ένα μήκος κλείδας των 90 bits θεωρείται ασφαλές, μετά από 50 χρόνια (2067) η κλείδα πρέπει να είναι 140 bits για να είναι ασφαλής ενάντια στις Brute Force Attack εκείνης της εποχής.

Από τα παραπάνω είναι προφανές ότι παρόλο που σήμερα μερικοί σύγχρονοι κρυπτογραφικοί αλγόριθμοι προσφέρουν μήκη κλείδας των 192 και 256 bits (όπως ο AES), αυτά τα μήκη φαίνεται να πλεονάζουν και να είναι υπερβολικά μεγάλα, τουλάχιστον για τα επόμενα 50 έτη. Γιατί μέχρι τότε, η τεχνολογική εξέλιξη σε λογισμικό και υλικό υπολογιστών δεν θέτει κάποια σοβαρή απειλή όταν ο επιτιθέμενος χρησιμοποιεί την μέθοδο Brute Force Attack. Φυσικά όλα αυτά θα ανατραπούν, εάν κάποια πολύ επαναστατική τεχνολογική εξέλιξη εμφανιστεί στο άμεσο μέλλον (όπως η πρακτική εκμετάλλευση των κβαντικών υπολογιστών – quantum computers).

Όπως αναφέραμε στην αρχή αυτού του Κεφαλαίου, η Εξαντλητική Έρευνα της Κλείδας (Brute Force Attack) είναι η πιο χρονοβόρα και δαπανηρή κρυπταναλυτική επίθεση και εφαρμόζεται μόνο όταν ο αλγόριθμος δεν έχει ένα γνωστό και εκμεταλλεύσιμο μειονέκτημα στην εσωτερική δομή του. Αυτό σημαίνει ότι εκτός από την προσπάθεια για την αύξηση του μήκους της κλείδας, μεγάλη σημασία πρέπει να δοθεί και στον τομέα της εύρεσης και ανάλυσης πιθανών αδυναμιών και κερκοθυρών (back doors) μέσα στους κρυπτογραφικούς αλγόριθμους. Διότι εάν κάποιος εκμεταλλευτεί κατάλληλα αυτές τις αδυναμίες, τότε θα μπορεί να παρακάμψει ένα μεγάλο μέρος ή ακόμα και την συνολική πολυπλοκότητα της κλείδας.

ΚΕΦΑΛΑΙΟ 6

ΠΑΡΑΓΩΓΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΩΝ

Όπως αναφέρθηκε στην εισαγωγή, δύο στοιχεία καθορίζουν τη ασφάλεια των κρυπτογραφικών συστημάτων, ο αλγόριθμος και η κλείδα. Για κρυπταναλυτικούς σκοπούς, ο αλγόριθμος θεωρείται ότι είναι γνωστός, είτε επειδή είναι εξ αρχής δημοσιευμένος, είτε διότι μπορεί να έχει αποκαλυφθεί. Έτσι, το πιο κρίσιμο στοιχείο ασφάλειας γίνεται η κλείδα, διότι εάν διαρρεύσει, τότε μπορούν να αποκωδικοποιηθούν όλα τα μηνύματα τα οποία αυτή έχει κρυπτογραφήσει. Επομένως, μέγιστη προσοχή πρέπει να δίνεται στη διαχείριση των κλειδών καθ'όλη τη διάρκεια της «ζωής» τους, δηλαδή κατά την παραγωγή, διανομή, εισαγωγή, αποθήκευση, ανανέωση και καταστροφή τους.

6.1. Παραγωγή κλειδών - Γεννήτριες Τυχαίων Χαρακτήρων (RNG)

Οι κλείδες πρέπει να έχουν επαρκή πολυπλοκότητα (μεγάλο μήκος) και μικρή κρυπτοπερίοδο (να αλλάζουν συχνά). Πρέπει όμως να έχουν και καλή ποιότητα, δηλαδή μεγάλη τυχαιότητα και μη προβλεψιμότητα. Οι κλείδες παράγονται με τη χρήση των Γεννητριών Τυχαίων Χαρακτήρων (RNG), οι οποίες ονομάζονται και Γεννήτριες Τυχαίων Bits (RBG). Εάν οι RNG δεν έχουν καλή ποιότητα (δηλαδή οι χαρακτήρες τους δεν είναι επαρκώς τυχαίοι και απρόβλεπτοι), τότε οι παραγόμενες κλείδες κινδυνεύουν να αποκαλυφθούν. Δηλαδή, εάν οι RNG δεν είναι ασφαλείς, αποτελούν το πιο αδύναμο στοιχείο του κρυπτοσυστήματος. Σε αυτή την παράγραφο, εξετάζουμε τα τεχνικά χαρακτηριστικά και τις αδυναμίες ασφάλειας των RNG και προτείνουμε βελτιώσεις στις μεθόδους σχεδιασμού και τις διαδικασίες αξιολόγησής τους.

Πρέπει να σημειωθεί ότι ο χρόνος επίθεσης με εξαντλητική έρευνα των κλειδών (exhaustive key search) μπορεί να μειωθεί, εάν η RNG η οποία τις παράγει έχει μικρότερη εντροπία (**entropy**) από ότι η κλείδα. Π.χ. εάν ένα κρυπτοσύστημα χρησιμοποιεί 128 bits κλείδες οι οποίες όμως παράγονται από μία PRNG η οποία έχει **seed** μεγέθους 64 bits, τότε το κρυπτοσύστημα δεν έχει μήκος κλείδας 2^128 bits – όπως αρχικά φαίνεται – αλλά 2^64 bits.

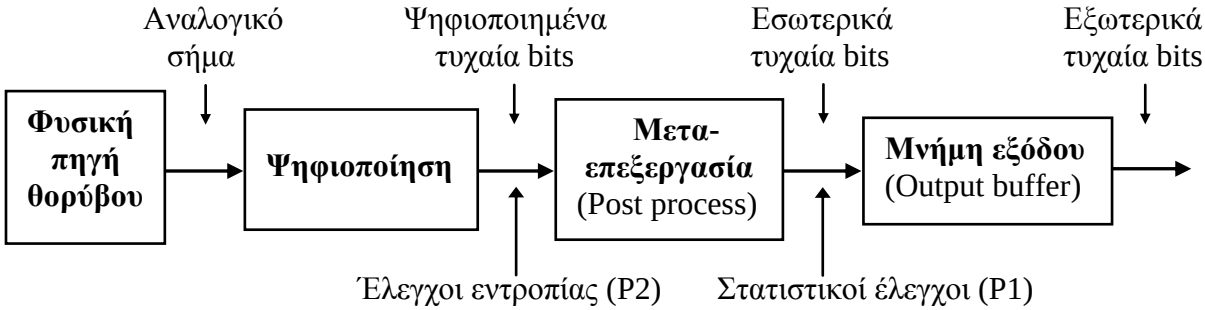
TRUE RNG (TRNG)	**PSEUDO RNG (PRNG)**
-Non Deterministic RNG	-Deterministic RNG (DRNG)
-Random output	-Pseudo random output
Input Entropy : Physical noise	Input Entropy : Chosen Seed
Implementation : Hardware	Implementation : Software
-Special devices -Hardware failures	-Depend from seed and internal state -Correlations of outputs
-Slower	-Faster
HYBRID RNG PRNG with regular re-seeding by a true random source	

Πίνακας 12. Τύποι των RNG

Υπάρχουν δύο βασικές κατηγορίες RNG, οι Πραγματικές ή Φυσικές RNG (μη Ντετερμινιστικές) και οι Γεννήτριες Ψευδο-Τυχαίων Χαρακτήρων PRNG (Ντετερμινιστικές). Οι βασικές ιδιότητες τους φαίνονται στον Πίνακα 12. Οι Υβριδικές RNG (HRNG), είναι μικτές RNG οι οποίες συνδυάζουν ιδιότητες των Φυσικών και των Ψευδο-Τυχαίων RNG, και συνήθως υλοποιούνται από μία PRNG η οποία επανατροφοδοτείται από μία TRNG (re-seeding). Στις επόμενες παραγράφους θα εξετάσουμε τα χαρακτηριστικά σχεδιασμού και ασφάλειας των TRNG , PRNG and HRNG.

6.2. Πραγματικές Γεννήτριες Τυχαίων Χαρακτήρων (TRNG)

Οι TRNG βασίζονται σε μια πηγή φυσικού θορύβου που παράγει ένα αναλογικό τυχαίο σήμα, το οποίο κατόπιν ψηφιοποιείται και επεξεργάζεται ώστε να παράγει τυχαία bits στην έξοδο, όπως φαίνεται στο Σχήμα 9.



Σχήμα 9. Γενικό διάγραμμα TRNG (με τα σημεία των ελέγχων Στατιστικής και Εντροπίας)

Η φυσική πηγή θορύβου στο Σχήμα 9 πρέπει να παράγει ένα πραγματικά τυχαίο σήμα και μπορεί να υλοποιηθεί με μία από τις ακόλουθες μεθόδους:

-Johnson noise (thermal noise in resistors)
-Shot noise (random current fluctuations)
-Avalanche noise (reverse biased Zener diode)
-Free running oscillators
-Quantum optics (reflected or passed photons through a mirror)
-Radioactive sources

Για να μειωθεί ο χρόνος σχεδιασμού, ο χώρος και το κόστος, εναλλακτική πηγή θορύβου μπορεί να είναι κάποιο στοιχείο υλικού του υπολογιστή, όπως ο χαοτικός στροβιλισμός αέρα στο σκληρό δίσκο (hard disk chaotic turbulence), η ανοικτή είσοδος μικροφώνου (unplugged microphone input) και η είσοδος βίντεο με σκεπασμένη κάμερα (video input with camera lens cap on).

Ανεξάρτητα από την μετα-επεξεργασία των bits (post process), η εντροπία της εξόδου δεν μπορεί να γίνει μεγαλύτερη από την εντροπία του ψηφιοποιημένου θορύβου. Η εντροπία δίδεται από τον παρακάτω τύπο και εκφράζει την τυχαιότητα του x_i . Αυτό σημαίνει ότι όσο η τιμή της εντροπίας αυξάνεται, τόσο πιο δύσκολο είναι να «μαντέψεις» το x_i .

$H(x) = \sum_{i=1}^{n} p(x_i) \log_2 [1/p(x_i)]$	όπου: x_i = μία από τις πιθανές τιμές των bits (0 ή 1) $p(x_i)$ = η πιθανότητα της εμφάνισης του xi n = ο συνολικός αριθμός των bits

6.2.1. Μετα- επεξεργασία των bits (post process)

Εφόσον η πηγή μίας TRNG είναι τυχαία, μπορεί να παράγει συσχετισμούς ή άνισες κατανομές μεταξύ των bits εξόδου. Όπως φαίνεται στο Σχήμα 1, για να ελαττώσουμε τους συσχετισμούς και ανισοκατανομές, μετά την ψηφιοποίηση εφαρμόζονται μέθοδοι μετα-επεξεργασίας των bits. Υπάρχουν πολλές τέτοιες μέθοδοι (de-skewing ή mixing methods) και μια λεπτομερής περιγραφή τους δίδεται στο **[9]**. Οι πλέον συνηθισμένες είναι οι εξής:

1. Mapping the bits with 0 or 1
2. Transition mappings (00 and 11)
3. Stream parity
4. Fast Fourier Transform (FFT)
5. Mixing of two or more inputs (XOR)
6. XOR with LFSR
7. XOR of overlapping bits
8. Compression of bits
9. Hashing of bits
10. Encryption of bits

Πρέπει να τονίσουμε ότι η μεταγενέστερη επεξεργασία αποτελεί ένα επιπρόσθετο μέτρο ασφάλειας, γιατί εάν η πηγή του φυσικού θορύβου αποτύχει, η TRNG δύναται να λειτουργήσει προσωρινά ως μία PRNG.

6.2.2. Διαδικασίες αξιολόγησης

Για να καθορίσουμε το επίπεδο ασφάλειας μίας TRNG, πρέπει πρώτα να αξιολογήσουμε την τυχαιότητα και την μη προβλεψιμότητα των bits εξόδου της και κατόπιν τις συνολικές αδυναμίες ασφάλειας της. Για αυτό το λόγο, η αξιολόγηση πρέπει να γίνεται σε δύο διαφορετικά στάδια:

Στο 1ο Στάδιο , το πρωτότυπο μιας TRNG αξιολογείται για:

1. Ασφαλή σχεδιασμό 2. Στατιστικές ιδιότητες (τυχαιότητα)

Στο 2ο Στάδιο , ολόκληρη η υλοποίηση της TRNG αξιολογείται για:

1. Ανθεκτικότητα δομικών στοιχείων
2. Γήρανση δομικών στοιχείων
3. Θερμοκρασιακά όρια
4. Δυσλειτουργίες ή Κατάρρευση
5. Ενδεχόμενες επιθέσεις

6.2.3. Στατιστικοί έλεγχοι τυχαιότητας

Για την αξιολόγηση της τυχαιότητας των bits εξόδου μιας RNG, ισχύουν όσα αναφέρθηκαν στην παράγραφο 3.3. για την έξοδο των κρυπτογραφικών αλγορίθμων. Επομένως, παραπέμπουμε τον αναγνώστη στους στατιστικούς ελέγχους του Πίνακα 3 και τη σχετική βιβλιογραφία **[4], [5], [6], [7].**

6.2.4. Αυτοέλεγχοι

Για να είναι ασφαλής μία TRNG, στην τελική υλοποίησή της πρέπει να ενσωματώνει αυτόματους ελέγχους, οι οποίοι όταν ανιχνεύουν δυσλειτουργίες, θα ειδοποιούν τον χειριστή. Αυτοί οι έλεγχοι πρέπει να διεξάγονται στην αρχή ή κατά τη διάρκεια της λειτουργίας και να είναι ενσωματωμένοι στην TRNG ή κατ' εξαίρεση να πραγματοποιούνται εξωτερικά (μέσω εντολής λογισμικού της TRNG). Οι βασικοί αυτοέλεγχοι είναι:

Έλεγχος έναρξης: Πιστοποιεί την αρχή λειτουργικότητας και την τυχαιότητα της πηγής θορύβου όταν η TRNG ξεκινά (ελάχιστες στατιστικές ιδιότητες).

On line έλεγχος : Ανιχνεύει την επαρκή ποιότητα της πηγής θορύβου, ή την επιδείνωση της στο χρόνο.

Συνολικός έλεγχος: Ανιχνεύει την συνολική κατάρρευση της πηγής θορύβου.
Συναγερμοί: Σε περίπτωση αδύναμων στατιστικών ελέγχων, δυσλειτουργιών και σε περίπτωση που κάποια λάθη ξεπερνούν τον προσδοκώμενο αριθμό.

Το Αμερικανικό πρότυπο FIPS 140-2 "Προϋποθέσεις Ασφάλειας για Κρυπτογραφικές Μονάδες" - βιβλιογραφία **[26],** ορίζει τέσσερις στατιστικούς ελέγχους: Monobit, Poker, Runs και Long Run. Σύμφωνα με αυτό το πρότυπο, αυτοί οι έλεγχοι πρέπει να εφαρμόζονται στην έναρξη μιας TRNG (ή κατόπιν εντολής) σε έξοδο (δείγμα) των 20.000 bits. Αυτό το μικρό δείγμα εξόδου επιλέχθηκε για να μειώσει το χρόνο των στατιστικών ελέγχων. Όμως το δείγμα αυτό δεν είναι επαρκές εάν θέλουμε να παράγουμε μια μακρά ψηφιακή ακολουθία (long keystream), όπως στα κρυπτοσυστήματα one time pad. Σε αυτές τις περιπτώσεις, πρέπει να διεξαχθούν περισσότεροι στατιστικοί έλεγχοι (όπως αυτοί στον Πίνακα 3) και σε μεγαλύτερα δείγματα εξόδου.

6.2.5. Επίπεδα Ασφάλειας μιας TRNG

Το Αμερικανικό πρότυπο FIPS 140-2 ορίζει τέσσερα Επίπεδα Ασφάλειας, τα οποία εξετάζουν τις βασικές παραμέτρους ασφάλειας των κρυπτογραφικών μονάδων. Εν συντομία, οι πιο σημαντικές από αυτές τις παραμέτρους είναι: Θύρες και διεπαφές, Πιστοποίηση αυθεντικότητας χρήστη, Φυσική ασφάλεια, Λειτουργικό περιβάλλον, Ηλεκτρομαγνητική συμβατότητα, Διαχείριση κλείδας, Αυτόματοι αυτοέλεγχοι κατά την έναρξη ή κατόπιν εντολής (έλεγχος κρυπταλγόριθμου, έλεγχος ακεραιότητας υλικού/λογισμικού, στατιστικοί έλεγχοι της εξόδου), Τεκμηριωμένη και πιστοποιημένη σχεδίαση, Ανίχνευση και αντίδραση σε παραβίαση, καθώς και μηδενισμός των κρυπτοπαραμέτρων σε περίπτωση αλλοίωσης.

Το Γερμανικό πρότυπο AIS 31 "Επίπεδα λειτουργικότητας και μεθοδολογία αξιολόγησης για πραγματικές (φυσικές) γεννήτριες τυχαίων χαρακτήρων" - βιβλιογραφία **[27],** ορίζει δύο επίπεδα ελέγχων για μια TRNG, σύμφωνα με την ισχύ ασφάλειας τους: Το επίπεδο P1 (μεσαίας ισχύος) και το επίπεδο P2 (υψηλής ισχύος). Τα βασικά χαρακτηριστικά αυτών των επιπέδων φαίνονται στον Πίνακα 13. Στο επίπεδο P1, οι στατιστικοί έλεγχοι καλύπτουν μόνο την τυχαιότητα των bits και δεν καλύπτουν την μη προβλεψιμότητά τους. Με άλλα λόγια, οι στατιστικοί έλεγχοι μπορούν να ανιχνεύουν ατέλειες της τυχαίας πηγής, αλλά δεν μπορούν να επαληθεύσουν την τυχαιότητά της. Για αυτό το λόγο, στο επίπεδο P2 προστίθενται οι έλεγχοι εντροπίας (έλεγχος Coron, έλεγχος Collision, κ.λ.π.) οι οποίοι μπορούν να ανιχνεύσουν την μη προβλεψιμότητα των bits και έτσι την τυχαιότητα της πηγής.

	P1 class (μέσης ισχύος)	**P2 class (υψηλής ισχύος)**
Κατηγορίες εφαρμογής	-Challenges -Initial vectors	- Cryptographic keys and parameters - Random padding - Passwords
Απαιτήσεις αξιολόγησης	- Statistically random output - Self tests during operation	- Stat tests + Entropy tests - Self tests during operation (higher than P1)

Πίνακας 13. Επίπεδα ελέγχων μιας TRNG

Όπως φαίνεται και στο Σχήμα 9, οι στατιστικοί έλεγχοι εφαρμόζονται μετά την μετα-επεξεργασία των bits (post process), αλλά οι έλεγχοι εντροπίας πραγματοποιούνται κατά την έξοδο του ψηφιοποιημένου σήματος, διότι η μετα-επεξεργασία ενδέχεται να καλύψει (κρύψει) κάποιες εξαρτήσεις των bits.

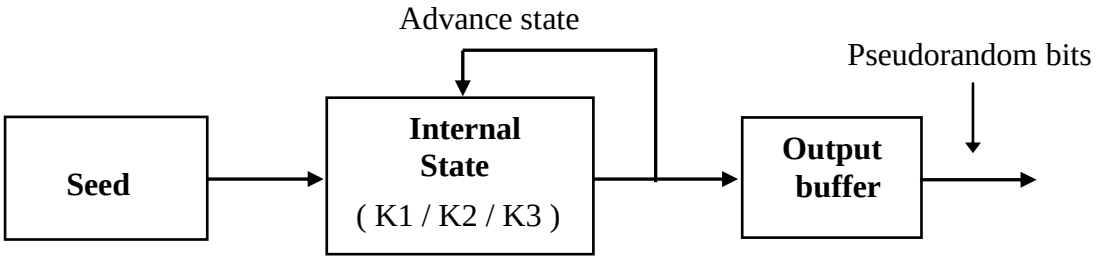
6.2.6. Κριτήρια επιλογής

Επιπροσθέτως των προϋποθέσεων ασφάλειας, υπάρχουν και μερικά άλλα κριτήρια για την επιλογή μιας κατάλληλης TRNG για μια κρυπτογραφική εφαρμογή, η οποία αφορά τα λειτουργικά χαρακτηριστικά της και την ενσωμάτωση της σε ένα σύστημα. Σύμφωνα με την εφαρμογή ή το συνολικό σύστημα στο οποίο μια TRNG πρέπει να ενσωματωθεί, η προτεραιότητα αυτών των προϋποθέσεων ενδέχεται να ποικίλλει. Στην βιβλιογραφία **[24]** περιέχεται μια λεπτομερής εξέταση αυτών των λειτουργικών χαρακτηριστικών. Γενικά μπορούμε εν συντομία να συνοψίσουμε τα κριτήρια ασφάλειας και λειτουργικής απόδοσης για μια TRNG στα ακόλουθα:

1. Πιστοποιημένη τυχαιότητα
2. Αυτοέλεγχος
3. Ρυθμός εξόδου (ταχύτητα)
4. Φυσικό μέγεθος
5. Ενσωματωμένη ή αυτόνομη
6. Απαιτήσεις τροφοδοσίας
7. Θερμοκρασία λειτουργίας
8. Τιμή

6.3. Γεννήτριες Ψευδο-Τυχαίων Χαρακτήρων (PRNG or DRNG)

Στις Γεννήτριες Ψευδο-Τυχαίων Χαρακτήρων (PRNG) ή Ντετερμινιστικές RNG (DRNG), η τυχαιότητα δεν βασίζεται σε μια φυσική πηγή θορύβου, αλλά σε μια προκαθορισμένη αρχική και «φαινομενικά τυχαία» παράμετρο, το **seed**. Εφόσον το **seed** είναι μια προκαθορισμένη παράμετρος (ή αλγόριθμος), η έξοδος μιας PRNG δεν είναι τυχαία, αλλά φαίνεται να είναι (ψευδοτυχαία). Όπως αναφέρθηκε στην παράγραφο 6.1, η χρήση των PRNG οφείλεται στην ταχύτητα και την ευκολότερη υλοποίησή τους σε λογισμικό. Όπως φαίνεται στο Σχήμα 10, το seed τροφοδοτεί την Εσωτερική Κατάσταση **(Internal State)**, που είναι μια Μηχανή Πεπερασμένων Καταστάσεων (Finite State Machine - FSM), δηλαδή μια μονάδα η οποία μπορεί πάρει μόνο συγκεκριμένες τιμές. Μετά τη φόρτωση της Εσωτερικής Κατάστασης (Internal State) με μια αρχική Κατάσταση (Initial State) από το seed, η Εσωτερική Κατάσταση αλλάζει κάθε φορά που δέχεται αίτημα για έναν νέο τυχαίο χαρακτήρα. Αυτό γίνεται με ανατροφοδότηση (feedback) από την έξοδο της (Επόμενη Κατάσταση - Advance State). Πρέπει να σημειώσουμε ότι ανεξάρτητα από οποιαδήποτε ενδιάμεση επεξεργασία των bits, η εντροπία των bits εξόδου δεν μπορεί να είναι μεγαλύτερη από την εντροπία του seed.



Επίπεδο K1: Counter, Επίπεδο K2: LFSR ή Block cipher (OFB) με γνωστό κλειδί.
Επίπεδο K3: Block cipher (OFB) με κρυφό κλειδί

Σχήμα 10. Γεννήτρια PRNG (για επίπεδα ασφαλείας K1, K2, K3 του AIS 20)

6.3.1. Εντροπία του Seed

Το seed στην PRNG πρέπει να δίνει αρκετή τυχαιότητα και μη προβλεψιμότητα για την Αρχική Κατάσταση (Initial State). Στον Πίνακα 14 δίνουμε κάποιες πηγές λογισμικού και υλικού για την υλοποίηση του seed, οι οποίες κατηγοριοποιούνται σε Χαμηλή, Μεσαία και Υψηλή Εντροπία, σύμφωνα με το επίπεδο της μη προβλεψιμότητάς τους.

Χαμηλή Εντροπία (Σταθερές συστήματος)	**Μέση Εντροπία** (Μεταβλητές και απρόβλεπτες)	**Υψηλή Εντροπία** (Εξωτερικές τυχαίες)
-Configuration files -Drive configuration -Environment strings	-Contents of screen -Computer's date and time -High resolution clock samples -Last key pressed -Log file blocks -Network statistics -Process statistics -Program counter for various Processes	-Cursor position with time -Keystrokes timing -Mouse click timing -Mouse movement -Memory statistics -Microphone input (micr. connected) -Video input

Πίνακας 14. Εντροπία διαφορετικών πηγών για υλοποίηση του seed

Όταν μια PRNG χρησιμοποιείται για παραγωγή κρυπτογραφικής κλείδας, υπάρχουν δύο σημαντικοί κανόνες που πρέπει να ακολουθούνται:

-Η εντροπία του **seed** πρέπει να είναι μεγαλύτερη από ότι η εντροπία της κρυπτογραφικής κλείδας (που είναι ίση με το μήκος της).

-Το **seed** πρέπει να ενημερώνεται συχνά (επανατροφοδότηση - re-seeding).

6.3.2. Στόχοι σχεδιασμού μιας PRNG

Οι βασικοί στόχοι σχεδιασμού για μια ασφαλή PRNG δίνονται παρακάτω με σειρά προτεραιότητας:

1. Η έξοδος να είναι δυσδιάκριτη από μια πραγματική τυχαία σειρά.
2. Η γνώση μιας εξόδου δεν προβλέπει μελλοντικές ή προηγούμενες εξόδους.
3. Καλή χρήση της εντροπίας στο seed.
4. Εγγυημένος μεγάλος κύκλος επανάληψης (long cycle length).
5. Μεγάλη Εσωτερική Κατάσταση προς αποφυγή της εξαντλητικής έρευνας.
6. Καλή απόδοση.
7. Απλός αλγόριθμος.

6.3.3. Επιθέσεις εναντίον των PRNG

Μια λεπτομερής περιγραφή των πιθανών επιθέσεων εναντίον των PRNG υπάρχει στο **[28]**. Οι πιο σημαντικές είναι οι ακόλουθες:

1. Εξαντλητική έρευνα του seed 2. Εξαντλητική έρευνα του state 3. Υπολογισμός της εξόδου 4. Κακόβουλες επιθέσεις λογισμικού 5. Αποκάλυψη / πρόβλεψη επόμενων 6. Αποκάλυψη / πρόβλεψη προηγούμενων	7. Έλεγχος της εντροπίας εισόδου 8. Επιλογή του seed εσόδου 9. Συντόμευση κύκλου λειτουργιών 10. Επιθέσεις στο χρόνο εκτέλεσης λειτουργιών

Υπάρχουν πολλά μέτρα προστασίας από τις ανωτέρω επιθέσεις, τα οποία αφορούν όχι μόνο την ασφάλεια της RNG, αλλά και την ασφάλεια του συνολικού συστήματος το οποίο παράγει και διαχειρίζεται τις κρυπτογραφικές κλείδες (μέτρα ασφάλειας υπολογιστή). Αυτά τα μέτρα περιλαμβάνουν την απομόνωση της μονάδας παραγωγής κλειδών (key generation module) με τη χρήση αυτόνομων υπολογιστών, την διενέργεια τακτικών ελέγχων ακεραιότητας (integrity checks) στον εκτελέσιμο κώδικα, τα αρχεία διαμόρφωσης, κ.λ.π., καθώς και την απόκρυψη κρίσιμων πληροφοριών ασφάλειας στη μνήμη του υπολογιστή (βιβλιογραφία **[29]**).

6.3.4. Επίπεδα ασφαλείας των PRNG (πρότυπο AIS 20)

Το Γερμανικό πρότυπο AIS 20 "Επίπεδα λειτουργικότητας και μεθοδολογία αξιολόγησης για ντετερμινιστικές γεννήτριες τυχαίων χαρακτήρων" – βιβλιογραφία **[31],** ορίζει τέσσερα επίπεδα ασφαλείας για τις υλοποιήσεις των PRNG, τα K1, K2, K3 και K4. Στον Πίνακα 15 δίνουμε τα βασικά χαρακτηριστικά, τις εφαρμογές και τις προϋποθέσεις ασφάλειάς τους.

Επίπεδο	Εφαρμογές	Απαιτήσεις Ασφαλείας
K1	-Challenges	Mutually different output vectors
K2	-Initial vectors	+ Output with similar statistical properties as ideal random numbers
K3	-Cryptographic keys -Random padding -Passwords	+ Minimum bounds for seed entropy + Protection of preceding and following outputs, in case of compromised output
K4	-Cryptographic keys -Random padding -Passwords	+ Protection of preceding outputs, in case of compromised internal state

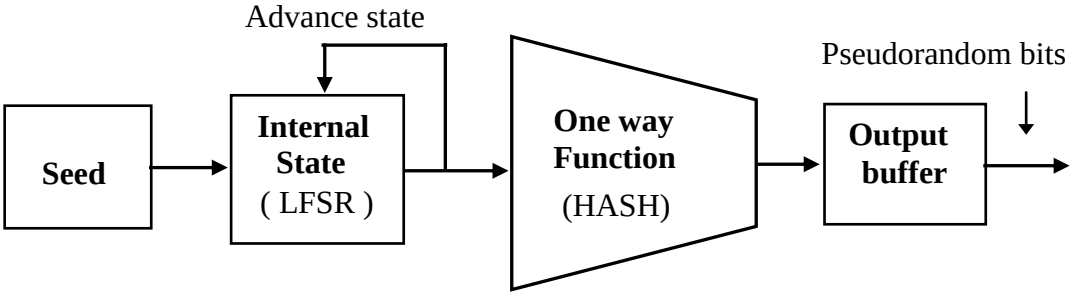
Πίνακας 15. Επίπεδα ασφαλείας υλοποίησης PRNG (Γερμανικό πρότυπο AIS 20)

6.3.5. Παραδείγματα επιπέδων ασφαλείας υλοποίησης

Το βασικό στοιχείο που ορίζει το επίπεδο ασφάλειας μιας PRNG είναι η Αρχική Κατάσταση **(Initial State)**. Στο Σχήμα 10 φαίνονται τρία παραδείγματα υλοποιήσεων ασφαλείας K1, K2, K3. Στο επίπεδο K1 η Αρχική Κατάσταση εφαρμόζεται από έναν μετρητή. Σε αυτό το επίπεδο, οι μόνες απαιτήσεις ασφάλειας είναι για διαφορετικές εξόδους χωρίς στατιστικές ιδιότητες. Στο επίπεδο K2 η Αρχική Κατάσταση υλοποιείται από έναν καταχωρητή LFSR ή ένα κώδικα ομάδας (block cipher - OFB) με γνωστή κλείδα. Σε αυτό το επίπεδο, υπάρχει μια επιπρόσθετη απαίτηση ασφάλειας για στατιστικές ιδιότητες εξόδου παρόμοιες με αυτές των ιδανικών τυχαίων χαρακτήρων. Στο

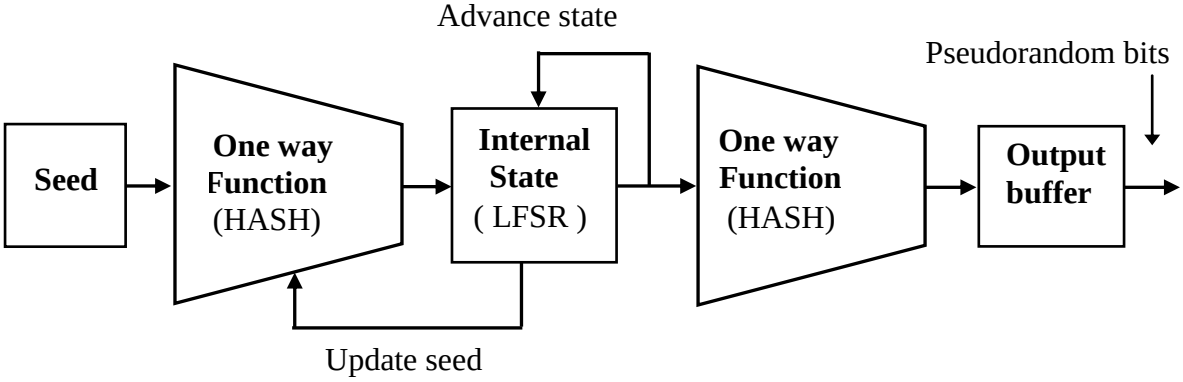
επίπεδο Κ3 η Αρχική Κατάσταση υλοποιείται από έναν κώδικα ομάδας (block cipher- OFB) με μυστική κλείδα. Αυτό το επίπεδο έχει όλες τις απαιτήσεις ασφάλειας των προηγούμενων επιπέδων Κ1 και Κ2, με την επιπρόσθετη απαίτηση για ελάχιστα όρια εντροπίας του seed, καθώς και για την προστασία των προγενέστερων και μεταγενέστερων εξόδων, σε περίπτωση που η έξοδος έχει αποκαλυφθεί (compromised output).

Στο Σχήμα 11, δίνουμε ένα άλλο παράδειγμα του επιπέδου Κ3, στο οποίο η Αρχική Κατάσταση (Initial State) υλοποιείται από ένα καταχωρητή LFSR και μετά από αυτόν προστίθεται μια Μονόδρομη Συνάρτηση (Λειτουργία Κατακερματισμού - **hash function**). Αυτή εμποδίζει έναν επιτιθέμενο, σε περίπτωση που γνωρίζει κάποια bits εξόδου, να υπολογίσει προγενέστερα και μεταγενέστερα bits της εξόδου.



Σχήμα 11. PRNG επιπέδου ασφαλείας Κ3 με Μονόδρομη Συνάρτηση

Στο Σχήμα 12, φαίνεται ένα παράδειγμα επιπέδου Κ4, όπου η συνολική Εσωτερική Κατάσταση (Internal State) υλοποιείται από έναν LFSR και δύο Μονόδρομες Συναρτήσεις (πριν και μετά τον LFSR). Η Μονόδρομη Συνάρτηση πριν τον LFSR ανανεώνει το seed και κατά συνέπεια την τιμή της Αρχικής Κατάστασης (Initial State). Αυτό όχι μόνο εμποδίζει τον υπολογισμό προγενέστερων και μεταγενέστερων bits εξόδου σε περίπτωση που έχουν αποκαλυφθεί bits (compromised output bits), αλλά εμποδίζει και τον υπολογισμό προγενέστερων εξόδων, σε περίπτωση που κάποια περιεχόμενα της Εσωτερικής Κατάστασης έχουν αποκαλυφθεί (compromised).

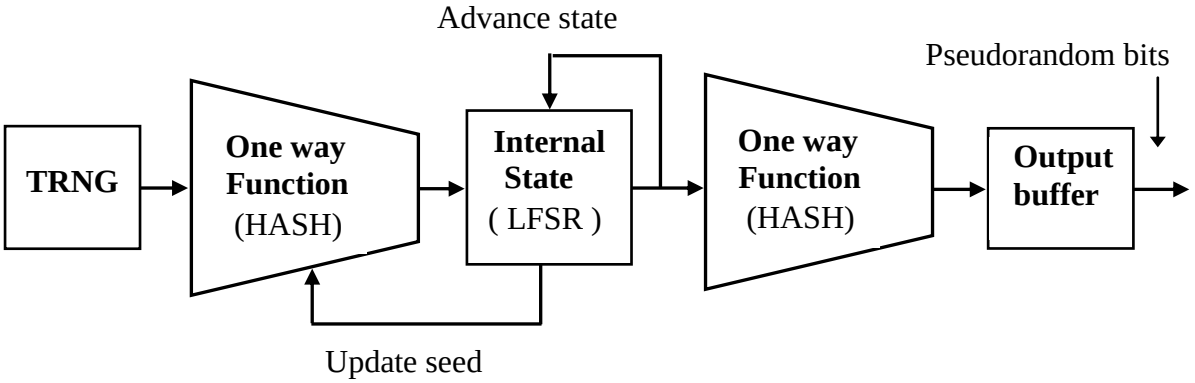


Σχήμα 12. PRNG επιπέδου Κ4 με δύο Μονόδρομες Συναρτήσεις

6.4. Υβριδικές Γεννήτριες Τυχαίων Χαρακτήρων

Οι Υβριδικές Γεννήτριες Τυχαίων Χαρακτήρων (HRNG) συνδυάζουν μερικές από τις ιδιότητες των TRNG και των PRNG. Όπως φαίνεται στο Σχήμα 13, υλοποιούνται συνήθως με τη χρήση μιας TRNG στην θέση του seed, η

οποία επανατροφοδοτεί συνεχώς την είσοδο (re-seeding). Η αντικατάσταση του seed με μία TRNG παρέχει μια πραγματικά τυχαία είσοδο, επομένως οι HRNG όχι μόνο παρέχουν προστασία από ενδεχόμενη αποκάλυψη των περιεχομένων της Αρχικής Κατάστασης (όπως και στο επίπεδο K4), αλλά παρέχουν και προστασία ενάντια στο συνολικό έλεγχο της Εσωτερικής Κατάστασης. Οι Υβριδικές Γεννήτριες Τυχαίων Χαρακτήρων παρέχουν επίπεδο προστασίας μεγαλύτερο του K4 και ανήκουν στο επίπεδο ασφαλείας H5 (πρότυπο AIS 20).



Σχήμα 13. Υβριδική RNG (επιπέδου H5), με TRNG στη θέση του Seed

Εκτός από το παράδειγμα του Σχήματος 13, πολλοί άλλοι τύποι HRNG μπορούν να σχεδιαστούν με συνδυασμό TRNG και PRNG. Ο πιο συνηθισμένος συνδυασμός είναι να αναμείξουμε τις εξόδους τους με μια λειτουργία XOR (exclusive OR). Ο George Marsaglia απέδειξε ότι ο συνδυασμός δύο ανεξάρτητων σειρών τυχαίων χαρακτήρων κάνει τους τελικούς χαρακτήρες να κατανέμονται πιο ομοιόμορφα από τους αρχικούς. Επίσης, ο συνδυασμός δύο PRNG παρέχει μεγαλύτερη περίοδο στα bits εξόδου, που είναι το ελάχιστο κοινό πολλαπλάσιο των ξεχωριστών περιόδων. Γενικά, ο συνδυασμός των RNG κάνει τα bits εξόδου περισσότερο ανεξάρτητα και ομοιόμορφα κατανεμημένα και δυσκολότερο να προβλεφθούν. Μία πρόταση στη βιβλιογραφία **[30]** είναι να χρησιμοποιούνται τέσσερις τύποι RNG, όπου τουλάχιστον ένας από αυτούς πρέπει να είναι TRNG και οι άλλοι να είναι PRNG διαφορετικών κατηγοριών.

