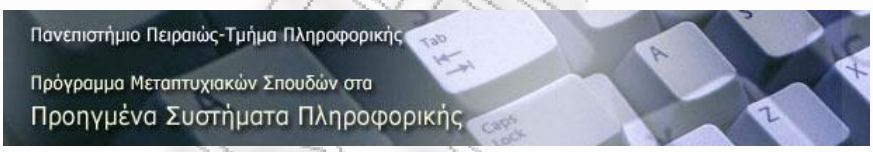
Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	«**Κρυπτογραφία** - **ασφάλεια** S-box **συμμετρικών αλγορίθμων**»
Ονοματεπώνυμο Φοιτητή	**Βερύκιος Θωμάς του Νικήτα**
Αριθμός Μητρώου	**ΜΠΣΠ** 08059
Κατεύθυνση	**Ευφυείς Τεχνολογίες Επικοινωνίας Ανθρώπου - Υπολογιστή**
Επιβλέπων	**Φούντας Ευάγγελος**, **Καθηγητής**



Ημερομηνία Παράδοσης 02 **Νοεμβρίου** 2010

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Φούντας Ευάγγελος Καθηγητής	Τσικούρας Παναγιώτης-Γεώργιος Καθηγητής	Αποστόλου Δημήτριος Λέκτορας

Ευχαριστίες

Με κάθε σεβασμό προς το πρόσωπό του, θα ήθελα να ευχαριστήσω τον Καθηγητή κ. Κωνσταντίνο Πατσάκη, για τη βοήθειά του αλλά και την υπομονή που έδειξε κατά τη διάρκεια της συνεργασίας μας, την συνεχή εμπιστοσύνη και καθοδήγησή του και κυρίως για την αμέριστη ηθική συμπαράσταση που μου προσέφερε.

Περίληψη

Το ζήτημα της διακίνησης της πληροφορίας με τρόπο τέτοιο ώστε να επιτυγχάνεται η απαιτούμενη ασφάλεια και ταυτόχρονα να αποτρέπονται πιθανές προσπάθειες παραβίασης ή αλλοίωσης του περιεχομένου της, αποτελεί αντικείμενο επιστημονικής μελέτης από την αρχαιότητα. Ειδικότερα με την ραγδαία ανάπτυξη των τεχνολογιών επικοινωνίας στη σύγχρονη εποχή η ανάγκη ύπαρξης ασφαλών συστημάτων διαχείρισης της πληροφορίας γίνεται ακόμη πιο επιτακτική. Η κρυπτογραφία και οι διάφορες μεθοδολογίες που έχουν αναπτυχθεί με βάση αυτή, αποδεικνύεται μια αποδοτική λύση στα συγκεκριμένα ζητήματα ασφαλείας. Στην παρούσα εργασία γίνεται μια παρουσίαση των θεμελιωδών όρων της κρυπτογραφίας και των ιστορικών της στοιχείων. Στη συνέχεια αναφέρονται τα είδη στα οποία διακρίνεται καθώς και οι σημαντικότεροι αλγόριθμοι που έχουν αναπτυχθεί. Όπως αποδεικνύεται από τις διάφορες επιστημονικές μελέτες που έχουν αναπτυχθεί, σημαντικό συστατικό ενός αλγόριθμου κρυπτογράφησης αποτελεί το κουτί αντικατάστασης S-box για το οποίο παρουσιάζεται ο τρόπος σχεδίασης και λειτουργίας του και ορίζονται οι βασικές του ιδιότητες ως προς την απαιτούμενη ασφάλεια. Τέλος, παρουσιάζονται κάποιες από τις σημαντικότερες μελέτες που πιστοποιούν την ασφάλεια των S-boxes στους συμμετρικούς αλγορίθμους και της αντίστασής τους σε επιθέσεις αλγεβρικής, διαφορικής ή γραμμικής κρυπτανάλυσης.

Abstract

The issue of distribution of information in such a way as to obtain the requisite security and at the same time to prevent possible attempts of tampering or altering its content is the subject of scientific study since the antiquity. Especially with the rapid development of communication technologies in the modern era, the need for safe systems of information management becomes even more imperative. Cryptography and various methodologies have been developed on this basis, proved an effective solution to specific security issues. This paper presents the fundamental terms of cryptography and the historical data. Here are the species which is distinguished and the main algorithms having been developed. As evidenced by various scientific studies that have been developed, an important component of encryption algorithm is the substitution box "S-box" for which it is shown the way of design and function and identified the key attributes to the required security. Finally, some of the most important studies are presented which certify the safety of S-boxes for symmetric algorithms and their resistance to attacks algebraic, differential or linear cryptanalysis.

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1

1.1 Εισαγωγή 9

1.2 Θεμελιώδεις ορισμοί 11

1.3 Αντικειμενικοί σκοποί της κρυπτογραφίας 13

1.4 Ιστορικά στοιχεία και περίοδοι κρυπτογραφίας 13

1.4.1 Πρώιμα στάδια της κρυπτογραφίας 13

1.4.2 Μεσαίωνας και κρυπτογραφία 14

1.4.3 Κρυπτογραφία τον 20ο αιώνα 15

1.4.4 Κρυπτογραφία στη σύγχρονη εποχή 17

1.5 Είδη κρυπτογραφίας 18

1.5.1 Συμμετρική κρυπτογραφία (Symmetric Cryptography) ή κρυπτογραφία μυστικού κλειδιού (Secret-Key Cryptography) 18

1.5.2 Ασύμμετρη Κρυπτογραφία (Asymmetric Cryptography) ή Κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography) 20

1.5.3 Υβριδική Κρυπτογραφία 21

1.6 Συμμετρική ή Ασύμμετρη Κρυπτογραφία - Μειονεκτήματα και πλεονεκτήματα 24

ΚΕΦΑΛΑΙΟ 2

2.1 Αλγόριθμοι Ασύμμετρης Κρυπτογράφησης 27

2.1.1 Αλγόριθμος Diffie και Hellman 27

2.1.2 Ο αλγόριθμος RSA (Rivest/Shamir/Adleman) 27

2.1.3 Αλγόριθμος Digital Signature Algorithm (DSA) 28

2.2 Αλγόριθμοι Συμμετρικής Κρυπτογράφησης 29

2.2.1 Ο αλγόριθμος DES (Data Encryption Standard) 29

2.2.2 Ο Αλγόριθμος AES (Advanced Encryption Standard) 33

2.2.3 Ο ΑΛΓΟΡΙΘΜΟΣ IDEA (International Data Encryption Algorithm) 34

2.3 Κρυπτογραφικά συστήματα και ασφάλεια 35
2.4 Επιθέσεις κρυπτανάλυσης σε αλγορίθμους 36

ΚΕΦΑΛΑΙΟ 3

3.1 Κουτιά αντικατάστασης (S-boxes) 39
3.2 Παράμετροι ασφάλειας S-box 40
3.3 Ιδιότητες ενός "ιδεατού" κουτιού αντικατάστασης 41
3.4 Ασφάλεια S-boxes σε πιθανές αλγεβρικές επιθέσεις 43
3.5 Ασφάλεια των S-boxes βασισμένων στην τεχνική Matrix Power 45
3.6 Ασφάλεια των S-boxes βασισμένων στις συναρτήσεις BENT 47

Βιβλιογραφία 51

Κεφάλαιο 1

1.1 **Εισαγωγή**

Είναι κοινά αποδεκτό ότι στην σύγχρονη εποχή καθοριστικός παράγοντας ενός άρτια δομημένου και λειτουργικού πληροφοριακού περιβάλλοντος αποτελεί το ζήτημα της ασφάλειας διακίνησης της πληροφορίας. Είναι ένα διαρκές ζήτημα που παρά την πιο ολοκληρωμένη και αυτοματοποιημένη επικοινωνιακή διαδικασία που προσφέρει η σύγχρονη τεχνολογία παραμένει αντικείμενο μελέτης των διαφόρων σχετιζόμενων επιστημονικών κλάδων. Συγκεκριμένα η αυτοματοποίηση των διαδικασιών δεν σημαίνει απαραίτητα και τη λύση του προβλήματος, αφού προσφέρει ταχύτητα στις διαδιδόμενες υπηρεσίες αλλά δεν υπόσχεται την πολυπόθητη ασφάλεια.

Το επιθυμητό επίπεδο ασφάλειας ενός συστήματος θα πρέπει να προσδιορίζεται αρχικά με τον βαθμό σημαντικότητας της πληροφορίας που μεταδίδεται στα μέλη του. Για παράδειγμα ένα σύστημα διαχείρισης προσωπικών δεδομένων απαιτεί αυξημένους κανόνες και όρους ασφαλείας και σε πολύ μεγαλύτερο βαθμό από ένα σύστημα που λειτουργεί για να μεταφέρει αρχεία ελάσσονος σημασίας όπως εικόνες και ήχους. Με την διαρκή ανάπτυξη της τεχνολογίας έχουν χρησιμοποιηθεί συστήματα ασφαλείας της πληροφορίας κυρίως σε επίπεδο υλικού, δίνοντας κυρίως έμφαση στο μέσο αποθήκευσης των δεδομένων και στον δίαυλο μεταφοράς τους. Ωστόσο, τέτοιου είδους συστήματα δεν διαθέτουν σχεδόν καμία ευελιξία ούτε εγγυώνται την ασφάλεια ευαίσθητων δεδομένων καθώς δεν υπάρχει επί της ουσίας κάποιο σύστημα που να αντιμετωπίζει αποτελεσματικά στο σύνολό του τα διάφορα θέματα ασφαλείας. Γι αυτό το λόγο και κυρίως από επιστημονική άποψη, η πιο διαδεδομένη λύση σε θέματα ασφαλείας αποτελεί στις μέρες μας η Κρυπτογραφία.

"*Cryptography* is the science of keeping secrets secret"

Hans Delfs - Helmut Knebl
(Introduction to Cryptography)

Ως βασικό αντικείμενο της η κρυπτογραφία έχει την ανάπτυξη και υλοποίηση τεχνικών τροποποίησης της μεταδιδόμενης πληροφορίας, με τέτοιο τρόπο ώστε να μην είναι δυνατή ή υποκλοπή τους από μέλη που δεν έχουν την ιδιότητα του αποστολέα ή του παραλήπτη και βρίσκονται εκτός της προβλεπόμενης και αποδεκτής διαδικασίας. Σε τεχνικό επίπεδο η κρυπτογράφηση μπορεί να εκτελέσει τις διαδικασίες της είτε σε επίπεδο software είτε σε επίπεδο hardware. Ο συνδυασμός των δυνατοτήτων αυτών και κυρίως η ενσωμάτωση των τεχνικών κρυπτογράφησης σε επίπεδο hardware έχει καλύτερα αποτελέσματα και κυρίως επιτυγχάνει την διαδικασία της κρυπτογράφησης σε μικρότερο χρόνο. Ο χρήστης του συστήματος δεν εμπλέκεται σε κανένα στάδιο της κρυπτογράφησης καθιστώντας την όλη διαδικασία ασφαλέστερη ενώ πολλές φορές ή όλη διαδικασία μπορεί να γίνεται με τέτοιο τρόπο που να μην γίνει αντιληπτή από τις εμπλεκόμενες πλευρές.

Το αυξημένο κόστος όμως της εφαρμογής τεχνικών κρυπτογράφησης σε επίπεδο hardware καθιστά δύσκολη την καθιέρωσή της και γι αυτό συνήθως

ακολουθείται μια μικτή διαδικασία κρυπτογράφησης που βασίζεται στην χρήση διαφόρων αλγορίθμων και τεχνικών σε επίπεδο software. Σε αυτό το επίπεδο το απαιτούμενο κόστος χρήσης είναι σημαντικά μικρότερο και αντιπαρέρχεται με αυτόν τον τρόπο στον βραδύτερο χρόνο εκτέλεσής της.

Ως όρος η κρυπτογραφία (Cryptography) προέρχεται από τις λέξεις 'κρυπτός' και 'γράφος' και αποτελεί την διαδικασία μετατροπής του αρχικού μηνύματος σε κρυπτογραφημένη μορφή με τη χρήση μιας μαθηματικής ακολουθίας και ενός κλειδιού κρυπτογράφησης. Ο σημαντικός της ρόλος στην διασφάλιση της μεταδιδόμενης πληροφορίας μεταξύ των διαφόρων πληροφοριακών συστημάτων είναι πλέον ευρύτατα αποδεκτός αφού εκτός των άλλων προσφέρει:

- **ü** πιστοποίηση τη της ταυτότητας των εμπλεκόμενων πλευρών κατά την διαδικασία της δημιουργίας και μεταφοράς της πληροφορίας,
- **ü** προστασία αποθηκευμένης πληροφορίας σε κάθε είδους πληροφοριακό σύστημα από πρόσβαση σε μη εξουσιοδοτημένους χρήστες,
- **ü** διασφάλιση πληροφοριών κατά το στάδιο της μεταφοράς τους μεταξύ των διαφόρων πληροφοριακών συστημάτων,
- **ü** αποτροπή κάθε είδους προσπάθειας αλλοίωσης, επιθυμητής ή μη, της αποθηκευμένης ή μεταδιδόμενης πληροφορίας.

Παρότι πολλοί επιστήμονες διατείνονται ότι η κρυπτογράφηση αποτελεί πανάκεια στο επίπεδο ασφάλειας ενός πληροφοριακού συστήματος ή υπολογιστικού δικτύου, η αλήθεια είναι ότι ενώ αποτελεί ένα εργαλείο προς την κατεύθυνση της ασφάλειας συχνά η χρήση της για κακόβουλους σκοπούς αλλοιώνει τον χαρακτήρα και την σπουδαιότητα ύπαρξης των μεθόδων και τεχνικών της. Επίσης η κρυπτογράφηση είναι προτιμότερο να χρησιμοποιείται κατά την μεταφορά της πληροφορίας και όχι για την αποθήκευση της καθώς πολλές φορές είναι πιθανό ο κωδικός κρυπτογράφησης να είναι ένας απλός αριθμός που μπορεί εύκολα να υποκλαπεί. Σε παρόμοια περίπτωση "χαλαρού" κλειδιού κρυπτογράφησης είναι πιθανή η υποκλοπή του ίδιου του κλειδιού και η αντικατάσταση του με άλλο με αποτέλεσμα την ολοκληρωτική απόκτηση πρόσβασης στην προς απόκρυψη πληροφορία. Είναι κατανοητό από τα παραπάνω, ότι παρά τα πολλά της πλεονεκτήματα και τον δείκτη ασφάλειας που παρέχει στα διάφορα υπολογιστικά συστήματα, η κρυπτογραφία έχει και εμφανώς ευάλωτα σημεία καθώς:

- **ü** εκτός της απλής υποκλοπής κάποιος κακόβουλος χρήστης μπορεί να προβεί σε τροποποίηση του περιεχομένου της πληροφορίας με σκοπό να το χρησιμοποιήσει προς δικό του όφελος,

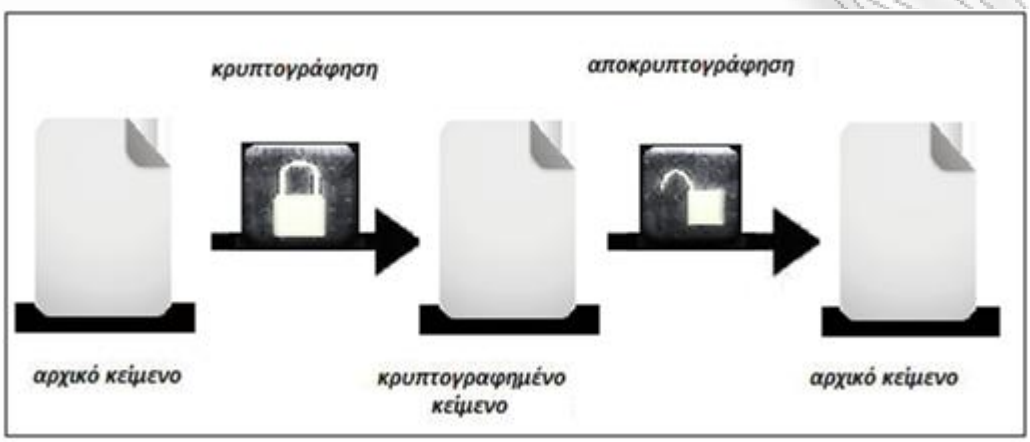
- είναι αδύνατη η αποτροπή κατά το ενδεχόμενο παραβίασης μη εξουσιοδοτημένου χρήστη από την ολοκληρωτική καταστροφή του περιεχομένου της πληροφορίας,
- είναι υπαρκτή η πιθανότητα κάποιος μη εξουσιοδοτημένος χρήστης να τροποποιήσει το κλειδί κρυπτογράφησης και να διατηρήσει την δομή της αποθηκευμένης πληροφορίας ή να προβεί στην καταγραφή των κλειδιών κωδικοποίησης για μελλοντική χρήση,
- είναι πιθανή η πρόσβαση στην πληροφορία από μη εξουσιοδοτημένους χρήστες πριν καν κρυπτογραφηθούν,
- είναι πιθανή η πρόσβαση στην πληροφορία από μη εξουσιοδοτημένους χρήστες μετά την διαδικασία της αποκρυπτογράφησης καθιστώντας άχρηστη την όλη προηγηθείσα διαδικασία.

1.2 **Θεμελιώδεις ορισμοί**

Πριν προχωρήσουμε την αναφορά μας στην ιστορία της κρυπτογραφίας, τις διαφορετικές τεχνικές που αναπτύχθηκαν από τα πρώτα στάδια εμφάνισής της έως τη σύγχρονη εποχή καθώς και τα διάφορα είδη στα οποία οι επιστημονική κοινότητα διαχωρίζει τις μεθόδους της, είναι απαραίτητο να αναφερθούμε συνοπτικά και στους θεμελιώδεις ορισμούς οι οποίοι την διέπουν. Η *κρυπτογραφία* έχει ως κύριο σκοπό της την ανάπτυξη τεχνικών και μεθόδων με τους οποίους θα επιτυγχάνεται η επικοινωνία ή η ανταλλαγή πληροφορίας μόνο μεταξύ εξουσιοδοτημένων μελών και όχι σε μέλη χωρίς τα αντίστοιχα δικαιώματα πρόσβασης.

Ένα κρυπτογραφικό σύστημα επιδιώκει την τροποποίηση της πληροφορίας που θα πρέπει να κρυπτογραφηθεί και ονομάζεται αρχικό κείμενο *(plaintext)* και την δημιουργία νέου διαφοροποιημένου κειμένου το ποίο καλείται κρυπτογραφημένο κείμενο (*ciphertext*). Το σύνολο της διαδικασίας που ακολουθείται για την δημιουργία μια μορφής κειμένου που θα είναι πολύ δύσκολο να υποκλαπεί ονομάζεται κρυπτογράφηση (*encryption*) και η αντίστροφη διαδικασία που προβλέπει την χρήση μεθόδων τέτοιων που να οδηγούν το σύστημα στην αποκάλυψη του αρχικού κειμένου ονομάζεται *αποκρυπτογράφηση (decryption*). Και οι δυο αυτές διαδικασίες χρησιμοποιούν κάποιες κωδικοποιημένες δυαδικές εκφράσεις για την επίτευξη της κρυπτογράφησης ή της αποκρυπτογράφησης οι οποίες καλούνται και κλειδιά κρυπτογράφησης. Για την παραβίαση των κρυπτογραφικών συστημάτων έχουν δημιουργηθεί και διατυπωθεί κατά καιρούς διάφοροι αλγόριθμοι και τεχνικές που αποκτούν πρόσβαση είτε στα κλειδιά είτε στα διάφορα τμήματα των κειμένων του συστήματος. Οι τεχνικές αυτές καλούνται τεχνικές κρυπτανάλυσης και θα αναλυθούν διεξοδικά στο επόμενο κεφάλαιο.

Συνοπτικά η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζεται γραφικά σχήμα 1.1 που ακολουθεί και παρουσιάζει τα βασικά στάδια ενός κρυπτογραφικού συστήματος ανεξάρτητα από το είδος της χρησιμοποιούμενης κρυπτογραφικής τεχνικής.



Σχήμα 1.1 Γενικά στάδια κρυπτογράφησης - αποκρυπτογράφησης

Βασική επιδίωξη ενός συστήματος κρυπτογράφησης είναι η δημιουργία ενός ικανού διαύλου επικοινωνίας για την όσο το δυνατόν ασφαλέστερης ανταλλαγής πληροφοριών μεταξύ των διαφόρων μελών του. Το σύστημα θα πρέπει να είναι σε θέση να αποτρέπει κάποια μη εξουσιοδοτημένα μέλη να υπεισέλθουν στο σύστημα επικοινωνίας ή αν αυτό συμβεί να παρέχει μηχανισμούς που θα διασφαλίζουν την μη αλλοίωση της μεταδιδόμενης πληροφορίας.