Για να ενσωματώσει τους διάφορους τύπους υβριδικών RNG, το πρότυπο AIS 31 αναβαθμίστηκε το 2011, με την προσθήκη νέων επιπέδων εφαρμογών, τα οποία συνδυάζουν TRNG με PRNG (βιβλιογραφία **[31]**). Ένας επιπρόσθετος λόγος για αυτήν την αναβάθμιση ήταν ότι εάν η πηγή του φυσικού θορύβου μιας TRNG αποτύχει, μπορεί να δουλέψει προσωρινά ως PRNG, δια μέσου της μετα-επεξεργασίας (post process), όπως αναφέρθηκε στην παράγραφο 6.3.1.

6.5. Συνολική αξιολόγηση του συστήματος παραγωγής κλειδών

Όπως αναφέρθηκε στην παράγραφο 6.3.2, προς αποφυγή διαφόρων επιθέσεων, πρέπει όχι μόνο να αξιολογήσουμε την ασφάλεια της RNG, αλλά και την λειτουργική ασφάλεια του συστήματος στο οποίο είναι ενσωματωμένη (Key Generation Unit - KGU). Για το λόγο αυτό, προτείνουμε την συνολική αξιολόγηση ασφαλείας του συστήματος παραγωγής κρυπτογραφικών κλειδών (υλικό και λογισμικό H/Y), σύμφωνα με το πρότυπο **FIPS 140-2** (NIST/USA), το οποίο θα περιγράψουμε στο Κεφάλαιο 9 και το πρότυπο **ISO 15408 (Common Criteria)**, το οποίο θα περιγράψουμε στο Κεφάλαιο 10.

Ενδεικτικά αναφέρουμε ότι το ISO 15408 περιέχει ένα σύνολο οδηγιών, προδιαγραφών και μεθόδων για την αξιολόγηση της ασφάλειας των προϊόντων Πληροφορικής (IT) και όπως φαίνεται στον Πίνακα 16, παρέχει επτά επίπεδα ασφαλείας, σύμφωνα με το εύρος των εσωτερικών ελέγχων και την διαδικασία του σχεδιασμού του αξιολογούμενου προϊόντος.

Assurance Levels	**Range of Checks**
EAL1	Functional Check
EAL2	Structural Check
EAL3	Formal Check and Testing
EAL4	Formal Design, Check and Inspection
EAL5	Semi-officially Design and Check
EAL6	Semi-officially Validated Design and Check
EAL7	Officially Validated Design and Check

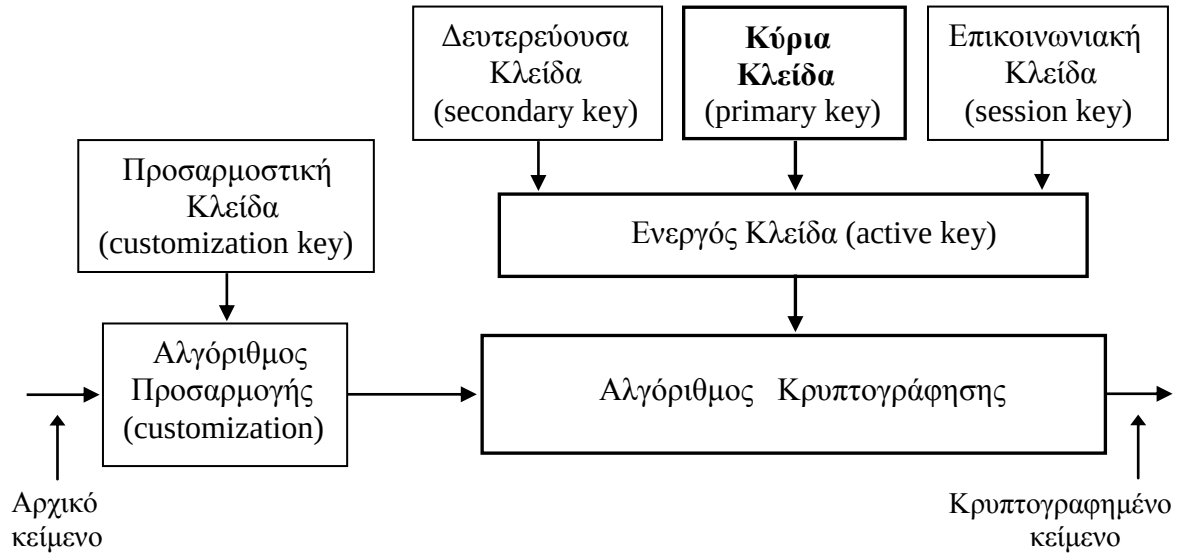
Πίνακας 16. Τα Επίπεδα Αξιολόγησης του ISO 15408 (Common Criteria)

6.6. Επιπρόσθετα μέτρα ασφάλειας

Εάν ένας χρήστης γνωρίζει τα χαρακτηριστικά στοιχεία μίας RNG από άποψη τεχνικής και ασφάλειας, θα είναι σε θέση να παράγει τις δικές του εμπιστευτικές και αξιόπιστες κρυπτογραφικές κλείδες. Αλλά πολλά κρυπτογραφικά συστήματα του εμπορίου (σε υλικό και λογισμικό), δεν έχουν θύρα εισαγωγής κλείδας **(Key Input Interface)** η οποία θα επιτρέψει στο χρήστη να φορτώσει δικές του κλείδες. Αντί γι' αυτό, κάποια συστήματα παρέχουν μια αυτόματη Μονάδα Εσωτερικής Παραγωγής Κλείδας (internal automatic key generation), της οποίας οι διαδικασίες παραγωγής, εισαγωγής και επανατροφοδότησης της κλείδας (key generation, loading and re-keying) δεν είναι διαθέσιμες στον χρήστη. Η έλλειψη θύρας εισαγωγής κλείδας, καθώς και η έλλειψη δυνατότητας εξωτερικής παραγωγής κλείδας, υποβαθμίζουν την ασφάλεια των κρυπτοσυστημάτων και είναι αναπόφευκτο να μειώνουν και την εμπιστοσύνη που τους έχουν οι χρήστες. Για αυτό και προτείνουμε οι χρήστες κατ'αρχήν να επιλέγουν κρυπτογραφικά συστήματα με δυνατότητα εξωτερικής εισαγωγής της κλείδας (Key Input Interface). Επί πλέον, προτείνουμε να μην χρησιμοποιούν την αυτόματη παραγωγή κλείδας εάν η μονάδα παραγωγής της (key production module) δεν είναι επίσημα πιστοποιημένη βάσει κάποιου διεθνώς αναγνωρισμένου προτύπου (π.χ. FIPS 140-2) και εάν οι διαδικασίες αυτόματης δημιουργίας, εισαγωγής και επανατροφοδότησης της κλείδας δεν είναι γνωστές ή επισήμως εγκεκριμένες από αρμόδιο φορέα.

6.7. Πολλαπλότητα των κλειδών

Ένας κρυπτογραφικός αλγόριθμος μπορεί να διαθέτει διαφορετικές κλείδες οι οποίες επενεργούν σε διαφορετικά σημεία. Τα πολλαπλά επίπεδα κλειδών μπορούν να προσφέρουν μεγαλύτερη ασφάλεια και ευελιξία, διότι με τη χρήση τους μπορεί να αυξηθεί το ενεργό μήκος της κλείδας, να προσαρμοστεί ο αλγόριθμος για κάθε χρήστη (customization), αλλά και να επιτευχθεί συχνότερη αλλαγή των κλειδών (μείωση της κρυπτοπεριόδου). Στο Σχήμα 14 δίνουμε ένα γενικό διάγραμμα για τα διαφορετικά είδη κλειδών τα οποία μπορεί να διαθέτει ένα κρυπτογραφικό σύστημα και παρακάτω δίνουμε μια σύντομη περιγραφή έκαστου είδους κλείδας.



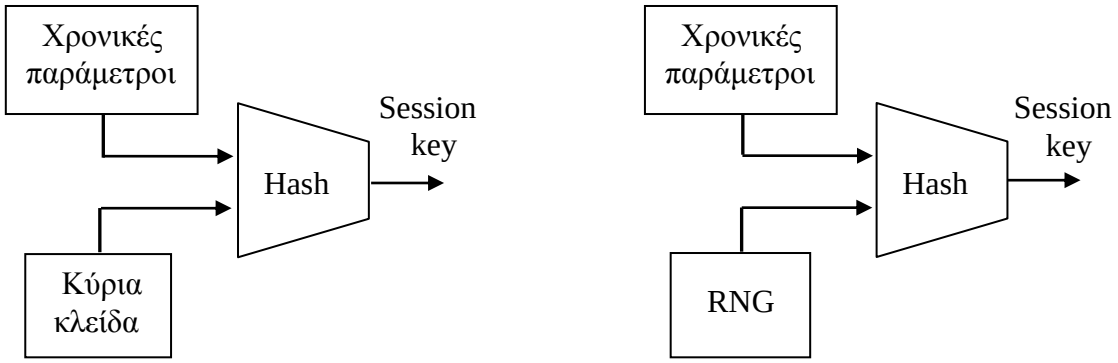
Σχήμα 14. Κρυπτογράφηση με διαφορετικά επίπεδα κλείδας

Ενεργός Κλείδα (active key) του αλγορίθμου, είναι η ιδεατή κλείδα με μήκος το οποίο συμμετέχει πραγματικά στην κρυπτογράφηση. Π.χ. ως γνωστό ο αλγόριθμος DES είχε ονομαστικό μήκος κλείδας 64 bits, αλλά το ενεργό μήκος της κλείδας του ήταν 56 bits, διότι τα 8 bits τα χρησιμοποιούσε για έλεγχο ισοτιμίας (parity). Όπως εξηγούμε παρακάτω, η Ενεργός Κλείδα συνήθως δημιουργείται μετά από συνένωση ή μίξη κάποιων επί μέρους κλειδών και μπορεί να έχει μικρότερο ή μεγαλύτερο μήκος από αυτές.

Κύρια Κλείδα (primary key) είναι η γενική κλείδα, της οποίας το μήκος καθορίζει τη βασική πολυπλοκότητα του αλγορίθμου. Εάν το κρυπτοσύστημα διαθέτει μόνο μία κλείδα (Κύρια Κλείδα), τότε αυτή ταυτίζεται με την Ενεργή Κλείδα (active key) διότι μόνο αυτή συμμετέχει στην κρυπτογράφηση. Πολλές φορές η Κύρια Κλείδα χρησιμοποιείται για την παραγωγή άλλων κλειδών, όπως την Κλείδα Επικοινωνίας (session key) και την Κλείδα Κρυπτογράφησης Κλειδών (Key Encryption Key ή Key Wrapping Key).

Επικοινωνιακή Κλείδα (session key) είναι μια κλείδα η οποία δημιουργείται αυτόματα σε κάθε νέα επικοινωνία (session), ώστε με την συχνή αλλαγή της να προσφέρει μια επιπρόσθετη ασφάλεια (αντίμετρο κρυπτανάλυσης). Παράγεται συνήθως μέσω μιας μονόδρομης συνάρτησης (hash function), η οποία παίρνει ως είσοδο την Κύρια Κλείδα και κάποια χρονικά δεδομένα (π.χ. ημερομηνία και ώρα της επικοινωνίας), όπως φαίνεται στο Σχήμα 15α. Κάποια κρυπτοσυστήματα δεν χρησιμοποιούν Κύρια Κλείδα,

αλλά όπως φαίνεται στο Σχήμα 15β, αντί για εξωτερικά εισαγόμενη Κύρια Κλείδα χρησιμοποιούν μία ενσωματωμένη RNG η οποία τροφοδοτεί τη μονόδρομη συνάρτηση. Η μέθοδος του Σχήματος 15α είναι γενικά πιο ασφαλής, διότι για την παραγωγή του session key χρησιμοποιείται η Κύρια Κλείδα την οποία παράγει και εισάγει ο χρήστης. Η περίπτωση του Σχήματος 15β είναι μεν λειτουργικά πιο εύκολη και πιο οικονομική (εφόσον η κλείδα παράγεται εσωτερικά και αυτόματα), αλλά πρέπει η ασφάλεια της RNG να είναι πιστοποιημένη σύμφωνα με όσα αναφέρθηκαν στην παράγραφο 6.1.6.



Σχήμα 15. Δύο μέθοδοι παραγωγής επικοινωνιακής κλείδας (session key)

Μηνιαία ή ημερήσια κλείδα είναι μια προαιρετική κλείδα η οποία προσφέρει επιπρόσθετη ασφάλεια, όπως και η επικοινωνιακή κλείδα, με τη διαφορά ότι παραμένει σταθερή κατά την διάρκεια του μήνα ή της ημέρας αντίστοιχα. Η παραγωγή της γίνεται με παρόμοιο τρόπο με αυτόν της επικοινωνιακής κλείδας. Εναλλακτικά, οι μηνιαίες ή οι ημερήσιες κλείδες μπορούν να είναι εξωτερικά παραγόμενες και εισαγόμενες. Κάθε πρώτη του μηνός - ή το πρωί κάθε ημέρας αντίστοιχα - οι μηνιαίες ή οι ημερήσιες κλείδες ενεργοποιούνται, βάσει ενός αυτόματου μηχανισμού ή χειροκίνητης διαδικασίας, η οποία ονομάζεται «ενημέρωση» της κλείδας (key update).

Δευτερεύουσα Κλείδα (secondary key) είναι μια ανεξάρτητη κλείδα, η οποία δίνει μία επιπρόσθετη πολυπλοκότητα στην κρυπτογραφική διαδικασία. Με αυτό τον τρόπο, το μήκος της Ενεργού Κλείδας ισούται με το άθροισμα των μηκών της Κύριας και της Δευτερεύουσας Κλείδας. Ένα τέτοιο παράδειγμα είναι η εφαρμογή των LRW, XEX και XTS modes στους block ciphers, όπου χρησιμοποιείται ένα είδος Δευτερεύουσας Κλείδας η οποία ονομάζεται «tweak» και είναι ίση με το μέγεθος των bits του block εισόδου του αλγορίθμου (βιβλιογραφία **[33]**, **[34]**, **[35]**. Έτσι, στην περίπτωση εφαρμογής των XTS και LRW modes στον αλγόριθμο AES-256, στην Κύρια Κλείδα των 256 bits προστίθεται μία Δευτερεύουσα Κλείδα (tweak) των 128 bits, οπότε το συνολικό μήκος της Ενεργού Κλείδας γίνεται 256+128=384 bits (βιβλ. **[36]**).

Προσαρμοστική Κλείδα (customization key) είναι επίσης μία ανεξάρτητη κλείδα, η οποία δίνει μία επιπρόσθετη πολυπλοκότητα. Αντίθετα με τη Δευτερεύουσα Κλείδα, δεν ενεργεί επί του κυρίως αλγορίθμου αλλά επί του αλγορίθμου προσαρμογής (customization algorithm). Αυτός είναι ένας προαιρετικός αλγόριθμος, ο οποίος προστίθεται από το χρήστη, συνήθως πριν

από τον κύριο αλγόριθμο, για να «ιδιωτικοποιήσει» την αλγοριθμική διαδικασία. Περισσότερα για το θέμα αυτό αναφέρουμε στην παράγραφο 7.3.

Τέλος, πρέπει να αναφέρουμε ότι ορισμένοι κρυπταλγόριθμοι έχουν δυνατότητα επιλογής του μήκους της κλείδας (π.χ. ο AES μπορεί να έχει 256 ή 192 ή 128 bits). Αυτό αποτελεί ένα πλεονέκτημα, διότι οι χρήστες μπορούν να επιλέξουν μεγαλύτερο μήκος κλείδας για μεγαλύτερη ασφάλεια ή να επιλέξουν μικρότερο μήκος κλείδας για να μειώσουν το χρόνο κρυπτογράφησης/αποκρυπτογράφησης, καθώς και τις διαδικασίες παραγωγής και διαχείρισης της κλείδας.

Όσα αναφέρθηκαν αφορούν κυρίως τις κλείδες των συμμετρικών κρυπταλγόριθμων, οι οποίες μας ενδιαφέρουν στο πλαίσιο της παρούσας μελέτης. Η έκδοση του NIST SP800-57 (βιβλιογραφία **[37]**) περιέχει ένα συγκεντρωτικό κατάλογο όλων των διαφορετικών ειδών και ονομασιών των κλειδών για συμμετρικούς και ασύμμετρους αλγόριθμους οι οποίοι χρησιμοποιούνται σε διάφορα κρυπτοσυστήματα.

6.8. Διανομή και ανταλλαγή των κλειδών

Στο προηγούμενη παράγραφο εξετάσαμε τις μεθόδους ασφαλείας κατά το πρώτο στάδιο της διαχείρισης των κλειδών, δηλαδή κατά την παραγωγή τους. Το δεύτερο στάδιο διαχείρισης των κλειδών είναι η ασφαλής διανομή των κλειδών στους νόμιμους αποδέκτες (π.χ. ανταποκριτές ενός τηλεπικοινωνιακού δικτύου). Παρακάτω εξετάζουμε τις επιπτώσεις ασφαλείας στις δύο περιπτώσεις κεντρικής διανομής κλειδών (τη φυσική και την ηλεκτρονική), καθώς και στην εναλλακτική περίπτωση της διμερούς ανταλλαγής κλειδών (key exchange ή key negotiation).

α. Φυσική διανομή των κλειδών

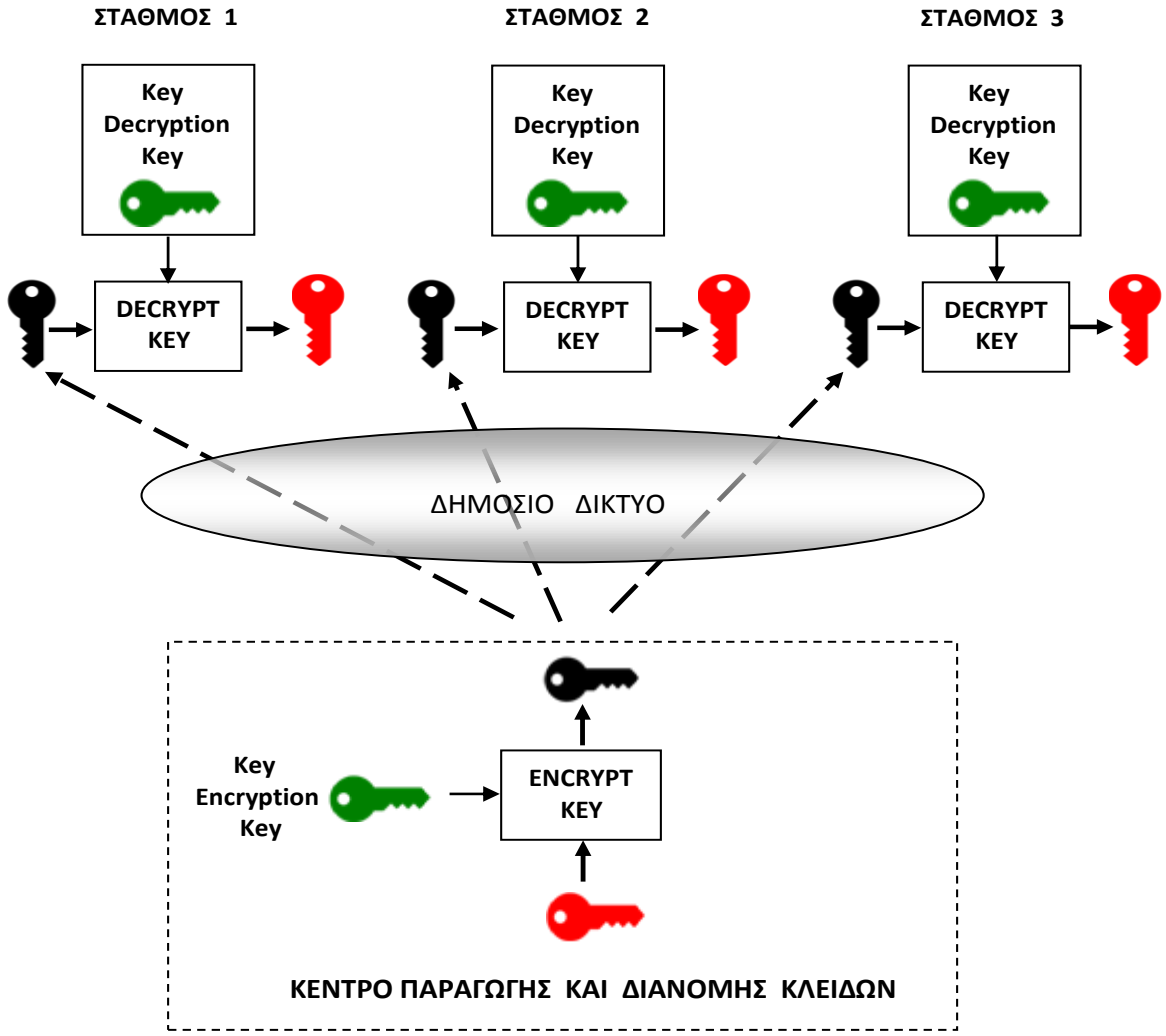
Τη φυσική διανομή των κλειδών αναλαμβάνουν ειδικά εξουσιοδοτημένα άτομα (crypto custodians), οι οποίοι τις συνοδεύουν συνεχώς και τις παραδίδουν με ασφάλεια στον τελικό χρήστη. Ασχέτως του βαθμού εμπιστοσύνης στον εξουσιοδοτημένο διανομέα των κλειδών, οι κλείδες πριν από την αποθήκευσή τους σε οποιοδήποτε αποθηκευτικό μέσο, είναι επιθυμητό πρώτα να κρυπτογραφούνται ώστε να προστατεύονται από τυχόν κλοπή, δολιοφθορά κλπ.

β. Ηλεκτρονική διανομή των κλειδών

Η φυσική διανομή των κλειδών παρέχει ασφάλεια (διότι οι κλείδες συνοδεύονται και παραδίδονται από εξουσιοδοτημένο άτομο), έχει όμως δύο μειονεκτήματα: Η διανομή παίρνει πολύ χρόνο και απαιτεί τη διάθεση ικανού αριθμού προσωπικού το οποίο θα διανέμει τις κλείδες, ιδιαίτερα όταν οι ανταποκριτές του δικτύου είναι γεωγραφικά διεσπαρμένοι. Αυτά τα δύο μειονεκτήματα μπορούν να αποφευχθούν με την ηλεκτρονική διανομή των κλειδών μέσω του τηλεπικοινωνιακού δικτύου (Electronic Key Distribution System). Όμως για να προστατευτούν οι κλείδες από τυχόν υποκλοπή τους μέσα από το τηλεπικοινωνιακό δίκτυο το οποίο είναι δημόσιο και δεν παρέχει ασφάλεια (όπως το Internet), πρέπει οπωσδήποτε να διαβιβάζονται κρυπτογραφημένες. Όπως αναφέραμε στη προηγούμενη παράγραφο, οι κλείδες οι οποίες κρυπτογραφούν τις κλείδες χρήσης, ονομάζονται Κλείδες

Κρυπτογράφησης Κλειδών (Key Encryption Keys - KEK ή Key Wrapping Keys - KWK).

Όπως φαίνεται στο Σχήμα 16, η διαδικασία ηλεκτρονικής διανομής κλειδών είναι η εξής : Στο Κέντρο Παραγωγής και Διανομής Κλειδών, η Κλείδα Χρήσης (κόκκινη) κρυπτογραφείται με την Κλείδα Κρυπτογράφησης Κλειδών (πράσινη) και αποστέλλεται κρυπτογραφημένη (μαύρη) στους ανταποκριτές (σταθμούς) του δικτύου. Σε κάθε σταθμό γίνεται η αντίστροφη διαδικασία, δηλαδή η κρυπτογραφημένη Κλείδα Χρήσης αποκρυπτογραφείται με την Κλείδα Κρυπτογράφησης Κλειδών και αναπαράγεται η Κλείδα Χρήσης.



Σχήμα 16. Γενικό διάγραμμα ηλεκτρονικής διανομής των κλειδών

Είναι προφανές ότι, στην περίπτωση που ο αλγόριθμος κρυπτογράφησης κλειδών είναι συμμετρικός, η Κλείδα Αποκρυπτογράφησης Κλειδών είναι ίδια με την Κλείδα Κρυπτογράφησης Κλειδών, ενώ εάν ο αλγόριθμος κρυπτογράφησης κλειδών είναι ασύμμετρος, οι κλείδες κρυπτογραφούνται με τη δημόσια Κλείδα Κρυπτογράφησης Κλειδών του αποδέκτη (public key) και κατόπιν αποκρυπτογραφούνται με την ιδιωτική Κλείδα Κρυπτογράφησης Κλειδών του αποδέκτη (private key).

γ. Διμερής ανταλλαγή κλειδών

Εκτός από τις δύο περιπτώσεις κεντρικής διανομής κλειδών (φυσική και ηλεκτρονική), υπάρχει και η εναλλακτική περίπτωση της διμερούς ανταλλαγής

κλειδών (αναφερόμενη στη βιβλιογραφία ως key exchange, key negotiation, key agreement, key establishment). Στην περίπτωση αυτή, οι δύο επιθυμούντες να επικοινωνήσουν «συμφωνούν» από κοινού στην κλείδα που θα χρησιμοποιήσουν. Υπάρχουν πολλές μέθοδοι και πρωτόκολλα διμερούς ηλεκτρονικής ανταλλαγής κλειδών όπως είναι η Diffie-Hellman, η El-Gammal, η Δημόσια Κλείδα (Public Key Infrastructure -PKI), η password authenticated κλπ. Τέτοιες μέθοδοι περιγράφονται λεπτομερώς στη βιβλιογραφία **[1]** και **[2]**.

Επειδή υπάρχουν πολλές μέθοδοι ηλεκτρονικής διανομής και ανταλλαγής των κλειδών, πρέπει να τονίσουμε ότι σε κάθε περίπτωση, η κρυπτογράφηση των κλειδών ή το πρωτόκολλο ανταλλαγής τους, πρέπει να γίνεται με ένα σύστημα το οποίο θα έχει κρυπτογραφική πολυπλοκότητα (ασφάλεια), αντίστοιχη με αυτή των διαβιβαζόμενων κλειδών. Αυτό σε επίπεδο κλείδας σημαίνει ότι η Κλείδα Κρυπτογράφησης Κλειδών πρέπει να έχει τουλάχιστον την ίδια εντροπία (ίδιο ή ανάλογο μήκος) με την διαβιβαζόμενη κλείδα.

Επειδή οι κρυπταλγόριθμοι οι οποίοι χρησιμοποιούνται για την κρυπτογράφηση κλειδών μπορεί να είναι είτε συμμετρικοί είτε ασύμμετροι, δίνουμε στον συγκριτικό Πίνακα 17 την αντιστοιχία του μήκους της κλείδας τους για το ίδιο επίπεδο ασφάλειας, με βάση τα σημερινά κρυπταναλυτικά δεδομένα (σύμφωνα με την έκδοση NIST SP800-57 (βιβλιογραφία **[37]**).

ΙΣΧΥΣ ΑΛΓΟΡΙΘΜΟΥ (βάσει του μήκους κλείδας σε bits)	**ΣΥΜΜΕΤΡΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ**	**ΑΣΥΜΜΕΤΡΟΙ ΑΛΓΟΡΙΘΜΟΙ**		
		FFC (π.χ. DSA, D-H)	**IFC (π.χ. RSA)**	**ECC (π.χ. ECDSA)**
≤ 80	**2TDEA (2-DES)**	**1024**	**1024**	**160-223**
112	**3TDEA (3-DES)**	**2048**	**2048**	**224-255**
128	**AES-128**	**3072**	**3072**	**256-383**
192	**AES-192**	**7680**	**7680**	**384-511**
256	**AES-256**	**15360**	**15360**	**512+**

Πίνακας 17. Αντιστοιχία μήκους κλείδας συμμετρικών - ασύμμετρων αλγορίθμων

Σημείωση : Η πρώτη στήλη του Πίνακα 17 εκφράζει το ενεργό (πραγματικό) μήκος της κλείδας, το οποίο ενδέχεται να είναι μικρότερο από το ονομαστικό. Π.χ. ενώ ο 3DES έχει θεωρητικό μήκος κλείδας 3X56=168 bits, εν τούτοις υπάρχει μια κρυπταναλυτική επίθεση η οποία μειώνει το ενεργό του μήκος σε 112 bits. Παρομοίως, για τον 2DES έχει ευρεθεί ότι εάν ο κρυπταναλυτής έχει στη διάθεσή του περίπου 2^{40} ζευγάρια ανοικτού/κλειστού κειμένου, η ενεργός κλείδα από την ονομαστική τιμή των 112 bits μειώνεται στα 80 bits, ενώ με 2^{56} ζευγάρια ανοικτού/κλειστού κειμένου, η ενεργός κλείδα μειώνεται στα 56 bits.

Πρέπει τέλος να τονίσουμε ότι, όπως αναφέρθηκε και στην παράγραφο 6.1.6 πολλοί χρήστες δεν εμπιστεύονται τις αυτοματοποιημένες μεθόδους παραγωγής και διανομής κλειδών και επιθυμούν να έχουν τη δική τους διαχείριση στις κλείδες. Για το λόγο αυτό, τα κρυπτογραφικά συστήματα πρέπει να έχουν την ηλεκτρονική διανομή των κλειδών ως προαιρετική επιλογή και όχι ως υποχρεωτική αυτοματοποιημένη λειτουργία.

6.9. Εισαγωγή, αποθήκευση και καταστροφή των κλειδών

Στα κρυπτογραφικά συστήματα εμπορικού τύπου, οι κλείδες για να διανεμηθούν αποθηκεύονται συνήθως σε κοινά ηλεκτρονικά μέσα (π.χ. CD ROM, USB κλπ.). Στα στρατιωτικά και κυβερνητικά κρυπτοσυστήματα οι κλείδες αποθηκεύονται εντός ειδικών συσκευών, οι οποίες γενικά ονομάζονται φορτωτές κλείδας (key loaders, key fills, key guns, data transfers devices κλπ.), οι οποίες έχουν την δυνατότητα αποθήκευσης πολλών κλειδών.

Όπως αναφέρθηκε, η κλείδα μετά την αρχική παραγωγή της, πρέπει να προστατεύεται έως το τέλος της χρήσης της. Δηλαδή, καθ'όλη τη διάρκεια της αποθήκευσής της στη συσκευή φόρτωσης έως την τελική διανομή της, την εισαγωγή της και την αποθήκευσή της εντός του κρυπτοσυστήματος, η κλείδα πρέπει είναι κρυπτογραφημένη.

Μετά τη λήξη της ισχύος τους, οι κλείδες πρέπει να καταστρέφονται, ώστε να μην μπορούν να χρησιμοποιηθούν ξανά, αλλά και να μην διαρρεύσουν. Επειδή σε πολλά συστήματα οι κλείδες αποθηκεύονται σε μορφή αρχείων ηλεκτρονικού υπολογιστή, η καταστροφή τους πρέπει να είναι απόλυτα ασφαλής, δηλαδή να μην χρησιμοποιείται μια απλή εντολή delete ή erase, αλλά ένα ειδικό πρόγραμμα ασφαλούς διαγραφής αρχείων (π.χ. Disk Wipe, Eraser, Shredit for Windows, Active@Kill Disk - Hard Drive Eraser κλπ.). Επίσης, η καταστροφή των κλειδών είναι επιθυμητό να είναι αυτόματη, δηλαδή το ίδιο το σύστημα μετά την λήξη ισχύος της κλείδας να την καταστρέφει, χωρίς να επεμβαίνει ανθρώπινο χέρι.

6.10. Αλλαγή και ανανέωση των κλειδών

Όπως επισημάνθηκε στην παράγραφο 1.6.4, η συχνή αλλαγή των κλειδών είναι ένας πολύ βασικός κανόνας για την ασφάλεια ενός κρυπτογραφικού συστήματος. Για την επιλογή της βέλτιστης κρυπτοπεριόδου, πρέπει να διεξαχθεί ανάλυση των κινδύνων τους οποίους αντιμετωπίζει το κρυπτογραφικό σύστημα, λαμβάνοντας υπόψη τους εξής κυριότερους παράγοντες:

-Η επικινδυνότητα του επιχειρησιακού του περιβάλλοντος.
-Η ισχύς και ο τρόπος υλοποίησης των μηχανισμών ασφαλείας του.
-Ο όγκος των κρυπτογραφημένων πληροφοριών.
-Η συχνότητα διακίνησης των κρυπτογραφημένων πληροφοριών
-Ο βαθμός ασφαλείας των κρυπτογραφημένων πληροφοριών.
-Η διάρκεια ασφαλείας των κρυπτογραφημένων πληροφοριών.
-Ο αριθμός των χρηστών και αριθμός των αντιγράφων των κλειδών.
-Η συχνότητα εναλλαγής του προσωπικού (βάρδιες).
-Ο τρόπος διακίνησης και εισαγωγής των κλειδών.
-Οι τεχνο-οικονομικές δυνατότητες του αντιπάλου.

Προφανώς, η αλλαγή των κλειδών είναι προτιμότερο να γίνεται από τον ίδιο το χρήστη, ο οποίος θα καθορίσει τη συχνότητα της αλλαγής των κλειδών (κρυπτοπερίοδο) σύμφωνα με την ασφάλεια των πληροφοριών τις οποίες διακινεί και σύμφωνα με τους κινδύνους που αυτός γνωρίζει ότι διατρέχει.

Παραδείγματος χάριν, ο χρήστης μπορεί να επιλέγει μεγαλύτερο μήκος κλειδών και συχνότερη αλλαγή τους, όταν διαβιβάζει υψηλής διαβάθμισης πληροφορίες, ενώ για χαμηλότερης διαβάθμισης πληροφορίες να επιλέγει μικρότερο μήκος κλειδών και αραιότερη αλλαγή τους. Με αυτό τον τρόπο μπορεί να μειώσει το χρόνο της επικοινωνίας, αλλά συγχρόνως να μειώσει το χρόνο και το κόστος της διαχείρισης των κλειδών. Πολλά όμως κρυπτοσυστήματα όπως αναφέρθηκε στην παράγραφο 6.1.6., δεν δίνουν τη δυνατότητα στον χρήστη να αλλάζει τις κλείδες, αλλά τις αλλάζουν αυτόματα βάσει κάποιων δικών τους κανόνων (π.χ. μια φορά την ημέρα ή σε κάθε νέα επικοινωνία με κλείδες οι οποίες παράγονται από μια ενσωματωμένη RNG).

Για μεγαλύτερη ασφάλεια και ευελιξία, όπως αναφέρθηκε και στην παράγραφο 6.1.6., προτείνουμε οι χρήστες να επιλέγουν κρυπτοσυστήματα με δυνατότητα εξωτερικής εισαγωγής κλείδας και να μην χρησιμοποιούν την αυτόματη παραγωγή κλείδας εάν η μονάδα παραγωγής της δεν είναι πιστοποιημένη βάσει κάποιου διεθνώς αναγνωρισμένου προτύπου και εάν οι διαδικασίες αυτόματης δημιουργίας, εισαγωγής και αλλαγής των κλειδών δεν είναι επισήμως πιστοποιημένες από αρμόδιο φορέα.

Η επιλογή μίας ασφαλούς περιόδου αλλαγής των κλειδών είναι ένα πολύ σημαντικό μέτρο κρυπτογραφικής ασφάλειας. Όμως η περαιτέρω ανάλυση του θέματος δεν αφορά την παρούσα διατριβή, διότι είναι ένα διαδικαστικό και όχι τεχνικό μέτρο το οποίο εφαρμόζεται κατά την λειτουργία του κρυπτοσυστήματος (μετά την αξιολόγησή του). Ο αναγνώστης μπορεί να βρει σημαντικές λεπτομέρειες για το θέμα αυτό στο **[37]** της βιβλιογραφίας.

6.11. Συμπεράσματα – Προτάσεις

Σε αυτό το κεφάλαιο εξετάσαμε τα εξής θέματα:

α. Παραγωγή των κλειδών : Παρουσιάσαμε τα βασικά χαρακτηριστικά, τα διάφορα είδη, καθώς και τις αδυναμίες ασφαλείας των Γεννητριών Τυχαίων Χαρακτήρων (RNG) βάσει των οποίων παράγονται οι κλείδες.

β. Διαχείριση κλειδών : Εξετάστηκε η ύπαρξη πολλών επιπέδων κλειδών σε ένα κρυπτογραφικό σύστημα και τα πλεονεκτήματα που αυτή προσφέρει. Επίσης, εξετάστηκε η ασφαλής διαχείριση των κλειδών καθ'όλη τη διάρκεια της ζωής τους, η οποία περιλαμβάνει την παραγωγή, την διανομή, την εισαγωγή και αποθήκευσή τους, την περιοδική αλλαγή/ανανέωσή τους, καθώς και την τελική καταστροφή τους μετά το τέλος της χρήσης τους.

Συνοψίζοντας τα συμπεράσματα, παρακάτω δίνουμε τα βασικά μέτρα ασφάλειας κατά το στάδιο σχεδιασμού και αξιολόγησης των RNG, και προτείνουμε κάποια επιπλέον μέτρα προκειμένου αυτές να είναι κατάλληλες για την παραγωγή κρυπτογραφικών κλειδών. Επίσης, συνοψίζουμε τα βασικά μέτρα ασφαλείας τα οποία πρέπει να λαμβάνονται σε όλες τις φάσεις διαχείρισης των κλειδών.