Σε θεωρητική βάση ένα σύστημα κρυπτογράφησης διακρίνεται από ένα σύνολο στοιχείων που συμβολίζονται ως εξής με την παράσταση (P,C,k,E,D). Οι παράμετροι P και C δηλώνουν τους χώρους όλων των πιθανών αρχικών κειμένων ή κρυπτογραφημένων κειμένων αντίστοιχα. Η παράμετρος k ορίζει το πεδίο τιμών για τα πιθανά κλειδιά κρυπτογράφησης και με τους συμβολισμούς E και D, σημειώνεται η συνάρτηση κρυπτογράφησης και η αντίστροφη συνάρτηση για την αποκρυπτογράφηση αντιστοίχως.

Ως πρώτο βήμα των διαδικασιών του συστήματος αποτελεί η δημιουργία του κλειδιού κρυπτογράφησης και η αποστολή του στο μέλος που διαδραματίζει τον ρόλο του παραλήπτη της κρυπτογραφημένης πληροφορίας. Κατά τη λειτουργία του συστήματος εισάγονται στη συνάρτηση κρυπτογράφησης δύο τιμές που η καθεμία τους αντλείται από τα σύνολα τιμών P και k, δηλαδή ένα αρχικό κείμενο και ένα κλειδί για την κρυπτογράφηση και αποδίδει στην έξοδο τους συστήματος μια τιμή που ανήκει στο σύνολο τιμών C. Αντίθετα κατά την αντίστροφη διαδικασία εισάγονται στην συνάρτηση αποκρυπτογράφησης τιμές από τα σύνολα τιμών C και k και παράγει το αρχικό κείμενο που ανήκει στο ορισμένο σύνολο τιμών P.

1.3 Αντικειμενικοί σκοποί της κρυπτογραφίας

Ως αντικειμενικούς σκοπούς της κρυπτογραφίας μπορούμε να αναφέρουμε τους παρακάτω:

1. ***Εμπιστευτικότητα (Confidentiality)***: Η πρόσβαση στην μεταδιδόμενη πληροφορία μπορεί να γίνει μόνο από έγκυρα και εξουσιοδοτημένα άτομα και κατά συνέπεια παραμένει ακατανόητη σε άτομα χωρίς την σχετική «άδεια». Ο όρος εμπιστευτικότητα πολλές φορές ταυτίζεται με τους όρους μυστικότητα ή ιδιωτικότητα και μπορεί να επιτευχθεί με διάφορες τεχνικές όπως η ανάπτυξη σχετικών μαθηματικών αλγορίθμων ή τη χρήση μέσων που προστατεύουν την πληροφορία σε φυσικό επίπεδο.

2. ***Ακεραιότητα (Integrity)***: Με τον όρο ακεραιότητα δεδομένων ορίζουμε την δυνατότητα της αλλοίωσης ή οποιασδήποτε μετατροπής της πληροφορίας μόνο από άτομα που διαθέτουν την απαραίτητη εξουσιοδότηση. Επιπρόσθετα κάθε ενέργεια μετατροπής –εισαγωγή, διαγραφή, αντικατάσταση- δεν μπορεί να πραγματοποιηθεί αν δεν υπάρχει αντίστοιχη δυνατότητα ανίχνευσής της.

3. ***Πιστοποίηση (Authentication)***: Κάθε πληροφορία που μεταδίδεται πρέπει απαραίτητα να μεταδίδεται μεταξύ αναγνωρισμένων αποστολέων και παραληπτών. Οι αποστολέας και παραλήπτης πρέπει να μπορούν να εξακριβώνουν τα στοιχεία τους καθώς και να ορίζουν την πηγή και τον προορισμό της πληροφορίας θεωρώντας πάντοτε ότι τα στοιχεία εξακρίβωσης δεν είναι ψευδή ή αλλοιωμένα.

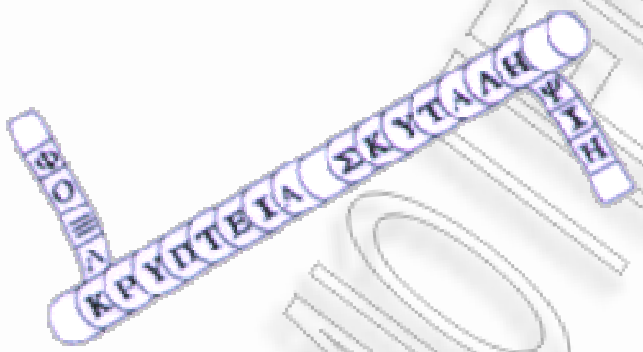
4. ***Μη απάρνηση (Non repudiation)***: Κατά την μετάδοση μιας πληροφορίας καμία από τις οντότητες αποστολέα ή παραλήπτη δεν μπορεί να αποποιηθεί την ευθύνη της δημιουργίας ή μετάδοσής της όπως και να αρνηθεί την αυθεντικότητα της. Πολλά προβλήματα μπορούν να δημιουργηθούν προς αυτή την κατεύθυνση όπως για παράδειγμα η περίπτωση που δυο εμπλεκόμενες πλευρές αρνηθούν την ήδη προηγηθείσα χρήση πληροφορίας για συγκεκριμένο σκοπό και επέλθει σύγκρουση που προϋποθέτει την ύπαρξη τρίτης αξιόπιστης οντότητας η οποία θα επιφορτιστεί με τον ρόλο της διαιτησίας.

1.4 Ιστορικά στοιχεία και περίοδοι κρυπτογραφίας

1.4.1 Πρώιμα στάδια της κρυπτογραφίας

Τα πρώτα ίχνη εμφάνισης κάποιων έστω στοιχειωδών τεχνικών κρυπτογράφησης καταγράφονται από τους ερευνητές στην Αίγυπτο κοντά στον ποταμό Νείλο περίπου τον 19ο π.Χ. αιώνα. Αντίστοιχα ευρήματα που φανερώνουν προσπάθειες κρυπτογράφησης συναντώνται σχεδόν σε όλους τους λαούς που ανέπτυξαν πολιτισμό όπως οι Ινδοί, οι Πέρσες και οι Ασσύριοι. Ακόμη πολλά λογοτεχνικά κείμενα και θρησκευτικά συγγράμματα της περιόδου αυτής περιέχουν αναφορές σε υποτυπώδεις

κρυπτογραφικές τεχνικές. Στον ελλαδικό χώρο κατά την αρχαιότητα χρησιμοποιήθηκαν διάφορες μέθοδοι απόκρυψης πληροφοριών με πιο διαδεδομένη την σπαρτιατική τεχνική της σκυτάλης. Η αναγκαιότητα της ασφάλειας στρατιωτικών πληροφοριών οδήγησαν τους Σπαρτιάτες κοντά στον 5ο π.Χ αιώνα στην επινόηση της συγκεκριμένης τεχνικής. Η μεθοδολογία της κρυπτογράφησης συνίσταται σε μια λωρίδα από δέρμα ή πάπυρο η οποία τυλιγόταν γύρω από μια ράβδο που ονομάστηκε σπαρτιάτικη σκυτάλη και μπορούσε να αποκρύπτει μηνύματα που αφορούσαν κυρίως στρατιωτικές επιχειρήσεις της εποχής.



Εικόνα 1.1 Άποψη της σπαρτιατικής σκυτάλης

Κατά τους αρχαίους χρόνους οι μέθοδοι που ακολουθήθηκαν στηριζόταν περισσότερο στις τεχνικές της στεγανογραφίας παρά στην κρυπτογραφία αυτή καθαυτή. Συστήματα με τα οποία πραγματοποιείται αντικατάσταση χαρακτήρων συναντώνται στη Ρωμαϊκή εποχή ενώ δεν υπάρχουν επιστημονικές καταγραφές της εποχής εκείνης για παρόμοια συστήματα στον ελληνικό χώρο. Χαρακτηριστικότερο δείγμα της Ρωμαϊκής κρυπτογράφησης αποτελεί ο αλγόριθμος του Καίσαρα ο οποίος θα υιοθετηθεί από πολλά μεταγενέστερα κρυπτογραφικά συστήματα και βασίζεται στην ανάμιξη και αντικατάσταση χαρακτήρων ενός κειμένου από άλλους και με τυχαία σειρά.

1.4.2 **Μεσαίωνας και κρυπτογραφία**

Όπως συνέβη με πολλούς επιστημονικούς τομείς κατά την μεσαιωνική περίοδο, έτσι και η κρυπτογραφία δεν αντιμετωπίσθηκε ως εξελικτική επιστήμη αλλά ως εφαρμογή μαύρης μαγείας και αποκρυφισμών. Αντίθετα στον αραβικό κόσμο τα μαθηματικά, η κρυπτογραφία και μια σειρά άλλων επιστημών εξελίσσεται και αναπτύσσεται με γρηγορότερους ρυθμούς. Λόγω της συντέλεσης σημαντικών και μακροχρόνιων πολεμικών συγκρούσεων κατά τους μεσαιωνικούς χρόνους, επήλθε πρόοδος στον τομέα της κρυπτογραφίας. Το έτος 1563 σημειώθηκε η έκδοση του βιβλίου «De furtivis literarum notis» από τον Ιταλό Giovanni Batista Porta, ο οποίος παρουσίασε για πρώτη φορά συστήματα με την μέθοδο της πολυαλφαβητικής κρυπτογράφησης. Παρόμοιο σύστημα κρυπτογράφησης παρουσιάστηκε και από τον Vigenere, το οποίο έχει τύχει τέτοιας αποδοχής από την επιστημονική κοινότητα που συναντάται σε εφαρμογές κρυπτογράφησης και στη σημερινή εποχή.

Αργότερα και περίπου στα 1671 μ.Χ επινοήθηκε από τον Leibniz ένα σύστημα που χρησιμοποιούσε μια δυαδική κλίμακα που μέχρι τις μέρες μας αποτελεί το θεμέλιο του κώδικα ASCII. Έναν αιώνα περίπου αργότερα, ο Thomas Jefferson το έτος 1795 μ.Χ θα εφεύρει μια πρώιμης μορφής κρυπτογραφική μηχανή που θα ονομαστεί τροχός κρυπτογράφησης ή "wheel cipher".

Εικόνα 1.2 Η μηχανή κρυπτογράφησης wheel cipher

Η εφεύρεση του τηλέγραφου και η ευκολία στην μετάδοση πληροφοριών έκανε περί τα μέσα του έτους 1844 μ.Χ περισσότερο επιτακτική την ανάγκη για ανάπτυξη μεθόδων κρυπτογράφησης και ασφάλειας των μεταδιδόμενων μηνυμάτων. Λίγες δεκαετίες αργότερα, το έτος 1861 μ.Χ σημειώνεται η πρώτη παραβίαση του κώδικα κρυπτογράφησης του Vigenere από τον Kasiski, έναν απόστρατο αξιωματικό του πρωσικού στρατού. Σαν επιστέγασμα της επιτυχίας του ο Kasiski συνέγραψε το βιβλίο «Η μυστική γραφή και η τέχνη της αποκρυπτογράφησης» όπου ανέλυε τις τεχνικές κρυπτογράφησης και αποκρυπτογράφησης.

1.4.3 **Κρυπτογραφία τον 20ο αιώνα**

Η περίοδος αυτή έχει σημαδευτεί από την διενέργεια των δυο παγκοσμίων πολέμων. Όπως και κατά την αρχαιότητα αλλά και τη μεσαιωνική περίοδο, υπήρξε περισσότερο αναγκαία από ποτέ η ανάπτυξη τεχνικών που θα προσέφεραν ασφάλεια στις πληροφορίες που μεταφέρονταν από και προς τις διάφορες εμπλεκόμενες πλευρές. Έτσι κατά την χρονική αυτή περίοδο σημειώνεται αλματώδης ανάπτυξη στο επιστημονικό πεδίο της κρυπτογραφίας, με την ανάπτυξη σύνθετων αλγορίθμων κρυπτογράφησης αλλά και διάφορων μηχανικών κατασκευών που θα τους υλοποιούσαν και θα προσέφεραν την προσδοκώμενη ασφάλεια. Οι μηχανικές αυτές κατασκευές ονομαζόταν κρυπτοσυσκευές και για την λειτουργία τους ήταν απαραίτητη η απασχόληση πολυάριθμου ανθρώπινου δυναμικού αλλά και η ιδιαίτερη τεχνολογική ισχύς. Ταυτόχρονα όμως με τις μεθόδους κρυπτογράφησης είχαμε παράλληλη άνθηση και των τεχνικών αποκρυπτογράφησης και κρυπτανάλυσης έτσι ώστε καμιά συσκευή ή αλγόριθμος δεν μπορούσε να θεωρηθεί απολύτως ασφαλής. Κατά την περίοδο των

παγκοσμίων πολέμων παρουσιάστηκε και χρησιμοποιήθηκες ευρέως το γερμανικό κρυπτογραφικό σύστημα το οποίο ονομάστηκε σύστημα Enigma και φαίνεται στην εικόνα 1.3.

Εικόνα 1.3 Η κρυπτογραφική συσκευή Enigma

Όπως ήδη αναφέρθηκε καμιά συσκευή κρυπτογράφησης δεν ήταν άτρωτη σε επιθέσεις κρυπτανάλυσης κι έτσι το 1932 σημειώθηκε από τον Πολωνό Marian Rejewski, η πρώτη επιτυχημένη επίθεση κρυπτανάλυσης στο σύστημα κρυπτογράφησης Enigma των Γερμανών και αποτέλεσε το μεγαλύτερο επίτευγμα της εποχής, αναφορικά με το πεδίο της κρυπτανάλυσης. Αντίστοιχα με την γερμανική πλευρά, οι δυνάμεις των συμμάχων ανέπτυξαν τις δικές τους συσκευές κρυπτογράφησης όπως η συσκευή TypeX των Βρετανών ή η αμερικανικής προέλευσης κρυπτομηχανή SIGABA (εικόνα 1.4).

Εικόνα 1.4 Η αμερικανική κρυπτομηχανή SIGABA

Οι δυο συμμαχικές κρυπτομηχανές στην ουσία ήταν συσκευές όμοιας φιλοσοφίας με την γερμανική μηχανή Enigma με τις απαραίτητες τροποποιήσεις και μετατροπές. Εκτός από αυτές τις μηχανές, παρουσιάσθηκε την εποχή εκείνη και η συσκευή κρυπτογράφησης Lacida η οποία ήταν πολωνικής προέλευσης. Ο Rejewski, ο πρώτος επιστήμονας που παραβίασε τη μηχανή Enigma δεν δυσκολεύτηκε να παραβιάσει και την κρυπτομηχανή Lacida το έτος 1941, γεγονός που είχε ως άμεση συνέπεια την απόσυρσή της.

1.4.4 **Κρυπτογραφία στη σύγχρονη εποχή**

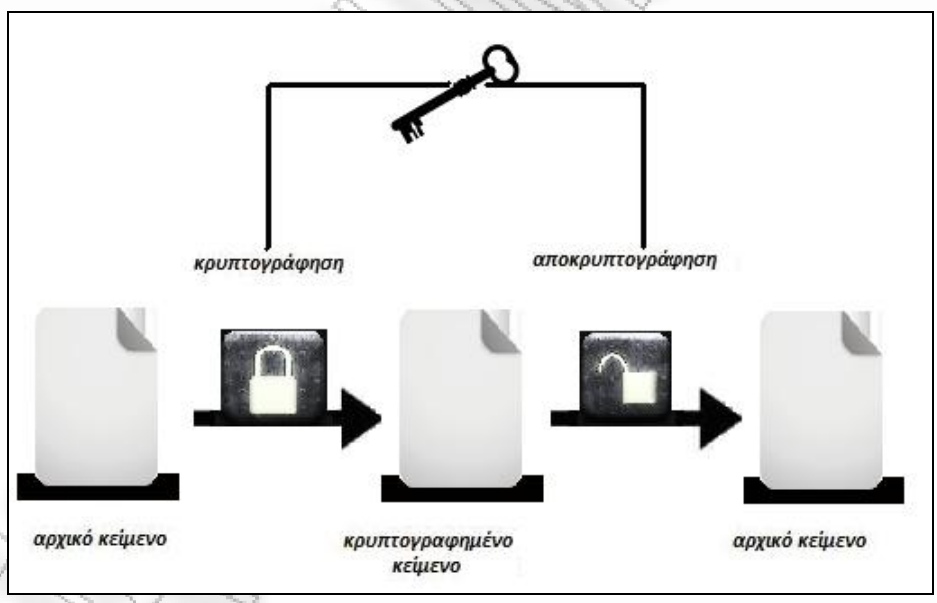
Η σύγχρονη εποχή στον επιστημονικό τομέα της κρυπτογραφίας προσδιορίζεται από τις μελέτες πρωτίστως του θεωρούμενου ως πατέρα της κρυπτογραφίας, Claude Shannon. Στις διάφορες επιστημονικές μελέτες βασίζονται οι σύγχρονες μεθοδολογίες των διαφόρων συστημάτων που επιχειρούν διαδικασίες κρυπτογράφησης ή κρυπτανάλυσης. Σημαντικά συγγραφικά του έργα αποτελούν η “Μαθηματική Θεωρία της Επικοινωνίας” και η “Θεωρία επικοινωνίας των συστημάτων μυστικότητας”. Η δεκαετία του ‘70 θεωρείται δεκαετία ορόσημο για την κρυπτογραφία αφού παρουσιάζεται ο αλγόριθμος κρυπτογράφησης ιδιωτικού κλειδιού DES (Data Encryption Standard) που αποτέλεσε για τις επόμενες δεκαετίες το πρότυπο δείγμα αλγορίθμου κρυπτογράφησης με παγκόσμια αναγνώριση.

Πολλές δεκαετίες αργότερα όπως θα δούμε και στο επόμενο κεφάλαιο, παρουσιάστηκαν διάφοροι αλγόριθμοι κρυπτογράφησης με τον αλγόριθμο AES να θεωρείται ως ο επικρατέστερος και καταλληλότερος να αντικαταστήσει τον θεωρητικά γερασμένο αλλά όχι ξεπερασμένο αλγόριθμο DES. Σημαντικά ζητήματα ασφαλείας των σύγχρονων αλγορίθμων έχουν κατά καιρούς διατυπωθεί και χρήζουν επιστημονικής αντιμετώπισης για την ασφαλέστερη και επιτυχή διαδικασία κρυπτογράφησης. Η παράλληλη εξέλιξη των τεχνικών κρυπτογράφησης και κρυπτανάλυσης καθιστά την προσπάθεια για εξεύρεση νέων και ισχυρών αλγορίθμων κρυπτογράφησης αναγκαία και επιτακτική. Όπως θα δούμε διάφοροι αλγόριθμοι έχουν αναπτυχθεί οι οποίοι και διακρίνονται σε κατηγορίες ανάλογα με την μεθοδολογία που ακολουθούν και το επιστημονικό πεδίο που καλύπτουν. Σε όλους όμως τους αλγορίθμους παραμένουν ίδια τα χαρακτηριστικά ασφάλειας των αλγορίθμων ανεξάρτητα από το είδος που αυτοί ανήκουν. Τα στοιχεία αυτά είναι τα μεγέθη των αρχικών κειμένων, ο αριθμός και το μήκος των κλειδιών κρυπτογράφησης και το μήκος των παραγόμενων κρυπτογραφημένων μηνυμάτων.

1.5 **Είδη κρυπτογραφίας**

1.5.1 **Συμμετρική κρυπτογραφία** (Symmetric Cryptography) **ή κρυπτογραφία μυστικού κλειδιού** (Secret-Key Cryptography)

Η συμμετρική κρυπτογραφία ή διαφορετικά κρυπτογραφία μυστικού κλειδιού έχει την βάση της στην δημιουργία και χρήση ενός μόνο κλειδιού με το οποίο διεξάγεται η διαδικασίας της κρυπτογράφησης της πληροφορίας και η αποκρυπτογράφηση της. Το κλειδί αυτό καλείται γνωστό ως συμμετρικό ή μυστικό κλειδί (secret key). Από τα όποια εμπλεκόμενα μέλη της διαδικασίας κρυπτογράφησης, τα μόνα που έχουν γνώση του μυστικού κλειδιού είναι ο αποστολέας της πληροφορίας και στη συνέχεια ο παραλήπτης. Κατά το πρώτο στάδιο της διαδικασίας κρυπτογράφησης το αρχικό μήνυμα-πληροφορία κωδικοποιείται με τη χρήση του συμμετρικού κλειδιού. Ως αποτέλεσμα προκύπτει ένα νέο μήνυμα σε μορφή που είναι αδύνατο να αναγνωστεί χωρίς επεξεργασία. Το γεγονός ότι η μεταδιδόμενη πληροφορία πλέον έχει αποκτήσει αυτήν την ακατανόητη μορφή προσφέρει την αναγκαία ασφάλεια και μυστικότητα. Στη συνέχεια και αφού η πληροφορία φτάσει στον εξουσιοδοτημένο παραλήπτη γίνεται χρήση του ίδιου μυστικού κλειδιού και επιτυγχάνεται η ανάκτηση του αρχικού μηνύματος και η αποκρυπτογράφηση του κρυπτογραφήματος. Η όλη διαδικασία αναπαρίσταται στο παρακάτω σχήμα:



Σχήμα 1.2 Διαδικασία συμμετρικής κρυπτογράφησης

Η χρήση του συμμετρικού συστήματος κρυπτογράφησης συναντάται στα επιστημονικά ευρήματα από την αρχαιότητα. Όπως είδαμε και σε προηγούμενη ενότητα ένας από τους πρώτους αλγορίθμους αντικατάστασης που χρησιμοποιεί κρυπτογραφική τεχνική ήταν ο αλγόριθμος του Καίσαρα. Στη σύγχρονη εποχή και με την εξέλιξη των διάφορων επιστημονικών τομέων έχουν αναπτυχθεί νέοι και ισχυρότερο αλγόριθμοι συμμετρικής κρυπτογραφίας. Κάποιοι από αυτούς με τους για τους οποίου θα γίνει

αναφορά και στο επόμενο κεφάλαιο είναι οι αλγόριθμοι DES (Data Encryption Standard), AES (Advanced Encryption Standard) και IDEA (International Data Encryption Algorithm). Άλλοι σημαντικοί αλγόριθμοι αυτού του είδους είναι οι Blowfish, RC-5, CAST-256, Camelia, Feal, Lucifer και άλλοι.