Μέτρα κατά τη διάρκεια σχεδιασμού των RNG

1. Η εντροπία του seed να είναι μεγαλύτερη από το μήκος της κλείδας (PRNG).
2. Συχνή αλλαγή των seeds (PRNG).
3. Συνδυαστική χρήση TRNG και PRNG (υβριδικές RNG).
4. Απομόνωση της Μονάδας Παραγωγής Κλείδας (KGU), με χρήση αυτόνομων Η/Υ.
5. Έλεγχος ακεραιότητας της KGU (εκτελέσιμος κώδικας, αρχεία διαμόρφωσης κλπ).
6. Προστασία των κρίσιμων πληροφοριών της κλείδας στη μνήμη του Η/Υ.
7. Αυτόματοι έλεγχοι κατά την έναρξη και τη διάρκεια λειτουργίας (TRNG).
8. Συναγερμοί για αρνητικά αποτελέσματα ελέγχου ή δυσλειτουργίες (TRNG).
9. Όταν είναι εφικτό, λήψη του τυχαίου θορύβου από το υλικό του Η/Υ.
10. Χρήση κρυπτογραφικών συστημάτων με θύρα Εισαγωγής Κλείδας.
11. Χρήση πιστοποιημένων εσωτερικών μονάδων παραγωγής κλειδών, με εγκεκριμένες διαδικασίες εισαγωγής και ανατροφοδότησης.

Μέτρα ασφάλειας κατά την αξιολόγηση των RNG

1. Η RNG να έχει αξιολογηθεί και πιστοποιηθεί, σύμφωνα με Διεθνή Κριτήρια (ISO 15408, AIS 20 & 31, FIPS 140-2 κλπ.).
2. Για μεγαλύτερα επίπεδα ασφαλείας, εκτός των στατιστικών ελέγχων, διεξαγωγή και ελέγχων εντροπίας για ανίχνευση ανισοκατανομών και εξαρτήσεων.
3. Έλεγχος όχι μόνο του σχεδιασμού αλλά και της σωστής υλοποίησης της RNG.
4. Έλεγχος ασφάλειας του συνολικού συστήματος στο οποίο η RNG είναι ενσωματωμένη ή συνδεδεμένη.

Θέματα των RNG που χρήζουν περαιτέρω έρευνα

1. Βελτίωση των Διεθνών Προτύπων για τις RNG, με περισσότερους on line ελέγχους σε μεγαλύτερα δείγματα εξόδου.
2. Έρευνα για τον καθορισμό του απαιτούμενου ελάχιστου αριθμού από ξεχωριστούς και ανεξάρτητους στατιστικούς ελέγχους.

Διαχείριση των κλειδών

1. Επιλογή πολλαπλών επιπέδων κλειδών για μεγαλύτερη ασφάλεια και ευελιξία (primary key, secondary key, session key κλπ.).
2. Κρυπτογραφική και διαδικαστική προστασία των κλειδών σε όλες τις φάσεις της «ζωής» τους (παραγωγή, διανομή, εισαγωγή, αποθήκευση, ανανέωση, καταστροφή).
3. Κρυπτογράφηση των κλειδών με σύστημα που έχει επίπεδο ασφάλειας ανάλογο με το δικό τους (ανάλογης πολυπλοκότητας και μήκους κλείδας).
4. Χρήση ασφαλών μεθόδων διαγραφής / καταστροφής των κλειδών μετά το τέλος της χρήσης τους.
5. Επιλογή κρυπτοσυστημάτων με δυνατότητα εξωτερικής εισαγωγής κλείδας
6. Αποφυγή της αυτόματης παραγωγής κλειδών εάν δεν είναι πιστοποιημένη.
7. Αποφυγή της αυτόματης αλλαγής κλειδών εάν δεν είναι πιστοποιημένη.

ΚΕΦΑΛΑΙΟ 7

ΥΛΟΠΟΙΗΣΗ - ΕΝΣΩΜΑΤΩΣΗ - ΤΡΟΠΟΠΟΙΗΣΗ ΑΛΓΟΡΙΘΜΟΥ

Όπως προαναφέραμε, η εξέταση της δομής του αλγορίθμου γίνεται με βάσει την ανάλυση του θεωρητικού του μοντέλου. Επίσης, οι έλεγχοι της τυχαιότητας και ομοιότητας των εξόδων του, γίνονται με στατιστικούς και κρυπταναλυτικούς ελέγχους πάνω στην λογισμική του εξομοίωση. Για τον λόγο αυτό, μετά από τους ελέγχους επί του θεωρητικού και λογισμικού μοντέλου του αλγορίθμου, απαιτούνται τα εξής:

α. Να εξεταστεί ο τρόπος υλοποίησης του αλγορίθμου, ώστε να ταυτοποιηθεί η θεωρητική του μορφή με την πρακτικά υλοποιημένη του μορφή.

β. Να εξεταστεί η πιστοποίηση της ενσωμάτωσης της υλοποιημένης μορφής του αλγορίθμου εντός του κρυπτοσυστήματος.

γ. Να εξεταστούν τα μέτρα ασφαλείας του κρυπτοσυστήματος έναντι των εξουσιοδοτημένων η μη εξουσιοδοτημένων τροποποιήσεων του αλγορίθμου (modifications).

δ. Να εξεταστεί η τυχόν δυνατότητα τροποποίησης/προσαρμογής του αλγορίθμου την οποία προσφέρουν κάποιοι κατασκευαστές (customization).

Στις επόμενες παραγράφους αναλύουμε τους ανωτέρω ελέγχους.

7.1. Υλοποίηση του αλγορίθμου σε υλικό/λογισμικό (hardware / software)

Γενικά, η υλοποίηση ενός κρυπτογραφικού αλγορίθμου σε υλικό (hardware) έχει περισσότερα πλεονεκτήματα σε σχέση με την υλοποίηση του σε λογισμικό (software). Τα κυριότερα πλεονεκτήματα είναι τα εξής:

Πλεονεκτήματα της υλοποίησης σε υλικό (hardware)

1. Αξιοπιστία: Μειώνει τις ενδεχόμενες βλάβες (failures) οι οποίες επηρεάζουν την ασφάλεια και την λειτουργικότητα.

2. Προστασία παραβίασης: Προσφέρει μεγαλύτερη προστασία έναντι παραβίασης (tamper protection).

3. Παράνομη τροποποίηση: Κάνει πιο δύσκολη την οποιαδήποτε παράνομη τροποποίηση (illegal modification).

4. Αντίστροφη μηχανική : Κάνει πιο δύσκολη την αντίστροφη μηχανική (reverse engineering).

5. Γεννήτριες τυχαίων χαρακτήρων (RNG): Δημιουργεί πιο ασφαλείς RNG, με μεγαλύτερη εντροπία και απροσδιοριστία (non deterministic).

6. Διαχωρισμός Red/Black: Προσφέρει ασφαλέστερο διαχωρισμό διαβαθμισμένων και αδιαβάθμητων δεδομένων.

7. Ασφαλής μηδενισμός: Δημιουργεί ένα ασφαλέστερο και ταχύτερο μηδενισμό κρυπτογραφικών παραμέτρων (περιπτώσεις έκτακτης ανάγκης).

8. Διαχείριση Κλειδών: Προσφέρει μία ασφαλέστερη Διαχείριση των Κλειδών (Key Management).

9. Κερκόπορτες : Αυξάνει πολύ την δυσκολία να εισαχθούν κερκόπορτες (trap doors) και κρυφοί δίαυλοι εισβολής (covert channels).

Ανάλογα με το είδος της τεχνολογίας hardware ή software η οποία θα χρησιμοποιηθεί για την υλοποίηση του αλγορίθμου, το επίπεδο προστασίας της υλοποίησης διαφέρει (π.χ. προστασία έναντι αντιγραφής ή τροποποίησης του αλγορίθμου). Στον Πίνακα 18 φαίνονται οι βαθμοί προστασίας σε σχέση με τα διαφορετικά είδη τεχνολογικής υλοποίησης.

ΤΕΧΝΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ	**ΒΑΘΜΟΣ ΠΡΟΣΤΑΣΙΑΣ**
Application Specific Integrated Circuits (ASIC)	HIGH
One Time Configurable Hardware (fuse based FPGA)	HIGH
Reconfigurable Hardware (flash based FPGA)	HIGH
Firmware (EPROM) Software on Microprocessors, Microcontrollers, DSP in controlled trusted environment	ENHANCED
Software on Microprocessors, Microcontrollers, DSP in commercial workstations	BASIC

Πίνακας 18 : Βαθμοί προστασίας της υλοποίησης του αλγορίθμου

Σε ότι αφορά την υλοποίηση του αλγορίθμου σε λογισμικό (software), πρέπει εν γένει να ισχύουν τα παρακάτω μέτρα ασφαλείας:

Μέτρα ασφαλείας για το κρυπτογραφικό λογισμικό

1. Χρήση ασφαλούς λειτουργικού συστήματος (Trusted Operating System).
2. Φυσικοί και λογικοί έλεγχοι πρόσβασης (access control).
3. Απομονωμένοι σταθμοί λειτουργίας (stand alone workstations).
4. Ασφάλεια του δικτύου (firewall, IDS, κλειστό δίκτυο κλπ.)
5. Ψηφιακά υπογεγραμμένο λογισμικό (για αυθεντικότητα - ακεραιότητα).
6. Επιπρόσθετο κρυπτογραφικό υλικό (hardware) στους σταθμούς εργασίας.
7. Διεξαγωγή θετικών και αρνητικών έλεγχων και συναγερμών (alarms).
8. Αυστηροί έλεγχοι για επιβλαβές λογισμικό (malicious software).
9. Περιοδικοί έλεγχοι των λειτουργιών ασφαλείας.

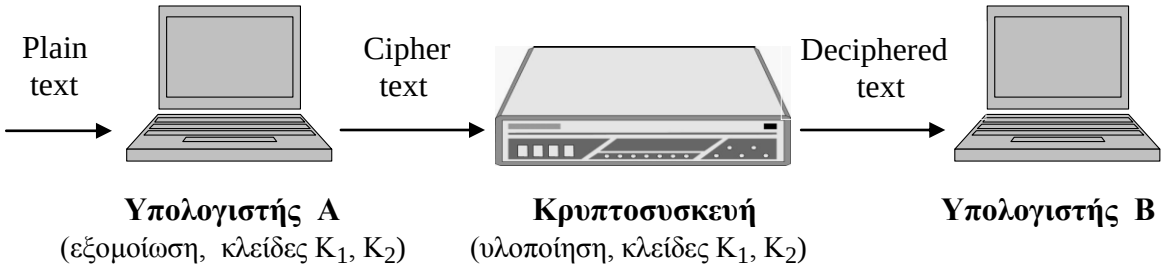
* Βασικός κανόνας : Οποιαδήποτε μορφής σύνδεση μειώνει την ασφάλεια *

7.2. Πιστοποίηση / ταυτοποίηση της ενσωμάτωσης του αλγορίθμου

Προκειμένου να γίνει η πιστοποίηση της ενσωμάτωσης ενός αλγορίθμου εντός μιας κρυπτοσυσκευής (ή εν γένει εντός ενός συστήματος), θα πρέπει να εφαρμόζεται μία μέθοδος η οποία έχει την γενική διάταξη Σχήματος 17. Όπως φαίνεται, κατ'αρχήν κρυπτογραφούμε ένα κείμενο στον υπολογιστή Α με την

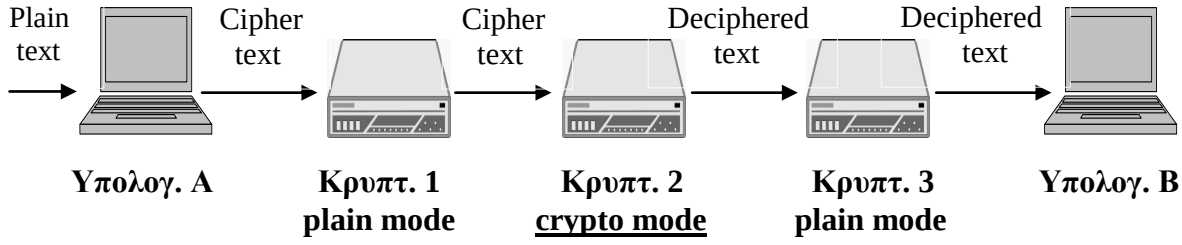
λογισμική εξομοίωση του αλγορίθμου χρησιμοποιώντας την κλείδα **K_1**. Κατόπιν διαβιβάζουμε το κρυπτογραφημένο κείμενο στην εξεταζόμενη κρυπτοσυσκευή , η οποία περιέχει τον υλοποιημένο αλγόριθμο. Η κρυπτοσυσκευή στην οποία έχουμε φορτώσει την ίδια κλείδα **K_1**, αποκρυπτογραφεί το κείμενο και στέλνει το αποτέλεσμα στον υπολογιστή Β. Εάν το αποκρυπτογραφημένο κείμενο το οποίο λάβαμε στον υπολογιστή Β είναι ίδιο με το αρχικό κείμενο, τότε πιστοποιείται ότι ο εξομοιωμένος αλγόριθμος του υπολογιστή Α είναι ίδιος με τον υλοποιημένο αλγόριθμο της κρυπτοσυσκευής. Σε περίπτωση που το κείμενο το οποίο λάβαμε στον υπολογιστή Β είναι πλήρως ή μερικώς αλλοιωμένο, τότε προφανώς οι αλγόριθμοι δεν είναι ίδιοι.

Στη συνέχεια αλλάζουμε την κλείδα μόνο στην κρυπτοσυσκευή, βάζοντας της μια διαφορετική κλείδα **K_2** και επαναλαμβάνουμε τη ίδια διαδικασία. Εφόσον η αποκρυπτογράφηση γίνεται με διαφορετική κλείδα, το κείμενο που θα λάβουμε στον υπολογιστή Β πρέπει να τώρα να είναι αλλοιωμένο (ακατάληπτο). Τέλος, βάζοντας και στον υπολογιστή Α την ίδια κλείδα **K_2** την οποία βάλαμε και στην κρυπτοσυσκευή, επαναλαμβάνουμε τη διαδικασία, οπότε τώρα το αρχικό κείμενο θα πρέπει να ληφθεί σωστά στον υπολογιστή Β. Με τις ανωτέρω διαδικασίες, επαληθεύουμε την ενσωμάτωση του αλγορίθμου εντός της κρυπτοσυσκευής.



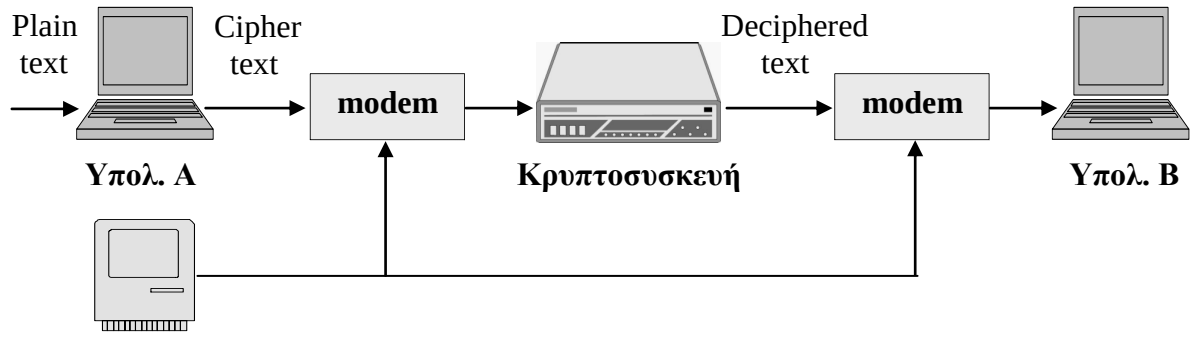
Σχήμα 17: Γενική διάταξη για την πιστοποίηση ενσωμάτωσης αλγορίθμου

Σε περίπτωση που οι κρυπτοσυσκευές για να λειτουργήσουν σε crypto-mode απαιτούν να γίνει αυθεντικοποίηση μεταξύ τους, εφαρμόζεται μια παραλλαγή της παραπάνω διάταξης. Όπως φαίνεται στο Σχήμα 18, στην είσοδο και έξοδο της ελεγχόμενης κρυπτοσυσκευής 2 (η οποία λειτουργεί σε crypto-mode), συνδέουμε τις κρυπτοσυσκευές 1 και 3 σε λειτουργία plain-mode, για να υλοποιήσουν το πρωτόκολλο αυθεντικοποίησης με την κρυπτοσυσκευή 2 και να μεταφέρουν αναλλοίωτα τα δεδομένα από την είσοδο στην έξοδο τους.



Σχήμα 18: Τροποποίηση του Σχ.17 για αυθεντικοποίηση των κρυπτοσυσκευών

Τα παραπάνω παραδείγματα διατάξεων πιστοποίησης ενσωμάτωσης του αλγορίθμου, ισχύουν όταν η επικοινωνία των κρυπτοσυσκευών είναι ασύγχρονη. Σε περίπτωση σύγχρονης επικοινωνίας πρέπει να υλοποιηθεί μια διάταξη παρόμοια με αυτή του Σχήματος 19.



Σχήμα 19: Τροποποίηση του Σχ.17 για σύγχρονη επικοινωνία.

Είναι προφανές ότι μια ανάλογη διαδικασία με τις παραπάνω, θα πρέπει να ακολουθήσουμε εάν ο κρυπτογραφικός αλγόριθμος αντί να είναι υλοποιημένος σε hardware εντός μιας κρυπτοσυσκευής, είναι υλοποιημένος σε software (π.χ. εντός ενός communication server).

7.3. Ασφάλεια έναντι τροποποιήσεων και συντηρήσεων

α. Είδη τροποποιήσεων

Οι διάφορες τροποποιήσεις (modifications) επί του αλγορίθμου (και επί του κρυπτοσυστήματος εν γένει) χωρίζονται σε τρεις τύπους ανάλογα με την επίπτωση που έχουν επί της ασφάλειας:

Τύπος 1 : Κρίσιμες για την ασφάλεια τροποποιήσεις, οι οποίες είναι αναγκαίες για την σωστή κρυπτογραφική λειτουργία.
Τύπος 2 : Βελτιώσεις ασφαλείας για την αποδοτική (efficient) ή την αποτελεσματική (effective) λειτουργία του κρυπτοσυστήματος.
Τύπος 3 : Λειτουργικές τροποποιήσεις που δεν αφορούν και δεν επηρεάζουν την ασφάλεια.

β. Μέτρα αποφυγής μη εξουσιοδοτημένων τροποποιήσεων

1. Επίσημη πρόταση για κάθε τροποποίηση (πλήρης περιγραφή, λόγοι της τροποποίησης).
2. Επίσημη έγκριση και επαναξιολόγηση του κρυπτοσυστήματος μετά κάθε τροποποίηση.
3. Νέα σήμανση του κρυπτοσυστήματος και καταγραφή της τροποποίησης στα εγχειρίδια συντήρησης.
4. Συντηρήσεις επί τόπου από εκπαιδευμένο και εξουσιοδοτημένο προσωπικό.
5. Επιθεώρηση μετά από κάθε συντήρηση.
6. Τεκμηρίωση κάθε συντήρησης.

7.4. Προσαρμογή του αλγορίθμου (customization)

Μερικοί κατασκευαστές δίνουν στους χρήστες τη δυνατότητα να κάνουν την δική τους τροποποίηση στον αρχικό αλγόριθμο που προσφέρουν. Η δυνατότητα αυτή ονομάζεται διεθνώς customization ή programmable cryptography και στο παρόν την ονομάζουμε «προσαρμογή».

Είναι γεγονός ότι η προσαρμογή ενός προϋπάρχοντος αλγορίθμου σε αντίθεση με την ανάπτυξη ενός εξ ολοκλήρου καινούργιου, είναι μια ελκυστική λύση, γιατί μειώνει κατά πολύ τον απαιτούμενο χρόνο και το κόστος. Ωστόσο, είναι προφανές ότι το customization θα πρέπει να σχεδιαστεί προσεκτικά και κάτω από την εκπαίδευση και καθοδήγηση τα κατασκευαστή, ο οποίος θα πρέπει να παράσχει και τα κατάλληλα ειδικά hardware/software εργαλεία για τον σχεδιασμό και έλεγχο του νέου αλγορίθμου, ώστε να μην επηρεαστεί η ασφάλεια του αρχικού αλγορίθμου

Πρέπει να σημειώσουμε ότι όσο αυτή η «προσωποποιημένη» τροποποίηση του αλγορίθμου παραμένει κρυφή , μπορεί να προσφέρει μία επιπρόσθετη ασφάλεια, ανεξαρτησία και προσαρμογή στις ανάγκες του χρήστη. Ωστόσο, στην περίπτωση αυτή έχουν μεγάλη σημασία η βαθιά τεχνογνωσία και η εμπιστευτικότητα του κατασκευαστή. Διαφορετικά, είτε μπορεί να μειωθεί η ασφάλεια του αρχικού αλγορίθμου, είτε ο τροποποιημένος αλγόριθμος μπορεί να διαρρεύσει.

Από τα ανωτέρω είναι φανερό ότι η προσαρμογή ενός αξιολογημένου, πιστοποιημένου και ισχυρού αλγορίθμου εάν δεν γίνει πολύ προσεκτικά, με βαθιά τεχνογνωσία και εμπιστευτικότητα, μπορεί να αποβεί επιζήμια. Επομένως, σε κάθε αξιολόγηση αλγορίθμου θα πρέπει να εξετάζεται η δυνατότητα της προσαρμογής του την οποία προσφέρει ο κατασκευαστής (customization), καθώς και οι συνθήκες κάτω από τις οποίες αυτή πραγματοποιείται. Και τέλος, είναι ευνόητο ότι μετά από οποιαδήποτε τροποποίηση ή προσαρμογή αλγορίθμου, πρέπει απαραίτητα να εκτελούνται επί του νέου τροποποιημένου αλγορίθμου όλοι οι έλεγχοι οι οποίοι αναφέρθηκαν στο Κεφάλαιο 3, ώστε να πιστοποιηθεί εκ νέου η ασφάλεια του.

ΚΕΦΑΛΑΙΟ 8

ΔΗΜΟΣΙΕΥΜΕΝΟΙ ΚΑΙ ΜΥΣΤΙΚΟΙ ΑΛΓΟΡΙΘΟΙ

8.1. Γενικά

Το θέμα της δημοσίευσης των κρυπτογραφικών αλγορίθμων έχει αποτελέσει αντικείμενο έντονων συζητήσεων. Οι Κυβερνητικές Υπηρεσίες υποστηρίζουν την μη δημοσίευση (security through obscurity), σε αντίθεση με την Πανεπιστημιακή Κοινότητα η οποία υποστηρίζει την δημοσίευση (security through design). Η διαφωνία αυτή είναι έντονη κυρίως στις ΗΠΑ και ο βασικός λόγος είναι ότι η επιστημονική κοινότητα δεν εμπιστεύεται τις Κυβερνητικές Υπηρεσίες (NSA) όταν προτείνουν στο κοινό τη χρήση κάποιου μυστικά σχεδιασμένου και πιστοποιημένου από αυτές κρυπταλγορίθμου, διότι υποπτεύονται ότι όχι μόνο γνωρίζουν πώς να τον διασπάσουν, αλλά έχουν εισάγει και σκόπιμες κερκόπορτες (trap doors) για να τον «απενεργοποιούν» παρακάμπτοντας την κλείδα.

Πολλοί πιστεύουν ότι κάποιοι καλοί δημοσιευμένοι κρυπταλγόριθμοι είναι καλλίτεροι από κάποιους μη δημοσιευμένους. Και τούτο διότι, δίνεται σε όλους η δυνατότητα να μελετήσουν τους δημοσιευμένους κρυπταλγόριθμους, έτσι ώστε να εντοπίσουν (και ενδεχομένως να διορθώσουν) τις τυχόν αδυναμίες τους. Ενώ εάν ένας μυστικός αλγόριθμος έχει αδυναμίες, αυτές μπορεί να μην εντοπισθούν από την μικρή ομάδα των σχεδιαστών και των αξιολογητών του.

Η αλήθεια είναι όμως ότι οι μυστικές υπηρεσίες έχουν πολύ μεγαλύτερη εμπειρία και τεχνογνωσία σε θέματα κρυπτολογίας (κρυπτογράφηση, κρυπτανάλυση) και προσλαμβάνουν εκατοντάδες επιστήμονες για να σχεδιάζουν, να αξιολογούν και να επιτίθενται σε κρυπτογραφικούς αλγορίθμους. Πολλές δε κρατικές υπηρεσίες, προσλαμβάνουν και διακεκριμένους πανεπιστημιακούς για να ασχοληθούν με θέματα κρυπτολογίας, με απόρρητα συμβόλαια τα οποία αναφέρουν σαφώς ότι δεν μπορούν να ανακοινώσουν καμία από τις εργασίες τους (non disclosure agreement).

Όπως αναφέραμε στην παράγραφο 1.6.1. της παρούσας μελέτης, για την προστασία μας από την κρυπτανάλυση ξεκινάμε με την χειρότερη υπόθεση, δηλαδή ότι ο αλγόριθμος είναι γνωστός στον αντίπαλο κρυπταναλυτή και ότι η προσπάθεια να σπάσει το μήνυμα συνίσταται στο να βρει μόνο το κλειδί. Αυτή η υπόθεση είναι συμβατή και με την γνωστή «αρχή του Kerchoff», δηλαδή ότι η ασφάλεια ενός κρυπτοσυστήματος, πρέπει να στηρίζεται όχι στην πολυπλοκότητα του αλγορίθμου, αλλά στο πλήθος των κλειδών του. Αυτό όμως με άλλα λόγια σημαίνει ότι, εάν ο αλγόριθμος είναι άγνωστος, ο κρυπταναλυτής δεν έχει κανένα στοιχείο, δεν μπορεί ούτε καν να ξεκινήσει την ανάλυσή του. Αυτός είναι και ο λόγος που καμία υπηρεσία ασφαλείας ή στρατιωτική υπηρεσία δεν δημοσιεύει τους κρυπτογραφικούς της αλγορίθμους.

Μία σημαντική επισήμανση είναι ότι, η δημοσίευση ενός κρυπταλγορίθμου αντί να αποβεί χρήσιμη για την αξιολόγηση του και την ενδεχόμενη βελτίωσή του, μπορεί να αποβεί παγίδα. Διότι, εάν ο αλγόριθμος έχει ελάττωμα και κάποιος το ανακαλύψει, μπορεί να μην το ανακοινώσει. Έτσι, αυτός θα μπορεί να τον διασπάει κρυφά και να υποκλέπτει τις

πληροφορίες, ενώ όλοι οι άλλοι θα τον χρησιμοποιούν, πιστεύοντας ότι είναι ασφαλής εφόσον κανείς δεν έχει ανακοινώσει κάποιο ελάττωμά του. Και είναι προφανές ότι οι μυστικές υπηρεσίες έχουν συμφέρον να χρησιμοποιούν αυτή την τακτική, δηλαδή να μην ανακοινώνουν τα ελαττώματα των δημοσιευμένων αλγορίθμων, ώστε να τους υποκλέπτουν ανυποψίαστα.

8.2. Ανάλυση κινδύνων για δημοσιευμένους και μυστικούς αλγόριθμους

Για να συγκρίνουμε την ασφάλεια των δημοσιευμένων και των μυστικών αλγορίθμων, πραγματοποιήσαμε μια ανάλυση των κινδύνων τους, σε σχέση με τις απειλές που οι αλγόριθμοι ενδέχεται να αντιμετωπίσουν. Τα αποτελέσματα της ανάλυσης παρουσιάζονται στον Πίνακα 19. Στην δεύτερη στήλη του πίνακα αναγράφεται το είδος της απειλής ή τρωτότητας, ενώ στην τρίτη και τέταρτη στήλη αναγράφεται η πιθανότητα εκμετάλλευσης της απειλής/τρωτότητας για κάθε είδος αλγορίθμου. Ο βαθμός κινδύνου για κάθε εκμετάλλευση απειλής/τρωτότητας φαίνεται με διαφορετικά χρώματα, όπου κόκκινο=Υψηλός κίνδυνος, μπλε=Μέτριος κίνδυνος, πράσινο=Μικρός κίνδυνος. Παρακάτω επεξηγούμε τα περιεχόμενα κάθε γραμμής του Πίνακα 19, σύμφωνα με όσα αναφέραμε στην προηγούμενη παράγραφο :

1. Αριθμός αξιολογητών του αλγορίθμου: Όπως αναφέρθηκε, οι σχεδιαστές/αξιολογητές των μυστικών αλγορίθμων είναι μεν λιγότεροι σε αριθμό, αλλά έχουν μεγαλύτερη εμπειρία και τεχνογνωσία. Για αυτό και ο μεγαλύτερος αριθμός των αξιολογητών δεν δίνει πολύ μεγαλύτερο πλεονέκτημα στους δημοσιευμένους αλγορίθμους.

2. Έλλειψη εμπειρίας και εργαλείων από τους σχεδιαστές/αξιολογητές: Όπως αναφέρθηκε, οι σχεδιαστές/αξιολογητές των μυστικών αλγορίθμων έχουν πολύ πιο μακρόχρονη εμπειρία και τεχνογνωσία (στο σχεδιασμό αλγορίθμων, σε κρυπταναλυτικές μεθόδους κλπ.), αλλά έχουν και στην διάθεσή τους πολύ πιο ισχυρά εργαλεία (μεγαλύτερη υπολογιστική ισχύ, ειδικό λογισμικό κλπ.).

3. Μη ανιχνευθείσες αδυναμίες από τους σχεδιαστές και αξιολογητές: Και στις δύο περιπτώσεις, οι αλγόριθμοι μπορεί να έχουν αδυναμίες, οι οποίες να μην έχουν εντοπιστεί από τους κατασκευαστές/αξιολογητές τους. Αυτό ενώ είναι πολύ επικίνδυνο για τους δημοσιευμένους αλγορίθμους (κάποιος μπορεί να βρει την αδυναμία και να τους διασπάσει), είναι πολύ λιγότερο επικίνδυνο για τους μυστικούς (εφόσον είναι άγνωστοι δεν μπορούν να κρυπταναλυθούν). Ο κίνδυνος μπορεί να προκύψει μόνο εάν οι μυστικοί αλγόριθμοι διαρρεύσουν, γεγονός το οποίο είναι εξαιρετικά δύσκολο λόγω των πολύ αυστηρών μέτρων ασφαλείας (κατά την σχεδίαση, υλοποίηση, τροποποίηση τους κλπ.) .

4. Ανιχνευθείσες αδυναμίες, αλλά μη αποκαλυφθείσες: Όπως αναφέρθηκε στην προηγούμενη παράγραφο, εάν κάποιος έχει ανακαλύψει ένα ελάττωμα στον αλγόριθμο, μπορεί να μην το ανακοινώσει, ώστε να τον διασπάει κρυφά και να υποκλέπτει τις πληροφορίες. Αυτό είναι πολύ πιθανό να συμβεί για τους δημοσιευμένους αλγορίθμους, ενώ είναι απίθανο να συμβεί για τους μυστικούς.

5. Αδυναμίες εισαχθείσες από λάθος στην υλοποίηση: Και στις δύο περιπτώσεις, στην υλοποίηση του αλγορίθμου μπορεί να υπάρχουν κάποιες αδυναμίες, οι οποίες να μην έχουν εντοπιστεί. Όμως, ενώ είναι πολύ πιθανό να

γίνει εκμετάλλευση αυτών των αδυναμιών για τους δημοσιευμένους αλγορίθμους, αυτό είναι δύσκολο να συμβεί για τους μυστικούς αλγορίθμους. Και τούτο διότι τα συστήματα τα οποία τους ενσωματώνουν είναι πολύ δύσκολο να πέσουν σε χέρια τρίτων, λόγω των πολύ αυστηρών μέτρων ασφαλείας κατά την διαχείριση τους (λειτουργία, διακίνηση, συντήρηση κρυπτοσυσκευών από ειδικά εξουσιοδοτημένο προσωπικό κλπ.).

ΑΠΕΙΛΗ / ΤΡΩΤΟΤΗΤΑ		ΕΚΜΕΤΑΛΛΕΥΣΗ ΑΠΕΙΛΗΣ / ΤΡΩΤΟΤΗΤΑΣ	
		Δημοσιευμένοι Αλγόριθμοι	**Μυστικοί Αλγόριθμοι**
1	Αριθμός αξιολογητών του αλγορίθμου	**Πολλοί**	**Λίγοι**
2	Έλλειψη εμπειρίας και εργαλείων από τους σχεδιαστές/αξιολογητές	**Πιθανό**	**Απίθανο**
3	Μη ανιχνευθείσες αδυναμίες από τους σχεδιαστές και αξιολογητές	**Πιθανό**	**Πιθανό**
4	Ανιχνευθείσες αδυναμίες, αλλά μη αποκαλυφθείσες	**Πιθανό**	**Απίθανο**
5	Αδυναμίες εισαχθείσες από λάθος στην υλοποίηση	**Πιθανό**	**Πιθανό**
6	Αδυναμίες εισαχθείσες σκοπίμως στην σχεδίαση ή στην υλοποίηση	**Πιθανό**	**Απίθανο**
7	Πρώτο βήμα για κρυπτανάλυση	**ΝΑΙ** (εφικτή)	**ΟΧΙ** (ανέφικτη)

● **Υψηλός κίνδυνος** ● **Μέτριος κίνδυνος** ● **Μικρός κίνδυνος**

Πίνακας 19. Ανάλυση κινδύνου δημοσιευμένων και μυστικών κρυπταλγορίθμων

6. Αδυναμίες εισαχθείσες σκοπίμως στην σχεδίαση ή στην υλοποίηση: Η πιθανότητα σκόπιμης εισαγωγής κάποιας κερκόπορτας (back door) -η οποία είναι δύσκολο να ανιχνευθεί- δεν μπορεί να αποκλεισθεί για τους δημοσιευμένους αλγορίθμους. Κάτι τέτοιο όμως πρέπει να θεωρείται απίθανο για τους μυστικούς αλγορίθμους, εφόσον η σχεδίαση/υλοποίηση του αλγορίθμου και η κατασκευή του κρυπτοσυστήματος γίνονται από διαβαθμισμένο προσωπικό και υπό την αυστηρή επίβλεψη ενός εθνικού φορέα.

7. Πρώτο βήμα για κρυπτανάλυση: Η κρυπτανάλυση είναι εφικτή για τους δημοσιευμένους αλγορίθμους, ενώ για τους μυστικούς είναι ανέφικτη. Διότι όπως αναφέρθηκε στην παρ. 8.1, μόνο σε γνωστό αλγόριθμο μπορεί ένας κρυπταναλυτής να ξεκινήσει την ανάλυση και επίθεσή του.

8.3. Διεθνείς πρακτικές

Προς επιβεβαίωση των όσων αναφέρθηκαν, κλείνουμε το παρόν κεφάλαιο με την επισήμανση ότι το NATO και η Ευρωπαϊκή Ένωση, έχουν κατατάξει τους κρυπτογραφικούς αλγόριθμους σε τρεις κατηγορίες ασφαλείας A, B και C , όπως φαίνεται παρακάτω:

α. Τύπου Α (υψηλή ασφάλεια): Μη δημοσιευμένοι αλγόριθμοι, οι οποίοι είναι αναπτυγμένοι, αξιολογημένοι και εγκεκριμένοι υπό τον έλεγχο του αρμόδιου Εθνικού Φορέα, ευρίσκονται κάτω από αυστηρό κυβερνητικό έλεγχο και παραμένουν μυστικοί σε "need to know basis".

β. Τύπου Β (μέτρια ασφάλεια): Αλγόριθμοι (μυστικοί ή δημοσιευμένοι) οι οποίοι είναι σχεδιασμένοι από Εθνικό ή Ιδιωτικό Φορέα, και είναι αξιολογημένοι και εγκεκριμένοι από τον αρμόδιο Εθνικό Φορέα.

γ. Τύπου C (μικρή ασφάλεια): Αλγόριθμοι οι οποίοι δεν είναι εγκεκριμένοι από τον αρμόδιο Εθνικό Φορέα.

Στον Πίνακα 20, παραθέτουμε ενδεικτικά από ενημερωτικό φυλλάδιο εταιρείας **[38]**, τους βαθμούς ασφαλείας που έχει χορηγήσει το NATO σε συγκεκριμένη περίπτωση κρυπτοσυσκευής, όταν αυτή χρησιμοποιεί αλγόριθμο Τύπου Α και όταν χρησιμοποιεί αλγόριθμο Τύπου Β. Βλέπουμε ότι για αλγόριθμο Τύπου Β ο βαθμός ασφαλείας φθάνει έως Απόρρητος (NS-NATO Secret), ενώ για αλγόριθμο Τύπου Α ο βαθμός ασφαλείας φθάνει έως Άκρως Απόρρητος (CTS-Cosmic Top Secret).

Overview of CryptoIP products

				Encryption algorithms and accreditation level			
				NATO Type A	NATO Type B	Custom-ised	Dual
Encryptors	TCE 621/M		Tactical unit Ethernet (El/Opt) USB, RS-232	NS*	NS*	NS*	
	TCE 621/C		Gigabit Ethernet (El/Opt)	CTS	NS	NS	NS
	TCE 621/B		100 Mb/s Ethernet (El/Opt)	CTS	NS	NS	NS
	TCE 621/A		10 Mb/s Ethernet (El/Opt)	CTS			
Management tools	TCE 671 – SMC		Security Management Centre	✓	✓	✓	✓
	TCE 114 – KGC		Offline key generation centre for production of keys	✓	✓	✓	✓
	Config-Tool		PC application to support definition and loading of configuration data	✓	✓	✓	✓
	CVM		Customisation Vector Management. A tool that lets you define and load the customisation vector for the AES algorithm			✓	✓
	SW-Loader		PC application that enables to load software for the encryption devices	✓	✓	✓	✓

CTS = Cosmic Top Secret NS = NATO Secret * = in evaluation

Thales Norway AS
PO Box 6611 Etterstad
0609 Oslo - Norway
Tel.: +47 22 63 83 00
Telefax: +47 22 63 83 01
info@no.thalesgroup.com
www.thalesgroup.com

Πίνακας 20. Βαθμοί ασφαλείας που χορηγεί το NATO σε κρυπτοσυσκευές με Τύπου Α και Β αλγόριθμους (από ενημερωτικό φυλλάδιο εταιρείας).

Μία ταξινόμηση των κρυπτογραφικών αλγορίθμων αντίστοιχη με αυτή του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης, έχει κάνει και η υπηρεσία ασφαλείας NSA των ΗΠΑ, η οποία ως γνωστόν είναι η πλέον ισχυρή κρατική υπηρεσία επί θεμάτων κρυπτολογίας (βιβλ. **[39]**, **[40**).

Μετά από όσα αναφέρθηκαν, εξάγουμε το γενικό συμπέρασμα ότι οι δημοσιευμένοι κρυπτογραφικοί αλγόριθμοι πρέπει να θεωρούνται ότι όχι μόνο παρέχουν μικρότερο βαθμό ασφαλείας από τους μυστικούς, αλλά ενδεχομένως να είναι και επικίνδυνοι, διότι η χρήση τους μπορεί να εφησυχάσει και να παραπλανήσει τους χρήστες. Και τούτο διότι, με την ευρεία δημοσίευσή τους, πρέπει να θεωρηθεί δεδομένο ότι οι δημοσιευμένοι αλγόριθμοι υφίστανται πολλές κρυπταναλυτικές επιθέσεις από υπηρεσίες ασφαλείας οι οποίες έχουν εμπειρία στην κρυπτανάλυση. Και βέβαια, οι υπηρεσίες αυτές δεν ανακοινώνουν τις επιτυχημένες κρυπταναλυτικές επιθέσεις τους στα διάφορα συνέδρια (όπως κάνουν διάφοροι ερευνητές), αλλά τις εκμεταλλεύονται κρυφά για την διάσπαση των κρυπτογραφημένων πληροφοριών του αντιπάλου. Απαραίτητη βέβαια προϋπόθεση είναι, οι μυστικοί κρυπταλγόριθμοι να είναι σχεδιασμένοι από μια υπηρεσία με υψηλή τεχνογνωσία και η οποία να εφαρμόζει αυστηρά μέτρα ασφαλείας που να αποτρέπουν την διαρροή του αλγορίθμου.

ΚΕΦΑΛΑΙΟ 9

ΠΡΟΤΥΠΟ ΑΞΙΟΛΟΓΗΣΗΣ FIPS 140-2 (NIST / USA)

Στα Κεφάλαια 9 και 10 θα αναφέρουμε τους κυριότερους Εθνικούς και Διεθνείς Κανονισμούς και Πρότυπα , οι οποίοι έχουν σχέση με την αξιολόγηση των κρυπτογραφικών συστημάτων. Σημειώνουμε ότι οι παρακάτω κανονισμοί αφορούν κυρίως ελέγχους φυσικής και λειτουργικής ασφάλειας και δεν περιλαμβάνουν αξιολόγηση του κρυπτογραφικού αλγορίθμου. Είναι όμως σημαντικοί στο είδος τους, για αυτό είναι πολύ χρήσιμο να τους συμβουλεύονται όσοι αξιολογούν κρυπτογραφικά συστήματα.

Αξιολόγηση κρυπτογραφικών μονάδων με το πρότυπο FIPS 140-2

Ο οργανισμός **NIST** (National Institute of Standards and Technology) των ΗΠΑ, εκδίδει πολλούς κανονισμούς γύρω από την ασφάλεια των πληροφοριών, την ασφάλεια των επικοινωνιών και την κρυπτογραφία. Ένας κανονισμός ο οποίος είναι σχετικός με την παρούσα μελέτη, είναι ο **FIPS 140-2** (SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES), βιβλ. **[26]**. Ο κανονισμός αυτός αφορά κυρίως την αξιολόγηση της λειτουργικής και φυσικής ασφάλειας των πάσης φύσεως κρυπτογραφικών μονάδων, οι οποίες συνήθως ενσωματώνονται σε συστήματα τηλεπικοινωνιών ή σε συστήματα ηλεκτρονικών υπολογιστών. Παρακάτω αναφέρουμε πολύ περιληπτικά τις βασικότερες διαδικασίες και ελέγχους τους οποίους προδιαγράφει ο FIPS 140-2.

α. Διαδικασίες: Οι αξιολογήσεις διεξάγονται από ειδικά εθνικά διαπιστευμένα εργαστήρια (Nationally Accredited Labs), τα οποία εφαρμόζουν τον κανονισμούς FIPS 140-2. Μετά από κάθε αξιολόγηση, ο Εθνικός Οργανισμός Πιστοποίησης Ασφαλείας (National Information Assurance Body), αφού λάβει υπόψη του την τεχνική αναφορά του διαπιστευμένου εργαστηρίου, εκδίδει την τελική πιστοποίηση για το αξιολογούμενο σύστημα. Κατά την αξιολόγηση, οι κρυπτογραφικές μονάδες βαθμολογούνται εντός τεσσάρων Επίπεδων Ασφαλείας (Security Levels 1, 2, 3, 4). Οι κρυπτογραφικές μονάδες από κατασκευαστικής πλευράς, ταξινομούνται σε τρεις κατηγορίες:

α) Single chip
β) Multiple chip embedded
γ) Multiple chip stand alone

β. Κατηγορίες διεξαγόμενων ελέγχων : Ο κανονισμός FIPS 140-2 δεν υπεισέρχεται σε αξιολόγηση αλγορίθμων. Ωστόσο, διεξάγει επί των κρυπτογραφικών μονάδων σημαντικούς ελέγχους λειτουργικής και φυσικής ασφάλειας, οι οποίοι σε πολύ γενικές γραμμές αφορούν τα εξής θέματα:

- Γενικές τεχνικές και φυσικές προδιαγραφές της κρυπτογραφικής μονάδας. Χρήση εγκεκριμένων αλγορίθμων και αντίστοιχων τρόπων λειτουργίας τους (modes of operation).
- Αναλυτική περιγραφή των υπομονάδων (hardware, software, firmware) και της πολιτικής ασφαλείας της κρυπτογραφικής μονάδας.

- Προδιαγραφές όλων των απαιτούμενων και των προαιρετικών διασυνδέσεων και των διαδρομών εισόδου-εξόδου (interfaces and input – output data paths). Λογικός διαχωρισμός των θυρών (data ports) των μη προστατευμένων κρισίμων παραμέτρων από τις υπόλοιπες θύρες δεδομένων.
- Καθήκοντα χρηστών, υπηρεσίες και αυθεντικότητα (roles, services and authentication). Διαχωρισμός απαιτούμενων και προαιρετικών καθηκόντων. Έλεγχοι αυθεντικότητας βάσει του καθήκοντος (role) ή της ταυτότητας (identity) του χειριστή.
- Έλεγχοι πρόσβασης (access controls) και έλεγχος ενεργειών (auditing).
- Ανίχνευση παραβίασης και προστασία έναντι παραβίασης (tamper detection, protection and response).
- Αυτόματος μηδενισμός κρυπτο-παραμέτρων σε έκτακτες περιπτώσεις (automatic zeroization).
- Αυτό-έλεγχοι (self tests): Με την έναρξη λειτουργίας (power up), αυτόματος έλεγχος ακεραιότητας του αλγορίθμου, έλεγχοι ακεραιότητας υλικού και λογισμικού, έλεγχοι κρισίμων λειτουργιών κλπ.
- Στατιστικοί έλεγχοι τυχαιότητας στις RNG, κατόπιν εντολής (στο Level 3) ή αυτόματα με την έναρξη λειτουργίας - power up (στο Level 4).
- Διαχείριση Κλειδών (Cryptographic Key Management) : Παραγωγή τυχαίων αριθμών (RNG) και κρυπτογραφικών κλειδών, ηλεκτρονική ανταλλαγή και αναγνώριση κλειδών (key establishment), διανομή και εισαγωγή των κλειδών, αποθήκευση και μηδενισμός των κλειδών.
- Διαχείριση Δομής (Configuration Management) των λειτουργικών απαιτήσεων και προδιαγραφών από πλευράς του κατασκευαστή.
- Έλεγχοι Ηλεκτρομαγνητικών Παρεμβολών (EMI) και Ηλεκτρομαγνητικής Συμβατότητας (EMC).
- Έλεγχοι για Μεθοδικό Σχεδιασμό (Design Assurance), με επίσημα μοντέλα λειτουργίας (formal models), έλεγχοι για αναλυτική τεκμηρίωση κλπ.

γ. Απαιτήσεις ανά επίπεδο ασφαλείας: Οι απαιτήσεις ασφαλείας του FIPS 140-2 φαίνονται συνοπτικά στους Πίνακες 21 και 22 και τις περιγράφουμε παρακάτω πολύ περιληπτικά ανά επίπεδο ασφαλείας. Σημειώνουμε ότι κάθε ανώτερο επίπεδο ασφαλείας περιλαμβάνει όλα τα μέτρα ασφαλείας του προηγούμενου επιπέδου και προσθέτει ορισμένα αυστηρότερα μέτρα:

Το Επίπεδο Ασφαλείας 1 είναι αρκετά απλό, με τη μοναδική απαίτηση οι κρυπτογραφικές μονάδες να χρησιμοποιούν πιστοποιημένους αλγόριθμους, χωρίς να απαιτείται κανενός είδους φυσική ασφάλεια. Παράδειγμα μιας κρυπτογραφικής μονάδας Επιπέδου Ασφαλείας 1, είναι μια κάρτα κρυπτογράφησης σε ένα κοινό ηλεκτρονικό υπολογιστή (PC encryption board).

Το Επίπεδο Ασφαλείας 2 προσθέτει απαιτήσεις για απόδειξη παραβίασης φυσικής ασφάλειας (physical tamper evidence). Αυτές μπορούν να υλοποιηθούν με σφραγίσματα ή κλειδώματα στα καλύμματα και στις φυσικές θύρες των modules, καθώς και με αδιαφανή επικάλυψη πάνω στα ολοκληρωμένα κυκλώματα (opaque tamper-evident coating). Αυτές οι απαιτήσεις παρέχουν προστασία των Κρίσιμων Παραμέτρων Ασφαλείας

(Critical Security Parameters -CSP), οι οποίες περιλαμβάνουν τις κρυπτογραφικές κλείδες, καθώς και τα στοιχεία αυθεντικότητας (passwords, PIN κλπ.). Επίσης, το Επίπεδο Ασφαλείας 2 απαιτεί ένα απλό στοιχείο αυθεντικότητας, όπως π.χ. ένα password (role-based authentication).

Το Επίπεδο Ασφαλείας 2 επιτρέπει στο software και firmware της κρυπτογραφικής μονάδας να εκτελεστούν σε ένα γενικής χρήσης ηλεκτρονικό υπολογιστή, του οποίου όμως το λειτουργικό σύστημα πρέπει να είναι πιστοποιημένο τουλάχιστον στο επίπεδο EAL2 (σύμφωνα με το πρότυπο ISO15408/ Common Criteria το οποίο θα εξεταστεί στο επόμενο Κεφάλαιο 10).

Το Επίπεδο Ασφαλείας 3, αντί για απλή απόδειξη παραβίασης, απαιτεί ανίχνευση και αντίσταση σε παραβιάσεις (tamper resistance), ώστε να αποτρέψει την πρόσβαση των εισβολέων στις Κρίσιμες Παραμέτρους Ασφαλείας (CSP). Η απαίτηση για επικάλυψη των ολοκληρωμένων κυκλωμάτων γίνεται ακόμα πιο αυστηρή, με σκληρά κεραμικά υλικά (hard opaque potting material). Επίσης, προσθέτει και απαιτήσεις για τον ασφαλή τρόπο μεταφοράς των CSP εντός και εκτός των modules. Τέλος, απαιτεί έλεγχο αυθεντικότητας βάσει της ταυτότητας του χρήστη (identity-based user authentication).

Το Επίπεδο Ασφαλείας 3 επιτρέπει στο software και firmware της κρυπτογραφικής μονάδας να εκτελεστούν σε ένα γενικής χρήσης ηλεκτρονικό υπολογιστή, του οποίου όμως το λειτουργικό σύστημα πρέπει να είναι πιστοποιημένο τουλάχιστον στο επίπεδο EAL3 (σύμφωνα με το πρότυπο ISO15408/ Common Criteria).

Το Επίπεδο Ασφαλείας 4, απαιτεί επιπρόσθετους μηχανισμούς φυσικής ασφάλειας οι οποίοι να αντιδρούν σε προσπάθειες μη εξουσιοδοτημένης φυσικής πρόσβασης. Όταν το module ανιχνεύσει μία προσπάθεια παραβίασης, κάθε ανοικτό (μη κρυπτογραφημένο) κείμενο που περιέχει Κρίσιμες Παραμέτρους Ασφαλείας πρέπει να «επιγραφτεί» με μηδενικά (overwritten with zeros -zeroized). Τα modules πρέπει επίσης να ανθίστανται σε περιβαλλοντολογικές επιθέσεις (σκόπιμες θερμοκρασιακές και ηλεκτρικές διακυμάνσεις για να μειωθούν οι αμυντικοί μηχανισμοί τους), ώστε να μπορούν να χρησιμοποιηθούν και σε μη προστατευμένα περιβάλλοντα (π.χ. εκτός διαβαθμισμένων χώρων). Τέλος, προσθέτει την απαίτηση για διπλό τρόπο ελέγχου αυθεντικότητας, δηλαδή ουσιαστικά την χρήση βιομετρικής αναγνώρισης ή φυσικών εμβλημάτων (tokens) επιπροσθέτως του password.

Το Επίπεδο Ασφαλείας 4 επιτρέπει στο software και firmware της κρυπτογραφικής μονάδας να εκτελεστούν σε ένα γενικής χρήσης ηλεκτρονικό υπολογιστή, του οποίου όμως το λειτουργικό σύστημα πρέπει να είναι πιστοποιημένο τουλάχιστον στο επίπεδο EAL3 (σύμφωνα με το πρότυπο ISO15408/ Common Criteria).

Το νέο Επίπεδο Ασφαλείας 5, το οποίο σχεδιάζεται να προστεθεί στον αναβαθμισμένο κανονισμό FIPS 140-3, προσθέτει απαιτήσεις για προστασία από ηλεκτρομαγνητικές επιθέσεις (EMI attacks), προστασία από εξέταση μέσω μη ορατών ακτινοβολιών (π.χ. ακτίνες-Χ), καθώς και κρυπτογράφηση / αυθεντικοποίηση όλων των αποθηκευμένων παραμέτρων ασφαλείας.

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP and EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.		Statistical RNG tests – callable on demand.	Statistical RNG tests – performed at power-up.
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Πίνακας 21. Συνοπτικές απαιτήσεις ασφαλείας του FIPS 140-2

	General Requirements for all Embodiments	**Single-Chip Cryptographic Modules**	**Multiple-Chip Embedded Cryptographic Modules**	**Multiple-Chip Standalone Cryptographic Modules**
Security Level 1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
Security Level 4	EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/ response envelope with tamper response and zeroization circuitry.

Πίνακας 22. Συνοπτικές απαιτήσεις φυσικής ασφαλείας του FIPS 140-2

ΚΕΦΑΛΑΙΟ 10

ΠΡΟΤΥΠΟ ΑΞΙΟΛΟΓΗΣΗΣ ISO/IEC 15408 (Common Criteria)

ΔΙΕΘΝΗ ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΡΟΪΟΝΤΩΝ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

10.1 Γενικά

Τα Κοινά Κριτήρια CC (Common Criteria ή CC) έχουν καθιερωθεί ως διεθνές πρότυπο (ISO 15408), καθορίζουν τις τεχνικές διαδικασίες και τις μεθοδολογίες για την αξιολόγηση της ασφάλειας των διαφόρων προϊόντων τεχνολογίας πληροφορικής (IT-Information Technology). Τα προϊόντα αυτά μπορεί να είναι πάσης φύσεως συστήματα ηλεκτρονικής επεξεργασίας πληροφοριών σε υλικό ή λογισμικό (software/hardware), όπως είναι λειτουργικά συστήματα Η/Υ, κρυπτογραφικά συστήματα, firewalls, συστήματα VPN, συστήματα ανίχνευσης εισβολών (IDS), συστήματα αυτόματης αναγνώρισης και αυθεντικότητας, smart cards, βιομετρικά συστήματα κλπ.

Όπως φαίνεται αναλυτικά στην ενδεικτική βιβλιογραφία **[41], [42], [43]**, τα Κοινά Κριτήρια (CC) για την αξιολόγηση της ασφάλειας της πληροφορικής τεχνολογίας, έχουν αναπτυχθεί κυρίως, για να υποστηρίξουν την αξιολόγηση των γενικών ιδιοτήτων ασφάλειας προϊόντων και συστημάτων πληροφορικής τεχνολογίας. Αποτελούν τη βάση για τον καθορισμό της αποδοτικότητας των λειτουργιών ασφαλείας και το επίπεδο αξιοπιστίας, το οποίο οι χρήστες μπορούν να έχουν, με την σωστή υλοποίηση των παραπάνω λειτουργιών. Ο στόχος των CC είναι ο καθορισμός κάποιων κοινών κριτηρίων, με τα οποία θα αξιολογείται οποιοδήποτε σύστημα πληροφορικής τεχνολογίας, και θα εξετάζεται αν αυτό πληροί, και σε πιο βαθμό, τις προδιαγραφές ασφαλείας που έχει θέσει ο χρήστης, ανάλογα με τις απαιτήσεις του

Τα CC δίνουν κριτήρια τεχνικής αξιολόγησης και μόνο, χωρίς να εξετάζουν τις μεθόδους αξιολόγησης ή το διαχειριστικό ή νομικό πλαίσιο, κάτω από το οποίο αυτά μπορεί να εφαρμοσθούν. Επίσης, οι κρυπτογραφικοί αλγόριθμοι καθώς και η προστασία από ηλεκτρομαγνητικές ακτινοβολίες, θεωρούνται πολύ εξειδικευμένα θέματα και δεν καλύπτονται από τα CC.

Οι Υπηρεσίες των τεχνολογικά προηγμένων χωρών (ΗΠΑ, Καναδάς, Αγγλία, Γαλλία, Γερμανία, Αυστραλία) έχουν αναπτύξει Εθνικά εργαστήρια ή έχουν συνάψει συμβάσεις με διαπιστευμένα ιδιωτικά εργαστήρια για να διεξάγουν τις αξιολογήσεις (ονομαζόμενα ως accredited labs ή evaluation facilities ή CLEF). Μετά από την αξιολόγηση, εκδίδεται το τελικό πιστοποιητικό από τον Εθνικό Οργανισμό Πιστοποίησης της εκάστοτε χώρας (Certification Body ή CB), η οποία εποπτεύει και ελέγχει τις εργασίες των εργαστηρίων. Τα επίπεδα αξιολόγησης ασφάλειας (Evaluation Assurance Levels) είναι επτά, από EAL1(μικρότερο) έως EAL7 (μεγαλύτερο). Τα πιστοποιημένα προϊόντα ανακοινώνονται επίσημα από κάθε χώρα και υπάρχουν ειδικοί δικτυακοί τόποι (websites) όπου μπορούν οι ενδιαφερόμενοι να ανατρέξουν για να πληροφορηθούν σχετικά.

Το υπό εξέταση προϊόν ή σύστημα IT συνοδευόμενο από τα έγγραφα λειτουργίας του για τον διαχειριστή και τον χρήστη, θα αναφέρεται ως Στόχος της Αξιολόγησης (Target Of Evaluation) ή συντομογραφικά ως TOE.

Το σύνολο των απαιτήσεων και προδιαγραφών οι οποίες χρησιμοποιούνται ως βάση για την αξιολόγηση ενός TOE, ονομάζεται Στόχος Ασφαλείας (Security Target) ή συντομογραφικά ως ST.

Σύμφωνα με τα παραπάνω, τα Common Criteria εξετάζουν τις ιδιότητες και προδιαγραφές ασφαλείας ενός συστήματος, όπως παρουσιάζονται στα τέσσερα παρακάτω επίπεδα:

α. Σκοπός της ασφάλειας του TOE (Purpose of the TOE security): Περιλαμβάνει τις προδιαγραφές ασφαλείας τις οποίες το TOE σκοπεύει να επιτύχει, τους κινδύνους ή απειλές, τα οποία θα αντιμετωπίσει, προϋποθέσεις για το περιβάλλον μέσα στο οποίο θα λειτουργήσει, καθώς και τρόπους χρήσης με τους οποίους θα γίνει αξιοποίηση του TOE.

β. Απαιτήσεις ασφάλειας του TOE (Security requirements of the TOE): Είναι οι απαιτήσεις ασφαλείας του TOE, ώστε να πληροί τον σκοπό που έχει δηλωθεί.

γ. Προδιαγραφές ασφαλείας του TOE (Security specifications of the TOE): Είναι οι ακριβείς προδιαγραφές των λειτουργιών ασφαλείας και των εξασφαλίσεων (assurances) που προσφέρονται από το TOE, έτσι ώστε να πληροί τις απαιτήσεις ασφαλείας που έχουν δηλωθεί.

δ. Περιγραφή του TOE, το οποίο είναι το πλήρες σύστημα ή προϊόν το οποίο υλοποιεί τις προδιαγραφές ασφαλείας.

10.2. Διαδικασίες αξιολόγησης

Αφού παρθεί η απόφαση να ζητηθεί η αξιολόγηση, ο Οργανισμός Πιστοποίησης (CB) ή οποιοδήποτε διαπιστευμένο Εργαστήριο Αξιολόγησης (Commercially Licensed Evaluation Facility - CLEF), μπορούν να δώσουν συμβουλές και να βοηθήσουν στην προετοιμασία του προϊόντος για την αξιολόγηση. Η διαδικασίες συνοπτικά είναι οι εξής:

-Ο κατασκευαστής ορίζει αποδεικτικά στοιχεία, συμπεριλαμβανομένης της τεχνικής υποστήριξης.

-Το CLEF κάνει εκτίμηση του προϊόντος ενάντια στον στόχο ασφάλειας.

-Το CLEF εκδίδει αναφορές προβλημάτων και τις γνωστοποιεί στον Οργανισμό Πιστοποίησης.

-Ο κατασκευαστής επιλύει τα προβλήματα.

-Τα έγγραφα του CLEF εκδίδονται καθώς η εργασία προχωρά.

-Το CLEF ολοκληρώνει την αξιολόγηση και υποβάλει την τεχνική του αναφορά ETR (Evaluation Technical Report) στον Οργανισμό Πιστοποίησης και στον κατασκευαστή.

-Ο Οργανισμός Πιστοποίησης αναθεωρεί την ETR για να επιβεβαιώσει ότι η πιστοποίηση μπορεί να προχωρήσει.

-Εκδίδεται το Πιστοποιητικό.

-Εφαρμόζεται σχέδιο για την διατήρηση της Πιστοποίησης.

10.2.1. Προετοιμασία

Καθορισμός του προϊόντος προς αξιολόγηση

Μπορεί να υπάρχουν διαφορετικές εκδοχές για την παραγωγή και προετοιμασία ενός προϊόντος. Η αξιολόγηση μπορεί να αρχίσει με μια έκδοση ενός προϊόντος και μετά να συνεχίσει με μια δεύτερη έκδοση. Ενδεχομένως, τμήματα του προϊόντος μπορεί να έχουν ήδη αξιολογηθεί με διαφορετικούς συνδυασμούς - π.χ. με Βρετανικό πρότυπο (ITSEC) ή το Αμερικάνικο (US TCSEC). Σε μερικές περιπτώσεις, η απόδειξη προηγούμενου ελέγχου μπορεί να ενσωματωθεί σε νέες αξιολογήσεις προς μείωση του κόστους και του χρόνου. Λαμβάνουμε υπ'όψη ότι η Πιστοποίηση CC θα εφαρμοστεί μόνο στην επίσημη έκδοση του προϊόντος στην ελεγμένη του δομή, η οποία εξακολουθεί να υποστηρίζεται από καθορισμένα προγράμματα.

Καθορισμός της λειτουργικότητας

Η λειτουργικότητα που απαιτείται εξαρτάται από τις απαιτήσεις της αγοράς και θα αναπτυχθεί παράλληλα με τις αισθητές απειλές. Οι πελάτες θα έχουν τις δικές τους απαιτήσεις οι οποίες μπορεί να ορίζονται σε ένα Προστατευτικό Προφίλ.

Καθορισμός του απαιτούμενου επιπέδου ασφαλείας

Όπως αναφέρθηκε, αυτά κατατάσσονται από το EAL1 έως το EAL7. Το κάθε επίπεδο ασφάλειας που ορίζεται, αυξάνει τις απαιτήσεις για υψηλότερο επίπεδο σχεδίασης, τεκμηρίωσης και απόδειξης (proof), καθώς το βάθος του ελέγχου.

Κόστος της αξιολόγησης

Τα CLEF είναι ανταγωνιστικοί εμπορικοί οργανισμοί και πρέπει να αμειφθούν για την υπηρεσίες τους. Επομένως πριν κάθε αξιολόγηση, μπορούν να ληφθούν προσφορές και να συγκριθούν προσεκτικά πριν γίνει μια επιλογή. Επίσης ο Οργανισμός Πιστοποίησης (CB) είναι ένας Κυβερνητικός Οργανισμός και απαιτείται να καλύπτει τα έξοδά του. Ένα ερωτηματολόγιο μπορεί να τεθεί από το CB και μπορεί να δοθεί μια προσφορά για υπηρεσίες πιστοποίησης, βασισμένη στις παρεχόμενες πληροφορίες.

Προετοιμάζοντας την απόδειξη

Μερικές από τις απαιτήσεις, όπως η σχεδίαση της τεκμηρίωσης, είναι ένα κανονικό προϊόν του κύκλου ανάπτυξης. Η παραγωγή ενός Στόχου Ασφάλειας είναι ένα κλειδί, τμήμα της πορείας αξιολόγησης. Μέσα σε αυτό ο developer καθορίζει τις λειτουργίες ασφάλειας και τα μέτρα ασφάλειας που υπολογίζονται στην αξιολόγηση. Ο Στόχος Ασφάλειας θα γίνει ένα δημοσίως διαθέσιμο έγγραφο, ώστε οι χρήστες να δουν ακριβώς ποιά τμήματα του προϊόντος έχουν αξιολογηθεί και να τα προσαρμόσουν στις δικές τους ανάγκες ασφάλειας (οι αξιολογούμενοι μπορούν να συνεργαστούν με τους αξιολογητές για να μην αποκαλυφθούν τυχόν εμπιστευτικές τους πληροφορίες). Οι συμβουλές είναι πάντα διαθέσιμες είτε από το CLEF, είτε από ένα ανεξάρτητο ειδικό, για να βοηθήσουν στην παραγωγή του Στόχου Ασφάλειας ή στην αναθεώρηση άλλων υποψηφίων προϊόντων πριν την αξιολόγηση.

10.2.2. Αξιολόγηση

Αφού δεσμεύθηκε ένα CLEF και συμφώνησε με τον Οργανισμό Πιστοποίησης στην καταλληλότητα του προϊόντος για αξιολόγηση, τότε η πορεία ελέγχου αρχίζει να υλοποιείται. Υπάρχουν αρκετά στάδια αξιολόγησης που καλύπτουν τις ακόλουθες δραστηριότητες:

- Παραγωγή Προγράμματος Εργασίας Αξιολόγησης. Εδώ αναγνωρίζονται τα διάφορα στάδια εργασίας που εκτελούνται. Το χρονικό διάγραμμα που έχει σχεδιαστεί για τον έλεγχο, πρέπει να είναι ρεαλιστικό.
- Εκτίμηση του Στόχου Ασφαλείας για το TOE. Αυτό είναι βασικό, καθώς όλες οι εργασίες αξιολόγησης εκτελούνται έναντι αυτού του εγγράφου. Ο Στόχος Ασφαλείας πρέπει να είναι καθαρός, συνεπής και να αποδεικνύει πως ο TOE μετράει τις αναγνωρίσιμες απειλές. Περιλαμβάνει τα εξής βασικά στοιχεία:
- Βεβαίωση της Ορθότητας του Συστήματος.
- Έλεγχος για Απόδειξη της Ασφάλειας.
- Εκτίμηση του Περιβάλλοντος Ανάπτυξης.
- Εκτίμηση του Επιχειρησιακού Περιβάλλοντος.
- Έλεγχος για γνωστές ευπάθειες.
- Έλεγχος διείσδυσης.
- Παραγωγή περιεκτικών αναφορών αξιολόγησης.

Συνιστάται, ο developer ή ο σπόνσορας να ορίσει έναν project manager για να συντονίσει όλες τις δραστηριότητες αξιολόγησης. Η εμπειρία έχει δείξει ότι η στενή συνεργασία μεταξύ του CLEF και του developer είναι το κλειδί για μία ομαλή αξιολόγηση και ένα καθαρό και συγκεκριμένο σημείο επαφής που διευκολύνει αυτή τη συνεργασία.

Καθώς προχωρά ο έλεγχος, οι αξιολογητές παράγουν λεπτομερείς αναφορές για τις εκτιμήσεις και τα αποτελέσματα που ισχύουν. Τα μικρά λάθη που ανακαλύπτονται κατά τη διάρκεια του ελέγχου αναφέρονται στις αναφορές παρατηρήσεων. Αυτές εφοδιάζουν με χρήσιμο υλικό τα σημεία των υψηλών προβλημάτων. Η επίδραση αυτών των λαθών κατανέμεται από τα συμφραζόμενα στο πως χρησιμοποιείται το προϊόν και σημειώνεται κάθε συμβουλή του developer για την διόρθωση του λάθους. Αν οι αξιολογητές ανακαλύψουν ελαττώματα τα οποία μπορεί να εκμεταλλευτεί ένας εισβολέας, θα πρέπει να ενημερωθεί ο Οργανισμός Πιστοποίησης. Η πολιτική θα πρέπει να είναι ότι, αυτά τα ελαττώματα πρέπει να διορθωθούν πριν εκδοθεί η πιστοποίηση.

Είναι δυνατόν να υπάρχουν και αναφορές παρατηρήσεων για ένα προϊόν οι οποίες δεν έχουν άμεση επίδραση, αλλά μπορεί να είναι σημαντικές σε μελλοντικές αξιολογήσεις. Μπορεί, επίσης, να περιέχουν σχόλια για το περιβάλλον ανάπτυξης ή περιπτώσεις ασυνήθιστων πρακτικών κωδικοποίησης. Τέτοια προβλήματα δεν είναι απαραιτήτως εμπόδιο για την πιστοποίηση.

Προστατευτικό Προφίλ (Protection Profile)

Το Προστατευτικό Προφίλ (Protection Profile) είναι μια ομάδα από απαιτήσεις ασφαλείας, η οποία είναι ανεξάρτητη από συγκεκριμένα προϊόντα ή

συστήματα και αφορά μια κατηγορία από TOE τα οποία καλύπτουν συγκεκριμένες ανάγκες των χρηστών. Συνήθως αποτελείται από :

Έναν κατάλογο απειλών

Έναν κατάλογο λειτουργικών απαιτήσεων

Έναν κατάλογο δραστηριοτήτων ασφάλειας

Ένα αιτιολογικό ότι αυτά απευθύνονται στην απειλή.

Τα Προστατευτικά Προφίλ μπορεί να έχουν σχεδιαστεί από μια ομάδα μελλοντικών καταναλωτών, οι οποίοι έχουν παρόμοιες IT ανάγκες ασφάλειας, ή από τον ίδιο τον developer λογισμικού.

Ένα Προστατευτικό Προφίλ δεν συνδέεται με κανένα δεδομένο προϊόν ή σύστημα, μάλλον καθορίζει τις ανάγκες ενός χρήστη ανεξάρτητα από κάθε συγκεκριμένο προϊόν. Η Πιστοποίηση ενός Προστατευτικού Προφίλ, θα διευκρινίσει τον βαθμό στον οποίο έχουν εκπληρωθεί οι απαιτήσεις του Προφίλ.

Τα Προστατευτικά Προφίλ είναι ιδιαιτέρως χρήσιμα γιατί βοηθούν στην διατύπωση των επιθυμητών προδιαγραφών. Από τους διάφορους χρήστες και κατασκευαστές έχουν εκπονηθεί πολλά είδη Προστατευτικών Προφίλ και προετοιμάζονται ακόμη περισσότερα. Τα Προστατευτικά Προφίλ που έχουν ήδη εκδοθεί, περιλαμβάνουν τις εξής γενικές κατηγορίες:

Έλεγχοι Πρόσβασης (access control systems).

Σηματοδότηση Ασφαλείας (security marking).

Βάσεις δεδομένων (Database Management Systems)

Προστασία δικτύων (Firewall κλπ.).

Έξυπνες κάρτες (smart cards).

10.3. Πιστοποίηση

Ο Οργανισμός Πιστοποίησης δρα σε όλα τα στάδια της αξιολόγησης, αν και ο πολύς όγκος της εργασίας γίνεται από το CLEF και τον developer. Ο Οργανισμός Πιστοποίησης εγκρίνει τον Στόχο Ασφάλειας και τα Προγράμματα Εργασίας Αξιολόγησης. Με εξαίρεση τις αξιολογήσεις EAL1, ο Πιστοποιητής παρίσταται σε ένα meeting έναρξης εργασιών με το CLEF και τον developer, προκειμένου να συζητηθεί η αξιολόγηση και να συμφωνηθούν τα προγράμματα δραστηριοτήτων. Εδώ, μπορεί να εντοπισθούν προβλήματα δυνατοτήτων και να συμφωνηθούν πράξεις για την αντιμετώπισή τους.

Καθώς ο έλεγχος προχωρά, ο Πιστοποιητής παρακολουθεί τις ανειλημμένες δραστηριότητες και εξετάζει όλες τις αναφορές παρατηρήσεων μαζί με τα αποτελέσματά τους. Ένας βασικός ρόλος του Οργανισμού Πιστοποίησης είναι να ελέγξει ότι η αξιολόγηση διεξάγεται σύμφωνα με την διατυπωμένη στα Κοινά Κριτήρια μεθοδολογία. Η οριζόμενη απόδειξη πρέπει να υποστηρίζει τα συμπεράσματα της αξιολόγησης και πρέπει να διεξάγεται ο κατάλληλος έλεγχος έτσι ώστε να αιτιολογεί το απαιτούμενο επίπεδο ασφάλειας της αξιολόγησης.

Ο Πιστοποιητής μπορεί να παρίσταται σε ένα ή περισσότερα meeting για την πρόοδο της αξιολόγησης, όπου μπορεί να αναθεωρηθεί η διεξαγωγή της αξιολόγησης. Σε πολύπλοκες αξιολογήσεις, μπορεί να συμφωνούνται νέα

εργασιακά προγράμματα. Επίσης, ο Πιστοποιητής παρίσταται και στους ελέγχους διείσδυσης (penetration tests).

Κατά την πορεία της αξιολόγησης, κυριαρχεί η προετοιμασία της Αναφοράς Τεχνικής Αξιολόγησης από το CLEF. Αυτή συγκεντρώνει όλα τα ευρήματα του CLEF και παρουσιάζει την απόδειξη του ελέγχου. Κατόπιν, η Αναφορά Τεχνικής Αξιολόγησης αποστέλλεται στον Οργανισμό Πιστοποίησης.

Ο Πιστοποιητής επανεξετάζει την Αναφορά Τεχνικής Αξιολόγησης και κάνει σχόλια, στα σημεία όπου είναι ίσως αναγκαία μια συμπληρωματική εξήγηση ή τα αποτελέσματα ελέγχου είναι ασαφή. Εξετάζονται όλες οι επίσημες αποδείξεις που δίδονται από τους αξιολογητές, και τα αποτελέσματα του ελέγχου συγκρίνονται με τον Στόχο Ασφαλείας για να εξασφαλιστεί ότι όλοι οι αντικειμενικοί σκοποί έχουν επιτευχθεί. Τα σχόλια δίδονται στο CLEF και στον developer και εκτιμούνται οι απαιτήσεις τους. Όταν ο Πιστοποιητής μείνει ικανοποιημένος με τον όγκο των αποδείξεων που του παρουσιάστηκε, συντάσσει μια Αναφορά Πιστοποίησης και εκδίδεται το Πιστοποιητικό.

10.4. Επαναξιολόγηση και Διατήρηση Πιστοποίησης

Αναπόφευκτα, τα ΙΤ προϊόντα αναπτύσσονται και είναι λογικό να κάνουν κάποιες βελτιωτικές τροποποιήσεις μετά την Πιστοποίηση. Ο Οργανισμός Πιστοποίησης συμβουλεύει αν μια επαναξιολόγηση είναι αναγκαία, όταν ένα προϊόν έχει τροποποιηθεί. Η ανάλογη εργασία μπορεί να μειωθεί κατά την διάρκεια της πρώτης αξιολόγησης, ταξινομώντας τα συστατικά του προϊόντος σύμφωνα με την επιρροή τους στα χαρακτηριστικά ασφάλειας. Όποτε γίνονται αλλαγές σε αξιολογημένα προϊόντα, ο developer μπορεί να χρησιμοποιήσει την ταξινόμηση για να καθορίσει ευκολότερα την επίδραση στην πιστοποίηση και να αναγνωρίσει κατάλληλη δράση.

Ευπάθειες μπορεί να ανακαλυφθούν σε προϊόντα τα οποία έχουν ήδη αξιολογηθεί. Σε τέτοιες περιπτώσεις, είναι φυσιολογική πρακτική για τον developer να εκδώσει μια διόρθωση. Όταν ένα προϊόν βρίσκεται σε Σχέδιο Διατήρησης Πιστοποίησης, η έκδοση μιας ή περισσοτέρων διορθώσεων δεν αναιρεί την πιστοποίηση. Αυτό είναι συνέπεια ενός διαβαθμισμένου σχεδίου όπου ένα μέτριο επίπεδο ασφάλειας δεν εντοπίζει και δεν αφαιρεί όλες τις ευπάθειες. Επίσης, είναι ευνόητο ότι η ραγδαία εξέλιξη των προϊόντων και του περιβάλλοντος, εισάγουν την πιθανότητα οι ευπάθειες αυτές να μην είχαν αντιμετωπιστεί κατά την αρχική πιστοποίηση. Οι χώρες που συμμετέχουν στην ανάπτυξη των Κοινών Κριτηρίων αξιολόγησης (Common Criteria), έχουν σχεδιάσει μία μέθοδο διατήρησης της ασφάλειας, συγκρινόμενη με το Σχέδιο Διατήρησης Πιστοποίησης που εκδίδεται από τον εκάστοτε Οργανισμό Πιστοποίησης. Αυτή η διατήρηση έχει σχεδιαστεί να βρίσκεται υπό τον έλεγχο του developer, είτε απ'ευθείας είτε μέσω ενός CLEF.

10.5. Κατηγορίες Ασφάλειας και Λειτουργικότητας (Assurance and Functionality Classes)

Τα Κοινά Κριτήρια έχουν 11 κατηγορίες Λειτουργικότητας (Functionality) και 10 κατηγορίες Ασφάλειας (Assurance), οι οποίες φαίνονται στον Πίνακα 23.