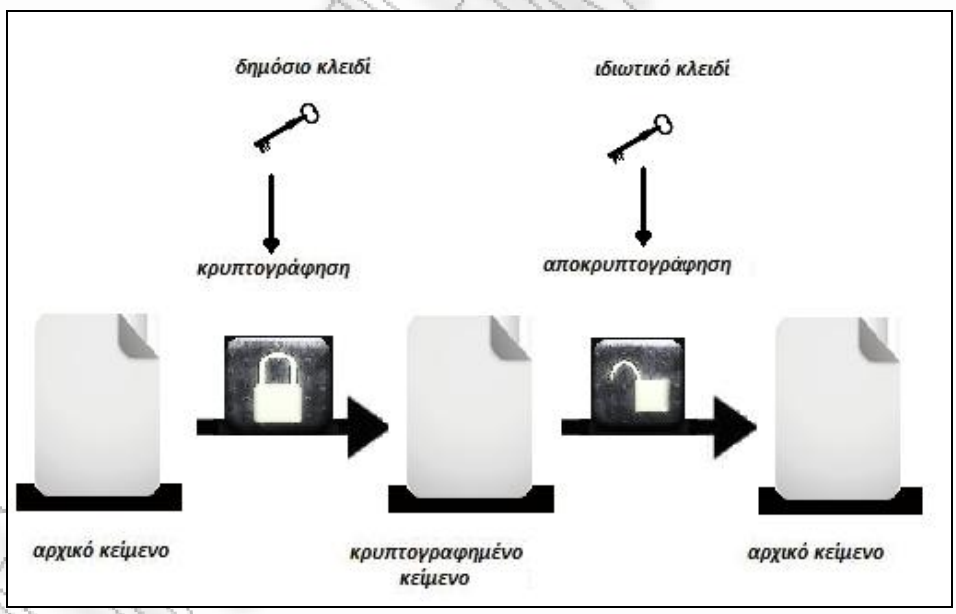
Τα συστήματα κρυπτογράφησης δεν απαιτούν ιδιαίτερα αυξημένους υπολογιστικούς πόρους γεγονός που επιτρέπει την εφαρμογή τους σε ένα ευρύ φάσμα διαφόρων λειτουργιών και καθημερινών δραστηριοτήτων. Επίσης από τις διάφορες επιστημονικές μετρήσεις προκύπτουν οι αυξημένες ταχύτητες που σημειώνονται τόσο κατά την διαδικασία της κρυπτογράφησης όσο και σε αυτή της αποκρυπτογράφησης, ενώ και σε πολλές περιπτώσεις το μέγεθος του κρυπτογραφημένου κειμένου είναι σημαντικά μικρότερο από το αρχικό κείμενο.

Σημαντική δικλείδα ασφαλείας των συμμετρικών αλγορίθμων αποτελεί η αναγκαιότητα της ανταλλαγής του μυστικού κλειδιού κρυπτογράφησης μεταξύ των μελών που συμμετέχουν στο κρυπτογραφικό σύστημα. Το γεγονός ότι στις περισσότερες των περιπτώσεων η ανταλλαγή αυτή μεταξύ των μελών γίνεται πριν ακόμα γίνει η αποστολή του αρχικού κειμένου καθιστά επιτακτική την ανάγκη ύπαρξης ενός ασφαλούς διαύλου που θα επιτρέπει τη μετάδοσή του. Εκτός από τους περιορισμούς αυτούς, στην πράξη οι δυο εμπλεκόμενες πλευρές είναι άγνωστες μεταξύ τους οπότε υπεισέρχεται μια ακόμη παράμετρος ασφαλείας, αυτή της ταυτοποίησης και επιβεβαίωση της αυθεντικότητας του κάθε μέλους του συστήματος, ώστε να καταστεί ανέφικτη η μετάδοση του κρυπτογραφημένου κειμένου ή του κλειδιού σε άτομο χωρίς την απαιτούμενη εξουσιοδότηση. Σημαντικός επίσης παράγοντας που θα πρέπει να ληφθεί υπόψη σε έναν αλγόριθμο συμμετρικής κρυπτογράφησης είναι και ο αριθμός των μελών στα οποία θα γίνει η μεταφορά των μηνυμάτων και των κλειδιών. Είναι κατανοητό ότι όσο μεγαλύτερος είναι αυτός ο αριθμός, ο απαιτούμενος αριθμός κλειδιών κρυπτογράφησης μεταβάλλεται αναλογικά. Για την ανταλλαγή πληροφοριών μεταξύ μελών αριθμού n, είναι απαραίτητη η ύπαρξη $n^2/2$ μοναδικών μυστικών κλειδιών, τα οποία θα πρέπει ανά διαστήματα να λαμβάνουν άλλες τιμές ώστε να προσφέρουν την μέγιστη ασφάλεια.

Οι αλγόριθμοι συμμετρικής κρυπτογράφησης διακρίνονται με τη σειρά τους σε δυο άλλες υποκατηγορίες: στους αλγόριθμους τμημάτων (Block ciphers) και στους αλγορίθμους ροής (Stream ciphers). Οι αλγόριθμοι τμημάτων μετατρέπουν ένα τμήμα του αρχικού κειμένου λειτουργώντας επαναληπτικά και με τη βοήθεια ενός μυστικού κλειδιού παράγουν ένα τμήμα κρυπτογραφημένου κειμένου ίδιου μεγέθους. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Οι αλγόριθμοι ροής σε αντίθεση με τους αλγόριθμους τμημάτων που λειτουργούν με μεγάλα τμήματα μηνυμάτων, λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits και θα καταλήγουν πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιούν το ίδιο κλειδί. Κύριο χαρακτηριστικό των αλγορίθμων αυτής της κατηγορίας είναι ότι η κρυπτογράφηση των bits ποικίλει κατά τη διάρκεια της λειτουργίας της κρυπτογράφησης.

1.5.2 **Ασύμμετρη Κρυπτογραφία** (Asymmetric Cryptography) **ή Κρυπτογραφία δημοσίου κλειδιού** (Public Key Cryptography)

Όπως είδαμε η κρυπτογραφία μυστικού κλειδιού αποτέλεσε το κυριότερο είδος κρυπτογραφίας από τους αρχαίους ακόμα χρόνους. Όμως για την αντιμετώπιση των προβλημάτων και των κενών ασφαλείας που παρέμεναν κατά την ανάγκη διασφάλισης της πληροφορίας, οι Whitfield Diffie και Martin Hellman εισήγαγαν περί τα μέσα της δεκαετίας του 1970 μια νέα μέθοδο, δημιουργώντας ένα νέο είδος κρυπτογραφίας το οποίο ονομάστηκε κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία. Η τεχνική αυτή, σε αντίθεση με το μοναδικό μυστικό κλειδί της συμμετρικής κρυπτογραφίας, έχει ως θεμελιώδες στοιχείο την ύπαρξη ενός ζεύγους κλειδιών (key pair). Τα κλειδιά αυτά σχετίζονται μεταξύ τους με κάποια αλγεβρική σχέση αλλά το σημαντικό είναι πως αν υποκλαπεί το ένα κλειδί δεν σημαίνει απαραίτητα ότι θα μπορεί να γίνει χρήση του ζεύγους των κλειδιών αφού απαιτείται οπωσδήποτε και η γνώση και του δεύτερου κλειδιού. Το γεγονός αυτό επιτρέπει την δημοσιοποίηση του ενός κλειδιού το οποίο για το λόγο αυτό καλείται δημόσιο κλειδί (public key) και είναι διαθέσιμο για την διαδικασία της κρυπτογράφησης του αρχικού μηνύματος. Αντίθετα το άλλο κλειδί του ζεύγους που θα χρησιμοποιηθεί για να γίνει η αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος πρέπει απαραίτητα να παραμείνει μυστικό και για το λόγο αυτό καλείται ιδιωτικό κλειδί (private key). Η διαδικασία που ακολουθεί η ασύμμετρη κρυπτογραφία παρουσιάζεται σχήμα 1.3.



Σχήμα 1.3 Διαδικασία ασύμμετρης κρυπτογράφησης

Οι αλγόριθμοι ασύμμετρης κρυπτογράφησης αντιμετωπίζουν ένα σημαντικό κενό ασφαλείας που παραμένει δυσεπίλυτο όταν χρησιμοποιούνται αλγόριθμοι μυστικού κλειδιού. Το κενό ασφαλείας συνίσταται στην μη διασφάλιση ύπαρξης ενός ιδιαίτερα ασφαλούς διαύλου ανταλλαγής των κλειδιών κρυπτογράφησης, ώστε να είναι δυνατή η επίτευξη της κρυπτογράφησης ή της αποκρυπτογράφησης των μηνυμάτων.

Το ζήτημα αυτό γίνεται ακόμη μεγαλύτερο όταν πρόκειται για συστήματα ανταλλαγής πληροφοριών από μεγάλο αριθμό μελών που πιθανότατα είναι άγνωστα μεταξύ τους ή έχουν σημαντική απόσταση ανάμεσά τους. Σημαντικό συστατικό στοιχείο ασφαλείας των αλγορίθμων ασύμμετρης κρυπτογράφησης αποτελεί η ύπαρξη ενός ισχυρού ζεύγους δημόσιου και ιδιωτικού κλειδιού κρυπτογράφησης. Τα κλειδιά αυτά κατασκευάζονται κατά περίπτωση με την χρήση αλγορίθμων και συναρτήσεων ώστε να δημιουργούνται με τυχαίο και μη καθορισμένο τρόπο.

Το κυριότερο στοιχείο ασφαλείας των αλγορίθμων κρυπτογράφησης δημοσίου κλειδιού αποτελεί η πρακτικά ανέφικτη αποκωδικοποίηση του μυστικού κλειδιού με μόνη γνώση αυτή του δημοσίου κλειδιού. Η παραδοχή αυτή στηρίζεται σε επιστημονικές μετρήσεις που αποδεικνύουν ότι οι απαιτήσεις σε υπολογιστικούς πόρους και η οικονομική επιβάρυνση για την ενέργεια αποκωδικοποίησης του μυστικού κλειδιού καθιστά ασύμφορη και κατ' επέκταση αδύνατη την επίτευξή της. Την ασφάλεια αυτή ενισχύει το γεγονός ότι κατά τη λειτουργία του το κρυπτογραφικό σύστημα δεν προϋποθέτει την ανταλλαγή του ιδιωτικού κλειδιού μεταξύ των διαφόρων μελών. Κάθε μέλος του συστήματος έχει γνώση του δικού του μυστικού κλειδιού το οποίο και δεν μεταδίδεται στο δίαυλο επικοινωνίας κι έτσι δεν μπορεί να παραβιαστεί ή να αλλοιωθεί το περιεχόμενό του. Αντίθετα το δημόσιο κλειδί λόγω της φύσης του παραμένει δημοσιευμένο και είναι γνωστό σε κάθε μέλος του συστήματος που μπορεί να προβεί στην κατά βούληση για τη διαχείρισή του.

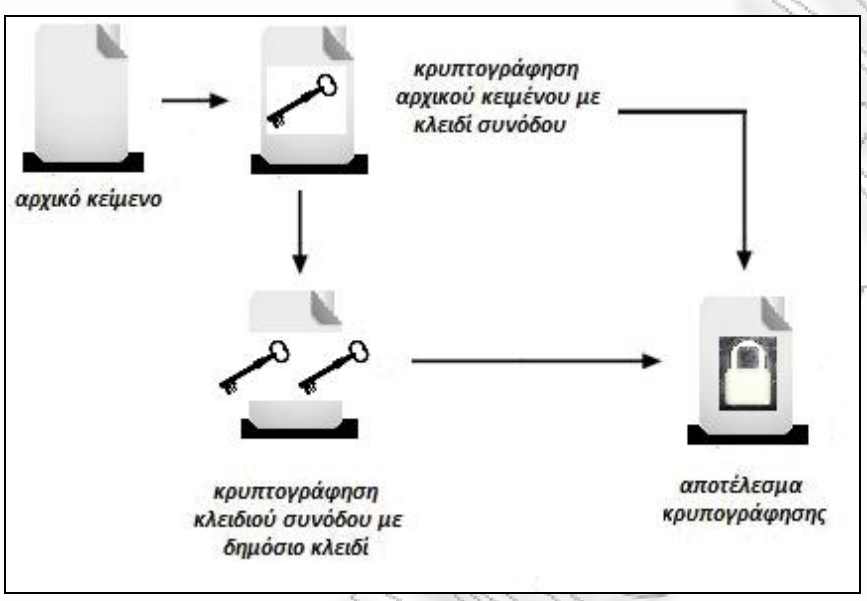
Σαν αρνητική απόρροια των ασφαλιστικών δικλείδων του συστήματος αλγορίθμων ασύμμετρης κρυπτογράφησης μπορεί να σημειωθεί η συντριπτικά μεγαλύτερη απαίτηση σε υπολογιστικούς πόρους σε σχέση με τα συμμετρικά συστήματα, ενώ και σε περιπτώσεις μηνυμάτων μεγάλου μεγέθους η ταχύτητα εκτέλεσης των διαδικασιών μειώνεται δραστικά. Προς την κατεύθυνση αυτή εισάγεται η έννοια της ψηφιακής υπογραφής ως τεχνική κρυπτογράφησης ιδιαίτερης ασφάλειας, η οποία επικεντρώνεται στην κρυπτογράφηση των μυστικών κλειδιών και όχι των μηνυμάτων και ανήκει στον κλάδο της Υβριδικής κρυπτογραφίας που παρουσιάζεται στην επόμενη ενότητα.

1.5.3 **Υβριδική Κρυπτογραφία**

Πολλά συστήματα κρυπτογράφησης δεν ακολουθούν τους αυστηρούς κανόνες της ασύμμετρης ή συμμετρικής κρυπτογράφησης κατά τρόπο που να μην μπορεί να γίνει κάποιος συνδυασμός και αξιοποίηση των θετικών τους στοιχειών. Τέτοια συστήματα που εκμεταλλεύονται σε μεγάλο βαθμό τα πλεονεκτήματα των χαρακτηριστικών ασφαλείας και των δυο κατηγοριών ονομάζονται υβριδικά κρυπτοσυστήματα ή συστήματα ψηφιακών φακέλων.

Κύριο πεδίο εφαρμογής της υβριδικής κρυπτογράφησης είναι το πεδίο της ανταλλαγής των ιδιωτικών κλειδιών στα συστήματα συμμετρικής κρυπτογράφησης. Κάθε ψηφιακός φάκελος συνθέτεται από το κείμενο που έχει ήδη κρυπτογραφηθεί με ένα μυστικό κλειδί καθώς και από το ίδιο το συμμετρικό κλειδί το οποίο με τη σειρά του έχει υποστεί κρυπτογράφηση από ένα δημόσιο συνήθως κλειδί. Στην ουσία στο σημείο

αυτό χρησιμοποιούνται οι τεχνικές της κρυπτογράφησης δημοσίου κλειδιού για την δημοσιοποίηση των κλειδιών τα οποία ονομάζονται και κλειδιά συνόδου.

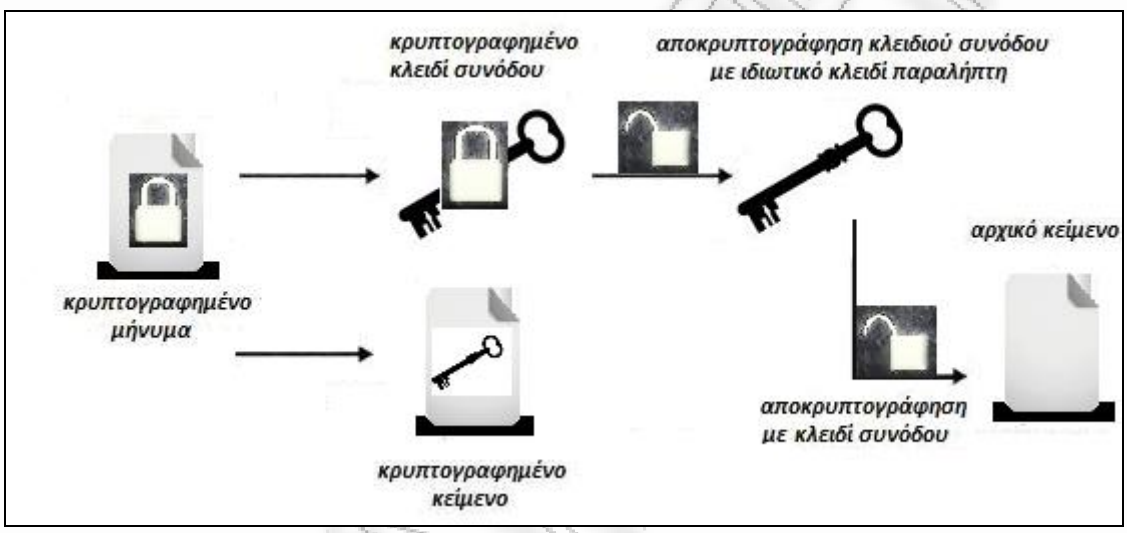


Σχήμα 1.4 Κρυπτογράφηση μέσω υβριδικού κρυπτοσυστήματος

Όταν ο αποστολέας προσπαθεί να μεταδώσει το μήνυμά του στον παραλήπτη επιλέγει ένα μυστικό κλειδί και εκτελεί την διαδικασία της κρυπτογράφησης με βάση αυτό το κλειδί. Στη συνέχεια το μυστικό κλειδί που επέλεξε στο πρώτο στάδιο το κρυπτογραφεί με ένα δημόσιο κλειδί που συνήθως προέρχεται από τον παραλήπτη του μηνύματος. Το επόμενο βήμα της διαδικασίας είναι η αποστολή του μηνύματος και του κλειδιού τα οποία είναι και τα δυο κρυπτογραφημένα. Η όλη διαδικασία κρυπτογράφησης με τη μέθοδο αυτή παρουσιάζεται στο σχήμα 1.4.

Στην περίπτωση που ο παραλήπτης επιθυμεί να αποκρυπτογραφήσει το μήνυμα που έλαβε από τον αποστολέα κάνει χρήση του προσωπικού του μυστικού κλειδιού για μπορέσει να αποκρυπτογραφήσει το μυστικό κλειδί κρυπτογράφησης και με το κλειδί που προκύπτει αποκρυπτογραφεί μήνυμα λαμβάνοντας την αρχική πληροφόρηση. Αυτή η αντίστροφη διαδικασία παραγωγής του αρχικού μηνύματος παρουσιάζεται σχηματικά στο σχήμα 1.5. Η διαδικασία είναι ανεξάρτητη του αριθμού παραληπτών των αρχικών μηνυμάτων. Αυτό που συμβαίνει σε τέτοιες καταστάσεις είναι η κρυπτογράφηση του μυστικού κλειδιού του αποστολέα με κάθε ένα δημόσιο κλειδί των παραληπτών και συνθέτεται το αποτέλεσμα της κρυπτογράφησης.

Με την χρήση των υβριδικών συστημάτων κρυπτογράφησης μπορούν να αντιμετωπιστούν κάποια από τα σημαντικότερα προβλήματα που απαντώνται στις περιπτώσεις κρυπτογράφησης με ασύμμετρους αλγορίθμους. Έτσι ενώ ένα σύστημα συμμετρικής κρυπτογράφησης είναι σημαντικά ταχύτερο από ένα σύστημα ασύμμετρης κρυπτογράφησης ειδικά σε περιπτώσεις κρυπτογράφησης κειμένων μεγάλου μεγέθους, ο συνδυασμός τους σε ένα υβριδικό κρυπτοσύστημα δημιουργεί ένα αποδοτικότερο σχήμα μοντέλου κρυπτογράφησης. Αλλά και στην περίπτωση μικρότερου μεγέθους κειμένων έχει υιοθετηθεί η μέθοδος της υβριδικής κρυπτογραφίας έτσι ώστε να μην προκαλείται σύγχυση αναφορικά αν το παράγωγο της διαδικασίας της κρυπτογράφησης είναι το αρχικό μήνυμα ή κάποιο μυστικό κλειδί.



Σχήμα 1.5 Αποκρυπτογράφηση μέσω υβριδικού κρυπτοσυστήματος

Ιδιαίτερο στοιχείο ασφαλείας των υβριδικών συστημάτων κρυπτογράφησης αποτελεί το γεγονός τα μέλη του συστήματος έχουν τη δυνατότητα να αλλάζουν τα μυστικά και δημόσια κλειδιά χωρίς περιορισμούς. Έτσι το συνδυαστικό σύστημα της υβριδικής κρυπτογράφησης καθίσταται ασφαλέστερο αλλά όπως είδαμε και παραπάνω και πιο γρήγορο σε σχέση με ένα απλό σύστημα κρυπτογράφησης δημοσίου κλειδιού που απαιτεί σημαντικά χρονικά διαστήματα εκτέλεσης των διαδικασιών του. Ένα υβριδικό σύστημα που εμφανίζεται ευρύτατα σε διάφορες εφαρμογές της κρυπτογραφίας, αποτελείται από τον αλγόριθμο ασύμμετρης κρυπτογράφησης RSA και από τον ισχυρό συμμετρικό αλγόριθμο κρυπτογράφησης DES.

1.6 **Συμμετρική ή Ασύμμετρη Κρυπτογραφία - Μειονεκτήματα και πλεονεκτήματα**

Ένα από τα σημαντικότερα ζητήματα που καλούνται να αντιμετωπίσουν τα συστήματα κρυπτογράφησης μυστικού κλειδιού είναι η προστασία του κλειδιού κατά την μετάδοσή του μέσα από έναν δίαυλο επικοινωνίας και η ασφαλής χρήση του μόνο σε μέλη με την κατάλληλη εξουσιοδότηση. Ιδιαίτερα με την ολοένα αυξανόμενη τεχνολογική ανάπτυξη που παρατηρείται στην εποχή που διανύουμε, κάποιος κακόβουλος χρήστης μπορεί με κατάλληλες τεχνικές και εργαλεία να υποκλέψει την διαδικασία ανταλλαγής του κλειδιού και είτε να αποκτήσει πρόσβαση σε αυτό είτε να αλλοιώσει το περιεχόμενό του με τρόπο ανάλογο των συμφερόντων του. Για αυτό το λόγο πρέπει να βρεθεί ένας ασφαλής τρόπος για τη μετάδοσή του, όπως για παράδειγμα μία συνάντηση μεταξύ των μελών του συστήματος στην οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιούν.

Προς την κατεύθυνση της επίλυσης του παραπάνω ζητήματος, τα συστήματα κρυπτογραφίας δημοσίου κλειδιού μπορούν να συνεισφέρουν σημαντικά στον τομέα της ασφάλειας. Η σημαντική διαφορά έγκειται στο γεγονός ότι δεν μεταδίδεται το κλειδί από το ένα μέλος στο άλλο, αφού κάθε ένα από αυτά έχει το δικό του ιδιωτικό κλειδί και έτσι θεωρητικά δεν μπορεί να υπάρχει δεδομένο που αφορά το κλειδί το οποίο να μπορεί να παραβιασθεί κατά τη μετάδοσή του. Όπως είδαμε και στην αντίστοιχη ενότητα τα ασύμμετρα συστήματα κρυπτογράφησης μπορούν να αντιστοιχίσουν μια ψηφιακή υπογραφή σε κάθε ένα από τα μέλη του συστήματος, επιβεβαιώνοντας την ταυτότητά τους ώστε να μην υπάρχει η λεγόμενη απάρνηση ταυτότητας ή η αποποίηση ευθύνης της μεταδιδόμενης πληροφορίας.

Σε σχέση με τα αντίστοιχα συμμετρικά κρυπτοσυστήματα, τα συστήματα κρυπτογράφησης δημοσίου κλειδιού υστερούν σημαντικά σε ταχύτητα. Ένα επιπλέον μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από διάφορους πιστοποιημένους οργανισμούς ώστε να επιβεβαιώνεται η κατοχή τους από τους εξουσιοδοτημένους χρήστες σε αντίθεση με τη συμμετρική στην οποία δεν απαιτείται η πιστοποίηση των κλειδιών.

Υπάρχουν καταστάσεις στις οποίες καμιά από τις δύο κατηγορίες δεν επαρκεί για την αντιμετώπιση των πιθανών κενών ασφαλείας και υπάρχει η ανάγκη του συνδυασμού και των δυο κατηγοριών κρυπτογράφησης. Για παράδειγμα αν ένα σύστημα θεωρείται κλειστό και χωρίς πρόσβαση από τρίτους χρήστες μπορεί να γίνεται αποθήκευση των κλειδιών κρυπτογράφησης χωρίς να διακινδυνεύεται η υποκλοπή τους. Αντίθετα σε συστήματα που χρησιμοποιούν μεθόδους κρυπτογράφησης για να αποθηκευτούν τοπικά κάποια δεδομένα τότε η κρυπτογράφηση δημοσίου κλειδιού αποτελεί πλεονασμό.

Η ασύμμετρη κρυπτογράφηση ορίζει ότι το ιδιωτικό κλειδί κάθε μέλους του συστήματος παραμένει μυστικό ενώ το δημόσιο γνωστοποιείται ευρύτερα χωρίς ιδιαίτερους περιορισμούς. Έτσι στα συστήματα αυτά απαιτείται η χρήση της υπηρεσίας της Έμπιστης Τρίτης Οντότητας (Trusted Third Party – TTP) η οποία παρέχει τις κατάλληλες εγγυήσεις για την ασφάλεια της κρυπτογράφησης. Σημαντική διαφορά των

δυο κατηγοριών αποτελεί και το γεγονός ότι στα συστήματα ασύμμετρης κρυπτογραφίας το ζεύγος του δημοσίου και ιδιωτικού κλειδιού μπορεί να παραμείνει αμετάβλητο και παράλληλα το μέγεθος ιδίως του δημοσίου κλειδιού συνήθως είναι μικρότερο από ένα κλειδί που χρησιμοποιείται στην συμμετρική κρυπτογράφηση.

Τα συμμετρικά συστήματα κρυπτογραφίας λόγω της ιδιαίτερης κατασκευής τους παρέχουν συνεχείς ροές παραγόμενης πληροφορίας και όχι απλά στατικά δεδομένα. Αντίθετα από την πρακτική της αμετάβλητης κατάστασης των κλειδιών κρυπτογράφησης στην κατηγορία των αλγορίθμων δημοσίου κλειδιού, στα συμμετρικά συστήματα προτείνεται και συνίσταται η συχνή και περιοδική μεταβολή του κλειδιού για την αποφυγή του ενδεχομένου της υποκλοπής. Σε επίπεδο μεγέθους κλειδιών συγκριτικά με αυτά των ασύμμετρων κρυπτοσυστημάτων, τα μεγέθη των κλειδιών στην συμμετρική κρυπτογράφηση είναι μικρότερου μήκους ενώ αντίθετα τα συστήματα δημιουργίας ψηφιακής υπογραφής από συμμετρικούς αλγορίθμους κρυπτογράφησης συνήθως χρησιμοποιούν κλειδιά μεγαλύτερου μεγέθους ώστε να επιτύχουν την πιστοποίηση της δημόσιας λειτουργίας.

Κεφάλαιο 2

2.1 **Αλγόριθμοι Ασύμμετρης Κρυπτογράφησης**

Στην ενότητα αυτή παρουσιάζουμε μερικούς από τους σημαντικότερους αλγόριθμους δημοσίου κλειδιού κάνοντας αναφορά στη γενική φιλοσοφία τους και στα στάδια που ακολουθούνται κατά τη λειτουργία τους. Η παρουσίαση αύτη ωστόσο γίνεται όσο το δυνατότερο συνοπτικά αφού σκοπός είναι η απλή παράθεσή τους, σε αντίθεση με την λεπτομερέστερη παρουσίαση των συμμετρικών αλγορίθμων που θα ακολουθήσει στην επόμενη ενότητα καθώς σε αυτού του είδους των αλγορίθμων συναντώνται τα κουτιά αντικατάστασης που θα μας απασχολήσουν στο τρίτο κεφάλαιο .

2.1.1 **Αλγόριθμος** Diffie **και** Hellman

Η παρουσίαση του αλγορίθμου αυτού παρουσιάσθηκε από τους Whitfield Diffie και Martin Hellman το 1976 και θεωρείται από τους πρώτους μηχανισμούς κρυπτογράφησης δημοσίου κλειδιού, ο οποίος αποτέλεσε αντικείμενο εκτενούς έρευνας και μελέτης από τους επιστήμονες της κρυπτογραφίας. Ο αλγόριθμος DH επιτρέπει στα μέλη αυτά να δημιουργήσουν ένα διαμοιραζόμενο μυστικό κλειδί και στην ουσία πρόκειται για έναν μηχανισμό ανταλλαγής κλειδιού μεταξύ των μελών που συμμετέχουν στη διαδικασία της κρυπτογράφησης. Με άλλα λόγια δεν αποτελεί έναν τρόπο κρυπτογράφησης υπό την ευρεία έννοια καθώς δεν χρησιμοποιείται για να αποκρύψει δεδομένα αλλά είναι μια μέθοδος που επιτρέπει την ασφαλή ανταλλαγή των κλειδιών που κρυπτογραφούν τα δεδομένα αυτά.

Κατά την εκτέλεσή του ο αλγόριθμος λειτουργεί με τη δημιουργία ενός μυστικού και ενός δημοσίου κλειδιού από τα δυο μέλη Α και Β χρησιμοποιώντας δύο παραμέτρους: έναν πρώτο αριθμό p και έναν τυχαίο ακέραιο g μικρότερο από τον p. Το δημόσιο κλειδί του μέλους Α ορίζεται ως g^a(mod p) και στέλνεται στο μέλος Β και αντίστοιχα αυτό του Β ορίζεται ως g^b(mod p) και στέλνεται στο μέλος Α. Ο Α χρησιμοποιώντας το κλειδί του Β και το δικό του μυστικό κλειδί θα δημιουργήσει ένα συμμετρικό κλειδί με βάση τον αλγόριθμο DH το οποίο ορίζεται ως $(g^b)^a$(mod p). Με τον ίδιο τρόπο και ο Β δημιουργεί το ίδιο ακριβώς συμμετρικό κλειδί με τον Α το $(g^a)^b$(mod p) κι έτσι μπορούν να επικοινωνήσουν με ασφάλεια ακόμα και σε ένα μη ασφαλές δίκτυο. Και τα δυο μέλη πλέον μπορούν να κρυπτογραφήσουν να μεταφέρουν ή να αποκρυπτογραφήσουν πληροφορίες χρησιμοποιώντας τα συμμετρικά τους κλειδιά g^{ab}.

2.1.2 **Ο αλγόριθμος** RSA (Rivest/Shamir/Adleman)

Ο αλγόριθμος RSA παρουσιάσθηκε από μια επιστημονική ομάδα του MIT το 1978 και πήρε το όνομα του από τα αρχικά των επιθέτων των επιστημόνων αυτών: Ron Rivest, Adi Shamir και Leonard Adleman. Αποτελεί ένα σύστημα κρυπτογραφίας δημοσίου κλειδιού και βασίζεται στο σύνθετο πρόβλημα της παραγοντοποίησης μεγάλων ακεραίων αριθμών. Ο αλγόριθμος RSA θεωρείται ένας από τους ασφαλέστερους

αλγορίθμους και χρησιμοποιείται στην κρυπτογράφηση δεδομένων καθώς και στη δημιουργία ψηφιακών υπογραφών.

Κατά τη λειτουργία του ο αλγόριθμος ακολουθεί συγκεκριμένα βήματα. Σε πρώτη φάση γίνεται επιλογή δυο μεγάλων πρώτων αριθμών p και q και στη συνέχεια λαμβάνεται το γινόμενό τους το οποίο και συμβολίζεται με n=p*q. Ακολούθως λαμβάνεται ο ελάχιστος αριθμός r για τον οποίο θα ισχύει r=(p-1)(q-1) και ένας αριθμός e μικρότερος του r, ο οποίος δεν έχει άλλους κοινούς διαιρέτες με του r εκτός του 1. Επίσης επιλέγεται ένας αριθμός d έτσι ώστε d*e-1= r*k, όπου r*k ισοδυναμεί με οποιοδήποτε παράγωγο του r ικανοποιεί την εξίσωση. Έτσι γίνεται ο υπολογισμών των παραμέτρων p, q, n ,r, e και d και μπορεί να δημιουργηθεί το δημόσιο και μυστικό κλειδί. Το δημόσιο κλειδί είναι (e, n) το οποίο και μπορεί να δημοσιευθεί και το μυστικό κλειδί είναι το (d, n). Έτσι για την κρυπτογράφηση θα πρέπει να γίνει μετατροπή κάθε χαρακτήρα του αρχικού μηνύματος m έτσι ώστε να παραχθεί το $c=m^e \pmod n$ το οποίο αποτελεί και το κρυπτογραφημένο μήνυμα. Για την αποκρυπτογράφηση του μηνύματος, γίνεται χρήση του ιδιωτικού κλειδιού και λαμβάνεται το αρχικό μήνυμα από τη σχέση $m=c^d \pmod n$.

2.1.3 **Αλγόριθμος** Digital Signature Algorithm (DSA)

Οι δυο βασικές υπηρεσίες που παρέχει ο αλγόριθμος DSA (Digital Signature Algorithm) είναι η διασφάλιση ότι ένα μήνυμα κατά τη μετάδοσή του δεν έχει υποστεί αλλοιώσεις στο περιεχόμενό του και κυρίως να πιστοποιεί την σωστή ταυτότητα του αποστολέα στον παραλήπτη. Ο αλγόριθμος αυτός παρουσιάσθηκε από το National Institute of Standards and Technology το 1991 και χρησιμοποιείται από για τη δημιουργία μιας ψηφιακής υπογραφής και κατά την αντίστροφη διαδικασία για την επιβεβαίωση της αυθεντικότητας της. Σε ένα σύστημα κρυπτογράφησης το μέλος που επιθυμεί την δημιουργία μιας ψηφιακής υπογραφής έχει ένα δημόσιο και ένα μυστικό κλειδί. Έτσι το μυστικό κλειδί χρησιμοποιείται για την δημιουργία της ψηφιακής υπογραφής και το δημόσιο κατά την επαλήθευση της εγκυρότητας της. Και για τις δυο αυτές λειτουργίες τα μηνύματα υπόκεινται στις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης με βάση τις λειτουργίες του αλγορίθμου SHA (Secure Hash Algorithm). Η ασφάλεια του αλγορίθμου εξασφαλίζει ότι μια ψηφιακή υπογραφή είναι αδύνατο να παραβιασθεί αν δεν επιτευχθεί η υποκλοπή του μυστικού κλειδιού από κάποιον επιτιθέμενο.

Ο αλγόριθμος ακολουθεί συγκεκριμένα βήματα κατά τη λειτουργία του. Αρχικά επιλέγεται ένας πρώτος αριθμός q των 160 bit. Στη συνέχεια για κάθε ακέραιο z, επιλέγεται ένας πρώτος αριθμός p μήκους L-bit, έτσι ώστε p=q*z+1 όπου $512 \leq L \leq 1024$ και ο L να διαιρείται με το 64. Ακολούθως επιλέγεται η παράμετρος h, όπου $1<h<p-1$ έτσι ώστε $g=h^z \pmod p >1$. Στο επόμενο βήμα λαμβάνεται ένας αριθμός x, όπου $0<x<q$ και υπολογίζεται ο αριθμός $y=g^x \pmod p$.Μετά τους υπολογισμούς αυτούς μπορούμε να ορίσουμε ως δημόσιο κλειδί το (p,q,g,y) και μυστικό κλειδί το x.
Για την δημιουργία της ψηφιακής υπογραφής σε ένα αρχικό μήνυμα m, θεωρούμε έναν τυχαίο αριθμό k όπου $0<k<q$ και υπολογίζεται η παράμετρος $r=(g^k \bmod p) \bmod q$. Επίσης υπολογίζεται η παράμετρος $s=(k^{-1}(M+x*r)) \bmod q$, όπου M είναι το επεξεργασμένο μήνυμα hash SHA1. Η ψηφιακή υπογραφή είναι το ζεύγος (r,s).

Για την επαλήθευση της υπογραφής, ο παραλήπτης του μηνύματος m υπολογίζει την παράμετρο $w=s^{-1} \bmod q$ και στη συνέχεια τις παραμέτρους $u1=(M*w) \bmod q$ και $u2=(r*w) \bmod q$, όπου M είναι το επεξεργασμένο μήνυμα hash SHA1. Στο τελικό βήμα υπολογίζεται η παράμετρος $v=((g^{u1}*g^{u2}) \bmod p) \bmod q$. Για να θεωρείται έγκυρη η ψηφιακή υπογραφή θα πρέπει να ισχύει v=r αλλιώς σε διαφορετική περίπτωση η υπογραφή απορρίπτεται.

2.2 **Αλγόριθμοι Συμμετρικής Κρυπτογράφησης**

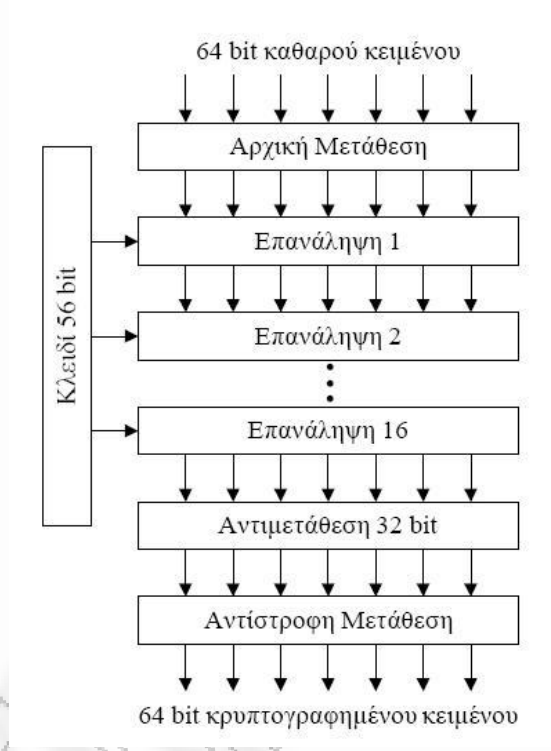
2.2.1 **Ο αλγόριθμος** DES (Data Encryption Standard)

Ο αλγόριθμος Data Encryption Standard (DES), που συναντάται στη βιβλιογραφία και ως Data Encryption Algorithm (DEA) αποτελεί ένα διεθνές πρότυπο κρυπτογράφησης που χρησιμοποιείται για δεκαετίες με πολύ ικανοποιητικά αποτελέσματα και χαρακτηριστικά ασφάλειας απέναντι σε διαφόρων ειδών επιθέσεις κρυπτανάλυσης. Η παρουσίασή του έγινε από την IBM έπειτα από απαίτηση της κυβέρνησης των Ηνωμένων Πολιτειών για μεγαλύτερη ασφάλεια στην κρυπτογράφηση των πληροφοριών από κάποιο σύστημα το οποίο θα είναι οικονομικό, ευρύτατα διαθέσιμο και ιδιαίτερα ασφαλές. Αρχικά χρησιμοποιούσε για την κρυπτογράφηση κλειδί μήκους 128 bit αλλά στη συνέχεια το μέγεθος του κλειδιού ήταν λέξεις των 56 bit. Η πρώτη προσέγγιση του συστήματος αυτού έγινε το 1974 με την παρουσίαση του αλγορίθμου Lucifer που πληρούσε σε ικανοποιητικό βαθμό τις παραπάνω απαιτήσεις του NIST (National Institute of Standards and Technology). Στη συνέχεια και μετά από διάφορες βελτιωτικές αλλαγές και τροποποιήσεις το 1977 κατοχυρώθηκε και υιοθετήθηκε με τη σημερινή του μορφή ως αλγόριθμος DES.