Κάθε μία από αυτές τις κατηγορίες (classes), διασπάται σε οικογένειες (families) και μετά σε συστατικά (components). Αυτό παρέχει μεγάλη ευλυγισία στην περιγραφή των απαιτήσεων λειτουργίας και ασφάλειας.

Λειτουργικότητα	**Ασφάλεια**
1. Έλεγχος γεγονότων (audit) 2. Επικοινωνίες 3. Κρυπτογραφική Υποστήριξη 4. Προστασία Δεδομένων Χρήστη 5. Αναγνώριση και Αυθεντικότητα 6. Μυστικότητα 7. Προστασία των Λειτουργιών Ασφάλειας του TOE 8. Εκμετάλλευση των Πόρων 9. Διαχείριση Ασφάλειας 10. Πρόσβαση (access) στον TOE 11. Εμπιστευτικές Δίοδοι/Κανάλια	1. Αξιολόγηση Προστατευτικού Προφίλ 2. Αξιολόγηση Στόχου Ασφάλειας 3. Διαχείριση Δομής (Configuration Management) 4. Παράδοση και Λειτουργία 5. Ανάπτυξη 6. Έγγραφα οδηγιών 7. Υποστήριξη Κύκλου Ζωής 8. Διατήρηση Πιστοποίησης 9. Έλεγχοι του κατασκευαστή 10. Εκτίμηση Ευπάθειας

Πίνακας 23. Κατηγορίες Ασφάλειας και Λειτουργικότητας των Common Criteria (Assurance and Functionality Classes)

10.6. Επίπεδα Ασφάλειας (Assurance Levels)

Τα Κοινά Κριτήρια έχουν επτά Επίπεδα Ασφάλειας ή Επίπεδα Εμπιστοσύνης (Evaluation Assurance Levels - EAL), από το κατώτερο EAL1 έως το ανώτερο EAL7. Αυτά τα επίπεδα είναι σχεδιασμένα να τροφοδοτούν μια ισορροπημένη δέσμη στοιχείων ασφάλειας για γενική χρήση. Τα επίπεδα αυτά αντιπροσωπεύουν ανερχόμενους βαθμούς εμπιστοσύνης (assurance), σε ότι αφορά την αποδοτικότητα και την αξιοπιστία των λειτουργιών ασφαλείας του Στόχου Αξιολόγησης (TOE). Όσο υψηλότερο είναι το επίπεδο, τόσο μεγαλύτερος είναι ο βαθμός αυστηρότητας που εφαρμόζεται όταν ο TOE έχει ανταποκριθεί στις απαιτήσεις ασφάλειάς του, π.χ., εντείνοντας την ανάλυση και την έρευνα για ευπάθειες ασφάλειας.

EAL 1 - Λειτουργικός Έλεγχος (Functional Check)

Το EAL 1 εφαρμόζεται όταν απαιτείται εμπιστοσύνη στην ορθή λειτουργία, αλλά οι απειλές για την ασφάλεια δεν θεωρούνται σοβαρές. Η αξιολόγηση του TOE περιλαμβάνει ανεξάρτητους ελέγχους επί των προδιαγραφών του, καθώς και εξέταση των εγχειριδίων του, προκειμένου να επιβεβαιωθεί ότι λειτουργεί σύμφωνα με τις οδηγίες και ότι προσφέρει χρήσιμη προστασία εναντίον των απειλών. Αυτό το επίπεδο ασφάλειας είναι ιδιαιτέρως κατάλληλο για παλαιότερα συστήματα, αφού μπορεί να πραγματοποιηθεί χωρίς την συνδρομή του developer και με μικρό κόστος.

EAL 2 - Δομικός Έλεγχος (Structural Check)

Το EAL 2 εφαρμόζεται όταν απαιτείται ένα χαμηλό έως μέσο επίπεδο επιβεβαιωμένης ασφάλειας. Η ανάλυση των λειτουργιών ασφάλειας εξετάζει τις προδιαγραφές λειτουργίας και διασύνδεσης, καθώς και το υψηλό επίπεδο

σχεδιασμού των υποσυστημάτων του TOE. Γίνονται ανεξάρτητες δοκιμές των λειτουργιών ασφάλειας και η απόδειξη απαιτείται από τον έλεγχο του "black box" του developer και την έρευνα για εμφανείς ευπάθειες. Το κόστος και ο χρόνος αξιολόγησης κυμαίνονται σε χαμηλά επίπεδα.

EAL 3 - Μεθοδικός έλεγχος και Δοκιμή (Formal Check and Testing)
Το EAL 3 εφαρμόζεται όταν απαιτείται ένα μέσο επίπεδο επιβεβαιωμένης ασφάλειας, με εμπεριστατωμένη εξέταση του TOE και της σχεδίασής του , χωρίς όμως να απαιτηθεί μια ουσιώδης ανακατασκευή του. Η ανάλυση περιλαμβάνει τον έλεγχο του "grey box", επιλεκτική ανεξάρτητη επικύρωση των αποτελεσμάτων των ελέγχων του developer, καθώς και την απόδειξη της έρευνας του developer για εμφανείς ευπάθειες. Απαιτούνται επίσης, έλεγχοι για τις προϋποθέσεις με τις οποίες το TOE θα λειτουργεί μέσα στο περιβάλλον του, καθώς και έλεγχοι για τη διαμόρφωσης της δομής του.

EAL 4 - Μεθοδικός Σχεδιασμός, Έλεγχος και Επιθεώρηση (Formal Design, Check and Inspection)
Το EAL 4 εφαρμόζεται όταν απαιτείται ένα μέσο έως υψηλό επίπεδο επιβεβαιωμένης ασφάλειας, για το οποίο μπορεί να απαιτηθούν κάποια έξοδα ανακατασκευής του TOE σε θέματα ασφαλείας. Η ανάλυση περιλαμβάνει το χαμηλού επιπέδου σχέδιο των ρυθμίσεων του TOE και ενός υποσυστήματος της εφαρμογής. Οι έλεγχοι περιλαμβάνουν ανεξάρτητη έρευνα για εμφανείς ευπάθειες, αξιολόγηση του μοντέλου κύκλου-ζωής (life-cycle) του TOE, αναγνώριση εργαλείων και αυτόματη διαχείριση δομής.

EAL 5 - Ημιεπίσημος Σχεδιασμός και Έλεγχος (Semi-officially Design and Check)
Το EAL 5 εφαρμόζεται όταν απαιτείται ένα υψηλό επίπεδο επιβεβαιωμένης ασφάλειας. Αυτό απαιτεί μία αυστηρή και προσεκτική σχεδιαστική προσέγγιση, η οποία και θα αποτρέψει τυχόν έξοδα για ανακατασκευή του TOE σε θέματα ασφαλείας. Η ανάλυση περιλαμβάνει όλες τις εφαρμογές. Η ασφάλεια συμπληρώνεται από ένα επίσημο μοντέλο, μια ημιεπίσημη παρουσίαση των λειτουργικών προδιαγραφών, υψηλού επιπέδου σχεδίαση και μία ημιεπίσημη επίδειξη ανταπόκρισης σε επιθέσεις. Η έρευνα για ευπάθειες πρέπει να εξασφαλίζει αντίσταση σε εισβολή επιτιθέμενων με δυνατότητα μέτριας επίθεσης. Επίσης, απαιτείται έρευνα για κρυφά κανάλια ανάλυσης (covert channels).

EAL 6 - Ημιεπισήμως Επικυρωμένος Σχεδιασμός και Έλεγχος (Semi-officially Validated Design and Check)
Το EAL 6 εφαρμόζεται όταν απαιτείται ένα εξειδικευμένο ασφαλές TOE για περιπτώσεις υψηλού κινδύνου, όπου η αξία των προστατευόμενων πληροφοριών δικαιολογεί τα επί πλέον έξοδα. Η ανάλυση υποστηρίζεται από μία διαμορφωμένη προσέγγιση σχεδιασμού και με μία δομική παρουσίαση της εφαρμογής. Η ανεξάρτητη έρευνα για ευπάθειες πρέπει να εξασφαλίζει αντίσταση σε εισβολή επιτιθέμενων με δυνατότητα υψηλής επίθεσης και να υπάρχει μια συστηματική έρευνα για κρυφά κανάλια. Ενισχύονται περαιτέρω οι

έλεγχοι για την συμπεριφορά του TOE εντός του λειτουργικού του περιβάλλοντος, καθώς και οι έλεγχοι διαχείρισης της δομής του.

EAL 7 - Επισήμως Επικυρωμένος Σχεδιασμός και Έλεγχος (Officially Validated Design and Check)

Το EAL 7 εφαρμόζεται όταν απαιτείται ένα εξειδικευμένο ασφαλές TOE για περιπτώσεις εξαιρετικά υψηλού κινδύνου, όπου η αξία των προστατευόμενων πληροφοριών δικαιολογεί τα υψηλότερα έξοδα. Επί πλέον των απαιτήσεων του EAL6, το επίσημο μοντέλο πρέπει να είναι εφοδιασμένο με ένα σχέδιο επίσημης παρουσίασης και λειτουργικών προδιαγραφών υψηλού επιπέδου, και να επιδεικνύει την αντίδραση σε επιθέσεις. Απαιτείται η απόδειξη των ελέγχων του "white box" του developer καθώς και πλήρης ανεξάρτητη επικύρωση των αποτελεσμάτων των ελέγχων του developer.

COMMON CRITERIA (ISO 15408)

(INTERNATIONAL SECURITY EVALUATION CRITERIA FOR IT SYSTEMS)

ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ (ASSURANCE LEVELS)

ΕΠΙΠΕΔΟ	ΕΥΡΟΣ ΤΩΝ ΕΛΕΓΧΩΝ *
EAL 1	Functional Check
EAL 2	Structural Check
EAL 3	Formal Check and Testing
EAL 4	Formal Design, Check and Inspection
EAL 5	Semi-officially Design and Check
EAL 6	Semi-officially Validated Design and Check
EAL 7	Officially Validated Design and Check

* **Αξιολόγηση από διαπιστευμένα εργαστήρια (Information Technology Security Evaluation Facilities - ITSEF), σύμφωνα με το εργαστηριακό πρότυπο ISO 17025.**
* **Πιστοποίηση από διαπιστευμένους Οργανισμούς Πιστοποίησης (Compliant Certification Bodies -CCB)**

Πίνακας 24. Επίπεδα Ασφαλείας (ή Επίπεδα Εμπιστοσύνης) των Common Criteria (Evaluation Assurance Levels)

10.7. Διεθνής συμφωνία CCRA

Βάσει των διεθνών κριτηρίων αξιολόγησης εκδίδονται πιστοποιητικά για κάθε προϊόν ασφαλείας πληροφοριών. Για να υπάρχει αμοιβαία εμπιστοσύνη μεταξύ των κρατών τα οποία εκδίδουν πιστοποιητικά και για να μην επαναλαμβάνονται σε κάθε κράτος οι αξιολογήσεις για το ίδιο προϊόν, έχει ιδρυθεί η διεθνή συμφωνία CCRA (Common Criteria Recognition

Arrangement). Έτσι, κάθε κράτος μέλος της συμφωνίας αναγνωρίζει τα πιστοποιητικά τα οποία έχουν εκδώσει οι άλλες χώρες-μέλη. Στην συμφωνία αυτή συμμετέχουν έως τώρα 28 χώρες **[**βιβλ. **41].**

Η συμφωνία διοικείται από την Επιτροπή Διαχείρισης (Management Committee - MC), της οποίας βασικό έργο είναι η διαπίστευση των νέων κρατών-μελών και των νέων οργανισμών και εργαστηρίων αξιολόγησης / πιστοποίησης, καθώς και ο έλεγχος της τήρησης των κριτηρίων αξιολόγησης από τα μέλη της συμφωνίας. Επίσης, έργο της επιτροπής είναι η συνεχής αναβάθμιση των κριτηρίων αξιολόγησης, το οποίο είναι ένα δύσκολο έργο λόγω της συνεχούς και ραγδαίας εξέλιξης των προϊόντων τεχνολογίας πληροφοριών. Η επιτροπή συνεδριάζει μία φορά τον χρόνο και ο πρόεδρός της εναλλάσσεται περιοδικά μεταξύ των αντιπροσώπων των κρατών-μελών.

Η επιτροπή διαχείρισης βοηθείται από την εκτελεστική υποεπιτροπή (Executive Subcommittee-ES) σε τεχνικά θέματα.

Υπάρχουν δύο κατηγορίες κρατών- μελών στην συμφωνία CCRA :

α. Χώρες παραγωγής πιστοποιητικών (certifications producing countries) : Είναι οι χώρες οι οποίες έχουν αναπτύξει τεχνογνωσία αξιολόγησης σύμφωνα με τα Common Criteria και έχουν μία οργανωμένη και ιεραρχική υποδομή, αποτελούμενη από εργαστήρια αξιολόγησης και οργανισμούς πιστοποίησης.

(1) Αρχική αξιολόγηση : Για να πιστοποιηθεί η ικανότητα και η τεχνογνωσία της κάθε χώρας, πρέπει υποβληθεί κατ'αρχήν σε σκιώδη πιστοποίηση (shadow certification). Κατά την σκιώδη πιστοποίηση γίνεται επίβλεψη όλων των διαδικασιών αξιολόγησης και πιστοποίησης τις οποίες εφαρμόζει η υποψήφια χώρα, από μία ειδική επιτροπή η οποία απαρτίζεται από εμπειρογνώμονες διαφόρων κρατών. Η υποψήφια χώρα θα πρέπει να προτείνει δύο συγκεκριμένα προϊόντα, επί των οποίων θα διεξαχθεί η σκιώδη πιστοποίηση. Η ειδική επιτροπή αφού αξιολογήσει την ικανότητα της υποψήφιας χώρας, συντάσσει πόρισμα με εισήγηση προς την Επιτροπή Διαχείρισης για την καταλληλότητα της χώρας.

(2) Περιοδικός έλεγχος : Μετά από την αρχική σκιώδη πιστοποίηση, όλα τα εργαστήρια αξιολόγησης και οι οργανισμοί παραγωγής πιστοποιητικών των χωρών μελών, υφίστανται εθελοντικούς περιοδικούς ελέγχους (Voluntary Periodic Assessment-VPA) από επιτροπή εμπειρογνωμόνων, για να διαπιστωθεί ότι εξακολουθούν να πληρούν τις απαραίτητες προϋποθέσεις.

β. Χώρες κατανάλωσης πιστοποιητικών (certifications consuming countries) : Είναι οι χώρες οι οποίες δεν έχουν αναπτύξει τεχνογνωσία αξιολόγησης σύμφωνα με τα Common Criteria και είναι μέλη της συμφωνίας για να ενημερώνονται και για να χρησιμοποιούν τα αξιολογημένα προϊόντα. Οι χώρες αυτές έχουν την δυνατότητα να αποκτήσουν τεχνογνωσία και αναβαθμισθούν στο μέλλον σε χώρες παραγωγής πιστοποιητικών. Στην κατηγορία αυτή ανήκει και η Ελλάδα.

ΚΕΦΑΛΑΙΟ 11

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΕΣ ΑΚΤΙΝΟΒΟΛΙΕΣ

11.1 Γενικά

Ο έλεγχος των ηλεκτρομαγνητικών (Η/Μ) ακτινοβολιών τις οποίες εκπέμπουν οι συσκευές, αποτελεί ένα σημαντικό κεφάλαιο της ασφάλειας των επικοινωνιών, διότι οι Η/Μ ακτινοβολίες εκτός από την επίδρασή τους στην λειτουργία των συσκευών, μπορούν να εκθέσουν και την ασφάλεια των πληροφοριών τις οποίες αυτές επεξεργάζονται. Επομένως, η ολοκληρωμένη αξιολόγηση μιας κρυπτοσυσκευής ή ενός κρυπτοσυστήματος πρέπει να περιλαμβάνει και τον έλεγχο των εκπεμπόμενων Η/Μ ακτινοβολιών τους.

α. Παρεμβάλλουσες ηλεκτρομαγνητικές ακτινοβολίες (EMI/RFI)

Οι Η/Μ ακτινοβολίες οι οποίες εκπέμπονται από τους πάσης φύσεως ηλεκτρικούς αγωγούς και τις ηλεκτρικές ή ηλεκτρονικές συσκευές, μπορούν να προκαλέσουν ανεπιθύμητες παρεμβολές στις γειτονικές τους συσκευές, και έτσι να τους δημιουργήσουν προβλήματα λειτουργίας. Το φαινόμενο αυτό είναι γνωστό ως Ηλεκτρομαγνητική Παρεμβολή (Electromagnetic Interference - EMI) και Παρεμβολή Ράδιο Συχνοτήτων (Radio Frequency Interference - RFI).

Γενικά, η Ηλεκτρομαγνητική Συμβατότητα (Electromagnetic Compatibility - EMC) είναι η ικανότητα μιας ηλεκτρικής διάταξης, συσκευής ή συστήματος, να λειτουργεί ικανοποιητικά στο ηλεκτρομαγνητικό της περιβάλλον, χωρίς να προκαλεί απαράδεκτες ηλεκτρομαγνητικές διαταραχές σε οτιδήποτε βρίσκεται στο εν λόγω περιβάλλον. Ηλεκτρομαγνητική Διαταραχή, είναι κάθε ηλεκτρομαγνητικό φαινόμενο που ενδέχεται να υποβαθμίσει τις επιδόσεις μιας συσκευής ή να επιδράσει δυσμενώς σε ζώσα ή αδρανή ύλη.

β. Συμβιβασμένες ηλεκτρομαγνητικές ακτινοβολίες (TEMPEST)

Οι Η/Μ ακτινοβολίες τις οποίες εκπέμπουν οι ηλεκτρικές συσκευές, μπορούν να διαδοθούν ασύρματα δια μέσου του ελεύθερου χώρου ή ενσύρματα κατά μήκος των αγώγιμων επιφανειών που βρίσκονται πλησίον τους, καθώς και δια μέσου άλλων διόδων εκπομπής (τηλεφωνικές γραμμές, γραμμές μεταφοράς ηλεκτρικής ενέργειας, κάθοδοι κεραιών, συστήματα συναγερμού κλπ).

Έτσι, αυτές οι ακτινοβολίες είναι δυνατόν να διαφύγουν από τον χώρο όπου είναι εγκατεστημένες οι συσκευές και να συλλεχθούν από έναν ράδιο-δέκτη, ο οποίος βρίσκεται σε σχετικά μακρινή απόσταση από την συσκευή η οποία τις εκπέμπει. Το πρόβλημα έγκειται στο γεγονός ότι, αυτές οι διαφεύγουσες ακτινοβολίες είναι διαμορφωμένες -σε κάποιο ποσοστό- με τις πληροφορίες τις οποίες επεξεργάζεται η συσκευή. Και έτσι, εάν ένας υποκλοπέας έχει ειδικό εξοπλισμό και γνώσεις, μπορεί με ειδική επεξεργασία των διαφευγουσών ακτινοβολιών να εξάγει τις πληροφορίες τις οποίες επεξεργάζεται η συσκευή.

Ο χώρος τριών διαστάσεων ο οποίος περιβάλλει τη συσκευή που επεξεργάζεται διαβαθμισμένες πληροφορίες, μέσα στον οποίο δεν θεωρείται πρακτικά δυνατή η υποκλοπή Η/Μ ακτινοβολιών ή υπάρχουν κατάλληλα μέτρα για να αναγνωρίσουν και να αποτρέψουν μία τέτοια υποκλοπή, καλείται **ελεγχόμενος χώρος**. Επειδή η ένταση των Η/Μ ακτινοβολιών μειώνεται όσο

αυξάνει η απόστασή τους από την συσκευή που τις εκπέμπει, ο κίνδυνος υποκλοπής τους μειώνεται όσο αυξάνεται ο ελεγχόμενος χώρος.

Κάθε διαφεύγουσα Η/Μ ακτινοβολία η οποία περιέχει κάποιο ποσοστό της επεξεργαζόμενης πληροφορίας της συσκευής, ονομάζεται **Συμβιβασμένη Ακτινοβολία (Compromising Emanation).** Αυτό μπορεί να οφείλεται είτε σε απ'ευθείας σύζευξη του σήματος που επεξεργάζεται η συσκευή λόγω χωρητικής και επαγωγικής σύζευξης, είτε σε δευτερεύουσα σύζευξη λόγω διαμόρφωσης κάποιων αρμονικών συχνοτήτων της συσκευής με το σήμα της πληροφορίας. Οι αρμονικές που εκπέμπονται από τις συχνότητες ρολογιού (clock) ή τις συχνότητες συγχρονισμού (synchronization) των συσκευών, είναι συνήθως οι στόχοι του υποκλοπέα. Εάν αυτές οι αρμονικές είναι διαμορφωμένες με την πληροφορία, τότε είναι εφικτό με ειδικές μεθόδους να εξαχθεί η πληροφορία. Ακόμα και οι κρυπτοσυσκευές όταν δεν έχουν προστασία TEMPEST, μπορούν να υποκλαπούν από την ακτινοβολία της ανοικτής πληροφορίας, δηλαδή προτού αυτή κρυπτογραφηθεί, με αποτέλεσμα να ελαττώνεται η αποτελεσματικότητα τους.

Η διαδικασία της ανάλυσης και μελέτης των ανεπιθύμητων και επικίνδυνων για την ασφάλεια διαφευγουσών ακτινοβολιών καλείται **TEMPEST** (Transient Electromagnetic Pulse Escape Safeguard Techniques). Ο όρος TEMPEST χρησιμοποιείται επίσης για να περιγράψει τα σχετικά ηλεκτρομαγνητικά φαινόμενα, καθώς και τους μηχανισμούς καταστολής τους. Το ΝΑΤΟ, η Ε.Ε. καθώς και οι αρμόδιοι εθνικοί φορείς των προηγμένων κρατών, εκδίδουν ειδικούς κανονισμούς για τη διεξαγωγή των μετρήσεων TEMPEST, οι οποίοι αναφέρουν και τα όρια εντός των οποίων πρέπει να εμπίπτουν οι μετρήσεις, ώστε οι συσκευές να είναι αποδεκτές. Επίσης, εκδίδουν καταλόγους με τις συσκευές που έχουν κριθεί κατάλληλες (TEMPEST Approved Products List). Τέλος, εκδίδουν κανονισμούς με τις διαδικασίες διαπίστευσης των εταιρειών οι οποίες παράγουν προϊόντα TEMPEST. Στο **[45]** της βιβλιογραφίας δίδεται ένας κατάλογος με τους σχετικούς κανονισμούς του ΝΑΤΟ και των ΗΠΑ και στο **[46]** φαίνεται ο σχετικός κανονισμός της Ε.Ε.

11.2. Υποκλοπή Η/Μ ακτινοβολιών

Η δυνατότητα υποκλοπής των διαφευγουσών ακτινοβολιών, οι αποστάσεις της διάδοσής τους, καθώς και η δυνατότητα ανάλυσής τους, εξαρτώνται από ποικίλους παράγοντες, όπως την σχεδίαση λειτουργίας των συσκευών, την εγκατάστασή τους, τις περιβαλλοντολογικές συνθήκες που σχετίζονται με την φυσική τους ασφάλεια, καθώς και τις συνθήκες ηλεκτρομαγνητικού θορύβου του χώρου. Για τους λόγους αυτούς, ένας αριθμός από τεχνικά μέτρα πρέπει να λαμβάνεται για την καταστολή αυτών των ακτινοβολιών. Οι εκπεμπόμενες ακτινοβολίες μιας συσκευής μπορούν να υποκλαπούν βασικά με δύο τρόπους:

α. Από την άμεση ακτινοβολία στο χώρο: Η άμεση ακτινοβολία μιας συσκευής μπορεί να ελεγχθεί πιο εύκολα. Η εμβέλειά της είναι σχετικά μικρή με εξαίρεση τις παλαιές οθόνες τύπου C.R.T. των τερματικών Η/Υ ή μικροϋπολογιστών (καθοδικοί σωλήνες τερματικών), οι οποίες λόγω των υψηλών τάσεων που χρησιμοποιούν μπορούν να υποκλαπούν και από απόσταση ενός χιλιομέτρου.

β. Μέσω αγώγιμων σωμάτων: Η διάδοση του σήματος μέσω αγώγιμων σωμάτων (καλωδίων, σωλήνων κλπ.) που διέρχονται πλησίον της συσκευής, δεν ελέγχεται εύκολα. Μπορούν βέβαια να τοποθετηθούν φίλτρα στα δίκτυα της ηλεκτρικής παροχής και των τηλεπικοινωνιών. Η επαγωγή όμως των σημάτων μπορεί να γίνει και σε σημείο μετά την τοποθέτηση των φίλτρων ή μέσω του δικτύου ύδρευσης, καλοριφέρ, κλπ. Έτσι, το σήμα μπορεί να μεταδοθεί σε μεγάλη απόσταση, όπου ο υποκλοπέας μπορεί να εγκαταστήσει μηχανήματα συλλογής.

11.3. Απειλές και κίνδυνοι

Οι ηλεκτρομαγνητικές απειλές κατά των εγκαταστάσεων και μέσων επικοινωνιών, εξαρτώνται από τους εξής παράγοντες:

α. Τις τεχνικές δυνατότητες του υποκλοπέα.

β. Τον βαθμό κινδύνου στον οποίο είναι διατεθειμένος να εκτεθεί ο υποκλοπέας για να πετύχει τους στόχους του.

γ. Την σημασία που αποδίδει ο υποκλοπέας στις πληροφορίες που θα συγκεντρώσει.

δ. Την δυνατότητα που έχει ο υποκλοπέας να προσεγγίσει τις εγκαταστάσεις και τα μέσα μας για να πετύχει τους στόχους του.

Η δυνατότητα πρόσβασης ή η εγγύτητα που ένας υποκλοπέας έχει προς το στόχο του, καθορίζει το βαθμό της ηλεκτρομαγνητικής απειλής. Όπου οι συσκευές μας ευρίσκονται σε απόσταση μικρότερη των 100μ. από μία πιθανή εχθρική εγκατάσταση, υπάρχει σοβαρή απειλή και πρέπει να ληφθούν πολύ αυστηρά μέτρα προστασίας. Τέτοιες εχθρικές εγκαταστάσεις είναι αυτές που καλύπτονται από διπλωματική ασυλία, όπως οι πρεσβείες, τα προξενεία, οι εμπορικές αποστολές ή άλλες επίσημες κυβερνητικές εκπροσωπήσεις, καθώς και εμπορικές παρουσίες που έχει διαπιστωθεί ότι σχετίζονται με εχθρικές υπηρεσίες πληροφοριών.

11.4. Μέτρα προστασίας

Η ολοκληρωμένη αξιολόγηση μιας κρυπτοσυσκευής ή ενός κρυπτοσυστήματος πρέπει να περιλαμβάνει και τον έλεγχο για μέτρα αποφυγής των εκπεμπόμενων Η/Μ ακτινοβολιών, τα οποία είναι σε γενικές γραμμές τα εξής:

11.4.1 Μείωση ακτινοβολίας συσκευών

Το βασικό μέτρο προστασίας είναι η ελαχιστοποίηση της Η/Μ ακτινοβολίας η οποία εκπέμπεται από το εσωτερικό των ηλεκτρονικών συσκευών. Αυτό επιτυγχάνεται κατασκευαστικά, με ειδική Η/Μ θωράκιση και απομόνωση των εσωτερικών κυκλωμάτων, καθώς και με ειδικά υλικά κατασκευής (π.χ. ειδικοί connectors εισόδου και εξόδου των σημάτων), ώστε να μη διαφεύγει ακτινοβολία μεταξύ των εσωτερικών βαθμίδων και εκτός των συσκευών. Στην Εικόνα 2 φαίνεται μια συσκευή στρατιωτικών προδιαγραφών TEMPEST, όπου είναι εμφανής η εξωτερική Η/Μ θωράκιση και οι ειδικοί connectors. Η αναλυτική περιγραφή των μεθόδων και των υλικών για την εσωτερική και εξωτερική θωράκιση των συσκευών, είναι θέμα εξειδικευμένο και ξεφεύγει από τα πλαίσια της παρούσας εργασίας.

Εικόνα 2. Συσκευή TEMPEST

Εάν για οικονομικούς ή λειτουργικούς λόγους δεν είναι δυνατή η προμήθεια συσκευών TEMPEST, οι υπάρχουσες συμβατικές συσκευές μπορούν να τοποθετηθούν εντός ειδικών Η/Μ θωρακισμένων κιβωτίων (TEMPEST enclosures), τα οποία αποτρέπουν την διαφυγή των Η/Μ ακτινοβολιών.

11.4.2. Προστασία των κέντρων επικοινωνιών / πληροφορικής

Εκτός από τον εσωτερικό περιορισμό της ακτινοβολίας των συσκευών, στα κέντρα επικοινωνιών και γενικότερα στους χώρους όπου υπάρχουν ηλεκτρονικές συσκευές επεξεργασίας διαβαθμισμένων πληροφοριών (π.χ. Μηχανογραφικά Κέντρα), πρέπει σε γενικές γραμμές να τηρούνται τα παρακάτω μέτρα προστασίας:

α. Γείωση των συσκευών.

β. Χρήση Η/Μ φίλτρων.

γ. Διαχωρισμός red και black κυκλωμάτων.

δ. Απομάκρυνση τηλεφώνων από τους χώρους ηλεκτρονικής επεξεργασίας διαβαθμισμένων πληροφοριών.

ε. Απομάκρυνση μεταλλικών αντικειμένων, τα οποία μπορούν να αποτελέσουν δευτερογενείς πηγές ακτινοβολίας.

στ. Αποφυγή τοποθέτησης συσκευών και οθονών πλησίον παραθύρων.

ζ. Απαγόρευση χρήσης ραδιόφωνων, τηλεοράσεων κλπ., μέσα σε χώρους ηλεκτρονικής επεξεργασίας διαβαθμισμένων πληροφοριών.

η. Οι επιφάνειες των τοίχων, των παραθύρων και των σημείων πρόσβασης των διαβαθμισμένων χώρων (πόρτες, αεραγωγοί κλπ), να προστατεύονται με ειδικά υλικά που εμποδίζουν την εκπομπή Η/Μ ακτινοβολιών.

11.4.3. Ηλεκτρομαγνητικά θωρακισμένος κλωβός (Faraday)

Αν σε μία υπηρεσία υπάρχει μεγάλος αριθμός συσκευών που διαχειρίζονται διαβαθμισμένες πληροφορίες, τότε ενδείκνυται να κατασκευαστεί ένας ειδικός χώρος θωρακισμένος από Η/Μ ακτινοβολίες και εντός αυτού να εγκατασταθούν όλες οι ευαίσθητες συσκευές (τηλεπικοινωνιακές συσκευές, κρυπτοσυσκευές, ηλεκτρονικοί υπολογιστές κλπ.). Αυτός ο θωρακισμένος ηλεκτρομαγνητικά χώρος, στην πράξη είναι ένας Κλωβός FARADAY , δηλαδή ένας μεταλλικός κλωβός ο οποίος είναι πολύ καλά γειωμένος και έτσι δεν επιτρέπει να διαφύγουν εκτός αυτού οι Η/Μ ακτινοβολίες.

Ο Κλωβός FARADAY μπορεί να είναι προκατασκευασμένος και αυτόνομος ή μπορεί να κατασκευαστεί με τροποποίηση του χώρου στον οποίο είναι εγκαταστημένες οι συσκευές, με τοποθέτηση πλεγμάτων ή μεταλλικών φύλλων στους τοίχους του δωματίου, την οροφή και το πάτωμα και στη

συνέχεια την πολύ καλή γείωση τους. Ακόμα και ειδικά μεταλλικά χρώματα μπορούν να προσφέρουν μια αρκετά καλή ηλεκτρομαγνητική θωράκιση. Οι κατασκευαστικές προδιαγραφές ενός τέτοιου κλωβού αναφέρονται στο **[47]** της βιβλιογραφίας.

11.4.4. Ζώνες Ασφάλειας (Tempest Zoning)

Όπως προαναφέρθηκε, ο κίνδυνος υποκλοπής των διαφευγουσών Η/Μ ακτινοβολιών μειώνεται όσο αυξάνεται ο **ελεγχόμενος χώρος** της εγκατάστασης. Έτσι, η μέθοδος Tempest Zoning συνίσταται στην καθιέρωση ζωνών ασφαλείας γύρω από τους χώρους εγκατάστασης των συσκευών, ώστε να εξασφαλισθεί η προστασία από υποκλοπή. Αυτό επιτυγχάνεται, μετρώντας την ολική εξασθένιση της ραδιοσυχνότητας που προξενείται από το σημείο που θα εγκατασταθούν οι συσκευές μέχρι τα όρια του διαθέσιμου ελεγχόμενου χώρου ή μέχρι την πιθανή θέση εγκατάστασης μηχανημάτων υποκλοπής Η/Μ ακτινοβολιών. Οι μετρήσεις γίνονται με ειδικό σύστημα φορητής κεραίας - δέκτη, το οποίο μετράει την εξασθένηση του σήματος το οποίο παράγεται από ένα σύστημα πομπού - γεννήτριας αναφοράς, σε όλη τη περιοχή συχνοτήτων. Περισσότερα για αυτό το θέμα περιέχονται στους διαβαθμισμένους κανονισμούς της Ε.Ε. και του NATO "IA Security Guidelines on Tempest Zoning Procedures, IASG 7-02" και "NATO Zoning Procedures, SDIP-28/1", (οι οποίοι αναφέρονται στη βιβλιογραφία **[46]** -Annex 3).

Όταν εφαρμοστεί κατάλληλα η μέθοδος των Ζωνών ασφάλειας, τότε μπορεί να ελαττωθεί σημαντικά το κόστος για την προστασία των Η/Μ ακτινοβολιών. Αυτό σημαίνει ότι μπορεί π.χ. να μην χρειαστεί να κατασκευαστεί ένας δαπανηρός κλωβός Faraday. Επίσης, εάν ο ελεγχόμενος χώρος είναι μεγάλος, τότε μπορούμε να χρησιμοποιήσουμε συσκευές με χαμηλότερες προδιαγραφές Tempest ή και συσκευές του εμπορίου, αντί να χρησιμοποιήσουμε συσκευές με στρατιωτικές προδιαγραφές Tempest, οι οποίες έχουν πολύ μεγαλύτερο κόστος (τετραπλάσια έως και πενταπλάσια τιμή).

11.4.5. Υπόγειες/Προστατευμένες Επικοινωνίες

Κάποια κέντρα επικοινωνιών εγκαθίστανται σε υπόγειες προστατευμένες εγκαταστάσεις οι οποίες εξασθενούν τις Η/Μ ακτινοβολίες αποτρέποντας την εξωτερική τους διαφυγή. Σε τέτοιες εγκαταστάσεις, τα μέτρα μπορούν να ελαττωθούν σημαντικά, υπό την προϋπόθεση ότι εφαρμόζονται σωστά μέτρα εγκατάστασης στις γραμμές επικοινωνιών, γραμμές μεταφοράς ηλεκτρικής ισχύος και άλλους αγωγούς που οδηγούνται έξω από την προστατευμένη περιοχή. Πρέπει όμως πάντοτε αυτοί οι χώροι να ελέγχονται, για να διαπιστωθεί ότι είναι κατάλληλοι για εφαρμογή περιορισμένων αντιμέτρων TEMPEST. Σε πολλές περιπτώσεις οι προστατευμένες εγκαταστάσεις αποτελούν την οικονομικότερη εναλλακτική λύση αντί της επιλογής συσκευών με προδιαγραφές TEMPEST.

11.5. Εργαστήριο μέτρησης Η/Μ ακτινοβολιών

Το εργαστήριο TEMPEST έχει σκοπό την μέτρηση των εκπεμπόμενων Η/Μ ακτινοβολιών από τις συσκευές, για να διαπιστώσει εάν οι ακτινοβολίες υπερβαίνουν τα επιτρεπτά όρια ισχύος, πάνω από τα οποία υπάρχει κίνδυνος

αυτές να υποκλαπούν και να εξαχθεί από αυτές η διαμορφωμένη πληροφορία. Κανονισμοί του NATO και της Ε.Ε. καθορίζουν τις διαδικασίες των μετρήσεων, καθώς και τα επιτρεπτά ποσοστά ισχύος των Η/Μ ακτινοβολιών. Βάσει αυτών, οι συσκευές υποβάλλονται σε ελέγχους και κατόπιν κατατάσσονται σε τρεις κατηγορίες πιστοποίησης (Α ή Β ή C). Οι κανονισμοί αυτοί είναι διαβαθμισμένοι και δεν μπορούν να αναφερθούν στην παρούσα εργασία.

Ο εξοπλισμός ενός εργαστηρίου μέτρησης ακτινοβολιών TEMPEST έχει μεγάλο κόστος, αποτελούμενος από εξειδικευμένες συσκευές εντός ειδικού κλωβού Faraday (κεραίες, δέκτες, συστήματα επεξεργασίας σε υλικό/λογισμικό κλπ). Αναλυτική περιγραφή του εξοπλισμού δίδεται στο **[47]** της βιβλιογραφίας.

Εικόνα 3. Εσωτερική άποψη εργαστηρίου μέτρησης Η/Μ ακτινοβολιών. Στους τοίχους και την οροφή διακρίνονται οι αιχμηρές επιφάνειες του «ανηχοϊκού» θαλάμου, ενώ αριστερά φαίνεται η κεραία συλλογής της ακτινοβολίας και δεξιά η προς μέτρηση συσκευή.

Εκτός από το μεγάλο κόστος, η δεύτερη δυσκολία είναι η εκπαίδευση και η εμπειρία του προσωπικού. Κατά τα διάφορα στάδια των μετρήσεων TEMPEST, εύκολα μπορούν να γίνουν λάθη και να παρερμηνευτούν τα αποτελέσματα. Υπάρχουν αρκετά τεχνάσματα που πρέπει να γίνουν, ώστε να μην αλλοιωθούν τα αποτελέσματα κατά τις μετρήσεις και κυρίως κατά την διαδικασία συσχέτισης (correlation) των εκπεμπόμενων ακτινοβολιών με τα σήματα ανοικτής πληροφορίας που υπάρχουν εντός της συσκευής. Η δυσκολία στην ανίχνευση των εκπεμπόμενων ακτινοβολιών έγκειται στο ότι καθώς το αρχικό σήμα με την ανοικτή πληροφορία διέρχεται από διάφορες βαθμίδες εντός της συσκευής, υφίσταται μετασχηματισμούς, δηλαδή αλλαγή στη μορφή του, χωρίς να αλλάζει το πληροφοριακό περιεχόμενο. Έτσι, ο αναλυτής θα πρέπει να συσχετίσει το μετασχηματισμένο σήμα που εκπέμπει η συσκευή με το αρχικό σήμα και να εξαχθεί η πραγματική πληροφορία. Η συσχέτιση γίνεται με οπτική παρατήρηση (αναλυτής φάσματος, παλμογράφος κλπ.) καθώς και με τη χρήση ειδικού υλικού/λογισμικού (correlator).

ΚΕΦΑΛΑΙΟ 12

ΕΚΤΙΜΗΣΗ ΤΗΣ ΙΣΧΥΟΣ ΤΟΥ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΑΛΓΟΡΙΘΜΟΥ

12.1. Γενικά

Στο παρόν Κεφάλαιο 12, θα γίνει μία συνολική εκτίμηση της ισχύος ασφαλείας του κρυπτογραφικού αλγορίθμου (security strength), βάσει των όσων έχουν αναφερθεί στα προηγούμενα Κεφάλαια. Η ισχύς ασφαλείας ενός κρυπτογραφικού αλγορίθμου (από εδώ και πέρα θα την αναφέρουμε απλά ως ισχύ), είναι ουσιαστικά το μέτρο της δυσκολίας το οποίο καταβάλει ένας επιτιθέμενος για να τον διασπάσει.

Η διαδικασία βαθμολόγησης της ισχύος ενός κρυπτογραφικού αλγορίθμου την οποία εισάγουμε στην παρούσα διατριβή, είναι η εξής: Κατ'αρχήν, ο αλγόριθμος κατατάσσεται σε μία από τέσσερεις γενικές κατηγορίες ισχύος, βάσει του μεγέθους της κλείδας του (Χαμηλή, Μέτρια, Υψηλή, Πολύ υψηλή). Κατόπιν, καθορίζεται διαδοχικά ο τελικός βαθμός της ισχύος του κρυπταλγορίθμου, βάσει των αποτελεσμάτων των ελέγχων τυχαιότητας και ομοιότητας επί των εξόδων του (τους οποίους περιγράψαμε στο Κεφάλαιο 3). Ο τελικός βαθμός δεν μπορεί να είναι μεγαλύτερος από τον αρχικό βαθμό που παίρνει ο κρυπτογραφικός αλγόριθμος λόγω του μεγέθους της κλείδας του. Είναι όμως πολύ πιθανόν να είναι μικρότερος του αρχικού βαθμού, λόγω σημαντικών αδυναμιών τις οποίες ενδεχομένως να παρουσιάζει ο αλγόριθμος είτε στην εσωτερική του δομή (π.χ. εάν υπάρχουν επιτυχείς κρυπταναλυτικές επιθέσεις ή θεωρητικές μέθοδοι επίθεσης για κάποια τμήματά του), είτε στην ενδεχόμενη μη τυχαιότητα και ομοιότητα των ψηφιακών ακολουθιών τις οποίες παράγει.

12.2. Μήκος της κλείδας

Όπως αναφέραμε στο Κεφάλαιο 5, η ασφάλεια ενός κρυπτογραφικού αλγόριθμου βασίζεται στην εσωτερική του πολυπλοκότητα και το μήκος της κλείδας του. Όταν όμως ο αλγόριθμος δεν έχει κάποιο γνωστό και εκμεταλλεύσιμο ελάττωμα στην δομή του, τότε η μόνη κρυπταναλυτική επίθεση που μπορεί να εφαρμοστεί σε αυτόν είναι η μέθοδος της Εξαντλητικής Έρευνας της Κλείδας (Exhaustive Search ή Brute Force Attack). Αυτή η διαδικασία επίθεσης είναι εξαιρετικά χρονοβόρα και εάν η κλείδα έχει επαρκές μήκος, τότε η εξαντλητική της έρευνα είναι πρακτικά ανεφάρμοστη και συνεπώς λέμε ότι ο αλγόριθμος είναι πρακτικά ασφαλής.

Ο Πίνακας 17 της σελίδας 57 (τον οποίο αναπαράγουμε παρακάτω ως Πίνακα 25), δίνει την αντιστοιχία της ισχύος των συμμετρικών και ασύμμετρων αλγορίθμων βάσει του μήκους της κλείδας τους, με βάση τα σημερινά κρυπταναλυτικά δεδομένα, σύμφωνα με την έκδοση NIST SP800-57 (βιβλιογραφία **[37]**). Είναι προφανές ότι ο Πίνακας 25 ισχύει όταν ο αλγόριθμος δεν έχει κάποιο τρωτό σημείο (η εκμετάλλευση του οποίου μπορεί να μειώσει το πλήθος των κλειδών ή να τις παρακάμψει), επομένως η μόνη δυνατή επίθεση σε αυτόν είναι η εξαντλητική έρευνα των κλειδών.

ΙΣΧΥΣ ΑΛΓΟΡΙΘΜΟΥ (βάσει του μήκους κλείδας σε bits)	ΣΥΜΜΕΤΡΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ	ΑΣΥΜΜΕΤΡΟΙ ΑΛΓΟΡΙΘΜΟΙ		
		FFC (π.χ. DSA, D-H)	IFC (π.χ. RSA)	ECC (π.χ. ECDSA)
≤ 80	2TDEA (2-DES)	1024	1024	160-223
112	3TDEA (3-DES)	2048	2048	224-255
128	AES-128	3072	3072	256-383
192	AES-192	7680	7680	384-511
256	AES-256	15360	15360	512+

Πίνακας 25. Αντιστοιχία ισχύος (μήκους κλείδας) συμμετρικών και ασύμμετρων αλγορίθμων (από το SP800-57 του NIST).

Σημείωση: Η πρώτη στήλη του Πίνακα 25 εκφράζει το ενεργό (πραγματικό) μήκος της κλείδας, το οποίο ενδέχεται να είναι μικρότερο από το ονομαστικό. Π.χ. ενώ ο 3DES έχει θεωρητικό μήκος κλείδας 3X56=168 bits, εν τούτοις υπάρχει μια κρυπταναλυτική επίθεση η οποία μειώνει το ενεργό του μήκος σε 112 bits. Παρομοίως, για τον 2DES έχει ευρεθεί ότι εάν ο κρυπταναλυτής έχει στη διάθεσή του περίπου 2^{40} ζευγάρια ανοικτού/κλειστού κειμένου, η ενεργός κλείδα από την ονομαστική τιμή των 112 bits μειώνεται στα 80 bits, ενώ με 2^{56} ζευγάρια ανοικτού/κλειστού κειμένου, η ενεργός κλείδα μειώνεται στα 56 bits.

Όπως φαίνεται, ο Πίνακας 25 περιλαμβάνει μόνο συγκεκριμένα μήκη κλειδών, από κρυπτογραφικούς αλγορίθμους οι οποίοι έχουν σχεδιαστεί στις ΗΠΑ (εκτός του AES) και έχουν εγκριθεί από το NIST. Για να κατατάξουμε την ισχύ των αλγορίθμων περιλαμβάνοντας όλα τα πιθανά ενδιάμεσα μήκη των κλειδών μεταξύ των 80 bits και 256 bits, εκπονήσαμε τον Πίνακα 26 στον οποίο κατατάξαμε την ισχύ των αλγορίθμων σε τέσσερεις κατηγορίες ισχύος : Χαμηλή , Μέτρια , Υψηλή και Πολύ υψηλή , βάσει της περιοχής τιμών στην οποία εμπίπτει το μήκος της κλείδας τους.

ΜΗΚΟΣ ΚΛΕΙΔΑΣ (Κ)	$80 \leq K \leq 112$	$112 < K < 128$	$128 \leq K \leq 192$	$192 < K \leq 256$
ΙΣΧΥΣ ΑΛΓΟΡΙΘΜΟΥ	ΧΑΜΗΛΗ	ΜΕΤΡΙΑ	ΥΨΗΛΗ	ΠΟΛΥ ΥΨΗΛΗ

Πίνακας 26. Συγκριτική ισχύς συμμετρικών κρυπταλγορίθμων βάσει του μήκους της κλείδας, με τα σημερινά κρυπταναλυτικά και τεχνολογικά δεδομένα (2017).

Σημειώνουμε ότι η ανωτέρω κατάταξη ισχύος των κρυπτογραφικών αλγορίθμων δείχνει κυρίως την σύγκριση μεταξύ τους, δηλαδή είναι σχετική και όχι απόλυτη. Για παράδειγμα, το μήκος κλείδας των 128 bits είναι αρκετά

ισχυρό για τα σημερινά δεδομένα, όπως δείξαμε στο Κεφάλαιο 5 (παράγραφος 5.6). Ωστόσο, το μήκος των 128 bits σε σύγκριση με τα 256 bits πρέπει να θεωρηθεί τουλάχιστον κατά ένα βαθμό κατώτερο. Σε κάθε περίπτωση, ένας αλγόριθμος με μεγαλύτερο μήκος κλείδας «αντέχει» κρυπταναλυτικά σε μεγαλύτερο βάθος χρόνου, όπως αναλύθηκε στην παράγραφο 5.6.

Ο Πίνακας 26, δείχνει την ισχύ των κρυπτογραφικών αλγορίθμων, με βάση τα σημερινά κρυπταναλυτικά και τεχνολογικά δεδομένα (έτος 2017). Όπως όμως αναφέραμε στην παρ. 5.6, για να αντισταθμιστεί η συνεχής εξέλιξη της ισχύος των Η/Υ (νόμος του Moore), η κλείδα πρέπει να αυξάνει κατά ένα bit κάθε χρόνο, ώστε να είμαστε ασφαλείς έναντι της εξαντλητικής έρευνας των κλειδών (Brute Force Attack – BFA). Ως συγκριτικό παράδειγμα, σχεδιάσαμε τον Πίνακα 27, ο οποίος δείχνει τα μήκη κλειδών τα οποία πρέπει να ισχύουν μετά από 20 χρόνια, ώστε οι κρυπταλγόριθμοι να είναι ασφαλείς έναντι της BFA, σύμφωνα με την αναμενόμενη τεχνολογική εξέλιξη (έτος 2037). Βλέπουμε ότι σε σχέση με τον Πίνακα 26, οι τιμές των κλειδών έχουν αυξηθεί κατά 20 (ένα bit για κάθε χρόνο).

ΜΗΚΟΣ ΚΛΕΙΔΑΣ (Κ)	**$100 \leq K \leq 132$**	**$132 < K < 148$**	**$148 \leq K \leq 212$**	**$212 < K \leq 276$**
ΙΣΧΥΣ ΑΛΓΟΡΙΘΜΟΥ	**ΧΑΜΗΛΗ**	**ΜΕΤΡΙΑ**	**ΥΨΗΛΗ**	**ΠΟΛΥ ΥΨΗΛΗ**

Πίνακας 27. Συγκριτική ισχύς συμμετρικών κρυπταλγορίθμων βάσει του μήκους κλείδας, μετά από 20 χρόνια, λόγω της αναμενόμενης τεχνολογικής εξέλιξης (2037).

Σε κάθε περίπτωση, η τελική επιλογή του κατάλληλου κρυπτογραφικού αλγορίθμου (ή του κρυπτογραφικού συστήματος εν γένει), πρέπει να γίνει με βάση την επιθυμητή χρονική διάρκεια προστασίας των κρυπτογραφημένων πληροφοριών, σε συνδυασμό με την ανάλυση του κινδύνου την οποία αντιμετωπίζει το κρυπτογραφικό σύστημα από ενδεχόμενες απειλές οι οποίες θα εκμεταλλευτούν κάποιες αδυναμίες του. Οι παράγοντες αυτοί θα εξεταστούν στα επόμενα Κεφάλαια 13 και 14.

12.3. Έλεγχος δειγμάτων εξόδου του αλγορίθμου

Όπως αναφέραμε στο Κεφάλαιο 3, για να διερευνηθεί η απαιτούμενη τυχαιότητα (randomness), η ανεξαρτησία (independency) και η μη προβλεψιμότητα (unpredictability) της παραγόμενης ψηφιακής ακολουθίας ενός αλγορίθμου, διεξάγονται επί των bits της εξόδου του ειδικοί στατιστικοί και κρυπταναλυτικοί έλεγχοι (οι κυριότεροι από αυτούς φαίνονται στον Πίνακα 3 (σελίδα 18).

Ανακεφαλαιώνοντας τα όσα αναφέρθηκαν στο Κεφάλαιο 3, η διαδικασία των ελέγχων είναι η εξής: Από το συνολικό πλήθος N των κρυπτογραφικών κλειδών, επιλέγουμε ένα μικρότερο πλήθος από n κλείδες με τη μέθοδο της δειγματοληψίας. Για κάθε μία από αυτές τις n κλείδες παράγουμε ένα δείγμα εξόδου του αλγορίθμου (ψηφιακή ακολουθία) και αποθηκεύουμε τα n δείγματα

σε αντίστοιχα αρχεία. Κατόπιν, υποβάλουμε όλα τα δείγματα στους στατιστικούς ελέγχους και αποθηκεύουμε τα αποτελέσματα των ελέγχων. Η τελική απόφαση για το επίπεδο της τυχαιότητας, ανεξαρτησίας και μη προβλεψιμότητας των εξόδων του υπό εξέταση αλγορίθμου, γίνεται βάσει του συνολικού ποσοστού επιτυχίας που έχουν οι στατιστικοί έλεγχοι στα εξετασμένα δείγματα. Τα βασικά προβλήματα που προκύπτουν εάν θέλουμε να έχουμε μια αξιόπιστη αλλά και πρακτικά εφικτή διενέργεια των ελέγχων, είναι τα εξής:

α. Πόσα δείγματα πρέπει να ελέγξουμε;

β. Πόσο πρέπει να είναι το μέγεθος κάθε δείγματος;

γ. Πως μπορούμε να μειώσουμε τον χρόνο των ελέγχων;

δ. Με ποια μέθοδο πρέπει να επιλέξουμε τις δειγματοληπτικές κλείδες;

ε. Πως βαθμολογούμε την ασφάλεια των αλγορίθμων με βάση τα αποτελεσμάτων των ελέγχων;

Το πρόβλημα (α) εξετάστηκε στις παραγράφους 3.8. και 3.10, το πρόβλημα (β) εξετάστηκε στην παράγραφο 3.9, το πρόβλημα (γ) εξετάστηκε στην παράγραφο 3.11 και το πρόβλημα (δ) εξετάστηκε στο Κεφάλαιο 4. Απομένει λοιπόν το πρόβλημα (ε), το οποίο θα το εξετάσουμε παρακάτω.

Υπολογισμός ποσοστού επιτυχίας

Για κάθε στατιστικό κριτήριο ελέγχου, από αυτά που θα επιλεγούν από τον Πίνακα 3, εξετάζουμε όσο το δυνατόν περισσότερα δείγματα εξόδου του αλγορίθμου και κατόπιν υπολογίζουμε το συνολικό ποσοστό της επιτυχίας, δηλαδή πόσα από τα δείγματα πέρασαν με επιτυχία το συγκεκριμένο στατιστικό κριτήριο. Όπως αναφέρεται στο **[6]** για κάθε έλεγχο καθορίζουμε ένα κριτήριο επιτυχίας, το οποίο ονομάζεται επίπεδο σημαντικότητας (significance level) και συμβολίζεται με α. Το α εκφράζει την πιθανότητα να παρουσιαστεί λάθος Τύπου 1, δηλαδή ο έλεγχος να δείξει ότι η ακολουθία δεν είναι τυχαία, ενώ στην πραγματικότητα είναι τυχαία. Παραδείγματος χάριν, αν θέσουμε $\alpha = 0.03$ σημαίνει ότι ένας αλγόριθμος περνάει με επιτυχία τον έλεγχο, όταν από τα 100 δείγματα εξόδου που εξετάσαμε, δεχόμαστε να μην είναι τυχαία το πολύ τρία.

Οι τυπικές τιμές του επιπέδου σημαντικότητας α για την κρυπτογραφία είναι γύρω στο 0.01, το οποίο σημαίνει ότι το πολύ μία στις 100 ακολουθίες του αλγορίθμου δεχόμαστε να μην είναι τυχαία. Ωστόσο, όπως αναφέρεται και στο **[48]**, στην πράξη οποιοδήποτε σύνολο από ψηφιακές ακολουθίες ενός αλγορίθμου κι αν επιλέξουμε, το πιθανότερο είναι ότι θα αποκλίνουν από αυτή την ιδανική περίπτωση. Μια πιο ρεαλιστική προσέγγιση, είναι να χρησιμοποιήσουμε ένα διάστημα εμπιστοσύνης (confidence interval- CI) για το ποσοστό των ακολουθιών οι οποίες αναμένεται να περάσουν το επιθυμητό $\alpha = 0.01$. Στην περίπτωση αυτή το πλέον ενδεδειγμένο διάστημα εμπιστοσύνης (CI) είναι το 95%. Αυτό σημαίνει ότι, εάν σε ένα έλεγχο αποτυγχάνουν παραπάνω από 5% των δειγμάτων, τότε ο αλγόριθμος θεωρείται «ύποπτος» για μη τυχαιότητα.

Ο μέγιστος αριθμός των απορριπτέων δειγμάτων m τα οποία μπορούμε να αποδεχτούμε σε κάθε έλεγχο με διάστημα εμπιστοσύνης 95% , δίδεται στο **[48]** από τον τύπο (1) :

$$m = n\left(a + 3\sqrt{\frac{\alpha\,(1-\alpha)}{n}}\right) \quad (1)$$

όπου n είναι ο συνολικός αριθμός των εξετασμένων δειγμάτων και α είναι το significance level (ο τύπος προκύπτει από την καμπύλη της κανονικής κατανομής, η οποία προσεγγίζει τη διωνυμική για μεγάλα n).

Στον Πίνακα 28 υπολογίζουμε τον μέγιστο αριθμό των απορριπτέων δειγμάτων, κατ'αρχήν λαμβάνοντας υπόψη μόνο το επίπεδο σημαντικότητας (στήλη 3) και κατόπιν λαμβάνοντας υπόψη το επίπεδο σημαντικότητας και το διάστημα εμπιστοσύνης CI (στήλη 4) βάσει του τύπου (1). Ο συνολικός αριθμός των δειγμάτων n στη δεύτερη στήλη του Πίνακα 27, αντιστοιχεί στο σφάλμα δειγματοληψίας e το οποίο έχουμε επιλέξει (πρώτη στήλη). Οι δύο πρώτες στήλες του Πίνακα 27 μεταφέρθηκαν από τον Πίνακα 8 (σελίδα 29).

ΣΦΑΛΜΑ ΔΕΙΓΜΑΤΟ-ΛΗΨΙΑΣ (e)	**ΣΥΝΟΛΙΚΟΣ ΑΡΙΘΜΟΣ ΔΕΙΓΜΑΤΩΝ** (n)	**ΜΕΓΙΣΤΟΣ ΑΡΙΘΜΟΣ ΑΠΟΡΡΙΠΤΕΩΝ ΔΕΙΓΜΑΤΩΝ** (m) (λαμβάνεται υπόψη το ακέραιο μέρος του αριθμού)	
		Για επίπεδο σημαντικότητας α = 0.01	Για επίπεδο σημαντικότητας α = 0.01 και CI = 95%
5 %	384	3,84	9,689
4 %	600	6,00	13,311
3 %	1067	10,67	20,420
2 %	2401	24,01	38,636
1 %	9604	96,04	125,292

Πίνακας 28. Μέγιστος αριθμός απορριπτέων δειγμάτων, με βάση το σφάλμα δειγματοληψίας e και τον αντίστοιχο συνολικό αριθμό δειγμάτων n.

Παράδειγμα: Έστω ότι σε ένα έλεγχο τυχαιότητας επιθυμούμε να έχουμε ένα πολύ μικρό σφάλμα δειγματοληψίας, της τάξης του 1%. Από τη δεύτερη στήλη του Πίνακα 28 προκύπτει ότι πρέπει να εξετάσουμε 9604 δείγματα. Εάν επιθυμούμε ο έλεγχος να είναι αυστηρός, πρέπει να επιλέξουμε ένα ποσοστό επιτυχίας της τάξης του 99%. Αυτό σημαίνει ποσοστό αποτυχίας 1% (επίπεδο σημαντικότητας α=0.01), δηλαδή μπορούμε να δεχθούμε ως απορριπτέα έως 96 δείγματα (τρίτη στήλη του Πίνακα 28). Επειδή όμως όπως αναφέρθηκε, ένα απόλυτο ποσοστό επιτυχίας 99% των δειγμάτων στην πράξη είναι σχεδόν ανέφικτο, μια πιο ρεαλιστική προσέγγιση είναι να χρησιμοποιήσουμε ένα διάστημα εμπιστοσύνης, εντός του οποίου θα ευρίσκεται με μεγάλη πιθανότητα το επιθυμητό ποσοστό επιτυχίας. Εάν λοιπόν επιλέξουμε ένα διάστημα εμπιστοσύνης 95%, από την τέταρτη στήλη του Πίνακα 28 βρίσκουμε ότι στον συγκεκριμένο έλεγχο μπορούμε να δεχθούμε έως 125 απορριπτέα δείγματα.

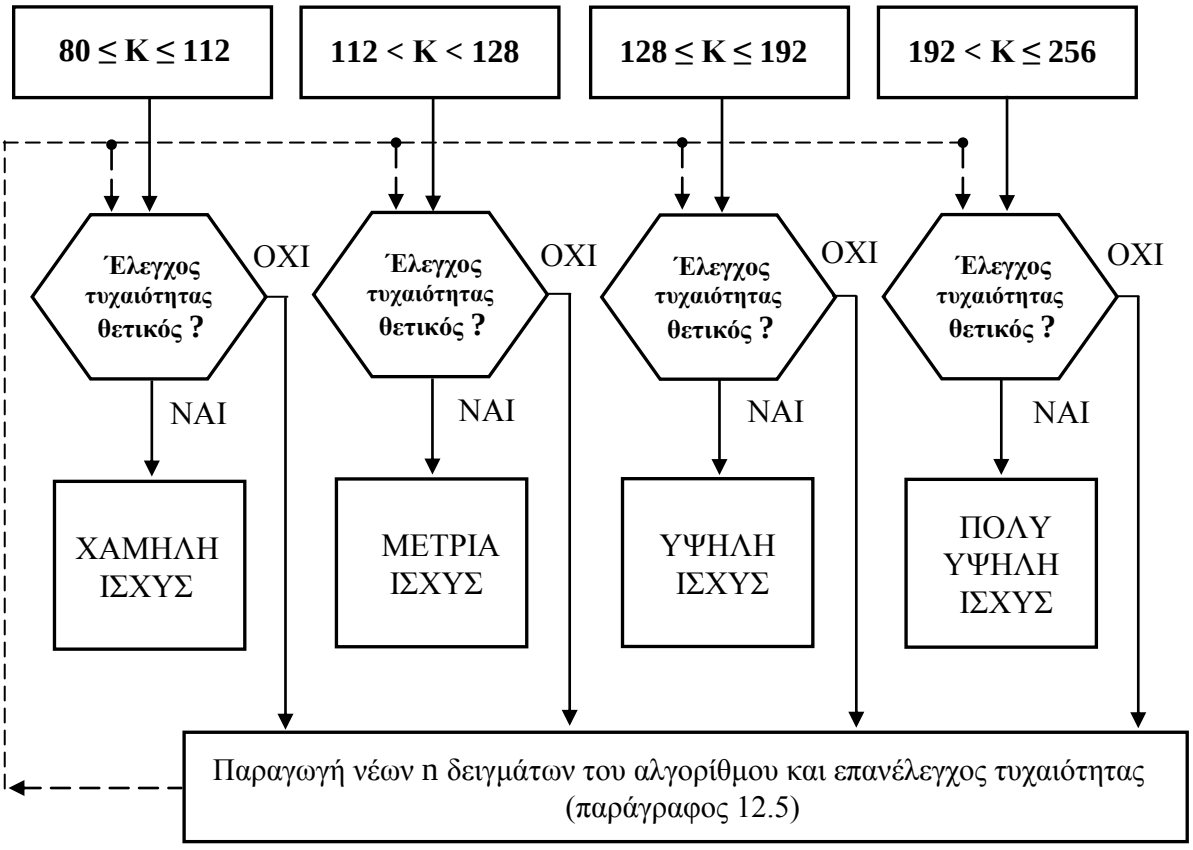
12.4. Διαδικασία βαθμολόγησης

Μετά τα όσα αναφέρθηκαν στις προηγούμενες παραγράφους, η διαδικασία βαθμολόγησης φαίνεται συνοπτικά στο Σχήμα 20: Αρχικά, ο κρυπτογραφικός αλγόριθμος κατατάσσεται σε μία από τέσσερεις γενικές κατηγορίες ισχύος, βάσει του μεγέθους της κλείδας του Κ, όπως αναφέρθηκε στην παράγραφο 12.2 (Πίνακας 26):

1η κατηγορία: **80 ≤ K ≤ 112** **3η** κατηγορία: **128 ≤ K ≤ 192**
2η κατηγορία: **112 < K < 128** **4η** κατηγορία: **192 < K ≤ 256**

Αφού κατατάξουμε τον εξεταζόμενο αλγόριθμο σε μία από τις παραπάνω κατηγορίες, κατόπιν εξετάζουμε το ποσοστό επιτυχίας των ελέγχων τυχαιότητας επί των δειγμάτων εξόδου του. Εάν ο έλεγχος τυχαιότητας είναι θετικός (δηλαδή εάν τα απορριφθέντα δείγματα δεν υπερβαίνουν τον αριθμό ο οποίος προκύπτει από τον Πίνακα 28), τότε κατατάσσουμε τον αλγόριθμο στην κατηγορία ισχύος η οποία προκύπτει από το μέγεθος της κλείδας του (Χαμηλή, Μέτρια, Υψηλή, Πολύ υψηλή), όπως φαίνεται στο Σχήμα 20.

Εάν ο έλεγχος τυχαιότητας του αλγορίθμου είναι αρνητικός (δηλαδή εάν τα απορριφθέντα δείγματα υπερβαίνουν τον αριθμό ο οποίος προκύπτει από τον Πίνακα 28), τότε παράγουμε μια νέα ομάδα από n δείγματα εξόδου του αλγορίθμου και διενεργούμε επανέλεγχο των στατιστικών ελέγχων τυχαιότητας, με την διαδικασία και τις προϋποθέσεις που περιγράφουμε στην παρ. 12.5.



Σχήμα 20. Βασική διαδικασία βαθμολόγησης κρυπτογραφικού αλγορίθμου

12.5. Έλεγχος νέων δειγμάτων

Εάν κατά τη διαδικασία η οποία φαίνεται στο Σχήμα 20, ο έλεγχος τυχαιότητας του αλγορίθμου είναι αρνητικός, αυτό δεν σημαίνει κατ'ανάγκη ότι ο αλγόριθμος δεν είναι τυχαίος. Σύμφωνα με το **[6]**, η αποτυχία σε κάποιον έλεγχο ενδεχομένως να μην οφείλεται στην χαμηλή ποιότητα του αλγορίθμου, αλλά σε κάποιο άλλο αίτιο, το οποίο μπορεί να είναι ένα από τα παρακάτω:

α. Εσφαλμένη υλοποίηση του εξεταζόμενου κρυπτογραφικού αλγορίθμου ή της RNG (σε υλικό ή λογισμικό).

β. Εσφαλμένη λογισμική υλοποίηση ενός στατιστικού τεστ ή λανθασμένη επιλογή στις παραμέτρους εισόδου του.

γ. Ελλιπώς σχεδιασμένο στατιστικό τεστ (π.χ. ανεπαρκής ανάλυση και τεκμηρίωσή του βάσει της θεωρίας πιθανοτήτων ή θεωρίας πολυπλοκότητας).

δ. Εσφαλμένο λογισμικό για την επεξεργασία των δεδομένων εισόδου του στατιστικού τεστ.

ε. Μη ακριβής μαθηματικός υπολογισμός των σταθερών (α, p), κυρίως σε ότι αφορά την τελειότερη αριθμητική προσέγγιση των τιμών τους.

στ. Εσφαλμένη επιλογή στα χαρακτηριστικά των δειγμάτων (π.χ. ακατάλληλος αριθμός ή μέγεθος των δειγμάτων, ακατάλληλο μέγεθος των blocks και των patterns των ελέγχων κλπ.).

Λόγω των ανωτέρω, εάν ο έλεγχος τυχαιότητας της πρώτης ομάδας n δειγμάτων του αλγορίθμου είναι αρνητικός, είναι λογικό να δώσουμε μια «δεύτερη ευκαιρία» στον αλγόριθμο, ώστε να αποκλείσουμε το ενδεχόμενο η αποτυχία να μην οφείλεται στον αλγόριθμο αλλά σε ένα από τα παραπάνω αίτια. Για να αντιμετωπιστεί αυτό το πρόβλημα, προτείνουμε ως λύση να παραχθεί μια νέα ομάδα από n δείγματα εξόδου του αλγορίθμου και να διενεργήσουμε υπό προϋποθέσεις ένα επανέλεγχο των ελέγχων τυχαιότητας. Έτσι, στην περίπτωση του επανελέγχου θα έχουμε τα εξής δύο ενδεχόμενα:

α. Ο επανέλεγχος είναι αρνητικός: Ο αλγόριθμος απορρίπτεται ως μη τυχαίος (εφόσον απέτυχε δύο συνεχόμενες φορές και για 2n δείγματα).

β. Ο επανέλεγχος είναι θετικός: Στην περίπτωση αυτή, εάν m_1 και m_2 είναι ο αριθμός των απορριφθέντων δειγμάτων του πρώτου και του δεύτερου ελέγχου αντίστοιχα, τότε το άθροισμά τους δεν πρέπει να υπερβαίνει το m το οποίο υπολογίζεται από τον τύπο (1) της παραγράφου 12.3, όπου στη θέση του n πρέπει να βάλουμε το 2n (διότι θα έχουν γίνει δύο έλεγχοι με n δείγματα έκαστος). Συνεπώς, εάν το άθροισμά των απορριφθέντων δειγμάτων είναι μικρότερο του m, ο αλγόριθμος είναι τυχαίος, ενώ εάν το άθροισμά των απορριφθέντων δειγμάτων είναι μεγαλύτερο του m, ο αλγόριθμος απορρίπτεται ως μη τυχαίος.

Παράδειγμα : Έστω ότι κατά τον αρχικό έλεγχο ενός αλγορίθμου εξετάζουμε 600 δείγματα και εξ αυτών απορρίπτονται 15. Σύμφωνα με τον Πίνακα 28 (στήλη 4) ο μέγιστος αριθμός απορριπτέων δειγμάτων είναι 13, οπότε ο πρώτος έλεγχος είναι αρνητικός. Πραγματοποιούμε λοιπόν ένα δεύτερο έλεγχο, κατά τον οποίο, εκ των νέων 600 δειγμάτων απορρίπτονται τα 6 (δηλαδή ο δεύτερος έλεγχος είναι θετικός). Έτσι, επί συνολικά 1200 εξετασμένων δειγμάτων έχουν απορριφθεί συνολικά 21 δείγματα.

Εφαρμόζοντας τον τύπο (1) για n=1200, βρίσκουμε ότι ο μέγιστος αριθμός απορριπτέων δειγμάτων είναι m=22. Επομένως, ο εξετασθείς αλγόριθμος περνάει με επιτυχία, εφόσον συνολικά απορρίφθηκαν 21 δείγματά του (λιγότερα από 22 που είναι το όριο).

Οφείλουμε να σημειώσουμε, ότι θα μπορούσε να πραγματοποιηθεί και δεύτερος, ίσως και τρίτος επανέλεγχος σύμφωνα με την ανωτέρω διαδικασία. Αυτό βέβαια εναπόκειται στην κρίση του αξιολογητή. Π.χ. ενδεχομένως κάποιος αξιολογητής να θελήσει να επαναλάβει τους ελέγχους, ώστε να διαπιστώσει εάν και πότε, τα αποτελέσματα των επανελέγχων «διορθώνουν» τα αποτελέσματα του πρώτου ελέγχου. Ωστόσο, ο αριθμός των επανελέγχων για κάποιο αλγόριθμο δεν μπορεί να είναι υπερβολικός, για πρακτικούς και για δεοντολογικούς λόγους. Οι πρακτικοί λόγοι αφορούν την εξαιρετικά χρονοβόρα διαδικασία της παραγωγής των δειγμάτων και της εκτέλεσης των ελέγχων. Και οι δεοντολογικοί λόγοι αφορούν την αποφυγή μιας ευνοϊκότερης μεταχείρισης του επανεξεταζόμενου αλγορίθμου, έναντι κάποιων άλλων αλγορίθμων (οι οποίοι έχουν επιτύχει με τον πρώτο έλεγχο). Για τους ανωτέρω λόγους, κατά την επίσημη και συγκριτική αξιολόγηση μεταξύ κάποιων αλγορίθμων, πιστεύουμε ότι ένας βέλτιστος κανόνας είναι, οι επανέλεγχοι να μην ξεπερνάνε τους δύο.

ΚΕΦΑΛΑΙΟ 13

ΕΚΤΙΜΗΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

13.1. Γενικά

Στο παρόν Κεφάλαιο 13, θα γίνει μία συνολική εκτίμηση της ασφάλειας του κρυπτογραφικού συστήματος, βάσει της ισχύος των επί μέρους μονάδων και των μηχανισμών του. Εκτός από την ισχύ του κρυπτογραφικού αλγορίθμου την οποία εξετάσαμε στο Κεφάλαιο 12, οι επί μέρους μονάδες οι οποίες εμπλέκονται στην συνολική αξιολόγηση της ασφάλειας ενός κρυπτογραφικού συστήματος, είναι αυτές οι οποίες υλοποιούν τους βασικούς μηχανισμούς ασφαλείας του , οι οποίοι εξετάστηκαν σε προηγούμενα Κεφάλαια και είναι οι:

1. Παραγωγή και διαχείριση των κλειδών: Εξετάστηκε στο Κεφάλαιο 6.
2. Υλοποίηση αλγορίθμου (hardware/software): Εξετάστηκε στο Κεφάλαιο 7.
3. Πρόσβαση των χρηστών (access control): Εξετάστηκε στο Κεφάλαιο 9.
4. Προστασία από παραβίαση (tamper proof): Εξετάστηκε στο Κεφάλαιο 9.
5. Αυτοέλεγχοι (self test): Εξετάστηκε στο Κεφάλαιο 9.
6. Προστασία από Ηλεκτρομαγνητικές Ακτινοβολίες: Εξετάστηκε στο Κεφάλαιο 11.

Πριν αναπτύξουμε την μεθοδολογία αξιολόγησης, θα πρέπει να υπενθυμίσουμε την βασική αρχή, ότι η τελική ασφάλεια ενός συστήματος, ισούται με την ασφάλεια της ασθενέστερης μονάδας του. Παραδείγματος χάριν, ακόμα και αν ένα κρυπτογραφικό σύστημα διαθέτει ένα πολύ ισχυρό αλγόριθμο, δεν μπορεί να θεωρηθεί ασφαλές εάν έχει ελαττώματα στο σύστημα διαχείρισης των κλειδών του (διότι εάν διαρρεύσει η κλείδα καταρρέει όλη η ασφάλεια του).

Κατά την αξιολόγηση ενός κρυπτογραφικού συστήματος, πρέπει να ληφθούν σοβαρά υπόψη και οι τυχόν προϋπάρχουσες πιστοποιήσεις οι οποίες αφορούν τη λειτουργική του ασφάλεια, βάσει Διεθνών ή Εθνικών Προτύπων Ασφαλείας. Τα βασικότερα Πρότυπα αυτού του είδους, είναι το FIPS 140-2 /NIST (USA) και το ISO 15408 (Common Criteria), τα οποία αναφέρθηκαν στο Κεφάλαιο 9 και στο Κεφάλαιο 10 αντίστοιχα της παρούσας διατριβής.

Στο τέλος του παρόντος κεφαλαίου, θα εξεταστούν οι προϋποθέσεις λειτουργίας του κρυπτογραφικού συστήματος, ώστε να ισχύει η πιστοποίησή του, καθώς και τα κριτήρια για τη χρονική διάρκεια της πιστοποίησης. Επίσης, θα εξεταστούν τα κριτήρια για την λήξη ή την ανανέωση της πιστοποίησης, καθώς και για την διεξαγωγή μίας νέας αξιολόγησης (επαναξιολόγηση).

13.2. Ασφάλεια ιδανικού κρυπτογραφικού συστήματος

Για να εκτιμήσουμε την ασφάλεια του εκάστοτε αξιολογούμενου κρυπτογραφικού συστήματος θα πρέπει να καθορίσουμε ένα σημείο αναφοράς. Στα πλαίσια της παρούσας διατριβής, ως σημείο αναφοράς θεωρούμε ένα ιδανικό κρυπτογραφικό σύστημα, στο οποίο όλοι οι μηχανισμοί ασφαλείας είναι σχεδιασμένοι και υλοποιημένοι με ένα τέλειο (ή πολύ επαρκή) τρόπο.

Κατά συνέπεια, η ασφάλεια ενός ιδανικού κρυπτογραφικού συστήματος αντιστοιχεί με την ασφάλεια (ισχύ) την οποία παρέχει ο κρυπτογραφικός του αλγόριθμος. Και τούτο διότι οι υπόλοιποι μηχανισμοί ασφαλείας του κρυπτοσυστήματος (οι οποίοι αναφέρθηκαν στην προηγούμενη παράγραφο), δεν μειώνουν την αρχική ασφάλεια την οποία παρέχει ο αλγόριθμος. Αυτή η αντιστοιχία φαίνεται στον Πίνακα 29. Όμως στην πράξη, πολύ λίγα κρυπτογραφικά συστήματα είναι ιδανικά, διότι στα περισσότερα υπάρχουν κάποια ελαττώματα ή ελλείψεις στον σχεδιασμό ή στην υλοποίηση των μηχανισμών ασφαλείας τους. Για το λόγο αυτό, στην επόμενη παράγραφο περιγράφουμε τη διαδικασία αξιολόγησης ενός κρυπτογραφικού συστήματος, κατά την οποία συνυπολογίζουμε τις ατέλειες των μηχανισμών ασφαλείας του.