Η κρυπτογράφηση με βάση τον αλγόριθμο αυτό γίνεται σε τμήματα μεγέθους 64 bits του αρχικού κειμένου, ενώ και το αποτέλεσμα στην έξοδο της διαδικασίας είναι ένα κρυπτογραφημένο τμήμα των 64-bit. Λόγω της συμμετρικής φύσης του αλγορίθμου, κατά τη λειτουργία του χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ο ίδιος αλγόριθμος και τα ίδια κλειδιά κρυπτογράφησης. Το μήκος του κλειδιού κρυπτογράφησης είναι 56-bits καθώς από τα 64-bit κάθε όγδοο bit χρησιμοποιείται για έλεγχο ισοτιμίας και δεν λαμβάνεται υπόψη. Οποιοσδήποτε αριθμός των 56-bit μπορεί να αποτελέσει το κλειδί κρυπτογράφησης αλλά και να μεταβληθεί αν αυτό κριθεί αναγκαίο. Επειδή όπως γίνεται κατανοητό το σημαντικό στοιχείο ασφάλειας του αλγορίθμου είναι η ύπαρξη ισχυρών κλειδιών κάποια κλειδιά που θεωρούνται αδύναμα και ευάλωτα σε υποκλοπές μπορεί να αποφευχθούν και να επιλεγούν στη θέση τους άλλα.

Ο αλγόριθμος ικανοποιεί σε μέγιστο βαθμό τις κύριες και θεμελιώδεις ιδιότητες της κρυπτογράφησης, την διάχυση και την σύγχυση. Έτσι το πιο ισχυρό και ουσιώδες τμήμα του αλγορίθμου αποτελείται από μια αντικατάσταση των διαφόρων bit και ακολούθως από μια μετάθεση, ενέργειες που βασίζονται στο κλειδί κρυπτογράφησης. Η διαδικασία αυτή που αποκαλείται κύκλος (round) επαναλαμβάνεται στο αρχικό κείμενο από τον DES 16 φορές έως ότου επιτευχθεί η επιθυμητή κρυπτογράφηση.

Στο σχήμα 2.1 φαίνεται συνοπτικά ο τρόπος κρυπτογράφησης με τον αλγόριθμο DES. Το αρχικό κείμενο των 64 bit κρυπτογραφείται σε ένα κρυπτογράφημα του ιδίου μεγέθους. Στην πρώτη φάση λειτουργίας του αλγορίθμου πραγματοποιείται μια μετάθεση στο αρχικό κείμενο με βάση έναν δεδομένο πίνακα αντικατάστασης και στην οποία δεν συμμετέχει το κλειδί κρυπτογράφησης. Στη συνέχεια με βάση τις συναρτήσεις των κλειδιών ο αλγόριθμος εκτελεί τους 16 κύκλους του και παράγει τα 64 bit του κρυπτογραφημένου μηνύματος. Στην προτελευταία φάση του DES το κρυπτογράφημα διαιρείται σε δυο τμήματα και γίνεται μια αντιμετάθεση των 32 πιο αριστερών bit με τα 32 πιο δεξιά. Στην τελευταία φάση γίνεται η αντίθετη διαδικασία που ακολουθήθηκε στο πρώτο βήμα με τον πίνακα αντικατάστασης.

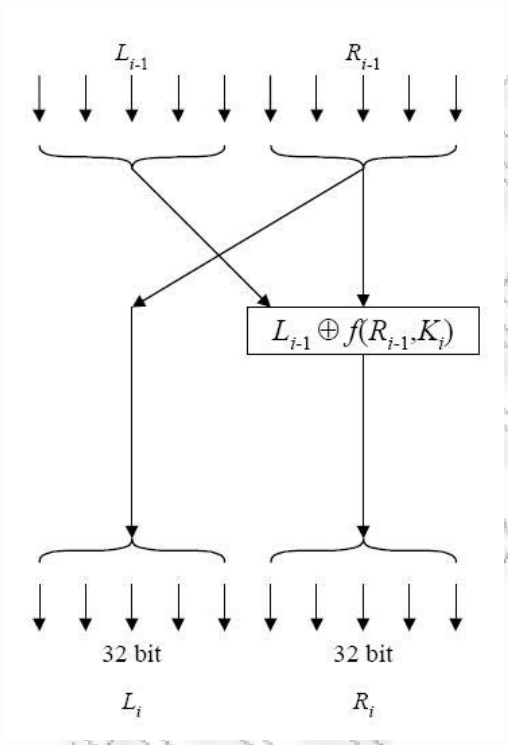


Σχήμα 2.1 Στάδια κρυπτογράφησης DES

Λόγω του ιδιαίτερου σχεδιασμού του αλγορίθμου DES, η αποκρυπτογράφηση μπορεί να γίνει χρησιμοποιώντας το ίδιο κλειδί που χρησιμοποιήθηκε κατά τη διαδικασία της κρυπτογράφησης. Απλώς όπως είναι προφανές θα πρέπει τα βήματα του αλγορίθμου να εκτελεστούν με την αντίστροφη σειρά.

Κατά τη λειτουργία των 16 ενδιάμεσων φάσεων πραγματοποιούνται ακριβώς οι ίδιες ενέργειες και το μόνο που αλλάζει είναι η συνάρτηση του κλειδιού σε κάθε γύρο. Η λειτουργία ενός ενδιάμεσου κύκλου κρυπτογράφησης του DES φαίνεται στο σχήμα 2.2. Σε κάθε τέτοιο κύκλο χρησιμοποιούνται τα κουτιά αντικατάστασης S-box τα οποία αναπαριστώνται ως πίνακες δυο διαστάσεων. Την είσοδο σε κάθε κύκλο αποτελούν δυο τμήματα των 32 bit και μετά από την εφαρμογή των μετασχηματισμών λαμβάνονται στην έξοδο επίσης δυο τμήματα των 32 bit. Το δεξιό τμήμα R_i προκύπτει

από την αποκλειστική διάζευξη XOR της αριστερής εισόδου και της συνάρτησης *f* που ορίζεται από την δεξιά είσοδο και το κλειδί K_i της συγκεκριμένης φάσης. Το αριστερό τμήμα της εξόδου είναι ταυτόσημο με την δεξιά είσοδο.



Σχήμα 2.2 Ενδιάμεση φάση λειτουργίας DES

Το κύριο συνθετικό κάθε ενδιάμεσου κύκλου και στο οποίο βασίζεται η ασφάλειά του αποτελεί η συνάρτηση του κλειδιού. Το κλειδί κάθε κύκλου προφανώς και είναι διαφορετικό. Το αρχικό κλειδί των 56 bit υπόκειται σε μια διαδικασία μετάθεσης και πριν κάθε κύκλο διαιρείται σε δυο τμήματα των 28 bit. Σε κάθε τέτοιο τμήμα εφαρμόζεται αριστερή ολίσθηση τόσων bit όσων ορίζει ο αριθμός κύκλου και έπειτα από μια νέα μετάθεση προκύπτει το υποκλειδί K_i. Κατά τη διαδικασία της αποκρυπτογράφησης η μοναδική διαφορά στη δημιουργία των κλειδιών είναι ότι δεν πραγματοποιείται αριστερή αλλά δεξιά ολίσθηση.

Κατά την εφαρμογή της συνάρτησης του κλειδιού κάθε κύκλου επεκτείνεται κάθε δεξί τμήμα R_{i-1} βάσει δεδομένων πινάκων, κατασκευάζοντας ένα νέο τμήμα των 48 bit που συμβολίζεται με E_i. Έπειτα ακολουθεί η πράξη της αποκλειστικής διάζευξης του E_i και του αντίστοιχου K_i του συγκεκριμένου κύκλου. Το τμήμα των 48 bit διαιρείται σε τμήματα των 6 bit με κάθε τμήμα να αποτελεί την είσοδο στα οκτώ κουτιά αντικατάστασης από τα οποία προκύπτουν ως έξοδοι τμήματα των 4 bit, δηλαδή ένα νέο τμήμα των 32 bit. Το τμήμα αυτό τελικά χρησιμοποιείται για μετάθεση από ένα κουτί P.

Υπάρχουν τρεις διαφορετικές παραλλαγές του τρόπου λειτουργίας του αλγορίθμου DES οι οποίες δεν θα αναπτυχθούν στην ενότητα αυτή. Πρόκειται για τους Electronic Code Book (ECB) , Chain Block Coding (CBC) και ο Cipher Feedback (CFB).Η μείωση του μεγέθους του κλειδιού καθιστά πιο εύκολη την πιθανή επίθεση κρυπτανάλυσης στον αλγόριθμο DES και το μόνο που παραμένει αποθαρρυντικό είναι το μεγάλο κόστος παραβίασης. Μια συνήθης πρακτική για την αποτροπή επιθέσεων και την καλύτερη ασφάλεια είναι η διπλή εφαρμογή του αλγορίθμου κατά την διαδικασία της κρυπτογράφησης, χωρίς αυτό να σημαίνει ότι απαλείφεται εντελώς ο κίνδυνος κρυπτανάλυσης. Η σημαντικότερη δικλείδα ασφαλείας του αλγορίθμου είναι η χρήση κλειδιού κρυπτογράφησης μεγάλου μεγέθους ενώ στη σύγχρονη κρυπτογραφία έχει υιοθετηθεί και η τεχνική Triple DES, η λειτουργία της οποίας παρουσιάζεται παρακάτω εν συντομία.

Triple DES

Ο αλγόριθμος Triple DES αποτελεί μια μικρή διαφοροποίηση του αρχικού αλγορίθμου DES. Αναφορικά με την ταχύτητα εκτέλεσης είναι τρεις φορές πιο αργός από τον DES αλλά η κατάλληλη χρήση του μπορεί να προσδώσει μέγιστη ασφάλεια στην διαδικασία της κρυπτογράφησης. Παρότι επιστημονικά καμία επιλογή αλγορίθμου και τεχνική κρυπτογράφησης δεν είναι άτρωτη σε επιθέσεις, το μεγάλου μήκους κλειδί του Triple DES είτε αντιμετωπίζει αποτελεσματικά τις όποιες προσπάθειες κρυπτανάλυσης είτε αυξάνει δραματικά το χρόνο για την παραβίαση του αλγορίθμου. Κατά τη λειτουργία του γίνεται χρήση δυο ή τριών κλειδιών και εναλλαγή καταστάσεων κρυπτογράφησης – αποκρυπτογράφησης. Υπάρχουν τέσσερις τέτοιοι διαφορετικοί τρόποι λειτουργίας με γνώμονα την επίτευξη της διαδοχικής κρυπτογράφησης και αποκρυπτογράφησης με διαφορετικά κλειδιά και την ενίσχυση του βασικού αλγορίθμου. Σε κάθε διαφορετική λειτουργία τα επιπλέον κλειδιά δημιουργούνται χρησιμοποιώντας κατάλληλους αλγορίθμους σε συνδυασμό με το ιδιωτικό κλειδί. Ως πιο ασφαλής τρόπος λειτουργίας είναι βάσει επιστημονικών μετρήσεων ο DES-EEE3, που χρησιμοποιεί τρεις διαδοχικές κρυπτογραφήσεις τρία διαφορετικά κλειδιά.

- Εκτέλεση τριών κρυπτογραφήσεων με τρία διαφορετικά κλειδιά (DES-EEE3)
- Εκτέλεση διαδοχικά κρυπτογράφησης - αποκρυπτογράφησης - κρυπτογράφησης με τρία διαφορετικά κλειδιά (DES-EDE3)
- Εκτέλεση τριών κρυπτογραφήσεων με δύο διαφορετικά κλειδιά (DES-EEE2)
- Εκτέλεση διαδοχικά κρυπτογράφησης - αποκρυπτογράφησης - κρυπτογράφησης με δύο διαφορετικά κλειδιά (DES-EDE2)

Στην περίπτωση των τριών κλειδιών ο Triple DES χρησιμοποιεί τρία κλειδιά των 64 bit δημιουργώντας συνολικό μήκος κλειδιού 192 bits. Όπως και στον αλγόριθμο DES από το αρχικό κλειδί των 64 bit λαμβάνουμε κλειδί των 56 bit αγνοώντας τα bit ισοτιμίας έτσι και στον triple DES από τα 192 bits του αρχικού κλειδιού λαμβάνουμε τελικά κλειδί συνολικού μήκους 168 bit αγνοώντας 8 bit ισοτιμίας για κάθε ένα από τα τρία διαφορετικά κλειδιά κρυπτογράφησης.

Η διαδικασία κρυπτογράφησης, επαναλαμβανόμενη τρεις φορές (triple) είναι πανομοιότυπη με αυτή του κλασικού αλγορίθμου DES. Έτσι το αρχικό κείμενο υπόκειται σε κρυπτογράφηση με το πρώτο κλειδί, στη συνέχεια οδηγείται σε αποκρυπτογράφηση με το δεύτερο κλειδί και τελικά υπόκειται σε εκ νέου κρυπτογράφηση με το τρίτο κλειδί.

2.2.2 **Ο Αλγόριθμος** AES (Advanced Encryption Standard)

Το έτος 2000 το NIST (National Institute of Standards and Technology) που ως τότε θεωρούσε τον αλγόριθμο DES ως τον ασφαλέστερο και συχνότερα χρησιμοποιούμενο αλγόριθμο συμμετρικής κρυπτογράφησης, ανακοίνωσε ότι ο αλγόριθμος Rijndael έχει επιλεγεί ώστε να είναι πλέον το πρότυπο Advanced Encryption Standard (AES). Η επιλογή αυτή ήταν το αποτέλεσμα μακρόχρονης διαδικασίας επιλογής η οποία ξεκίνησε από τον Σεπτέμβριο του 1997. Η διαδικασία επιλογής διαιρέθηκε σε διάφορα στάδια και το τέλος κάθε σταδίου σήμαινε και τη διεξαγωγή συνεδρίου για την επιλογή του κατάλληλου προτύπου. Τον Αύγουστο του 1998 κατά το τέλους του πρώτου σταδίου ήταν ήδη υποψήφιοι 15 αλγόριθμοι οι οποίοι και αξιολογήθηκαν για την ασφάλειά τους, το κόστος τους, τη δομή του αλγορίθμου καθώς και τα ιδιαίτερα χαρακτηριστικά υλοποίησής τους. Το Μάρτιο του 1999, σε δεύτερο συνέδριο αναλύθηκαν τα αποτελέσματα των διαφόρων υποψηφιοτήτων και τον Αύγουστο του ίδιου έτους επιλέχθηκαν οι επικρατέστεροι πέντε αλγόριθμοι. Επρόκειτο για τους αλγορίθμους MARS της IBM, Rijndael των Daemen και Rijmen και οι αλγόριθμοι Serpent, RC6 και TwoFish. Στη συνέχεια έγινε συστηματική ανάλυση και μελέτη των αλγορίθμων αυτών ώσπου τον Απρίλιο του 2000 σε νέο συνέδριο ζητήθηκαν οι προτιμήσεις των διαφόρων συμμετεχόντων. Ως επικρατέστερη επιλογή ορίσθηκε ο αλγόριθμος Rijndael και τον Οκτώβριο του 2000 το NIST επισήμως ανακοίνωσε ότι ο συγκεκριμένος αλγόριθμος έχει επιλεγεί ως το πρότυπο Advanced Encryption Standard (AES). Η προτυποποίησή του έγινε τελικά το Νοέμβριο του 2001 όπου και αντικατέστησε τον αλγόριθμο DES ως ασφαλέστερο και προτεινόμενο αλγόριθμο κρυπτογράφησης.

Ο αλγόριθμος AES ομοίως με τον DES λειτουργεί με διάφορες παραλλαγές ανάλογα με το μέγεθος κλειδιού που χρησιμοποιεί. Έτσι διακρίνεται στις λειτουργίες AES-128, AES-192 και AES-256 αν το κλειδί κρυπτογράφησης αποτελείται αντίστοιχα από 128, 192 ή 256 bit. Κατά την υλοποίησή του εκτελούνται σε ένα αρχικό μη κρυπτογραφημένο κείμενο των 128 bit οι διάφοροι κύκλοι επαναλήψεων οι ποίοι είναι ανάλογοι με το μέγεθος του κλειδιού. Αρχικά εισάγεται το τμήμα του αρχικού κειμένου μαζί με το αρχικό κλειδί κρυπτογράφησης και στη συνέχεια σε κάθε κύκλο επανάληψης η είσοδος προκύπτει από το τμήμα κειμένου του κύκλου που προηγήθηκε και το νέο κλειδί του συγκεκριμένου κύκλου. Η έξοδος από την όλη διαδικασία είναι ένα κρυπτογραφημένο κείμενο μεγέθους 128 bit όσο και το αρχικό κείμενο.

Οι διάφορες λειτουργίες του AES εκτελούνται σε ενδιάμεσα μέρη τα οποία καλούνται καταστάσεις (States) και η αναπαράσταση κάθε μιας από αυτές γίνεται με έναν πίνακα δύο διαστάσεων. Κάθε τέτοιος πίνακας κατάστασης αποτελείται από

τέσσερις γραμμές και αριθμό στηλών ανάλογο με το μέγεθος του αρχικού κειμένου. Η κατάσταση state κάνει χρήση της μεταβλητής s και δύο δεικτών για την αναπαράστασή της στον πίνακα. Το αρχικό κείμενο ορίζεται ως N_b και μπορεί να πάρει τις τιμές 4, 6 και 8 αν πρόκειται για τμήμα κειμένου των 32 bit, με δεδομένου ότι το μέγεθος του αρχικού κειμένου μπορεί ναι είναι της τάξης των 128, 192 ή 256 bit. Αντίστοιχα ορίζεται και η παράμετρος N_k που δηλώνει το μέγεθος των κλειδιών κρυπτογράφησης σε τμήματα των 32 bit. Στον αλγόριθμο AES τα πιθανά μεγέθη κλειδιών είναι επίσης 128, 192 ή 256 bit οπότε και η παράμετρος N_k μπορεί να λάβει τις τιμές 4, 6 και 8 ανά περίπτωση. Ο αριθμός των επαναληπτικών γύρων του αλγορίθμου συμβολίζεται με N_r, μεταβάλλεται ανάλογα με το μέγεθος του κλειδιού και μπορεί να πάρει τις τιμές 10, 12 και 14 και αποτελούν τιμές αυστηρά καθορισμένες από το πρότυπο AES.

Αρχικά το τμήμα του μη κρυπτογραφημένου κειμένου αναπαρίσταται στον πίνακα κατάστασης state. Ακολουθεί μια λειτουργία κατά την οποία προστίθεται το κλειδί του συγκεκριμένου κύκλου που έχει δημιουργηθεί από την διαδικασία επέκτασης κλειδιού και μετά από τους διάφορους επαναληπτικούς κύκλους παράγεται η τελική μορφή της κατάστασης state που παρέχει το κρυπτογραφημένο κείμενο. Κατά τη λειτουργία του αλγορίθμου πραγματοποιούνται τέσσερις διαφορετικές διαδικασίες οι οποίες είναι: η ShiftRows κατά την οποία γίνεται ολίσθηση των διαφόρων bytes που βρίσκονται στον πίνακα State, η SubBytes για την αντικατάσταση των bytes βάσει κάποιου πίνακα αντικατάστασης, η MixColumns κατά την οποία πραγματοποιείται ανάμιξη των διαφόρων bytes και η διαδικασία AddRoundKey με την οποία πραγματοποιείται η πρόσθεση ενός κλειδιού στον πίνακα State. Οι συγκεκριμένοι μετασχηματισμοί μπορούν με μια αντιστροφή στη σειρά τους να χρησιμοποιηθούν και για την λειτουργία της αποκρυπτογράφησης.

2.2.3 **Ο ΑΛΓΟΡΙΘΜΟΣ** IDEA (International Data Encryption Algorithm)

Ο αλγόριθμος αυτός παρουσιάστηκε κατά το 1990 από τους James Massey και Xuejlia Lai ως ένα πρότυπο με την αρχική ονομασία Proposed Encryption Standard - PES. Οι συνεχείς βελτιώσεις του προτύπου και οι διάφορες τροποποιήσεις του οδήγησαν στην διατύπωση του αλγορίθμου IPES (Improved Proposed Encryption Standard) και αργότερα, το 1992 στην εισαγωγή του αλγορίθμου με την τελική μορφή που πήρε την ονομασία International Data Encryption Algorithm – IDEA.

Κατά τη λειτουργία του ο αλγόριθμος χρησιμοποιεί κλειδί μήκους των 128 bit σε τμήματα αρχικών μη κρυπτογραφημένων τμημάτων κειμένου μήκους 64-bit. Όπως και διάφοροι παρόμοιοι αλγόριθμοι, ο IDEA χρησιμοποιεί τις κατά Shannon ισχυρές κρυπτογραφικές τεχνικές της σύγχυσης και της διάχυσης και ο η ίδια μέθοδος ακολουθείται τόσο κατά την κρυπτογράφηση τόσο κατά την αποκρυπτογράφηση. Ο αλγόριθμος χρησιμοποιεί διαδοχικά τρεις αλγεβρικές τεχνικές για να επιτύχει την κρυπτογράφηση: την αποκλειστική διάζευξη XOR, τον πολλαπλασιασμό και την πρόσθεση.