	ΑΝΤΙΣΤΟΙΧΙΑ			
ΙΣΧΥΣ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΑΛΓΟΡΙΘΜΟΥ	Χαμηλή	Μέση	Υψηλή	Πολύ Υψηλή
ΑΣΦΑΛΕΙΑ ΙΔΑΝΙΚΟΥ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ	Χαμηλή	Μέση	Υψηλή	Πολύ Υψηλή

Πίνακας 29. Αντιστοιχία της ασφάλειας ενός ιδανικού κρυπτοσυστήματος με την ισχύ του κρυπταλγορίθμου τον οποίο χρησιμοποιεί.

13.3. Διαδικασία αξιολόγησης κρυπτογραφικού συστήματος

Στο διάγραμμα ροής του Σχήματος 21, παρουσιάζουμε τα βήματα της διαδικασίας αξιολόγησης ενός κρυπτογραφικού συστήματος. Όπως φαίνεται, το πρώτο βήμα, το οποίο λαμβάνουμε ως αφετηρία της αξιολόγησης (επάνω αριστερά στο σχήμα), είναι ο καθορισμός της ισχύος του κρυπτογραφικού αλγορίθμου, ο οποίος έχει αξιολογηθεί με τις διαδικασίες τις οποίες αναφέραμε στο προηγούμενο Κεφάλαιο 12. Στο Σχήμα 21, ως παράδειγμα έχουμε υποθέσει ότι ο αλγόριθμος έχει πολύ υψηλή ισχύ. Κατόπιν ελέγχουμε έναν προς έναν, τους μηχανισμούς ασφαλείας (οι οποίοι αναφέρθηκαν στην παράγραφο 13.1), σε ότι αφορά την επάρκεια της ισχύος τους, δηλαδή την πληρότητα του σχεδιασμού τους και τον τρόπο υλοποίησής τους.

13.3.1. Παραγωγή και Διαχείριση των κλειδών

Ο πλέον σημαντικός μηχανισμός ασφαλείας ο οποίος και εξετάζεται πρώτος, αφορά τη Παραγωγή και Διαχείριση των κλειδών. Σύμφωνα με όσα αναφέραμε στο Κεφάλαιο 6, για να διατηρήσει το κρυπτογραφικό σύστημα το βαθμό ασφαλείας τον οποίο παρέχει ο κρυπτογραφικός του αλγόριθμος, θα πρέπει οπωσδήποτε να δίνει την δυνατότητα εξωτερικής παραγωγής και εισαγωγής των κλειδών, ώστε ο χρήστης να μπορεί να τις παράγει και να τις εισάγει σύμφωνα με τις δικές του διαδικασίες ασφαλείας.

α. Αξιολόγηση της γεννήτριας τυχαίων χαρακτήρων (RNG)

Η παραγωγή των κλειδών γίνεται μέσω γεννητριών τυχαίων χαρακτήρων (RNG), των οποίων οι διαδικασίες αξιολόγησης αναφέρθηκαν στο Κεφάλαιο 6. Ειδικότερα, η αξιολόγηση της τυχαιότητας των ψηφιακών ακολουθιών μίας RNG, πρέπει να γίνει με την ίδια διαδικασία αξιολόγησης της τυχαιότητας των εξόδων του αλγορίθμου, η οποία περιγράφηκε στην παράγραφο 12.3. Δηλαδή θα πρέπει να παράγουμε ένα μεγάλο αριθμό δειγμάτων εξόδου της RNG και να τα υποβάλουμε στους ιδίους ελέγχους τυχαιότητας στους οποίους υποβάλαμε και τις εξόδους του αλγορίθμου. Ο αριθμός των δειγμάτων n, το επιθυμητό σφάλμα δειγματοληψίας e , καθώς και ο μέγιστος αριθμός των απορριπτέων δειγμάτων m (βλέπε Πίνακα 28), πρέπει να είναι ίδια με αυτά τα οποία χρησιμοποιήθηκαν για την αξιολόγηση της τυχαιότητας των εξόδων του αλγορίθμου, για τον οποίο θα παράγει κλείδες η RNG.

Σε ότι αφορά το μήκος των δειγμάτων της RNG, είναι λογικό να μην είναι τόσο μεγάλο όσο το μήκος των αλγοριθμικών εξόδων (το οποίο στην παρ. 3.9. προτείναμε, ως μία βέλτιστη πρακτική λύση, να είναι της τάξης του 1 Mbit). Και τούτο διότι, η γεννήτρια θα παράγει πολύ μικρότερου μήκους εξόδους (της τάξης των 128 έως 256 bits, όσο είναι το μήκος της εκάστοτε κλείδας). Ωστόσο, όπως αναφέραμε στην παράγραφο 6.2.4., το πρότυπο FIPS 140-2 προτείνει κατά την έναρξη λειτουργίας μιας TRNG, την εφαρμογή μόνο τεσσάρων στατιστικών ελέγχων (Monobit, Poker, Runs και Long Run), σε ένα δείγμα των 20.000 bits (ώστε να μειώσει τον απαιτούμενο χρόνο). Όμως αυτό το δείγμα δεν είναι επαρκές, εάν θέλουμε να παράγουμε μια μακρά ψηφιακή ακολουθία κλείδας, όπως στα κρυπτοσυστήματα τύπου “one time pad”. Σε αυτές τις περιπτώσεις, πρέπει να διεξαχθούν περισσότεροι στατιστικοί έλεγχοι (όπως αυτοί στον Πίνακα 3) και σε μεγαλύτερα δείγματα εξόδου. Για τους ανωτέρω λόγους, ως μία βέλτιστη πρακτική λύση προτείνουμε το μέγεθος των δειγμάτων εξόδου της RNG, να είναι όσο το μέγεθος των εξόδων του αλγορίθμου, δηλαδή της τάξης του 1Mbit. Ωστόσο, η τελική απόφαση εναπόκειται στον αξιολογητή, η οποία βέβαια θα εξαρτηθεί και από την υπολογιστική ισχύ που διαθέτει.

Όπως είπαμε, για την παραγωγή των κλειδών πολλοί χρήστες προτιμούν να χρησιμοποιούν δική τους RNG. Πολλά όμως κρυπτοσυστήματα προσφέρουν (προαιρετικά) δικό τους σύστημα παραγωγής κλειδών (KGU). Εάν ο χρήστης επιθυμεί να χρησιμοποιήσει το προαιρετικό KGU, θα πρέπει να αξιολογήσει την RNG του, σύμφωνα με όσα αναφέραμε. Ωστόσο, η αξιολόγηση της προαιρετικής RNG δεν πρέπει να επηρεάσει την αξιολόγηση του κρυπτογραφικού συστήματος (όπως φαίνεται στο Σχήμα 21), διότι το κρυπτοσύστημα μπορεί να είναι ασφαλές, ενώ η RNG του να μην είναι.

β. Παραγωγή κλειδών από ενσωματωμένη RNG

Εάν το κρυπτογραφικό σύστημα δεν έχει την δυνατότητα εξωτερικής παραγωγής και εισαγωγής των κλειδών (δηλαδή παράγει τις κλείδες με ενσωματωμένη γεννήτρια RNG και τις εισάγει αυτόματα στον αλγόριθμο χωρίς την παρέμβαση του χρήστη), τότε όπως φαίνεται και στο Σχήμα 21, υπάρχουν δύο υποπεριπτώσεις:

(1). Εάν η ενσωματωμένη RNG είναι πιστοποιημένη (σύμφωνα με όσα αναφέρθηκαν στα Κεφάλαια 9 και 10), τότε η ασφάλεια του συστήματος μειώνεται κατά ένα βαθμό σε σχέση με το βαθμό ισχύος που έχει ο κρυπτογραφικός του αλγόριθμος. Οπότε, για το παράδειγμα του Σχήματος 21, το κρυπτογραφικό σύστημα παίρνει ένα προσωρινό βαθμό «Υψηλή Ασφάλεια» και κατόπιν ακολουθεί η αξιολόγηση των υπόλοιπων μηχανισμών ασφαλείας του (οι οποίοι ενδεχομένως να μειώσουν περαιτέρω την ασφάλειά του).

(2). Εάν η RNG δεν είναι πιστοποιημένη, τότε η ασφάλεια του συστήματος μειώνεται κατά δύο βαθμούς σε σχέση με το βαθμό ισχύος του κρυπτογραφικού του αλγορίθμου. Οπότε για το παράδειγμα του Σχήματος 21, το κρυπτογραφικό σύστημα λαμβάνει ένα προσωρινό βαθμό «Μέση Ασφάλεια» και κατόπιν ακολουθεί η αξιολόγηση των υπόλοιπων μηχανισμών ασφαλείας του (οι οποίοι ενδεχομένως να μειώσουν περαιτέρω την ασφάλειά του).

13.3.2. Υπόλοιποι μηχανισμοί ασφαλείας

Μετά την αξιολόγηση του μηχανισμού Παραγωγής και Διαχείρισης των κλειδών, ακολουθεί η αξιολόγηση των υπολοίπων μηχανισμών ασφαλείας οι οποίοι αναφέρθηκαν στην παράγραφο 13.1, δηλαδή της Υλοποίησης του αλγορίθμου (hardware ή software), της Πρόσβασης των χρηστών (access control), της Προστασίας από παραβίαση (tamper proof), των Αυτοελέγχων (self tests) και της Προστασίας από ηλεκτρομαγνητικές ακτινοβολίες (TEMPEST). Έτσι, θα έχουμε τρεις περιπτώσεις:

α. Όλοι οι μηχανισμοί ασφαλείας είναι επαρκείς:

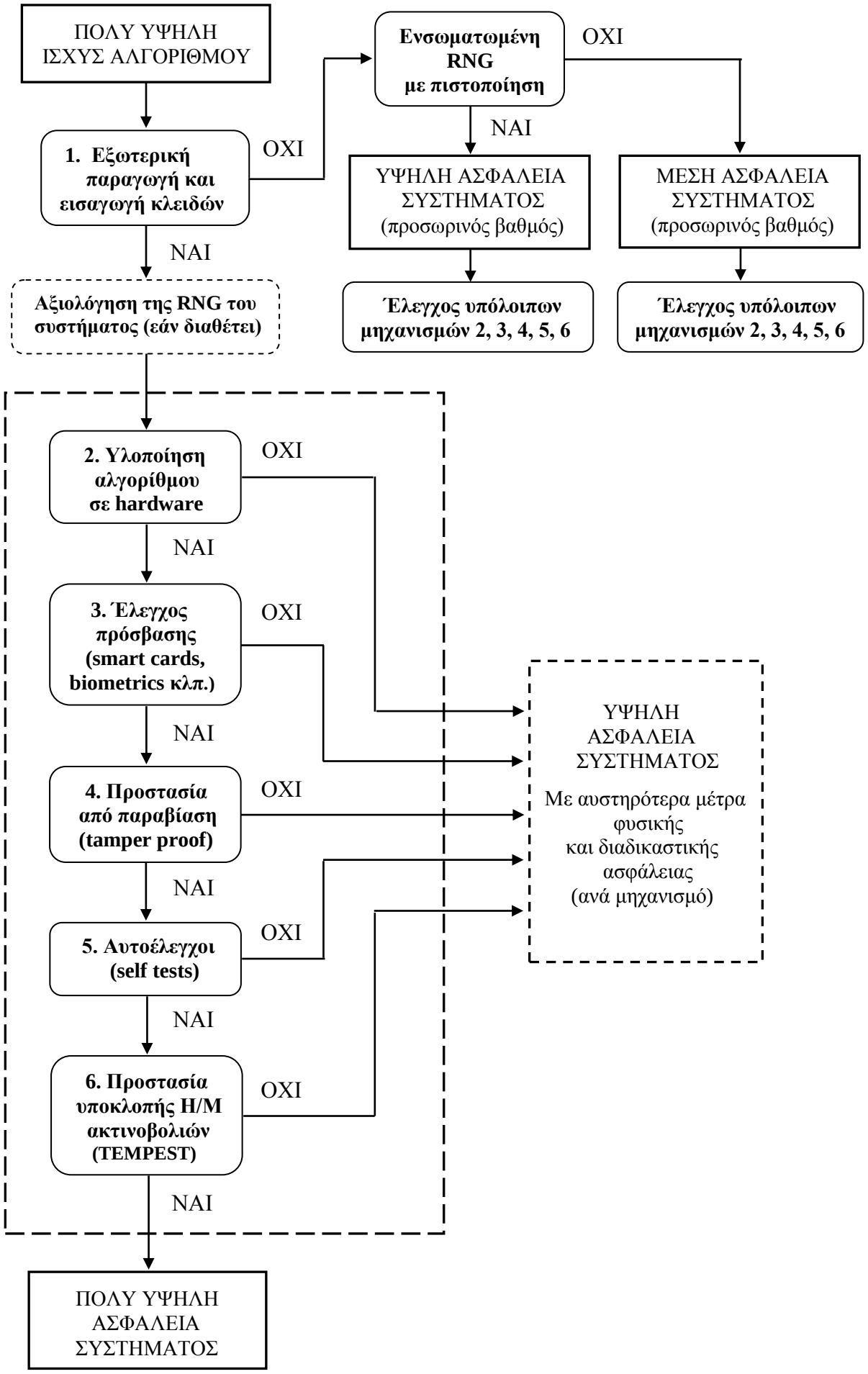
Εφόσον όλοι οι μηχανισμοί είναι επαρκείς (ενδείξεις «ΝΑΙ» στο διάγραμμα ροής), τότε η ασφάλεια του κρυπτογραφικού συστήματος αντιστοιχεί με το βαθμό ισχύος που έχει ο κρυπτογραφικός του αλγόριθμος (Πίνακας 29). Δηλαδή για το παράδειγμα του Σχήματος 21, το κρυπτογραφικό σύστημα έχει Πολύ Υψηλή Ασφάλεια.

β. Όλοι οι μηχανισμοί ασφαλείας είναι ανεπαρκείς:

Εφόσον όλοι οι μηχανισμοί είναι ανεπαρκείς (ενδείξεις «ΟΧΙ» στο διάγραμμα ροής), τότε η ασφάλεια του κρυπτογραφικού συστήματος μειώνεται κατά ένα βαθμό σε σχέση με το βαθμό ισχύος που έχει ο κρυπτογραφικός του αλγόριθμος (Πίνακας 29). Δηλαδή για το παράδειγμα του Σχήματος 21, το κρυπτογραφικό σύστημα έχει Υψηλή Ασφάλεια. Επί πλέον, προστίθεται και η προϋπόθεση ότι πρέπει να ληφθούν αυστηρότερα μέτρα φυσικής και διαδικαστικής ασφάλειας (ανά περίπτωση μηχανισμού), ώστε να αντιμετωπιστούν οι κίνδυνοι της ανεπάρκειας των μηχανισμών.

γ. Ορισμένοι από τους μηχανισμούς ασφαλείας είναι ανεπαρκείς:

Εφόσον μόνο ορισμένοι (και όχι όλοι) οι μηχανισμοί είναι ανεπαρκείς, τότε η ασφάλεια του κρυπτογραφικού συστήματος μπορεί να μη μειωθεί κατά ένα βαθμό σε σχέση με το βαθμό ισχύος του κρυπτογραφικού του αλγορίθμου. Ανάλογα με την κρίση του αξιολογητή και ανάλογα με το βαθμό της ανεπάρκειας ορισμένων μηχανισμών του, μπορεί να διατηρήσει την Πολύ Υψηλή Ασφάλεια λόγω του αλγορίθμου του (παράδειγμα Σχήματος 21), με κάποια ειδικά μέτρα φυσικής και διαδικαστικής ασφάλειας (ανά περίπτωση μηχανισμού), ώστε να αντιμετωπιστούν οι κίνδυνοι της ανεπάρκειας των μηχανισμών.



<u>Σχήμα 21</u>. Διαδικασία αξιολόγησης κρυπτογραφικού συστήματος - Έλεγχος των μηχανισμών ασφαλείας 1,2,3,4,5,6 (για την περίπτωση αλγορίθμου πολύ υψηλής ισχύος).

Σημειώσεις:

1. Στην περίπτωση των προσωρινών βαθμών της Υψηλής και Μέσης Ασφάλειας συστήματος (επάνω δεξιό τμήμα του Σχήματος 21), ο έλεγχος των υπόλοιπων μηχανισμών ασφαλείας 2, 3, 4, 5, 6, μπορεί να μειώσει περαιτέρω την τελική ασφάλεια. Π.χ. εάν οι μηχανισμοί ασφαλείας δεν είναι επαρκείς, ο προσωρινός βαθμός της Υψηλής Ασφάλειας πιθανόν να μειωθεί σε Μέση Ασφάλεια και ο προσωρινός βαθμός της Μέσης Ασφάλειας πιθανόν να μειωθεί σε Χαμηλή Ασφάλεια.

2. Οι απαντήσεις στο διάγραμμα ροής του Σχήματος 21, ενδεχομένως να μην είναι ένα απόλυτο ΝΑΙ (επαρκής ισχύς) ή ΟΧΙ (ανεπαρκής ισχύς), αλλά μία ενδιάμεση κατάσταση. Σε αυτή την περίπτωση, η αξιολόγηση της επάρκειας της ισχύος του κάθε μηχανισμού ασφαλείας εναπόκειται στην κρίση του αξιολογητή.

3. Για την ισχύ των μηχανισμών ασφαλείας, θα παίξει σημαντικό ρόλο, η πιστοποίηση του κρυπτογραφικού συστήματος σύμφωνα με τα πρότυπα FIPS 140-2 και ISO 15408. Προτείνουμε οι μηχανισμοί ασφαλείας να θεωρηθούν επαρκείς εάν το κρυπτοσύστημα έχει βαθμό ασφαλείας 3 ή ανώτερο (Security Level 3 για το FIPS 140-2 και EAL 3 για το ISO 15408), και ανεπαρκείς εάν το κρυπτοσύστημα έχει βαθμό ασφαλείας 2 ή κατώτερο (Security Level 2 για το FIPS 140-2 και EAL 2 για το ISO 15408).

4. Θα πρέπει να λαμβάνεται υπόψη ότι ορισμένοι από τους μηχανισμούς ασφαλείας είναι αλληλοσυμπληρούμενοι και αλληλοεξαρτώμενοι.

Παραδείγματα:

1. Αν σε ένα κρυπτογραφικό σύστημα ο αλγόριθμος είναι υλοποιημένος σε λογισμικό (software), αλλά πρόκειται να εγκατασταθεί εντός ενός ασφαλούς χώρου, με αυστηρά μέτρα φυσικής προστασίας, αυστηρά μέτρα ελέγχου του εισερχόμενου προσωπικού, και διενεργούνται αυτόματοι αυτοέλεγχοι ακεραιότητας του αλγορίθμου στην εκκίνηση του συστήματος, τότε μπορεί να περάσει με επιτυχία τον έλεγχο υπ'αρ. 2 του Σχήματος 21.

2. Αν ένα κρυπτογραφικό σύστημα δεν έχει επαρκή ενσωματωμένα μέτρα έναντι παραβίασης (tamper), αλλά πρόκειται να εγκατασταθεί εντός ενός πολύ ασφαλούς χώρου (με πολύ αυστηρά μέτρα φυσικής προστασίας και πολύ αυστηρά μέτρα ελέγχου του εισερχόμενου προσωπικού κλπ.), τότε μπορεί να περάσει με επιτυχία τον έλεγχο υπ'αρ. 4 του Σχήματος 21.

3. Αν ένα κρυπτογραφικό σύστημα δεν έχει επαρκή ενσωματωμένα μέτρα ηλεκτρομαγνητικής προστασίας, αλλά πρόκειται να εγκατασταθεί εντός θωρακισμένου θαλάμου (κλωβός Faraday), τότε μπορεί να περάσει με επιτυχία τον έλεγχο υπ'αρ. 6 του Σχήματος 21.

13.4. Προϋποθέσεις ισχύος της αξιολόγησης

Μετά από την διεξαγωγή μιας αξιολόγησης**,** οι τρεις βασικές προϋποθέσεις οι οποίες πρέπει να τηρούνται κατά τη διάρκεια της λειτουργίας του κρυπτογραφικού συστήματος ώστε να ισχύει η αξιολόγησή του και η δοθείσα σε αυτό αντίστοιχη πιστοποίηση, αφορούν τα εξής τρία βασικά μέτρα ασφαλείας των κλειδών :

α. Παραγωγή των κλειδών από μία RNG με πιστοποιημένη τυχαιότητα και η οποία έχει αντίστοιχη εντροπία με αυτή του κρυπταλγορίθμου.

β. Τήρηση αυστηρών μέτρων προστασίας των κλειδών, καθ'όλη την διάρκεια της χρήσης τους (ασφαλής διαχείριση).

γ. Συχνή αλλαγή των κλειδών (μικρή κρυπτοπερίοδος).

Τα ανωτέρω μέτρα έχουν συζητηθεί διεξοδικά στο Κεφάλαιο 6.

13.5. Διάρκεια ισχύος αξιολόγησης - Επαναξιολόγηση

Η χρονική διάρκεια κατά την οποία θα ισχύει μία αξιολόγηση, εκτός από την αυστηρή τήρηση των προαναφερθέντων μέτρων ασφαλείας της κλείδας, εξαρτάται και από την εμφάνιση με την πάροδο του χρόνου, κάποιων κρυπταναλυτικών απειλών εναντίον του κρυπτογραφικού συστήματος. Η αντιμετώπιση αυτών των απειλών μπορεί να γίνει είτε με έκτακτη επαναξιολόγηση (επείγουσα), είτε με τακτική επαναξιολόγηση (προληπτική - περιοδική).

α. Έκτακτη επαναξιολόγηση

Θα πρέπει να διεξαχθεί άμεσα μία έκτακτη επαναξιολόγηση του κρυπτογραφικού αλγορίθμου, όταν εμφανιστεί κάποια από τις παρακάτω σοβαρές κρυπταναλυτικές απειλές:

α. Έχει γίνει γνωστή μια μέθοδος κρυπταναλυτικής επίθεσης εναντίον του αλγορίθμου (στην περίπτωση που ο αλγόριθμος είναι δημοσιευμένος).

β. Υπάρχει ένδειξη ή βεβαιότητα ότι έχει γίνει διαρροή του αλγορίθμου ή κάποιων στοιχείων της δομής του (στην περίπτωση που ο αλγόριθμος είναι μυστικός).

Η έκτακτη επαναξιολόγηση διεξάγεται ώστε να διαπιστωθεί εάν ο κρυπταλγόριθμος εξακολουθεί να είναι ασφαλής και κατά πόσον διατρέχουν κίνδυνο οι πληροφορίες οι οποίες έχουν κρυπτογραφηθεί με αυτόν. Στην περίπτωση που η επαναξιολόγηση δείξει ότι ο κρυπταλγόριθμος δεν παρέχει πλέον το ίδιο επίπεδο ασφάλειας, θα πρέπει να αντικατασταθεί άμεσα με κάποιον ισχυρότερο. Επίσης, για προληπτικούς λόγους και εφόσον είναι δυνατόν, όλες οι αποθηκευμένες κρυπτογραφημένες πληροφορίες με τον παλαιό αλγόριθμο θα πρέπει να ανασυρθούν και να επανακρυπτογραφηθούν με τον νέο αλγόριθμο και μετά να επαναποθηκευτούν.

Ανάλογα με την περίπτωση, ως εναλλακτική ή προσωρινή λύση μέχρι να επιλεγεί κάποιος νέος ισχυρότερος αλγόριθμος, ενδεχομένως να εξακολουθήσει να χρησιμοποιείται ο παλαιός αλγόριθμος με αύξηση της συχνότητας αλλαγής των κλειδών του (μείωση της κρυπτοπεριόδου) ή με επικρυπτογράφηση της εξόδου του από ένα άλλο αλγόριθμο.

Με την πάροδο του χρόνου, εκτός από τις κρυπταναλυτικές απειλές εναντίον του αλγορίθμου, είναι ενδεχόμενο να εμφανιστούν και κάποιες νέες μέθοδοι επίθεσης εναντίον των μηχανισμών ασφαλείας του κρυπτογραφικού συστήματος, οι οποίοι αναφέρθηκαν στην προηγούμενη παράγραφο. Στην περίπτωση αυτή θα πρέπει να διεξαχθεί έκτακτη επαναξιολόγηση και στους μηχανισμούς ασφαλείας.

β. Τακτική επαναξιολόγηση

Όπως αναφέραμε στην προηγούμενη παράγραφο, η έκτακτη επαναξιολόγηση του κρυπτογραφικού συστήματος διεξάγεται όταν διαπιστώσουμε την ύπαρξη μίας σοβαρής απειλής. Όμως αυτή η διαπίστωση μπορεί να γίνει καθυστερημένα και έτσι ενδεχομένως να έχει ήδη υπάρξει κάποια ζημία στην ασφάλειά μας (π.χ. κρυπτανάλυση του αλγορίθμου και αποκρυπτογράφηση διαβαθμισμένων πληροφοριών). Για το λόγο αυτό, θα πρέπει να διεξάγεται περιοδικά μία τακτική επαναξιολόγηση του κρυπτογραφικού συστήματος, ώστε να προληφθούν εγκαίρως τυχόν επιθέσεις εναντίον του. Η διαδικασία της τακτικής επαναξιολόγησης είναι ίδια με την διαδικασία της αρχικής αξιολόγησης (η οποία περιγράφηκε στην παράγραφο 13.3.), θα πρέπει όμως κατά την διάρκειά της να ερευνηθούν και να ληφθούν σοβαρά υπόψη οι εξής παράγοντες:

α. Η εξέλιξη της τεχνολογίας στον τομέα της ισχύος (ταχύτητας) των ηλεκτρονικών υπολογιστών.

β. Η εξέλιξη των μεθόδων των κρυπταναλυτικών επιθέσεων, καθώς και των επιθέσεων στους υπόλοιπους μηχανισμούς ασφαλείας.

γ. Η εξέλιξη στις μεθόδους αξιολόγησης των κρυπτογραφικών συστημάτων.

Είναι προφανές ότι θα πρέπει να διεξάγεται συνεχώς έρευνα για την εξεύρεση νέων βελτιωμένων μεθόδων και πρακτικών αξιολόγησης (π.χ. προσθήκη νέων στατιστικών ελέγχων, αύξηση της υπολογιστικής ισχύος ώστε να εξετάζονται περισσότερα δείγματα κλπ.). Και είναι πολύ σημαντικό, σε κάθε επαναξιολόγηση (τακτική ή έκτακτη) να λαμβάνονται υπόψη αυτές οι βελτιωμένες μέθοδοι και πρακτικές, διότι μπορεί να αποκαλύψουν κάποια καινούργια τρωτά σημεία στο αξιολογούμενο κρυπτογραφικό σύστημα.

Σε ότι αφορά την συχνότητα με την οποία θα πρέπει να διεξάγεται η τακτική (περιοδική) επαναξιολόγηση, αυτή εξαρτάται από την εξέλιξη την οποία θα έχουν με την πάροδο του χρόνου οι ανωτέρω τρεις παράγοντες (α), (β) και (γ). Ωστόσο, ο μόνος από αυτούς ο οποίος μπορεί να προβλεφθεί με ικανοποιητική προσέγγιση, είναι ο πρώτος (εξέλιξη της ισχύος των ηλεκτρονικών υπολογιστών). Σύμφωνα με τα συμπεράσματα της παραγράφου 5.6, για να αντισταθμιστεί η συνεχής εξέλιξη της ισχύος των Η/Υ λόγω του νόμου του Moore, η κλείδα πρέπει να αυξάνει κατά ένα bit κάθε χρόνο, ώστε να είμαστε ασφαλείς έναντι της εξαντλητικής έρευνας των κλειδών (Brute Force Attack – BFA). Ως αποτέλεσμα αυτού του γεγονότος, στον Πίνακα 30 δείχνουμε τα μήκη των κλειδών τα οποία πρέπει να ισχύουν κάθε 5 χρόνια, ώστε οι κρυπταλγόριθμοι να είναι ασφαλείς έναντι της BFA, σύμφωνα με την αναμενόμενη τεχνολογική εξέλιξη.

ΕΤΟΣ	ΙΣΧΥΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ			
	ΧΑΜΗΛΗ	**ΜΕΤΡΙΑ**	**ΥΨΗΛΗ**	**ΠΟΛΥ ΥΨΗΛΗ**
2017	**$80 \leq K \leq 112$**	**$112 < K < 128$**	**$128 \leq K \leq 192$**	**$192 < K \leq 256$**
2022	**$85 \leq K \leq 117$**	**$117 < K < 133$**	**$133 \leq K \leq 197$**	**$197 < K \leq 261$**
2027	**$90 \leq K \leq 122$**	**$122 < K < 138$**	**$138 \leq K \leq 202$**	**$202 < K \leq 266$**
2032	**$95 \leq K \leq 127$**	**$127 < K < 143$**	**$143 \leq K \leq 207$**	**$207 < K \leq 271$**
2037	**$100 \leq K \leq 132$**	**$132 < K < 148$**	**$148 \leq K \leq 212$**	**$212 < K \leq 276$**

Πίνακας 30. Αντιστοιχία του μήκους της κλείδας K (σε bits) και της ισχύος των κρυπταλγορίθμων ανά 5 χρόνια, σύμφωνα με την αναμενόμενη τεχνολογική εξέλιξη (νόμος του Moore).

Από τον Πίνακα 30 βλέπουμε ότι, ένας αλγόριθμος ο οποίος έχει κλείδα 128 bits ενώ σήμερα θεωρείται ότι έχει υψηλή ισχύ (έτος 2017), μετά από 5 χρόνια θα έχει μέτρια ισχύ (έτος 2022), ενώ μετά από 20 χρόνια θα έχει χαμηλή ισχύ (έτος 2037).

Από όσα αναφέρθηκαν, θεωρούμε ότι η βέλτιστη περίοδος διεξαγωγής της τακτικής επαναξιολόγησης ενός κρυπτογραφικού αλγορίθμου είναι κάθε 5 χρόνια. Διότι όπως φαίνεται από τον Πίνακα 30, ουσιαστικά κάθε 5 χρόνια υποβαθμίζεται κατά 5 bits η ισχύς του. Αυτό βέβαια ισχύει υπό την προϋπόθεση ότι δεν έχουν εμφανιστεί εν τω μεταξύ κάποιες μη αναμενόμενες κρυπταναλυτικές και τεχνολογικές εξελίξεις (π.χ. κβαντικοί υπολογιστές).

ΚΕΦΑΛΑΙΟ 14

ΕΠΙΛΟΓΗ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

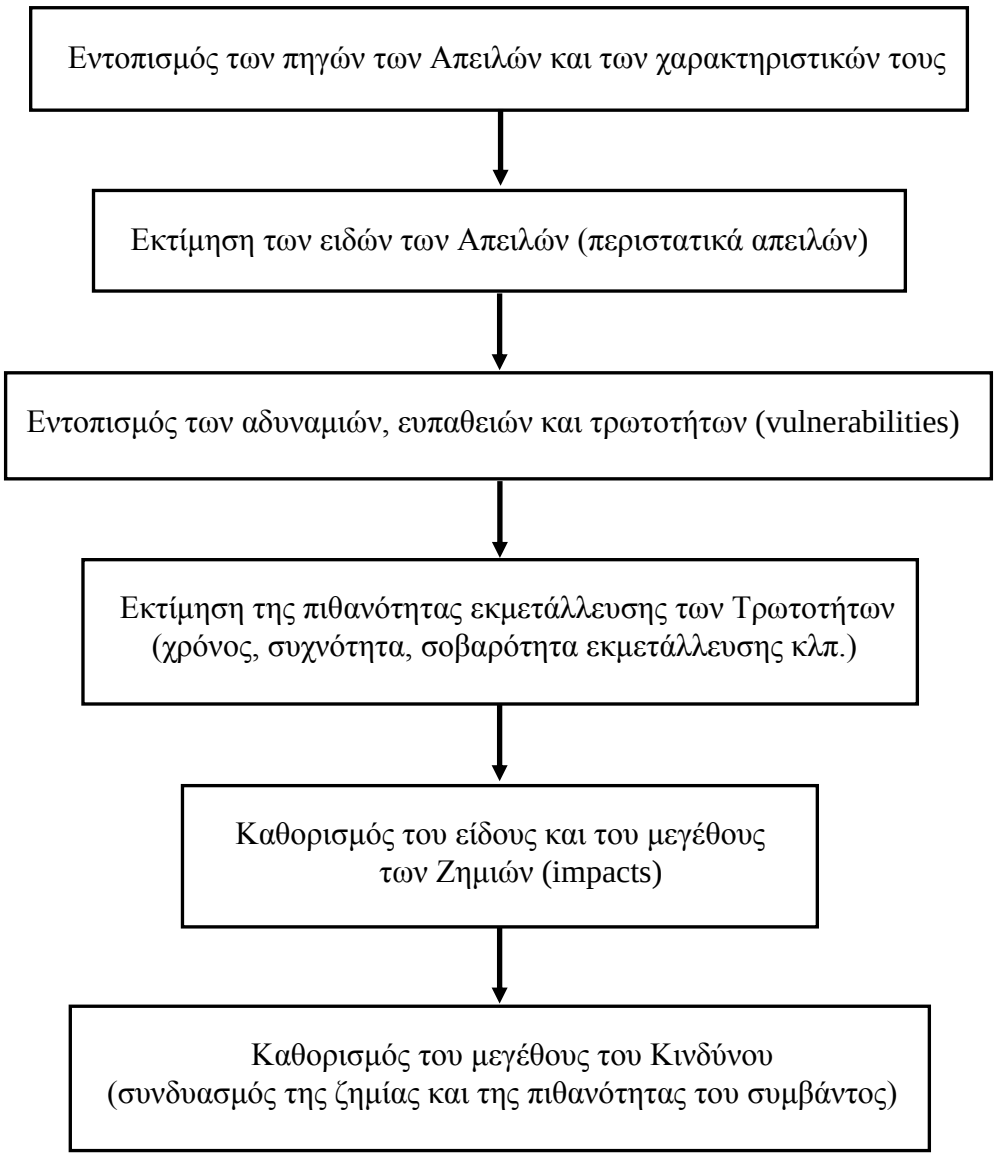
Στο παρόν Κεφάλαιο 14 θα αναπτυχθούν η μεθοδολογία και τα κριτήρια τα οποία πρέπει να εφαρμόσει ένας χρήστης, για να επιλέξει το καταλληλότερο κρυπτογραφικό σύστημα για τις ανάγκες του.

14.1. Ανάλυση και εκτίμηση κινδύνου

Η βασική διαδικασία για την σωστή επιλογή ενός κρυπτογραφικού συστήματος, είναι η ανάλυση και εκτίμηση των κινδύνων στους οποίους ενδέχεται να εκτεθεί το κρυπτοσύστημα, μέσα στο περιβάλλον στο οποίο πρόκειται να λειτουργήσει (risk analysis and assessment). Ο κίνδυνος εκφράζει το κατά πόσο κάποιες απειλές (threats) θα εκμεταλλευτούν κάποιες τρωτότητες (vulnerabilities) του συστήματος. Το μέγεθος του κινδύνου υπολογίζεται από τον μέγιστο βαθμό της ζημίας (impact) την οποία θα υποστεί ο χρήστης, εάν θα υπάρξει κάποιο σοβαρό πλήγμα στις βασικές απαιτήσεις της ασφάλειας των πληροφοριών, δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τους. Ανάλογα με το μέγεθός τους, οι ζημίες μπορεί να προκαλέσουν διακοπή των λειτουργιών ενός συστήματος, να καταστρέψουν μονάδες του σε υλικό ή λογισμικό (assets), να βλάψουν την αξιοπιστία και τη φήμη του οργανισμού ο οποίος διαχειρίζεται το σύστημα ή ακόμα και να θέσουν σε κίνδυνο ανθρώπινες ζωές. Πριν προχωρήσουμε στην εκτίμηση των κινδύνων του κρυπτοσυστήματος, θα κάνουμε μια σύντομη ανασκόπηση της διαδικασίας ανάλυσης κινδύνου (βάσει του **[49]** της βιβλιογραφίας).

Στο Σχήμα 22 φαίνεται η βασική διαδικασία της ανάλυσης και εκτίμησης κινδύνου, καθώς και η σχέση μεταξύ της απειλής, της τρωτότητας και της ζημίας, οι οποίοι ονομάζονται παράγοντες κινδύνου (risk factors). Όπως φαίνεται, η ανάλυση του κινδύνου ξεκινάει από τον εντοπισμό της πηγής της απειλής. Πηγής της απειλής μπορεί να είναι ένας αντίπαλος ο οποίος έχει τη δυνατότητα να υποκλέψει τις επικοινωνίες μας. Έτσι, μπορεί να πάρει υπό την κατοχή του κρυπτογραφημένα μηνύματα τα οποία να προσπαθήσει να τα αποκρυπτογραφήσει (απειλή). Και ενδεχομένως, λόγω κάποιου ελαττώματος στον αλγόριθμο ή λόγω του μικρού μήκους της κλείδας (τρωτότητες), να κατορθώσει να διασπάσει κάποια μηνύματα (πρόκληση ζημίας). Στην περίπτωση αυτή, ο βαθμός του προκύπτοντος κινδύνου εξαρτάται από τον όγκο και την σημαντικότητα των αποκρυπτογραφημένων πληροφοριών.

Πηγή της απειλής όμως, μπορεί να είναι και ένα φυσικό φαινόμενο π.χ. ένας κεραυνός, ο οποίος να διακόψει την παροχή ρεύματος (απειλή), λόγω έλλειψης αντικεραυνικής προστασίας (τρωτότητα). Έτσι, μπορεί να διακοπεί η λειτουργία ενός τηλεπικοινωνιακού δικτύου και επομένως να παύσει η παροχή υπηρεσιών στους χρήστες ή να καταστραφούν αποθηκευτικά μέσα με συνέπεια την απώλεια πληροφοριών (πρόκληση ζημιών). Στην περίπτωση αυτή, ο βαθμός του κινδύνου εξαρτάται από τις επιχειρησιακές και οικονομικές επιπτώσεις λόγω της διακοπής των υπηρεσιών (μη διαθεσιμότητα πληροφοριών) ή λόγω της καταστροφής πληροφοριών ή λόγω του κόστους επισκευής και αντικατάστασης του κατεστραμμένου υλικού/λογισμικού.