Το αρχικό μη κρυπτογραφημένο κείμενο διαιρείται σε τέσσερα τμήματα των 16 bit, τα οποία αποτελούν και την είσοδο στον πρώτο από τους οκτώ κύκλους του αλγορίθμου. Σε κάθε έναν από αυτούς τους κύκλους εφαρμόζεται αποκλειστική διάζευξη XOR, πρόσθεση και πολλαπλασιασμός στα τέσσερα τμήματα μεταξύ τους και με έξι υποκλειδιά μεγέθους 16 bit. Ανάμεσα στους διάφορους κύκλους τα δεύτερα και τρίτα τμήματα του κειμένου εναλλάσσονται και τελικά δημιουργείται ένας μετασχηματισμός εξόδου κατά τον οποίον συνδυάζονται κατάλληλα τα τέσσερα τμήματα των 16 bit και τα τέσσερα υποκλειδιά, με διαδοχικούς πολλαπλασιασμούς και προσθέσεις. Η σύνθεση των τεσσάρων τμημάτων οδηγεί στο τελικό κρυπτογραφημένο κείμενο. Από τις διάφορες επιστημονικές μετρήσεις προκύπτει ότι η ταχύτητα υλοποίησης του αλγορίθμου IDEA είναι διπλάσια από αυτήν του αλγορίθμου DES που χρησιμοποιεί παρόμοια τεχνική κρυπτογράφησης αλλά διπλάσιο αριθμό κουτιών αντικατάστασης.

2.3 **Κρυπτογραφικά συστήματα και ασφάλεια**

Η επιλογή του κρυπτογραφικού συστήματος που θα χρησιμοποιηθεί σε μια διαδικασία κρυπτογράφησης δεν αποτελεί μια τυχαία ενέργεια αλλά απαιτεί χρόνο και σαφή προσδιορισμό των χαρακτηριστικών ασφαλείας που τον διακρίνουν και τον καθιστούν “άτρωτο” σε πιθανές απόπειρες επιθέσεων. Η μακροχρόνια επιστημονική έρευνα έχει αποδείξει ότι υπό συγκεκριμένες προϋποθέσεις όλοι οι αλγόριθμοι μπορούν να παραβιασθούν ή να αλλοιωθεί η λειτουργία τους. Επειδή βέβαια σε αρκετές περιπτώσεις για την επιτυχημένη επίθεση κρυπτανάλυσης σε έναν αλγόριθμο, μπορεί να απαιτούνται μεγάλα χρονικά διαστήματα ή τεράστιες οικονομικές απαιτήσεις, γεγονότα που από μόνα τους αποτρέπουν την ανάπτυξη και σχεδίαση της επίθεσης, τα συγκεκριμένα συστήματα πρακτικά μπορεί να θεωρηθούν απαραβίαστα. Μια διάκριση που γίνεται λοιπόν στα διάφορα συστήματα κρυπτογράφησης έχει ως κριτήριό της την αντοχή των αλγορίθμων που χρησιμοποιούν σε κρυπταναλυτικές επιθέσεις και κατά πόσο αυτά διατηρούν τη δομή και τις ιδιότητές τους αναλλοίωτες παρά τις όποιες ενέργειες παραβίασης.

Σε θεωρητική βάση ένας αλγόριθμος κρυπτογράφησης θεωρείται ασφαλής όταν μπορεί να διατηρήσει απαραβίαστη την πληροφορία που να κρυπτογραφήσει και να αποκαλύψει το αρχικό μήνυμα μόνο σε παραλήπτη με ανάλογα δικαιώματα. Ένα σύστημα κρυπτογράφησης θα πρέπει να μελετάται και να σχεδιάζεται ανεξάρτητα με τις όποιες ήδη υπάρχουσες θεωρίες κρυπτανάλυσης και να μην υλοποιείται με βάση τις ως τώρα γνωστές δυνατότητες κρυπταναλυτικής ισχύος, αλλά να μπορεί να προσφέρει ασφάλεια αδιαφορώντας για μεγέθη όπως τα μήκη των κλειδιών και των αρχικών κειμένων, η δεδομένη υπολογιστική ισχύς ή οι χρονικοί περιορισμοί. Έτσι θα μπορούσαμε να ορίσουμε την υπολογιστική ασφάλεια ενός κρυπτογραφικού συστήματος ως την ανθεκτικότητά του σε επιθέσεις κακόβουλων χρηστών σε τέτοιο βαθμό που να θεωρούνται απαραβίαστες με τα σημερινά δεδομένα.

Συνήθως μια απόπειρα κρυπταναλυτικής επίθεσης ξεκινά όταν ήδη ο κρυπταναλυτής έχει αποκτήσει πρόσβαση είτε σε κάποιο κλειδί κρυπτογράφησης είτε

σε τμήμα του αρχικού ή κρυπτογραφημένου κειμένου. Σημαντικές κατευθύνσεις προς την εξεύρεση λύσης σε τέτοιες περιπτώσεις μπορούν να δώσουν οι θεωρίες της Πληροφορίας και Πολυπλοκότητας τόσο ως προς την διασφάλιση των προς κρυπτογράφηση κειμένων αυτών καθαυτών όσο και ως προς την διατύπωση σύνθετων υπολογιστικών αλγορίθμων που καθιστούν απαγορευτικές τις πιθανότητες εμφάνισης κρυπταναλυτικής επίθεσης.

2.4 **Επιθέσεις κρυπτανάλυσης σε αλγορίθμους**

Οι διάφορες τεχνικές κρυπτανάλυσης βασίζονται στην πρακτική της ανάλυσης ενός κρυπτογραφημένου μηνύματος με σκοπό να το παραβιάσουν ή να υποκλέψουν τον τ κώδικα κρυπτογράφησής του. Γενικότερα η κρυπτανάλυση έχει ως αντικείμενό της την μελέτη των διαφορετικών τεχνικών που μπορούν να χρησιμοποιηθούν προς την κατεύθυνση της απόκτησης πρόσβασης σε ένα κείμενο που έχει ήδη κρυπτογραφηθεί χωρίς να χρησιμοποιήσουν την προβλεπόμενη και “νόμιμη” οδό της χρήσης του κλειδιού αποκρυπτογράφησης. Οι κρυπταναλυτικές επιθέσεις προσπαθούν να εντοπίσουν πιθανές αδυναμίες των μεθόδων που χρησιμοποιήθηκαν για την κρυπτογράφηση του αρχικού κειμένου ή για την δημιουργία των κλειδιών κρυπτογράφησης ενώ από την άλλη πλευρά, τα αποτελέσματά τους μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των αδυναμιών αυτών από τους σχεδιαστές των κρυπτογραφικών συστημάτων.

Στις περισσότερες των περιπτώσεων κάποιος κρυπταναλυτής μπορεί να έχει στη διάθεσή του πλήθος πληροφοριών όπως τα αρχικά μηνύματα, τα κλειδιά κρυπτογράφησης, τμήματα κρυπτογραφημένων κειμένων και γενικότερα την όλη δομή και φιλοσοφία του αλγορίθμου που επιθυμούν να παραβιάσουν. Το γεγονός αυτό είναι και το πιο πιθανό αφού όπως θεωρείται αποδεκτό στο επιστημονικό πεδίο της κρυπτογραφίας, ένα σύστημα κρυπτογράφησης που προσπαθεί να διατηρήσει μυστική την ύπαρξή του ή ακόμα χειρότερα την ύπαρξη των αλγορίθμων που το συνθέτουν, τότε πρόκειται για ένα σύστημα που δεν μπορεί να αποτελέσει πρότυπο κρυπτογράφησης σε ευρεία κλίμακα.

Οι τύποι των επιθέσεων κρυπτανάλυσης μπορούν γενικότερα να διακριθούν σε έξι κατηγορίες που είναι άμεσα συνυφασμένες με το είδος της πληροφορίας που διαθέτει ο κρυπταναλυτής που σχεδιάζει την επίθεση. Στη συνέχεια παρουσιάζονται οι κατηγορίες των επιθέσεων με αύξουσα σειρά κατάταξης αναφορικά με την ποιότητα της πληροφορίας που είναι διαθέσιμη στον κρυπταναλυτή ή διαφορετικά σε φθίνουσα σειρά κατάταξης αναφορικά με το επίπεδο δυσκολίας τους ως προς την κρυπτανάλυση. Το ζητούμενο της κρυπτανάλυσης είναι σε κάθε περίπτωση είναι το να μπορεί ο κρυπταναλυτής να αποκτήσει τη δυνατότητα αποκρυπτογράφησης νέων τμημάτων κρυπτογραφημένων μηνυμάτων χωρίς την ανάγκη ύπαρξης επιπρόσθετης πληροφόρησης. Το ιδεατό βεβαίως επίπεδο μια κρυπταναλυτικής επίθεσης είναι όπως γίνεται κατανοητό η αποκωδικοποίηση του μυστικού κλειδιού της διαδικασίας της κρυπτογράφησης. Οι κατηγορίες των επιθέσεων λοιπόν είναι οι παρακάτω:

- *ciphertext-only* attack: Ο κρυπταναλυτής διαθέτει κάποιο δείγμα του κρυπτογραφημένου κειμένου χωρίς το αρχικό κείμενο που αντιστοιχεί σε αυτό. Παρόλο που θεωρητικά είναι εύκολη η υποκλοπή της πληροφορίας με την επίθεση αυτή, πρακτικά επιτυγχάνεται πολύ δύσκολα αφού προϋποθέτει τη γνώση μεγάλου δείγματος του κρυπτογραφημένου κειμένου.

- known-plaintext attack: Είναι το είδος της επίθεσης κατά την οποία ο κρυπταναλυτής έχει στη διάθεσή του τόσο το δείγμα του κρυπτογραφημένου κειμένου όσο και το αρχικό κείμενο που αντιστοιχεί σε αυτό.

- *chosen-plaintext* attack: Ο κρυπταναλυτής έχει τη δυνατότητα να επιλέξει μια ποσότητα αρχικού κειμένου από το οποίο στη συνέχεια θα αποκτήσει πρόσβαση και στο αντίστοιχο κρυπτογραφημένο κείμενο.

- *chosen-ciphertext* attack: Στην περίπτωση αυτή ο κρυπταναλυτής μπορεί να επιλέξει ένα τμήμα του κρυπτογραφημένου κειμένου και να προσπαθήσει να αποκτήσει πρόσβαση στο αντίστοιχο αρχικό κείμενο. Οι επιθέσεις τέτοιου τύπου συναντώνται συνήθως σε συστήματα κρυπτογράφησης δημοσίου κλειδιού.

- *adaptive-chosen-plaintext* attack: Αποτελεί μια ειδική περίπτωση της *chosen-plaintext* attack κατά την οποία ο κρυπταναλυτής είναι ικανός να επιλέξει δυναμικά τα δείγματα του αρχικού μηνύματος μεταβάλλοντας τις όποιες επιλογές έχει κάνει με βάση τα αποτελέσματα προηγούμενων κρυπτογραφήσεων.

- *adaptive-chosen-ciphertext: Αποτελεί μια ειδική περίπτωση της chosen-ciphertext* attack. Ο κρυπταναλυτής μπορεί να εξαπολύσει μια τέτοια επίθεση στην περίπτωση που έχει ελευθερία χρήσης του μηχανισμού αποκρυπτογράφησης αλλά είναι αδύνατη η απόκτηση πρόσβασης του κλειδιού αποκρυπτογράφησης από αυτόν.

Κεφάλαιο 3

3.1 **Κουτιά αντικατάστασης** (S-boxes)

Τα κουτιά αντικατάστασης (S-boxes) αποτελούν στις περισσότερες περιπτώσεις το μοναδικό μη γραμμικό στάδιο ενός αλγορίθμου κρυπτογράφησης. Κατά τη λειτουργία του, το κουτί αντικατάστασης προβαίνει σε αντιστοίχηση μια ακολουθίας από m bits που λαμβάνει ως είσοδο με μια άλλη ακολουθία από n bits η οποία αποτελεί το αποτέλεσμα στην έξοδό του. Η αναπαράστασή τους συνήθως γίνεται με έναν πίνακα και για την υλοποίηση τους από τις κυριότερες γλώσσες προγραμματισμού, χρησιμοποιείται ένας πίνακας όπου, στην περίπτωση S-box μικρού μεγέθους, έχει μία διάσταση, η είσοδος αποτελεί τον δείκτη του πίνακα αυτού ενώ το περιεχόμενό του αποτελεί την έξοδο. Τα κουτιά αντικατάστασης προσθέτουν την ιδιότητα της σύγχυσης (confusion) στους αλγόριθμους κρυπτογράφησης που τα χρησιμοποιούν. Κατά τη λειτουργία τους δημιουργούν αόριστες και δύσκολα ανιχνεύσιμες διαφορές μεταξύ του αρχικού μηνύματος και του παραγόμενου κρυπτογραφήματος.

Οι συναρτήσεις αντικατάστασης πρέπει να είναι αντιστρέψιμες έτσι ώστε να επιτρέπουν την αποκωδικοποίηση του κρυπτογραφημένου μηνύματος αλλά με τον τρόπο αυτό καθιστούν όλο το σύστημα του αλγορίθμου μη ασφαλές. Για να επιτευχθεί η απαιτούμενη ασφάλεια θα πρέπει οι συναρτήσεις αντικατάστασης να ενισχυθούν με την ιδιότητα της διάχυσης (diffusion) και με την λειτουργία της ανάμειξης των κλειδιών κρυπτογράφησης κατά τα διάφορα στάδιά της εφαρμογής τους. Η εισαγωγή της ιδιότητας της σύγχυσης σε έναν αλγόριθμο κρυπτογράφησης προσφέρει σημαντικό βαθμό αντίστασης σε περιπτώσεις που θα υπάρξει πιθανή γραμμική ή διαφορική επίθεση κρυπτανάλυσης.

Η διαφορική κρυπτανάλυση (differential cryptanalysis) στηρίζεται στην ανάλυση της εξέλιξης που παρουσιάζουν οι διαφορές ανάμεσα σε δύο σχετιζόμενα plaintexts, που κρυπτογραφούνται με το ίδιο κλειδί. Με προσεκτική ανάλυση των σχετιζόμενων δεδομένων, μπορεί κάποιος να δημιουργήσει πιθανά κλειδιά που μπορεί να χρησιμοποιήθηκαν για την κρυπτογράφηση (το πιο πιθανό από αυτά τα κλειδιά θεωρείται το σωστό). Αυτές οι τεχνικές αρχικά αναπτύχθηκαν από τον Murphy, αλλά αναπτύχθηκαν και τελειοποιήθηκαν από τους Biham και Shamir, που τις χρησιμοποίησαν σε επιθέσεις εναντίον του αλγόριθμου DES. Οι τεχνικές γραμμικής κρυπτανάλυσης (linear cryptanalysis) χρησιμοποιούν μία γραμμική προσέγγιση για να περιγράψουν την συμπεριφορά ενός αλγορίθμου τμημάτων. Αν κάποιος έχει στην διάθεσή του αρκετά ζεύγη plaintext και του αντίστοιχου κρυπτογραφήματος που προκύπτει, μπορεί να ανακτήσει κομμάτια πληροφορίας που αποτελούν το κλειδί. Όσο μεγαλύτερο είναι το μέγεθος της πληροφορίας που έχει κάποιος στην διάθεσή του, τόσο πιο πιθανή είναι η δημιουργία του σωστού κλειδιού. Η τεχνική αυτή αναπτύχθηκε κυρίως από τον Matsui εναντίον του αλγόριθμου DES. Τα βασικότερα χαρακτηριστικά των τεχνικών γραμμικής και διαφορικής κρυπτανάλυσης συνδυάστηκαν με επιτυχία από τους Langford και Hellman, για να δημιουργηθεί η διαφορική-γραμμική κρυπτανάλυση.

Ο απλούστερος τύπος ενός κουτιού αντικατάστασης δέχεται μια ακολουθία bits στην είσοδό του και με την βοήθεια ενός πίνακα - lookup table - καθορίζει την ακολουθία bits στην έξοδο του. Κατά την διαδικασία της αποκρυπτογράφησης αυτός ο

πίνακας προφανώς αντιστρέφεται. Η σχεδίαση και κατασκευή των κουτιών αντικατάστασης είναι εξ ορισμού μια δύσκολη διαδικασία και απαιτεί βαθιά γνώση και μελέτη των διάφορων σύγχρονων μεθόδων κρυπτανάλυσης. Γενικότερα η χρήση κάποιων συγκεκριμένων patterns στην είσοδο του κουτιού θα παράγει patterns στην έξοδο με μια πιθανότητα σχεδόν ισοδύναμη μιας τυχαία συνάρτησης. Για παράδειγμα αν χρησιμοποιηθεί η αποκλειστική διάζευξη XOR για όλα τα bits της εισόδου ένα ιδανικό κουτί αντικατάστασης θα παρήγαγε την ίδια τιμή XOR σε ακριβώς μισές από τις αντίστοιχες ακολουθίες εξόδου.

3.2 **Παράμετροι ασφάλειας** S-box

Οι παράμετροι που καθιστούν ασφαλές ένα κουτί αντικατάστασης και αφορούν το αντικείμενο της επιστήμης της κρυπτογραφίας είναι:

- ü *το μέγεθος του S-box και*
- ü *ο τρόπος συμπλήρωσης του περιεχομένου του πίνακά του.*

Μια ορθολογική και αποδεκτή τεχνική σχεδίασης ενός κουτιού αντικατάστασης απαιτεί να τεθούν επίσης κάποια βασικά τα κριτήρια αξιολόγησης και να οριστούν οι παραπάνω παράμετροι με τρόπο τέτοιο ώστε να ικανοποιούνται τα κριτήρια αυτά. επιλεγούν οι δύο παράμετροι ώστε να πληρούνται τα κριτήρια αυτά. Στην βιβλιογραφία συναντούμε διάφορες προσεγγίσεις για τα κριτήρια αυτά όμως οι Adams και Tavares παρέθεσαν με σαφήνεια τα παρακάτω κριτήρια τα οποία καθιστούν ένα κουτί αντικατάστασης ασφαλές και ιδανικό για την χρήση του σε έναν αλγόριθμο κρυπτογράφησης. Τα κριτήρια αυτά είναι:

- ü **Non-Linearity (Μη γραμμικότητα).** Ένα κουτί αντικατάστασης το οποίο είναι γραμμικό μπορεί εύκολα να αποτελέσει τον αδύναμο κρίκο σε μια ενδεχόμενη επίθεση κρυπτανάλυσης. Έτσι το κριτήριο της μη γραμμικότητας αποτελεί βασικό συστατικό στοιχείο ενός κουτιού αντικατάστασης για την ασφάλεια ενός αλγορίθμου.

- ü **Bijection (Αμφίεση).** Το κριτήριο της αμφίεσης αυτό είναι απαραίτητο για τον μονοσήμαντο ορισμό της διαδικασίας της αποκρυπτογράφησης. Σε πολλούς αλγορίθμους κρυπτογράφησης το κουτί μπορεί να παίζει σημαντικό ρόλο και στην διαδικασία της αποκρυπτογράφησης ενώ σε κάποιους άλλους να μην έχει τόσο σημαντική συμβολή. Για παράδειγμα στα δίκτυα Feistel δεν απαιτούνται κουτιά αντικατάστασης που να ικανοποιούν το κριτήριο της αμφίεσης.

- ü **Κριτήριο Strict avalanche (Αυστηρή χιονοστιβάδα).** Οι Webster και Tavares, χρησιμοποιώντας τα χαρακτηριστικά της διάχυσης και σύγχυσης που έθεσε ο Shannon, εισήγαγαν το κριτήριο της «αυστηρής χιονοστιβάδας». Για να ικανοποιεί το κριτήριο αυτό ένα κουτί αντικατάστασης θα πρέπει για κάθε bit της εισόδου του η

αντιστροφή του προκαλεί την αντιστροφή σε οποιοδήποτε από τα bit της ακολουθίας εξόδου, με πιθανότητα ίση με 1/2.

- **Output independence (Ανεξαρτησία εξόδου).** Το κριτήριο αυτό ικανοποιείται όταν δεν υπάρχουν εμφανείς συσχετίσεις στις ακολουθίες των bits εισόδου και εξόδου. Η απουσία τέτοιων συσχετίσεων διατηρεί αόριστο των χώρο αναζητήσεων σε πιθανή ενέργεια κρυπταναλυτικής επίθεσης.

Γίνεται λοιπόν κατανοητό ότι η ασφάλεια των συμμετρικών αλγορίθμων εξαρτάται από τις ιδιότητες των κουτιών αντικατάστασης που χρησιμοποιούνται στα βήματα του αλγορίθμου κρυπτογράφησης. Γενικότερα όσο μεγαλύτερο είναι το μέγεθος ενός S-box τόσο μεγαλύτερη ασφάλεια παρέχει στον αλγόριθμο. Αν και τα S-boxes μπορεί να είναι μη γραμμικά η μη προσεκτική σχεδίασή της δομής και των χαρακτηριστικών τους μπορεί να αποβεί μοιραία σε μια πιθανή επίθεση κρυπτανάλυσης.