Σχήμα 22. Βασική διαδικασία Ανάλυσης και Εκτίμησης Κινδύνου

14.2. Εκτίμηση κινδύνου κρυπτογραφικού συστήματος

Όπως αναφέραμε, εκτός από την ισχύ του κρυπτογραφικού αλγορίθμου, οι επί μέρους μονάδες οι οποίες εμπλέκονται στην συνολική αξιολόγηση της ασφάλειας ενός κρυπτογραφικού συστήματος, είναι αυτές οι οποίες υλοποιούν τους βασικούς μηχανισμούς ασφαλείας του.

Σύμφωνα λοιπόν με όσα αναφέρθηκαν στην προηγούμενη παράγραφο, παρουσιάζουμε στον Πίνακα 31 το μέγεθος του κινδύνου στον οποίο εκτίθεται ένα κρυπτογραφικό σύστημα, ανάλογα με το είδος και τον τρόπο υλοποίησης του αλγορίθμου και των μηχανισμών ασφαλείας του. Τα είδη των υφιστάμενων απειλών εναντίον του κρυπτοσυστήματος, καθώς και οι πιθανές τρωτότητες τις οποίες ενδέχεται να έχει, ελήφθησαν από τις σχετικές αναλύσεις οι οποίες έγιναν στο Κεφάλαιο 7 (τρόπος υλοποίησης αλγορίθμου), στο Κεφάλαιο 8 (δημοσιευμένοι και μυστικοί αλγόριθμοι) και στα Κεφάλαια 9 και 10 (είδη και αξιοπιστία μηχανισμών ασφαλείας).

ΕΙΔΗ ΑΠΕΙΛΩΝ οι οποίες μπορούν να εκμεταλλευτούν αντίστοιχες τρωτότητες	**ΤΡΩΤΟΤΗΤΕΣ** (ανάλογα με το είδος και τον τρόπο υλοποίησης)			
	ΔΗΜΟΣΙΕΥΜΕΝΟΣ ΑΛΓΟΡΙΘΜΟΣ		**ΜΥΣΤΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ**	
	SOFTWARE υλοποίηση	**HARDWARE** υλοποίηση	**SOFTWARE** υλοποίηση	**HARDWARE** υλοποίηση
Κρυπτανάλυση	**Πολύ μεγάλος**	**Μεγάλος**	**Μέτριος**	**Μικρός**
Εισαγωγή κερκόπορτας (trap door)	**Πολύ μεγάλος**	**Μεγάλος**	**Μέτριος**	**Μικρός**
Παράκαμψη απλού κωδικού (PIN, password κλπ.)	**Μεγάλος**	**Μέτριος**	**Μεγάλος**	**Μέτριος**
Παράκαμψη βιομετρικού κωδικού	**Μικρός**	**Μικρός**	**Μικρός**	**Μικρός**
Παραβίαση (tamper)	**Μεγάλος**	**Μικρός**	**Μεγάλος**	**Μικρός**

Πίνακας 31. Μέγεθος κινδύνου ενός κρυπτοσυστήματος , ανάλογα με το είδος και τον τρόπο υλοποίησης του αλγορίθμου και των μηχανισμών ασφαλείας.

Στον Πίνακα 32, παρουσιάζουμε το μέγεθος του κινδύνου υποκλοπής της ηλεκτρομαγνητικής ακτινοβολίας (TEMPEST), ανάλογα με την ακτίνα του ασφαλούς ελεγχόμενου χώρου εντός του οποίου ευρίσκεται ένα κρυπτογραφικό σύστημα. Ο κίνδυνος υπολογίστηκε σύμφωνα με όσα αναφέρθηκαν στο Κεφάλαιο 11 και αφορά συστήματα τα οποία δεν έχουν Η/Μ θωράκιση και δεν είναι εγκατεστημένα εντός προστατευτικού κλωβού (Faraday). Ο βαθμοί του κινδύνου είναι ενδεικτικοί και όχι απόλυτοι, διότι αφενός το μέγεθος της ισχύος των ακτινοβολιών εξαρτάται από το είδος του εξοπλισμού (hardware) και τις τεχνικές της εγκατάστασης (γειώσεις, φίλτρα κλπ.), αφετέρου η δυνατότητα υποκλοπής εξαρτάται και από την ποιότητα του εξοπλισμού του αντιπάλου.

Και τέλος, στον Πίνακα 33, παρουσιάζουμε το μέγεθος του κινδύνου στον οποίο εκτίθεται ένα κρυπτοσύστημα, ανάλογα με την ηλικία του αλγορίθμου και των μηχανισμών ασφαλείας του. Ο βαθμός κινδύνου είναι ενδεικτικός και όχι απόλυτος, και υπολογίστηκε σύμφωνα με όσα αναφέρθηκαν στην παράγραφο 5.6 του Κεφαλαίου 5 (αναμενόμενη τεχνολογική εξέλιξη). Στη τελευταία στήλη του Πίνακα 33, δίδονται γενικές συστάσεις για την αντιμετώπιση του σχετικού κινδύνου.

Ακτίνα r ελεγχόμενου χώρου (μέτρα)	**$0 < r \leq 20$**	**$20 < r \leq 50$**	**$50 < r \leq 100$**	**$r > 100$**
Κίνδυνος υποκλοπής Η/Μ ακτινοβολίας	**ΥΨΗΛΟΣ**	**ΑΥΞΗΜΕΝΟΣ**	**ΜΕΤΡΙΟΣ**	**ΜΙΚΡΟΣ**

Πίνακας 32. Κίνδυνος υποκλοπής της Η/Μ ακτινοβολίας ανάλογα με την ακτίνα του ελεγχόμενου χώρου (για κρυπτοσυστήματα χωρίς Η/Μ θωράκιση και εκτός προστατευτικού κλωβού Faraday).

Ηλικία (T) του κρυπτογραφικού συστήματος (έτη)	**ΚΙΝΔΥΝΟΣ ΑΣΦΑΛΕΙΑΣ**	**Παρατηρήσεις / Συστάσεις**
$1 < T \leq 5$	**Πολύ μικρός**	----------
$5 < T \leq 10$	**Μικρός**	----------
$10 < T \leq 15$	**Μέτριος**	----------
$15 < T \leq 20$	**Αυξημένος**	Αύξηση του μήκους της κλείδας (εφόσον είναι εφικτό)
$20 < T \leq 25$	**Υψηλός**	Αντικατάσταση του αλγορίθμου
$25 < T \leq 30$	**Πολύ υψηλός**	Αντικατάσταση των μηχανισμών ασφαλείας
$T > 30$	**Εξαιρετικά υψηλός**	Αντικατάσταση του κρυπτοσυστήματος

Πίνακας 33. Μέγεθος κινδύνου ενός κρυπτοσυστήματος, ανάλογα με την ηλικία του αλγορίθμου και των μηχανισμών ασφαλείας του.

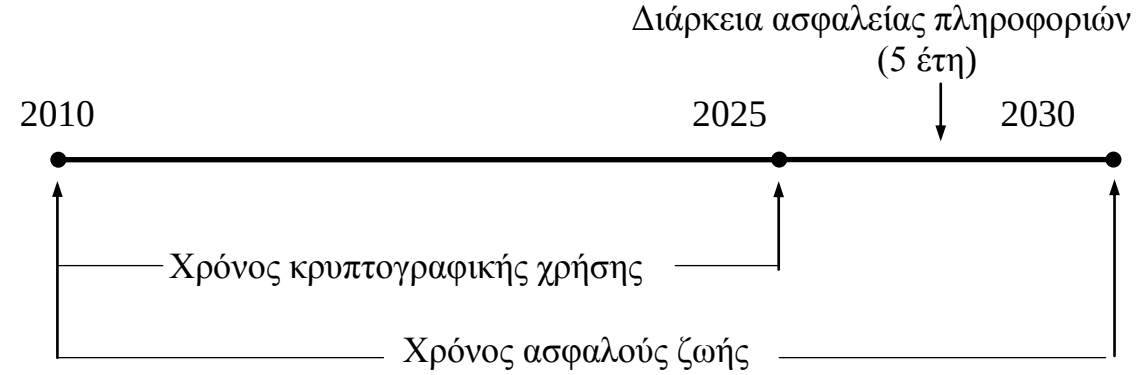
14.3. Χρόνος ζωής κρυπταλγορίθμου και κρυπτοσυστήματος

Χρόνος ασφαλούς ζωής ενός κρυπταλγορίθμου είναι το χρονικό διάστημα κατά το οποίο θεωρούμε ότι αντέχει σε κρυπταναλυτικές επιθέσεις και επομένως είναι ασφαλής η χρήση του **[37]**. Όμως για την σωστή επιλογή ενός κρυπταλγορίθμου δεν πρέπει να λάβουμε υπόψη μόνο το χρόνο για τον οποίο αυτός είναι ασφαλής, αλλά και τον χρόνο για τον οποίο οι πληροφορίες θέλουμε να παραμείνουν εμπιστευτικές. Διότι μετά την κρυπτογράφησή τους, οι πληροφορίες αποθηκεύονται και μπορεί να αποκρυπτογραφηθούν πολύ αργότερα (π.χ. για μια περαιτέρω επεξεργασία ή αποστολή). Έτσι, ο χρόνος Ασφαλούς Ζωής ενός κρυπταλγορίθμου T_{AZ} δίδεται από τη σχέση :

$$T_{AZ} = T_{AK} + T_{EP} \quad (1)$$

όπου T_{AK} είναι το χρονικό διάστημα Ασφαλούς Κρυπτογραφικής χρήσης του αλγορίθμου και T_{EP} είναι το επιθυμητό χρονικό διάστημα Εμπιστευτικότητας των Πληροφοριών.

Παράδειγμα: Ας υποθέσουμε ότι ένας αλγόριθμος χρησιμοποιείται από το 2010 και σύμφωνα με όσα έχουμε αναφέρει, εκτιμήσαμε ότι μετά από 20 έτη (δηλαδή το έτος 2030), πρέπει να λήξει η χρήση του διότι θα έχει υποβιβαστεί σημαντικά η ασφάλειά του. Αυτό σημαίνει ότι ο χρόνος T_{AZ} στον τύπο (1) είναι 20 έτη. Εάν ο αλγόριθμος χρησιμοποιηθεί για κρυπτογράφηση πληροφοριών οι οποίες έχουν χρόνο ασφαλείας 5 έτη (χρόνος T_{EP}), αυτό σημαίνει ότι ο αλγόριθμος πρέπει να χρησιμοποιείται για κρυπτογράφηση μόνο για 20-5=15 έτη (χρόνος T_{AK}). Για τα υπόλοιπα πέντε έτη πρέπει να χρησιμοποιείται μόνο για αποκρυπτογράφηση των πληροφοριών τις οποίες κρυπτογράφησε. Διότι εάν π.χ. υποθέσουμε ότι ο αλγόριθμος εξακολουθεί να κρυπτογραφεί μετά από 16 έτη (το 2026), τότε μετά από 5 έτη (δηλαδή το 2031) οι πληροφορίες θα είναι εκτεθειμένες διότι ο αλγόριθμος δεν θα είναι πλέον ασφαλής. Τα παραπάνω φαίνονται στο διάγραμμα του Σχήματος 23.



Σχήμα 23. Παράδειγμα ασφαλούς χρόνου ζωής κρυπταλγορίθμου

Ο τύπος (1) ισχύει για τους κρυπτογραφικούς αλγορίθμους, διότι αναφέρεται μόνο στην κρυπτογράφηση και επομένως αφορά μόνο την εμπιστευτικότητα των πληροφοριών. Μπορούμε όμως να τον επεκτείνουμε στον τύπο (2) ο οποίος αφορά τα κρυπτογραφικά συστήματα, εάν συνυπολογίσουμε και το χρονικό διάστημα ασφαλούς χρήσης των υπολοίπων μηχανισμών ασφαλείας (οι οποίοι αναφέρθηκαν στο Κεφάλαιο 13). Έτσι ο τύπος (2) θα αφορά την ολική ασφάλεια των πληροφοριών (εμπιστευτικότητα, αυθεντικότητα, ακεραιότητα, διαθεσιμότητα):

$$T_{AZ} = T_{AE} + T_{AP} \quad (2)$$

όπου T_{AE} είναι το χρονικό διάστημα Ασφαλούς Επεξεργασίας, το οποίο εκτός από την κρυπτογράφηση περιλαμβάνει και τις λειτουργίες των μηχανισμών ασφαλείας, ενώ T_{AP} είναι το επιθυμητό χρονικό διάστημα της συνολικής Ασφάλειας των Πληροφοριών (εμπιστευτικότητα, αυθεντικότητα, ακεραιότητα, διαθεσιμότητα).

14.4. Επιλογή κρυπτογραφικού συστήματος

Για την σωστή επιλογή ενός κρυπτογραφικού συστήματος, θα πρέπει να καθοριστούν δύο βασικά στοιχεία: Το μέγεθος της υφιστάμενης απειλής και το μέγεθος της ζημίας σε περίπτωση κάποιου πλήγματος στην ασφάλεια του.

α. Μέγεθος της απειλής: Το μέγεθος της απειλής καθορίζεται ανάλογα με τους κινδύνους στους οποίους θα εκτεθεί το σύστημα μέσα στο επιχειρησιακό του περιβάλλον. Όπως αναφέραμε, για το σκοπό αυτό θα πρέπει να εντοπιστούν οι πηγές των απειλών και τα χαρακτηριστικά τους. Δηλαδή θα πρέπει να γίνει έρευνα για την ύπαρξη των παρακάτω στοιχείων:

-Εξωτερικοί εισβολείς (ανταγωνιστικές εταιρείες, ξένες υπηρεσίες κλπ.). Επίσης, εξέταση των επιπτώσεων από φυσικές καταστροφές (κεραυνοί, πλημμύρες σεισμοί, πυρκαγιές κλπ.).

-Εσωτερικοί εισβολείς (π.χ. κακόβουλοι ή μη εξουσιοδοτημένοι υπάλληλοι). Επίσης, εξέταση των επιπτώσεων από τυχόν λάθη και παραλείψεις ή από βλάβες υλικού/λογισμικού.

-Προθέσεις, κίνητρα και οφέλη των εισβολέων.

-Τεχνογνωσία και υποδομή των εισβολέων.

-Οικονομική δυνατότητα των εισβολέων (για να επενδύσουν σε τεχνογνωσία και σε υποδομή).

β. Μέγεθος της ζημίας : Όπως αναφέραμε, ο κίνδυνος υπολογίζεται από το μέγιστο βαθμό ζημίας (impact), όταν μειωθεί κάποια από τις βασικές απαιτήσεις της ασφάλειας των πληροφοριών (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα). Στον Πίνακα 34 φαίνονται τα επίπεδα της ζημίας και η αντίστοιχη περιγραφή τους ανά απαίτηση ασφαλείας (από το **[50]**).

Security Objective	Potential Impact		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Πίνακας 34. Επίπεδα της ζημίας και η αντίστοιχη περιγραφή τους ανά απαίτηση ασφαλείας (SECURITY OBJECTIVE).

Συνήθως όμως οι χρήστες και οι υπηρεσίες, εκφράζουν τον υφιστάμενο κίνδυνο, βάσει του βαθμού ασφαλείας των πληροφοριών, ο οποίος αντιστοιχεί στο μέγεθος της ζημίας στην περίπτωση ανεπιθύμητης διαρροής τους. Δηλαδή ο βαθμός ασφαλείας των πληροφοριών εκφράζει τον κίνδυνο απώλειας της εμπιστευτικότητάς τους (πρώτη γραμμή του Πίνακα 34 - Confidentiality). Έτσι, αντί για τα τρία γενικά επίπεδα ζημίας Χαμηλό (Low), Μέσο (Moderate) και Υψηλό (High) του Πίνακα 34, όλες οι κρατικές υπηρεσίες του ΝΑΤΟ και της Ε.Ε., έχουν καθορίσει πέντε βαθμούς ασφαλείας των πληροφοριών: Άκρως απόρρητο (Top Secret), Απόρρητο (Secret), Εμπιστευτικό (Confidential), Περιορισμένης χρήσεως (Restricted) και Αδιαβάθμητο (Unclassified). Στη χώρα μας, σύμφωνα με τον Εθνικό Κανονισμό Βιομηχανικής Ασφάλειας (ΕΚΒΑ - βιβλ. **[51]**), οι διαβαθμίσεις ασφαλείας φαίνονται στον Πίνακα 35:

ΑΡΘΡΟ 4

ΔΙΑΒΑΘΜΙΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

1. Ο βαθμός της παρεχόμενης προστασίας πρέπει να ανταποκρίνεται στην κρισιμότητα και στη σπουδαιότητα της πληροφορίας ή του υλικού το οποίο πρέπει να προστατευθεί. Για να καταδειχθεί και εξασφαλισθεί ο βαθμός προστασίας που πρέπει να παρέχεται στο εθνικό υλικό, θα πρέπει όλα τα έγγραφα και οι πληροφορίες να διαβαθμίζονται ανάλογα με χαρακτηρισμό που δίδεται από τον εκδότη, και να κοινοποιούνται σε περιορισμένο προσωπικό κατάλληλα εξουσιοδοτημένο.

2. Οι βαθμοί ασφαλείας και η σημασία τους περιγράφονται όπως παρακάτω:

α. ΕΤΝΑ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ (ΕΤΝΑ-ΑΑΠ)

(1) Ο χαρακτηρισμός αυτός δίδεται σε υλικό-πληροφορίες, οι οποίες εάν αποκαλυφθούν σε μη εξουσιοδοτημένο προσωπικό, θα προκαλέσουν εξαιρετικά βαριές ζημιές στην Εθνική Άμυνα και ασφάλεια της χώρας, καθώς και στα ζωτικά της συμφέροντα.

(2) Επισημαίνεται ότι ο όρος «ΕΤΝΑ», δεν αποτελεί διαβάθμιση υλικού, αλλά ένδειξη που προέρχεται από τη λέξη "ΕΘΝΙΚΟ", για να είναι δυνατή η αναγραφή της με τα ίδια τυπογραφικά στοιχεία και στην Ελληνική και στις γλώσσες που χρησιμοποιούν το λατινικό αλφάβητο.

β. ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ (ΑΑΠ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό-πληροφορίες, οι οποίες εάν αποκαλυφθούν σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να προκαλέσουν σοβαρές ζημιές στην Εθνική Άμυνα και ασφάλεια της χώρας, καθώς και στα ζωτικά της συμφέροντα.

γ. ΑΠΟΡΡΗΤΟ (ΑΠ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό-πληροφορίες οι οποίες εάν αποκαλυφθούν σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να προκαλέσουν ζημιές στην Εθνική Άμυνα και ασφάλεια της χώρας, καθώς και στα ζωτικά της συμφέροντα.

δ. ΕΜΠΙΣΤΕΥΤΙΚΟ (ΕΠ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό-πληροφορίες, οι οποίες εάν αποκαλυφθούν σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να βλάψουν την Εθνική Άμυνα και ασφάλεια της χώρας, καθώς και τα ζωτικά της συμφέροντα.

ε. ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ (ΠΧ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό-πληροφορίες, οι οποίες εάν αποκαλυφθούν σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να επηρεάσουν δυσμενώς την Εθνική Άμυνα και ασφάλεια της χώρας, καθώς και τα ζωτικά της συμφέροντα.

στ. ΑΔΙΑΒΑΘΜΗΤΟ (ΑΔ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό πληροφορίες, των οποίων λαμβάνουν γνώση μόνο τα απαραίτητα υπηρεσιακά πρόσωπα και πάντοτε με βάση την αρχή «ΑΝΑΓΚΗ ΓΝΩΣΗΣ».

Πίνακας 35. Απόσπασμα από τον Εθνικό Κανονισμό Βιομηχανικής Ασφάλειας (ΕΚΒΑ), ΦΕΚ Αρ. Φύλλου 336 / 16 Μαρτίου 2005, σελίδα 4165.

Λαμβάνοντας από τον Πίνακα 35 τους τέσσερεις κύριους βαθμούς ασφαλείας (Άκρως απόρρητο, Απόρρητο, Εμπιστευτικό και Περιορισμένης χρήσεως), καταρτίσαμε τον Πίνακα 36, ο οποίος δείχνει την απαιτούμενη

ασφάλεια που πρέπει να διαθέτει το κρυπτογραφικό σύστημα που θα επιλέξουμε, ανάλογα με το μέγεθος της απειλής και το μέγιστο βαθμό ασφαλείας των πληροφοριών μας. Η ασφάλεια του κρυπτογραφικού συστήματος υπολογίζεται σύμφωνα με όσα αναφέραμε στο Κεφάλαιο 13.

ΜΕΓΙΣΤΟΣ ΒΑΘΜΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ	**ΜΕΓΕΘΟΣ ΑΠΕΙΛΗΣ**			
	ΠΟΛΥ ΥΨΗΛΟ	**ΥΨΗΛΟ**	**ΜΕΣΟ**	**ΧΑΜΗΛΟ**
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	**ΠΟΛΥ ΥΨΗΛΗ**	**ΠΟΛΥ ΥΨΗΛΗ**	**ΥΨΗΛΗ**	**ΥΨΗΛΗ**
ΑΠΟΡΡΗΤΟ	**ΥΨΗΛΗ**	**ΥΨΗΛΗ**	**ΜΕΣΗ**	**ΜΕΣΗ**
ΕΜΠΙΣΤΕΥΤΙΚΟ	**ΜΕΣΗ**	**ΜΕΣΗ**	**ΧΑΜΗΛΗ**	**ΧΑΜΗΛΗ**
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	**ΧΑΜΗΛΗ**	**ΧΑΜΗΛΗ**	**ΧΑΜΗΛΗ**	**ΧΑΜΗΛΗ**

Πίνακας 36. Απαιτούμενη ασφάλεια του κρυπτογραφικού συστήματος (με κόκκινο), ανάλογα με το μέγεθος της απειλής και το μέγιστο βαθμό ασφαλείας των πληροφοριών.

ΚΕΦΑΛΑΙΟ 15

ΑΝΑΚΕΦΑΛΑΙΩΣΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

15.1. Ανακεφαλαίωση

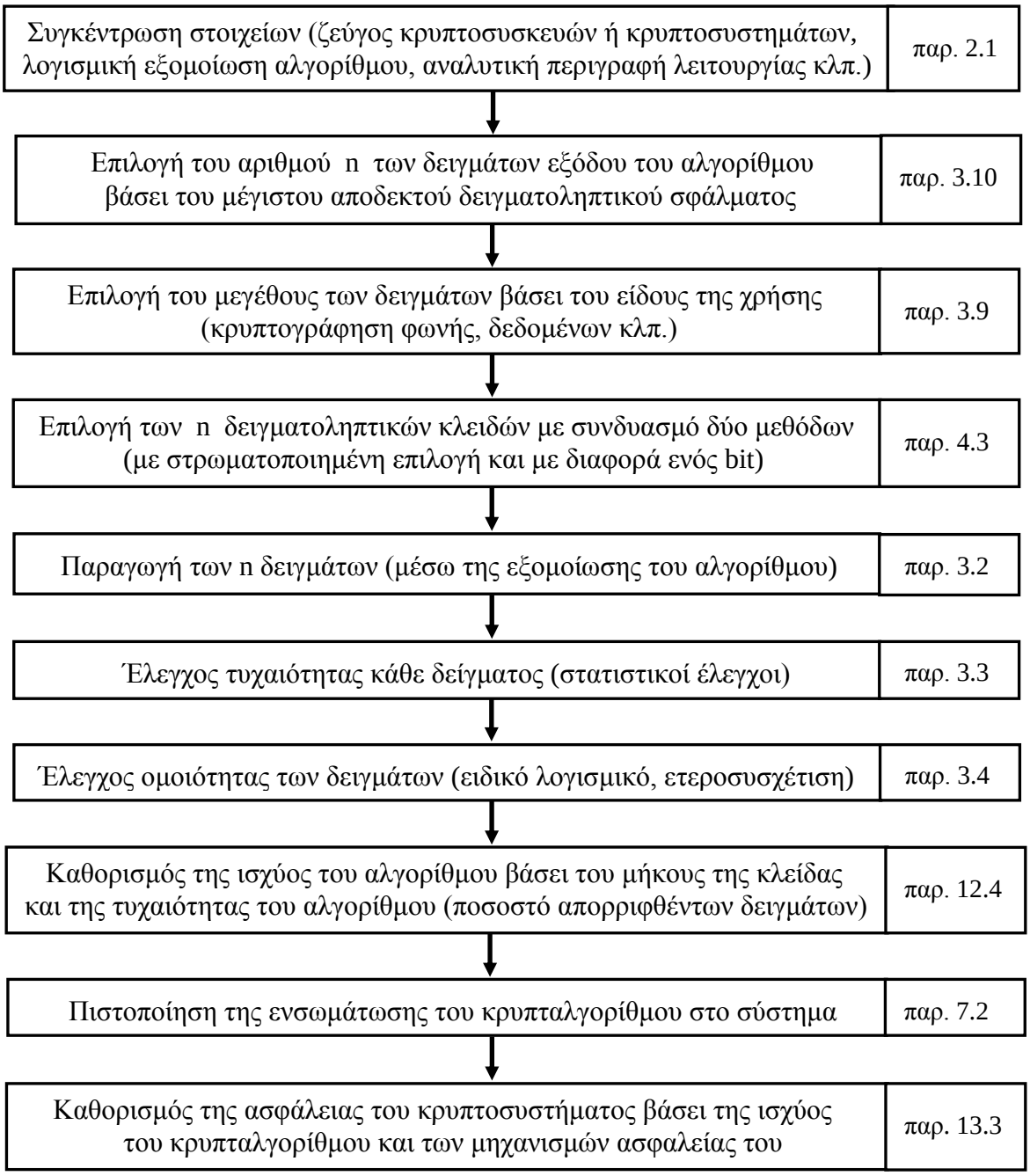
Ο στόχος της παρούσας διατριβής ήταν σε πρώτη φάση να μελετήσει τις ευπάθειες και τις τρωτότητες των διαφόρων κρυπτογραφικών συστημάτων, καθώς και τους τρόπους με τους οποίους αυτές μπορούν να εντοπιστούν, ώστε να αποφευχθεί η εκμετάλλευσή τους για κρυπταναλυτικές επιθέσεις. Και σε δεύτερη και κύρια φάση, ο στόχος της διατριβής ήταν να μελετήσει τις τεχνικές παραμέτρους και τα διάφορα προβλήματα που ανακύπτουν, κατά τις αξιολογήσεις της ασφάλειας των κρυπτογραφικών συστημάτων. Κατά τη διάρκεια αυτή, προτάθηκαν συγκεκριμένες μέθοδοι, κριτήρια και τεχνικές διαδικασίες βασισμένες σε επιστημονικά δεδομένα, με στόχο την όσο το δυνατόν πιο αξιόπιστη αξιολόγηση της ασφάλειας την οποία παρέχουν τα διάφορα κρυπτογραφικά συστήματα.

Η αξιολόγηση ενός κρυπτογραφικού συστήματος είναι μία εξαιρετικά σύνθετη και πολύπλοκη εργασία, η οποία περιλαμβάνει πολλά στάδια. Και τούτο διότι ένα ολοκληρωμένο κρυπτογραφικό σύστημα αποτελείται από πολλές αλληλοεξαρτώμενες μονάδες, η λειτουργία των οποίων θα πρέπει να εξεταστεί. Από όλες τις μονάδες του κρυπτογραφικού συστήματος, η πιο σημαντική είναι αυτή του κρυπτογραφικού αλγορίθμου, για αυτό και εξετάζεται στο πρώτο στάδιο της αξιολόγησης. Κατά την φάση αυτή, αξιολογούμε το μήκος της κλείδας ως προς την αντοχή του στη εξαντλητική έρευνα (με κριτήριο την σημερινή και την μέλλουσα υπολογιστική ισχύ), καθώς και την τυχαιότητα των παραγόμενων ψηφιακών ακολουθιών του αλγορίθμου με τη διενέργεια εδικών στατιστικών ελέγχων. Με τον τρόπο αυτό γίνεται μία εκτίμηση της ισχύος ασφαλείας του αλγορίθμου, δηλαδή της αντοχής του στις κρυπταναλυτικές επιθέσεις.

Μετά από την εξέταση του αλγορίθμου, είναι απαραίτητο να διεξαχθούν και περαιτέρω έλεγχοι στο κρυπτοσύστημα. Αυτοί αφορούν τον τρόπο υλοποίησης και ενσωμάτωσης του αλγορίθμου εντός του συστήματος, τον τρόπο παραγωγής και διαχείρισης των κλειδών, καθώς και τον τρόπο υλοποίησης των περιφερειακών μηχανισμών ασφαλείας (ασφάλεια πρόσβασης, ασφάλεια παραβίασης, αυτοέλεγχοι, ασφάλεια ηλεκτρομαγνητικών ακτινοβολιών κλπ.). Έτσι, η αξιολόγηση ενός κρυπτογραφικού συστήματος ουσιαστικά περιλαμβάνει δύο κύρια στάδια, την αξιολόγηση του κρυπταλγορίθμου και την αξιολόγηση των μηχανισμών ασφαλείας του.

15.2. Συμπεράσματα

Συνοψίζοντας τα σημαντικότερα συμπεράσματα από τις μελέτες των προηγούμενων κεφαλαίων, στο διάγραμμα του Σχήματος 24 δείχνουμε κατά χρονική σειρά εκτέλεσης τα βασικά στάδια και διαδικασίες της αξιολόγησης ενός κρυπτογραφικού συστήματος, καθώς και την παράγραφο στην οποία αναλύθηκε κάθε ένα από τα ανωτέρω στάδια.



Σχήμα 24. Διαδικασία αξιολόγησης κρυπτογραφικού συστήματος

Όπως αναφέραμε και στην εισαγωγή, η ολοκληρωμένη αξιολόγηση των κρυπτογραφικών συστημάτων είναι ένα δύσκολο, εξειδικευμένο και ευαίσθητο έργο για το οποίο υπάρχουν ελάχιστες αναφορές στη διεθνή βιβλιογραφία. Ωστόσο, σήμερα με την πληθώρα των κρυπτογραφικών συστημάτων τα οποία κυκλοφορούν στο εμπόριο, αυξάνονται οι δημόσιοι και οι ιδιωτικοί φορείς, οι οποίοι επιθυμούν να αναπτύξουν δικά τους μέσα και τεχνογνωσία, ώστε να ελέγχουν, να αξιολογούν και να συγκρίνουν τα κρυπτογραφικά συστήματα, διότι έτσι μπορούν να επιλέξουν ορθότερα και ασφαλέστερα τα συστήματα αυτά για τις ανάγκες τους. Πιστεύουμε ότι η παρούσα διατριβή μπορεί να αποτελέσει ένα εφαρμοσμένο και επιστημονικά τεκμηριωμένο τεχνικό πρότυπο για την αξιολόγηση των κρυπτογραφικών συστημάτων, συμβάλλοντας έτσι και στην διαρκή βελτίωσή τους.

..... * .....

Βιβλιογραφία :

1. Alfred Menezes, Paul C. van Oorschot, Scott A.Vanstone, "*Handbook of Applied Cryptography"*, CRC Press 1997.

2. Bruce Schneier, "*Applied Cryptography"*, John Wiley, New York, 1996.

3. D.W.Davies, W.L.Price, *"Security for computer networks",* D.W.Davies, W.L.Price, Wiley & Sons/1984.

4. Donald Knuth, "*The Art of Computer Programming-Volume 2/ Seminumerical Algorithms",* Addison-Wesley 1998.

5. G.Marsaglia, G.: DIEHARD: *"Battery of Tests of Randomness"*. Available at: http://stat.fsu.edu/pub/diehard/ (1996), http://stat.fsu.edu/pub/diehard/

6. NIST Special Publication 800-22, *"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"* National Institute of Standards and Technology (NIST), April 2010.

7. Helen Gustafson et. al., *"A computer package for measuring strength of encryption algorithms,"* Journal of Computers & Security, vol. 13, no. 8, 1994, pp. 687-697.

8. Juan Soto, "*Statistical Testing of Random Number Generators"*, National Institute of Standards and Technology (NIST).

9. D.Eastlake, S.Crocker, J.Schiller, "*RFC 1750 - Randomness Recommendations for Security"*, Network Working Group, December 1994.

10. «Στοιχεία πιθανοθεωρίας μετ'εφαρμογών», Γεώργιος Γρ. Ρούσσας, Πάτρα 1973.

11. «Θεωρία σημάτων - Απλών και Στοχαστικών - Μέρος Ι και Μέρος ΙΙ», Νικόλαος-Σταμάτιος Τζάννες, Πάτρα 1976.

12. "Signal Processing - Continuous and Discrete", Massachusetts Institute of Technology, Fall Term 2008.

13. "Measuring Signal Similarities" (using the MATLAB software) https://www.mathworks.com/help/signal/examples/measuring-signal-similarities.html

14. Harrison M. Wadsworth, *"Handbook of Statistical Methods for Engineers and Scientists",* Mc Graw-Hill, 1990.

15. «Μεθοδολογία δειγματοληψίας - Τεχνικές και εφαρμογές» Χαράλαμπου Χ. Δαμιανού - Εκδόσεις Αίθρα.

16. "Determining sample size" - Glen D. Israel - University of Florida.

17. M. Blaze, W. Diffie, R.L. Rivest, B. Schneier, T. Shimomura, E. Thompson and M. Wiener,*"Minimal key lengths for symmetric ciphers to provide adequate Commercial security"*, (January 1996), www.bsa.org/policy/encryption/cryptographers c.html.

18. Daniel J. Bernstein and Peter Schwabe, *"New AES software speed records"*, http://cr.yp.to/aes-speed/aesspeed-20080926.pdf

19. Kris Gaj and Pawel Chodowiec, *"FPGA and ASIC Implementations of AES"*, http://teal.gmu.edu/courses/ECE746/project.

20. Helion Technology, *"Overview Datasheet - High Performance AES (Rijndael) cores for ASIC"*, http://www.heliontech.com/downloads.

21. G.E. Moore, *"Cramming more components onto integrated circuits"*, *Electronics*, 38(8), (Apr. 1965).

22. Intel, *"Moores Law: An Intel Perspective"*, Intel Corporation, 2005.

23. Ralph K. Cavin, Paolo Lugli and Victor V. Zhirnov, *"Science and Engineering Beyond Moores Law"*, *Proceedings of the IEEE*, 100, (May, 2012).

24. M.Dugan, "*Analysis of existing implementations of TRNG"*, May 2005.

25. Carl Ellison, "*P1363:Appendix E-Cryptographic Random Numbers, Draft V1.0"*, November 1995.

26. FIPS 140-2, *"Security Requirements for cryptographic modules"*, National Institute of Standards and Technology (NIST), May 2001.

27. W.Killmann, W.Schindler, AIS 31: *"Functionality classes and evaluation methodology for true (physical) random number generators"*, version 3.1., Bundesamt fur Sicherheit in der Informationstechnik (BSI), Bonn 2001.

28. Tim Matthews , *"Suggestions for Random Number Generators in software"*, RSA Data Security Engineering Report, December 1995.

29. Robert W. Baldwin, *"Preliminary Analysis of the BSAFE 3.x Pseudorandom Number Generators,"* RSA Laboratories Technical Bulletin, Number 8, September 1998.

30. W.W. Tsang, C.W. Tso, Lucas Hui, K.P. Chow, K.H. Pun, C.F. Chong, H.W. Chan *"Development of Cryptographic Random Number Generators*", Department of Computer Science and Information Systems, University of Hong Kong, August 2003.

31. AIS 20, *"Functionality classes and evaluation methodology for deterministic random number generators"*, Bundesamt fur Sicherheit in der Informationstechnik (BSI), December 1999.

32. Viktor Fischer, "A Closer Look at Security in Random Number Generators Design", Laboratoire Hubert Curien, Jean Monnet University, May 2012.

33. M. Liskov, R. Rivest, and D. Wagner "Tweakable block ciphers" In *Advances in Cryptology – CRYPTO '02*. Lecture Notes in Computer Science, vol 2442, Springer-Verlag, 2002.

34. P. Rogaway "Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC". Advances in Cryptology - Asiacrypt 2004. Lecture Notes in Computer Science, vol.3329,Springer-Verlag, 2004.

35. IEEE Std 1619-2007, *The XTS-AES Tweakable Block Cipher*, Institute of Electrical and Electronics Engineers, Inc., Apr. 18, 2008.

36. https://www.jetico.com/web_help/bc8/html/02_basic_concepts/06_encryption_mode.htm

37. NIST.SP.800-57pt1r4 - KEY MANAGEMENT RECOMMENDATIONS-1.pdf

38. https://www.zsis.hr/UserDocsImages/Sigurnost/pdfs/TCE621_B_C_AES&DUAL.pdf

39. Bob Wheeler "Suite B: Classified Network Security Goes Commercial" , July 2009, The Linley Group, Inc.

40. "Fact Sheet NSA Suite B Cryptography" https://web.archive.org/web/20051211150701/http://www.nsa.gov/ia/industry/crypto_suite_b.cfm

41. https://www.commoncriteriaportal.org/

42. "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model", Version 3.1, Revision 1 (CCMB-2006-09-001), September 2006. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

43. https://en.wikipedia.org/wiki/Common_Criteria

44. "TEMPEST Introduction", Secure Systems & Technologies http://sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf

45. "TEMPEST standards overview", Secure Systems & Technologies http://sst.ws/downloads/TEMPEST_Standards_overview_iss_4.pdf

46. "Information Assurance Security Guidelines on Accreditation of EU TEMPEST Companies" http://data.consilium.europa.eu/doc/document/ST-16267-2012-INIT/en/pdf

47. Γιώργος Μαρινάκης "Προστασία από ηλεκτρομαγνητικές ακτινοβολίες", Μεταπτυχιακή εργασία Ε.Μ.Π., Φεβρουάριος 2011.

48. Juan Soto, Jr.," Randomness Testing of the Advanced Encryption Standard Candidate Algorithms", NIST, IR 6390, September 1999.

49. NIST.SP.800-30 (Revision1)- Guide for Conducting Risk Assessments , September 2012.

50. NIST SP 800-60 v1r1- Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

51. Εθνικός Κανονισμός Βιομηχανικής Ασφάλειας (ΕΚΒΑ), ΦΕΚ Αρ. Φύλλου 336/16 Μαρτίου 2005).

..... * .....