Πολλές επιστημονικές μελέτες έχουν αναπτυχθεί με αντικείμενο τις όσο το δυνατόν ιδανικότερες ιδιότητες των κουτιών αντικατάστασης, ώστε να είναι ανθεκτικά στις επιθέσεις. Για παράδειγμα οι E. Biham και A. Shamir προτείνουν ότι ένα ιδανικό S- box θα πρέπει να έχει όλες τις εισόδους στον πίνακα αποκλειστικής διάζευξης XOR ίσες με 0 ή 2.

3.3 Ιδιότητες ενός "ιδεατού" κουτιού αντικατάστασης

Ένα m x n S-box μπορεί να αναπαρασταθεί ως ένας δυαδικός πίνακας 2^m x n, M, στον οποίον κάθε στήλη είναι ένα δυαδικό διάνυσμα που αντιστοιχεί σε μια Boolean συνάρτηση για τις m μεταβλητές εισόδου και καθορίζει τη σχέση κάθε bit εξόδου για κάθε αντίστοιχο εισερχόμενο. Έτσι, η σειρά i του πίνακα M, $1 \le i \le 2^m$ αποτελεί το διάνυσμα εξόδου των n bits που αντιστοιχεί στο i-οστό διάνυσμα εισόδου. Ένα S-box με καλές avalanche ιδιότητες θα είναι αυτό που το άθροισμα (mod 2) από κάθε ζεύγος γραμμών του πίνακα M θα είναι κατά προσεγγιστικά κατά το ήμισυ με τιμές ίσες με μηδέν και κατά το άλλο ήμισυ ίσες με ένα.

Σε περισσότερο εμπεριστατωμένες επιστημονικές έρευνες αποδεικνύεται πως αν οι στήλες στα κουτιά αντικατάστασης είναι βασισμένες στις συναρτήσεις Bent, τότε το S-Box συμπεριφέρεται σαν ασφαλές κουτί το οποίο ανταποκρίνεται στις avalanche ιδιότητες. Κάθε αλλαγή στα m bits εισόδου θα προκαλέσει μεταβολή σε κάθε ένα από τα n bits εξόδου με πιθανότητα1/2. Στον πίνακα M, μια στήλη θεωρείται ότι ως bent στήλη, αν κάθε κανονικοποιημένο διάνυσμα των μετασχηματισμών Walsh-Hadamard της δυαδικής στήλης έχει όλους τους συντελεστές της με τιμές 1 ή -1. Ο μετασχηματισμός Walsh-Hadamard είναι ανάλογος με τον μετασχηματισμό Fourier.

Ένας μεγάλος αριθμός από γνωστά δυαδικά διανύσματα μπορούν να χρησιμοποιηθούν στην κατασκευή ενός πίνακα S-box, M. Από μελέτη του E. Biham επίσης, προκύπτει ότι αν όλοι οι γραμμικοί συνδυασμοί των στηλών του κουτιού

αντικατάστασης είναι επίσης bent τότε το S-box θα είναι πιο ανθεκτικό σε επιθέσεις γραμμικής κρυπτανάλυσης.

Θεωρητικά, ένα ιδεατό S-box θα πρέπει να πληροί τις ιδιότητες που συνοπτικά παρουσιάζονται παρακάτω:

I. Κάθε γραμμικός συνδυασμός των στηλών του S-box να είναι bent

II. Κάθε είσοδος στον πίνακα XOR να είναι ίση με 0 ή 2

III. Το S-box να ικανοποιεί το κριτήριο maximum order strict avalanche

IV. Το S-box να ικανοποιεί το κριτήριο maximum order bit independence

V. Τα βάρη κάθε γραμμής του M να έχουν μα διωνυμική κατανομή με μέσο n/2

VI. Τα βάρη κάθε ζεύγους γραμμών του M να έχουν μα διωνυμική κατανομή με μέσο n/2

VII. Το βάρος κάθε στήλης να είναι βάρος Hamming 2^{n-1}

Όπως έχει ήδη αναφερθεί τα S-boxes που ικανοποιούν την ιδιότητα (I) αποδεικνύονται πιο ασφαλή και ανθεκτικά σε επίθεση γραμμικής κρυπτανάλυσης. Τα κουτιά αντικατάστασης που ικανοποιούν την ιδιότητα (II) επιτυγχάνουν καλύτερη ασφάλεια σε περιπτώσεις διαφορικής κρυπτανάλυσης. Οι ιδιότητες (I), (V) και (VII) εξασφαλίζουν την ύπαρξη καλών στατικών χαρακτηριστικών ενώ οι (II), (III) και (IV) εξασφαλίζουν την ύπαρξη καλών δυναμικών χαρακτηριστικών.

Αν και αυτές οι ιδιότητες έχουν μελετηθεί ευρύτατα δεν έχει αποσαφηνιστεί ως τώρα από άλλες ερευνητικές προσεγγίσεις σε τι βαθμό είναι δυνατό να επιτευχθούν στην πράξη. Οι αλγόριθμοι αντικατάστασης που χρειάζονται μεγάλου μεγέθους S-boxes συχνά χρησιμοποιούν τυχαία S-boxes αντί να κατασκευάσουν νέα επειδή οι τεχνικές κατασκευής έχουν παραδοσιακά μεγάλο χρόνο υλοποίησης. Επίσης είναι δύσκολο να κατασκευαστούν κουτιά αντικατάστασης χρησιμοποιώντας συγκεκριμένες μαθηματικές τεχνικές που θα είχαν ως αποτέλεσμα ένα S-box με τυχαία παραγόμενα χαρακτηριστικά. Για το λόγο αυτό, τα υπάρχοντα συστήματα παράγουν τυχαία S-boxes και στη συνέχεια κάνουν το απαραίτητο έλεγχο για τις επιθυμητές ιδιότητες. Αυτή η μέθοδος βέβαια θεωρείται υπολογιστικά μη αποδοτική ιδίως όταν πρόκειται για κουτιά αντικατάστασης μεγάλου μεγέθους. Οπότε το ιδανικό για την αύξηση της ασφάλειας των αλγορίθμων κρυπτογράφησης είναι η κατασκευή S-boxes τα οποία θα πληρούν όσο το δυνατόν περισσότερες από τις ιδιότητες που αναφέρθηκαν παραπάνω, θα έχουν μειωμένο χρόνο κατασκευής και θα εμφανίζονται ανθεκτικά σε πιθανές κρυπταναλυτικές επιθέσεις κάθε είδους.

Δυο από τις πιο κοινές επιθέσεις που έχει αποδεδειγμένα δεχθεί ο αλγόριθμος DES στηρίζονται στην γραμμική κατασκευή των S-boxes. Οι Chaum and Evertse μπόρεσαν να εντοπίσουν τμήματα των 6 Bits τα οποία όταν γίνουν XOR στην είσοδο του S-Box παράγουν κατά την έξοδο τα ίδια τμήματα. Έτσι ομαδοποιώντας αυτές τις γραμμικές δομές μπόρεσαν να καταφέρουν επιτυχημένη επίθεση στον αλγόριθμο. Επίσης οι Biham and Shamir απέδειξαν ότι με συγκεκριμένες αλλαγές στην είσοδο του S-box μπορεί με μεγάλη πιθανότητα να εντοπιστούν τα αντίστοιχα τμήματα εξόδου τα οποία έχουν τις περισσότερο μη ομαλά κατανεμημένες αλλαγές.

Σημαντική συνεισφορά προς την κατεύθυνση της αντίστασης σε κρυπταναλυτικές επιθέσεις και την παρεχόμενη ασφάλεια των αλγορίθμων έχουν οι τέλειες μη γραμμικές συναρτήσεις όπως προκύπτει κι από την μελέτη των Meier and Staffelbach. Για την κατασκευή ενός ασφαλούς S-box είναι απαραίτητο κάθε bit της εξόδου να είναι μια τέλεια μη γραμμική συνάρτηση της εισόδου και συνάμα κάθε γραμμικός συνδυασμός των μεταβλητών εξόδου να είναι τέλεια μη γραμμικός. Ένα ιδανικά μη γραμμικό S-box το οποίο θεωρείται άτρωτο σε επιθέσεις διαφορικής κρυπτανάλυσης στις οποίες χρησιμοποιούνται μέθοδοι μη ισορροπημένων παραγώγων, μπορεί να προσφέρει ασφάλεια αν σχεδιαστεί έχοντας τουλάχιστον διπλάσιο αριθμό μεταβλητών εισόδου από τον αριθμό των μεταβλητών εξόδου του. Από την μελέτη της βιβλιογραφίας και ειδικά των μελετών του Nyberg ο σχεδιασμός τέτοιων S-box μπορεί να γίνει με την μέθοδο Maiorana-McFarland και της κατασκευής συναρτήσεων Bent.

3.4 **Ασφάλεια** S-boxes **σε πιθανές αλγεβρικές επιθέσεις**

Όπως ήδη έχει αναφερθεί η σωστή επιλογή σχεδίασης των s-box εξαρτάται και από τις επιθέσεις που καλείται να αντιμετωπίσει ένας αλγόριθμος. Για παράδειγμα στην περίπτωση του αλγορίθμου AES οι Courtois και Pieprzyk πρότειναν μια επίθεση κρυπτανάλυσης που αξιοποιεί τις αλγεβρικές ιδιότητες των S-boxes. Ειδικότερα, αν γίνει δυνατή η γνωστοποίηση πολλών εξισώσεων μικρού αριθμού μονωνύμων των S-boxes ο αλγόριθμος τμημάτων μπορεί να αναπαρασταθεί από πολλές εξισώσεις μικρού αριθμού μεταβλητών. Έτσι με την επίλυση αυτών των πολυμεταβλητών εξισώσεων (multivariate equations) με τη χρήση ενός αλγορίθμου που καλείται XSL, μπορεί να επιτευχθεί η αποκάλυψη του κλειδιού του αλγόριθμου κρυπτογράφησης.

Πριν προχωρήσουμε στην μελέτη της συμβολής των κουτιών αντικατάστασης στην αποτροπή αλγεβρικών επιθέσεων, δίνουμε έναν ορισμό για το τι θεωρείται από αλγεβρική άποψη ως αντίσταση στις αλγεβρικές επιθέσεις (resistance of algebraic attacks - RAA):

Σε ένα σύνολο r εξισώσεων από t πλήθος μονωνύμων που ανήκουν στο F_2^n, ορίζουμε την παράσταση $\Gamma = ((t-r)/n)^{[(t-r)/n]}$ ως αντίσταση στις αλγεβρικές επιθέσεις (RAA).

Προς την κατεύθυνση αυτή και την αναζήτηση πρακτικών λύσεων σχεδιασμού κατάλληλων S-boxes για την αντιμετώπιση των διαφόρων αλγεβρικών επιθέσεων οι Cheon και Lee μελέτησαν την ανάπτυξη γραμμικά ανεξάρτητων πολυμεταβλητών εξισώσεων των κουτιών αντικατάστασης με τη χρήση τριών παραδοχών:

- **ü** Η πρώτη ορίζει ότι αν μια Boolean διανυσματική συνάρτηση είναι μη γραμμική τότε και οι συστατικές της συναρτήσεις θα είναι γραμμικά ανεξάρτητες. Έτσι έγινε εφαρμογή σε n × n S-boxes x^{2^k+1} και n × 2n S-boxes (x^{2^k+1} , $x^{2^{k+1}+1}$) που είναι μη γραμμικά όταν για τον μέγιστο κοινό διαιρέτη (greatest common divisor) ισχύει gcd(n, 2k) = 1 and |k − n/2| > 1, αντιστοίχως.

- **ü** Η δεύτερη ορίζει ότι αν για μια Boolean διανυσματική συνάρτηση F(x, y) : F_2^n × F_2^n -> F_2^m και g : F_2^n-> F_2^n τότε η συνάρτηση F(x, g(x)) έχει m γραμμικώς ανεξάρτητες συστατικές συναρτήσεις δηλαδή F(x, y).

- **ü** Η τρίτη η γραμμική ανεξαρτησία των πολυμεταβλητών συναρτήσεων παραμένει αμετάβλητη από σχετικούς μετασχηματισμούς των εισόδων και των γραμμικών μετασχηματισμών των εξόδων του S-boxes.

Η εφαρμογή των τριών αυτών παραδοχών θα εφαρμοστεί σε S-boxes με διαφορετικά χαρακτηριστικά ώστε να αποσαφηνιστεί η καλύτερη επιλογή στην αντιμετώπιση των αλγεβρικών επιθέσεων. Αρχικά χρησιμοποιείται η μέθοδος της *εναλλαγής εκθετών* κι έτσι μπορεί να αποδειχθεί ότι με αυτή τη δομή των κουτιών αντικατάστασης οι συναρτήσεις τάξης 5n της αντίστροφης συνάρτησης x*y=1 στο F_2^n ή και των σχετικών μετασχηματισμών τους είναι γραμμικά ανεξάρτητες για κάθε θετικό ακέραιο n.

Στη συνέχεια γίνεται χρήση του εκθέτη Gold και του εκθέτη Kasami. Όταν για τον μέγιστο κοινό διαιρέτη ισχύει: gcd(k, n) = 1,τότε ο εκθέτης 2^k+1 ονομάζεται εκθέτης Gold. Κάθε διαφορικό μονώνυμο μπορεί να μετατραπεί σε μονώνυμο με εκθέτη Gold με έναν αντίστοιχο μετασχηματισμό.
Όταν για τον μέγιστο κοινό διαιρέτη ισχύει: gcd(n, k) = 1 και k > 1, τότε ο εκθέτης 2^{2k} − 2^k + 1 καλείται εκθέτης Kasami. Ο συγκεκριμένος εκθέτης διατηρεί το βάρος Hamming k + 1, αλλά με την έκθεση στην δύναμη 2^k + 1, προκύπτει η διαφορική εξίσωση F_1 : $y^{2^k+1} - x^{2^k+1}$.

Το θεώρημα που ακολουθεί ορίζει το μέγεθος της αντίστασης σε αλγεβρικές επιθέσεις όταν τα κουτιά αντικατάστασης έχουν κατασκευαστεί χρησιμοποιώντας την τεχνική του εκθέτη Kasami.

Θεωρούμε y = $x^{2^{2k}-2^k+1}$ με μέγιστο κοινό διαιρέτη gcd(k, n) = 1 στο F_2^n. Μπορούμε να παράγουμε n γραμμικά ανεξάρτητες εξισώσεις με n^2+n μεταβλητές. Τότε η αντίσταση στης αλγεβρικές επιθέσεις RAA δίνεται από τη σχέση Γ = n^n.

Οι δυο τύποι των S-Boxes που κάνουν χρήση των εκθετών Gold και Kasami προσφέρουν μεγαλύτερη ασφάλεια σε πιθανές γραμμικές οι διαφορικές κρυπταναλυτικές επιθέσεις. Παρόλο που οι διάφορες τεχνικές που είδαμε παραπάνω έχουν παρόμοια αποτελέσματα, αξιολογώντας τα δεδομένα που προκύπτουν από την

εφαρμογή τους στην πράξη, οδηγούμαστε στο συμπέρασμα ότι τα S-boxes που προσφέρουν την μεγαλύτερη ασφάλεια είναι αυτά που σχεδιάζονται με τη χρήση εκθετών Kasami σε αντίθεση με αυτά των εκθετών gold που προσφέρουν χαμηλότερου επιπέδου ασφάλεια κρυπτογράφησης.

3.5 **Ασφάλεια των** S-boxes **βασισμένων στην τεχνική** Matrix Power

Όπως είδαμε στην περίπτωση σχεδίασης κουτιών αντικατάστασης και όπως απέδειξαν οι Courtois και Pieprzyk πολλές κρυπταναλυτικές επιθέσεις είχαν ως στόχο τους μια μικρή αλγεβρική δομή των αλγορίθμων και την ευαισθησία της σε αλγεβρικές επιθέσεις. Οι τεχνικές επιθέσεων βασίζονται στη δημιουργία ενός συστήματος αλγεβρικών εξισώσεων πολυωνυμικού τύπου για την αναπαράσταση της εισόδου, της εξόδου και του κλειδιού κρυπτογράφησης. Οι διάφοροι τύποι αλγεβρικών επιθέσεων άλλαξαν κάποια από τα ήδη διατυπωμένα αξιώματα ασφαλείας των συστημάτων κρυπτογράφησης:

- **ü** Η πολυπλοκότητα δεν είναι πλέον υποχρεωτικό να αυξάνεται εκθετικά με τον αριθμών των γύρων.

- **ü** Ο αριθμός των απαιτούμενων αρχικών μηνυμάτων προς κρυπτογράφηση μπορεί να είναι αρκετά μικρός

- **ü** Η γενικότερη στρατηγική δεν θα πρέπει να έχει κανένα αντίκτυπο αναφορικά με την πολυπλοκότητα της επίθεσης.

Με βάση τα νέα δεδομένα και με σκοπό την ασφαλή κρυπτογράφηση ο Courtois επισήμανε ότι ο σχεδιασμός των αλγορίθμων δεν θα είναι ποτέ πλέον ο ίδιος και πρότεινε λύσεις επικεντρωμένες στην κατασκευή κουτιών αντικατάστασης τυχαίου και μεγάλου μεγέθους που θα αποτρέπουν τις αλγεβρικές επιθέσεις. Από την άλλη πλευρά βασικός γνώμονας για την ανάπτυξη ασφαλών κουτιών αντικατάστασης θα μπορούσε να προκύψει από μια ρήση Shannon, σύμφωνα με την οποία η πολυπλοκότητα της επίθεσης σε έναν αλγόριθμο θα πρέπει να απαιτεί *"…τόσο κόπο όσον θα απαιτούσε η επίλυση η επίλυση ενός συστηματος από παρόμοιες εξισώσεις με μεγάλο αριθμό αγνώστων σύνθετου τύπου (complex type)"*.

Συνδυάζοντας τις παραπάνω εκτιμήσεις οι Sakalauskas και Luksys προτείνουν μια τεχνική σχεδίασης ασφαλών κουτιών αντικατάστασης, στα οποία η είσοδος και οι μεταβλητές των κλειδιών φαίνονται να είναι σύνθετου τύπου κατά Shannon, αφού οι εξισώσεις που περιέχουν αυτές τις μεταβλητές δεν είναι αλγεβρικές. Επίσης η πολυπλοκότητα της λύσης του συστήματος αυτών των εξισώσεων είναι ένα NP-hard πρόβλημα ενώ η γενικότερη κατασκευή των S-boxes ανταποκρίνεται στους ιδιότητες της σύγχυσης και διάχυσης.

Σύμφωνα με τους Impagliazzo και Luby δοθέντος ενός σχήματος κρυπτογράφησης ιδιωτικού κλειδιού κάποιος μπορεί να κατασκευάσει μια μονόδρομη συνάρτηση (one way function – OWF). Αποδεικνύεται επίσης ότι υπάρχει ένα ασφαλές σχήμα κρυπτογράφησης ιδιωτικού κλειδιού αν και μόνο αν υπάρχει μια μονόδρομη συνάρτηση. Με βάση αυτό το θεώρημα θα γίνει και η κατασκευή του S-box έχοντας ως βάση την μονόδρομη συνάρτηση. Ο σχεδιασμός του S-box θα γίνει με βάση το συγκεκριμένο αξίωμα της μονόδρομης συνάρτησης και όπως αποδεικνύεται οι εξισώσεις που αναπαριστούν το σύστημα εισόδου και εξόδου του δεν είναι πολυωνυμικές κι έτσι είναι ασφαλές στις διάφορες επιθέσεις που κάνουν χρήση των μεθόδων XL και XSL. Η ασφάλεια κρυπτογράφησης προσεγγίζεται με δυο τρόπους. Αρχικά με την θεώρηση ενός συστήματος από γενικευμένες εξισώσεις S-box και την φυσική διασύνδεσή τους με τις μονόδρομες συναρτήσεις που χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία και στη συνέχεια με την ανάλυση ασφαλείας εναντίον κρυπταναλυτικών επιθέσεων σε αλγορίθμους τμημάτων.

Τα κουτιά αντικατάστασης που σχεδιάζονται με αυτή την τεχνική χρησιμοποιούν μια γενίκευση της παραδοσιακής modular εκθετικής συνάρτησης που αναγνωρίζεται ως μονόδρομη συνάρτηση OWF. Έτσι για την κατασκευή τους χρησιμοποιείται η εισαγωγή ενός συνόλου αριστερών και δεξιών ενεργειών M_G στο σύνολο πινάκων του πίνακα αντικατάστασης M του S-box, που θεωρούνται συναρτήσεις ***matrix power***. Δηλαδή ο πίνακας αντικατάστασης M του S-box υψώνεται σε δύναμη από το πεδίο M_G, η οποία μπορεί να αντληθεί είτε από την αριστερή είτε από την δεξιά πλευρά. Οι σχετιζόμενες μονόδρομες συναρτήσεις στη νέα αυτή θεώρηση μπορούν να καλούνται πλέον matrix power μονόδρομες συναρτήσεις. Όπως έχει επιστημονικά αποδειχθεί συναρτήσεις αυτού του είδους συνδέονται με άλλα παρόμοια NP-hard προβλήματα που είναι γνωστά στα συστήματα κρυπτογράφησης ως προβλήματα αποσύνθεσης. Έτσι η ασφάλεια που παρέχεται με τα S-box που κατασκευάζονται με την μέθοδο matrix power στηρίζονται στην πολυπλοκότητα και επίλυση ταυτόχρονα δυο προβλημάτων: ενός ιδιαίτερου λογαριθμικού προβλήματος και ενός matrix power προβλήματος.

Για την υλοποίηση των δεξιών και αριστερών ενεργειών M_G επί του πίνακα M χρησιμοποιούνται οι παραστάσεις $o_L : M_G \times M \rightarrow M$ και $o_R : M \times M_G \rightarrow M$. Τότε για κάθε $L, R \in M_G$ και για κάθε $X \in M$ υπάρχουν κάποια $Y,Z \in M$ τέτοια ώστε $L \circ X = Y$ και $X \circ R = Z$. Έτσι για την κατασκευή ορίζουμε το S-box ως D στο διάστημα $\mathbf{F}_2^{n-1}$ και με την διαδικασία της επέκτασης κλειδιού λαμβάνουμε τους πίνακες κλειδιών K, L και R διαστάσεων m x m. Οι μετασχηματισμοί της εισόδου του S-box στην έξοδο C προκύπτουν από τις παραστάσεις: $D + K + 1 = X$ και $L \circ X \circ R = C$. Από τη στιγμή που το M_G αποτελεί ένα σύνολο πινάκων, τότε θα υπάρχει και ο αντίστροφος πίνακας R^{-1} τέτοιος ώστε $R^{-1} \times R = R \times R^{-1} = I$, όπου I ο μοναδιαίος πίνακας. Έτσι αντί να χρησιμοποιήσουμε τον πίνακα R κάνουμε χρήση του R^{-1} για λόγους συμμετρίας. Ο τελεστής κρυπτογράφησης που αντιστοιχεί σε αυτό το S-box σημειώνεται ως $E_{R'LK}$ και συμβολικά η όλη διαδικασία κρυπτογράφησης μπορεί να παρασταθεί ως $E_{R'LK}(D) = C$.

Το αλγεβρικά αδύναμο σημείο ενός κουτιού αντικατάστασης βασίζεται στη αλγεβρική περιγραφή του από ένα σύνολο αλγεβρικών εξισώσεων που σχετίζονται με

τα δεδομένα αρχικού μηνύματος και κρυπτογραφήματος αλλά και των κλειδιών στους διάφορους γύρους λειτουργίας του. Γενικότερα οι αλγεβρικές επιθέσεις λειτουργούν σε ένα κουτί αντικατάστασης όπως σε ένα σύστημα εισόδου-εξόδου το οποίο περιγράφεται από αλγεβρικές σχέσεις και σκοπεύουν να αποκωδικοποιήσουν τις μεταβλητές των κλειδιών επιλύοντας το σύστημα των εξισώσεων, έχοντας ως γνωστά ένα ή περισσότερα ζεύγη plaintext - ciphertext. Το κυριότερο μαθηματικό εργαλείο αλγεβρικής κρυπτανάλυσης είναι οι αλγόριθμοι XL και XSL. Στην περίπτωση του AES για παράδειγμα όπου χρησιμοποιείται η εκθετική συνάρτηση αναπαριστώντας τον αλγόριθμο με ένα σύστημα με ένα πολυωνυμικό σύστημα διαφορικών εξισώσεων πολλών μεταβλητών ο XL επιτρέπει την κατασκευή ενός συστήματος εξισώσεων του οποίου η επίλυση αν και αποτελεί ένα NP-hard πρόβλημα, έχει μεγάλη πιθανότητα να επιφέρει πλήγμα στον αλγόριθμο.

Η αναπαράσταση των κουτιών αντικατάστασης με την μέθοδο matrix power αποτρέπει την επιτυχή λειτουργία του αλγορίθμου XL αφού όπως αποδεικνύεται, το σύστημα των εξισώσεων που αναπαριστούν τη λειτουργία του S-box δεν είναι πολυωνυμικό αναφορικά με τις μεταβλητές κλειδιών l_{is}, r_{tj} και k_{st} και έτσι δεν μπορεί να υπάρξει μετασχηματισμός τέτοιος που να επιτρέπει την επιτυχή αλγεβρική επίθεση όταν το ζεύγος $D=\{d_{st}\}$ $C=\{c_{ij}\}$ είναι γνωστό. Το κυριότερο ζήτημα κατά την υλοποίηση του κουτιού αντικατάστασης είναι η δημιουργία των πινάκων τυχαίων κλειδιών L και R έχοντας τους αντίστροφους τους από το κλειδί κρυπτογράφησης. Ένας τρόπος επίλυσης είναι να χρησιμοποιηθεί το σύνολο αναπαράστασης των πινάκων στο σύνολο πινάκων $GL(m,GF(2^n))$. Οι παράμετροι ασφαλείας του κουτιού αντικατάστασης είναι το μέγεθος m του πίνακα και το μήκος n του δυαδικού περιεχομένου του. Από την εφαρμογή της τεχνικής matrix power στην πράξη αποδεικνύεται ότι όσο υψηλότερες είναι οι τιμές των m και n τόσο λιγότερα matrix power S-boxes είναι απαραίτητα για τον αλγόριθμο.

3.6 **Ασφάλεια των** S-boxes **βασισμένων στις συναρτήσεις** bent

Η μελέτη των διαφόρων κρυπτοσυστημάτων και η ανάλυση των τεχνικών ασφάλειάς τους έχει αποδείξει την σχέση της κατάλληλης επιλογής και σχεδίασης των κουτιών αντικατάστασης και της ανθεκτικότητάς τους στις διάφορες επιθέσεις κρυπτανάλυσης. Στην περίπτωση κρυπτοσυστημάτων με τα χαρακτηριστικά του DES και τις διαφορικές κρυπταναλυτικές επιθέσεις που περιγράφονται από τους Biham και Shamir, γίνεται σαφές ότι η ανάπτυξη κατάλληλων κουτιών αντικατάστασης που βασίζονται στις συναρτήσεις bent αποτελεί την πιο κατάλληλη λύση για την ασφάλεια των συμμετρικών αλγορίθμων των δικτύων μετάθεσης-αντικατάστασης SPN.

Προς αυτή την κατεύθυνση ο C. M. Adams απέδειξε το παρακάτω θεώρημα:

Ένα s-box S διαστάσεων mxn το οποίο αναπαρίσταται ως ένα δυαδικός πίνακας διαστάσεων 2^m x με στήλες φ_i, θα έχει ίσης πιθανότητας εξόδους αποκλειστικής διάζευξης XOR αν υπάρχει min(m,n) φ_i τέτοιο ώστε όλοι οι μη μηδενικοί μετασχηματισμοί (mod 2) αυτών των φ_i αντιστοιχούν σε bent συναρτήσεις.

Τα κουτιά αντικατάστασης που ικανοποιούν το παραπάνω θεώρημα καλούνται "*bent-function-based s-boxes*".

Παρόλο που η μελέτη έχει βασιστεί στα κουτιά αντικατάστασης διαστάσεων m x n όπου m << n τίθεται ένα ενδιαφέρον ζήτημα για το αν μπορούν να κατασκευαστούν κουτιά αντικατάστασης διαστάσεων 6 x 4 (όπως αυτά που χρησιμοποιούνται στον DES) τα οποία θα ικανοποιούν το παραπάνω θεώρημα. Προς αυτή την κατεύθυνση κινήθηκε η μελέτη του Nyberg ο οποίος ονόμασε τα bent-function-based s-boxes ως τέλεια μη γραμμικά S-boxes και αποφάνθηκε ότι δεν μπορούν να υπάρξουν κουτιά αντικατάστασης τέτοιων διαστάσεων που να βασίζονται στις συναρτήσεις bent. Ειδικότερα όρισε ότι για να είναι ένα s-box διαστάσεων m x n βασισμένο σε bent συναρτήσεις θα πρέπει το m να είναι τουλάχιστον διπλάσιο από το n. Αυτό λοιπόν σημαίνει ότι αν σε ένα κρυπτοσύστημα απαιτούνται S-boxes όπου m<2n, τότε δεν μπορούν να χρησιμοποιηθούν bent-function-based s-boxes αλλά αντίθετα να κατασκευαστούν κουτιά αντικατάστασης που να ικανοποιούν έστω και μερικώς το παραπάνω θεώρημα.

Αν και τα αποτελέσματα της μελέτης του Nyberg απέδειξαν ότι S-boxes που ικανοποιούν το πιο πάνω θεώρημα μπορούν να κατασκευαστούν μόνο αν $m \geq 2n$, μεταγενέστερες έρευνες εντόπισαν ότι υπάρχει κάποια αδυναμία των S-boxes για κάθε m>n. Ειδικότερα στην περίπτωση του DES, εάν επρόκειτο να χρησιμοποιηθούν 6 x 4 bent-function-based s-boxes τότε θα μπορούσε να γίνει επίθεση ανάλυσης με περίπου 2^{30} ζεύγη επιλεγμένων διανυσμάτων εισόδου. Γενικεύοντας τα αποτελέσματα αυτά μπορούμε να αναφέρουμε ότι κάθε S-box όπου m>n έχει περισσότερα διανύσματα εισόδου από αυτά της εξόδου. Αυτό σημαίνει ότι θα υπάρχει τουλάχιστον μια περίπτωση στην οποία δυο ή περισσότερα διανύσματα εισόδου θα αντιστοιχούν στην ίδια έξοδο. Η αδυναμία ύπαρξης τέτοιων bent-function-based κουτιών αντικατάστασης έγκειται στο γεγονός ότι σε αυτές τις περιπτώσεις υπάρχει μια σταθερή πιθανότητα επαλήθευσης των διανυσμάτων εισόδου η οποία μπορεί να χρησιμοποιηθεί για την κρυπτανάλυση όλου του συστήματος. Στις περιπτώσεις όπου ισχύει $m \leq n$ αυτό το ενδεχόμενο επιτυχημένης επίθεσης είναι πρακτικά αδύνατο να εμφανιστεί καθώς κάθε διάνυσμα εισόδου αντιστοιχεί σε μια μοναδική έξοδο.

Γίνεται κατανοητό ότι παρά το γεγονός ότι η XOR κατανομή αντιμετωπίζει ιδανικά τις επιθέσεις διαφορικής κρυπτανάλυσης και τα κουτιά αντικατάστασης που βασίζονται στις συναρτήσεις Bent διαθέτουν αυτό το σημαντικό χαρακτηριστικό, είναι απαραίτητο να ληφθούν υπόψη και άλλοι σημαντικοί παράγοντες που θα προσφέρουν την επιθυμητή ασφάλεια και θα περιορίζουν την αδυναμία που εμφανίζουν σε συγκεκριμένες περιπτώσεις τα bent-function-based s-boxes. Ως καλύτερη λύση λοιπόν για την ασφάλεια των αλγορίθμων μπορεί να θεωρηθεί η κατασκευή m x n s-boxes όπου $m \leq n$, τα οποία θα ανταποκρίνονται μερικώς στο θεώρημα που διατυπώθηκε στην αρχή της ενότητας αλλά ταυτόχρονα θα ικανοποιούν και άλλα επιπρόσθετα και απολύτως απαραίτητα χαρακτηριστικά. Με αυτό τον τρόπο επιτυγχάνεται σε σημαντικό βαθμό η ανθεκτικότητα των αλγορίθμων στην διαφορική

κρυπτανάλυση, εξασφαλίζοντας ότι δεν υπάρχουν υψηλής πιθανότητας έξοδοι XOR στα s-boxes που μπορούν να αποτελέσουν χαρακτηριστικά ευαίσθητα σε διαφορικές επιθέσεις.

Αν θέλουμε να ορίσουμε ένα s-box S το οποίο να βασίζεται μερικώς στις συναρτήσεις Bent τότε θα πρέπει να θεωρήσουμε ένα κουτί αντικατάστασης του οποίου οι στήλες του δυαδικού πίνακα M που αναπαριστά το κουτί S να είναι bent αλλά ταυτόχρονα τουλάχιστον ένας από τους μη μηδενικούς συνδυασμούς των στηλών αυτών (με άθροιση κατά mod2) να μην είναι bent. Για τη σχεδίαση αυτού του κουτιού αντικατάστασης θεωρούμε ένα ακέραιο n πολλαπλάσιο του m και έστω ότι n=r*m όπου r>1. Επιλεγούμε n δυαδικά διανύσματα bent φ_i μήκους 2^m, έτσι ώστε οι γραμμικοί συνδυασμοί αυτών των διανυσμάτων να αθροίζονται κατά mod 2 σε υψηλά μη γραμμικά διανύσματα. Στη συνέχεια επιλέγουμε τα μισά από τα φ_i να έχουν βάρος 2^{m-1}

2 2

+ και τα άλλα μισά να έχουν βάρος 2^{m-1} - . Αυτά τα δυο βάρη είναι τα πιθανά βάρη των δυαδικών διανυσμάτων Bent μήκους 2^m . Ορίζουμε τα n φ_i να είναι οι στήλες του πίνακα M που αναπαριστά το κουτί αντικατάστασης.

Ελέγχουμε ότι ο πίνακας M έχει 2^m γραμμές και ότι το βάρος Hamming κάθε γραμμής και η απόσταση Hamming μεταξύ των ζευγών των γραμμών είναι περίπου n/2. Συνήθως αυτά τα ζεύγη των βαρών και αποστάσεων έχουν κατά μέσο όρο τιμή n/2 αλλά και μια μικρή μη μηδενική διασπορά. Αν οι παραπάνω περιορισμοί δεν ικανοποιούνται συνεχίζουμε επιλέγοντας τα κατάλληλα διανύσματα bent ως υποψήφια φ_i και ελέγχουμε τον πίνακα που προκύπτει ως αποτέλεσμα μέχρι το σημείο όπου θα ικανοποιούνται οι περιορισμοί.

Συμπερασματικά μπορούμε να σημειώσουμε ότι:

- **ü** το γεγονός ότι ο πίνακας αναπαράστασης M έχει κατά προσέγγιση σε κάθε γραμμή του μισά μηδενικά στοιχεία και μισά ίσα με την τιμή 1, διασφαλίζει ότι το s-box θα προσφέρει στον αλγόριθμο την απαιτούμενη διάχυση,

- **ü** το γεγονός ότι το άθροισμα κατά mod2 κάθε ζεύγους γραμμών έχει κατά προσέγγιση μισά μηδενικά στοιχεία και μισά ίσα με την τιμή 1 διασφαλίζει ότι το s-box θα προσφέρει στον αλγόριθμο την απαιτούμενη ιδιότητα avalanche,

- η χρήση διανυσμάτων bent για την κατασκευή των στηλών του πίνακα M διασφαλίζει ότι κάθε bit εξόδου θα ανταποκρίνεται ιδανικά σε αλλαγές του διανύσματος εισόδου υπό την έννοια του κριτηρίου highest-order strict avalanche.

Συμπεράσματα

Όπως είδαμε στην εκπόνηση της μελέτης αυτής ο ρόλος της κρυπτογραφίας και των διάφορων εφαρμογών της από τα πρώιμα στάδια της μετάδοσης πληροφορίας έως και τη σύγχρονη εποχή που διανύουμε, αποτελεί θεμελιώδες παράγοντα ασφαλείας και για το λόγο αυτό αποτέλεσε αντικείμενο ενδελεχούς επιστημονικής έρευνας ώστε να αναπτυχθούν τεχνικές τέτοιες που επιτρέπουν την εξασφάλιση της απρόσκοπτης μετάδοσης της επιθυμητής πληροφορίας από τον αποστολέα στον παραλήπτη, χωρίς ανεπιθύμητες παρεμβολές και αλλοιώσεις.

Προς την κατεύθυνση αυτή δημιουργήθηκαν και διακριθήκαν συγκεκριμένα είδη κρυπτογραφίας με βασικότερα την συμμετρική και ασύμμετρη κρυπτογραφία, είδη τα οποία στηρίζονται στην ύπαρξη ανάλογων αλγορίθμων-τεχνικών κρυπτογράφησης, όπου κάθε ένας έχει τα δικά του χαρακτηριστικά-ιδιότητες και ιδιαίτερο τρόπο λειτουργίας και προσέγγισης του παράγοντα της παρεχόμενης ασφάλειας. Βασικότεροι αλγόριθμοι που παρουσιάστηκαν και αποτελούν ακόμα και σήμερα χαρακτηριστικούς εκπροσώπους της κατηγορίας στην οποία ανήκουν, είναι οι Diffie - Hellman, RSA και DSA αναφορικά με την ασύμμετρη κρυπτογραφία και οι DES, AES και IDEA αναφορικά με την συμμετρικοί κρυπτογράφηση. Κάθε ένα διαφορετικό είδος ανταποκρίνεται στα ζητήματα ασφαλείας είτε σε επίπεδο δημιουργίας κλειδιών και μηνυμάτων είτε σε επίπεδο μετάδοσής τους διαμέσου καναλιών επικοινωνίας και διακρίνεται από αντίστοιχα πλεονεκτήματα και μειονεκτήματα. Σημεία υπεροχής αλγορίθμων έναντι άλλων είναι το στοιχείο της ταχύτητας, η πιστοποίηση της ταυτότητας των χρηστών, η διατήρηση της ιδιότητας και ευθύνης δημιουργίας, αποστολής ή λήψης της πληροφορίας από τους χρήστες και πλήθος άλλων.

Βασικό συμπέρασμα επίσης αποτελεί το γεγονός πως σε πολλές περιπτώσεις καμιά από τις δύο κατηγορίες δεν είναι αρκετή για την αντιμετώπιση των πιθανών ζητημάτων παραβίασης των κρυπτοσυστημάτων και έτσι θεωρείται ως άμεση απόρροια, η απαίτηση για τον συνδυασμό και των δυο κατηγοριών κρυπτογράφησης, όπως για παράδειγμα με την χρήση υβριδικών συστημάτων ψηφιακής υπογραφής. Ειδικά στις περιπτώσεις των συμμετρικών αλγορίθμων που εξετάσαμε διεξοδικότερα, συμπεράναμε ότι το ζήτημα της ασφάλειας εξαρτάται από τις ιδιότητες των κουτιών αντικατάστασης που χρησιμοποιούνται στα βήματα του αλγορίθμου κρυπτογράφησης. Επιχειρώντας μια γενικότερη προσέγγιση θα επισημαίναμε ότι όσο μεγαλύτερο είναι το

μέγεθος ενός κουτιού αντικατάστασης S-box τόσο μεγαλύτερη ασφάλεια παρέχει στον αλγόριθμο. Εκτός από αυτό, εξίσου σημαντικός παράγοντας ασφάλειας είναι και ο τρόπος συμπλήρωσης του περιεχομένου του πίνακα του κουτιού αντικατάστασης. Ένα ιδανικό κουτί αντικατάστασης το οποίο και θεωρείται ασφαλές σε επιθέσεις διαφορικής κρυπτανάλυσης στις οποίες γίνεται χρήση μεθόδων μη ισορροπημένων παραγώγων, μπορεί να επιτύχει την επιθυμητή ασφάλεια αν κατασκευαστεί με τουλάχιστον διπλάσιο αριθμό μεταβλητών εισόδου από τον αριθμό των μεταβλητών εξόδου του όπως για παράδειγμα με τις μεθόδους Maiorana-McFarland ή της κατασκευής συναρτήσεων Bent.

Τα S-boxes αποτελούν πολύ σημαντικά συστατικά στοιχεία τόσο κατά το στάδιο της ανάπτυξης ενός αλγορίθμου κρυπτογράφησης όσο και κατά την λειτουργία του στην πράξη. Η κυριότερη αναγκαιότητα της ύπαρξής τους έγκειται στο γεγονός ότι πρέπει να άρουν την γραμμικότητα αυτών των αλγορίθμων ώστε αυτοί να είναι κατά το δυνατόν ασφαλέστεροι. Όπως γνωρίζουμε οι υπολογιστές διακρίνονται για την δυαδική τους μορφή και γι' αυτό το λόγο τα κουτιά αντικατάστασης δρουν κυρίως σε ομάδες κάποιων bits των μηνυμάτων προς κρυπτογράφηση. Η ύπαρξη κουτιών αντικατάστασης με σαφείς και ισχυρές ιδιότητες είναι απαραίτητη προϋπόθεση για την ασφάλεια που μπορεί να προσφέρει η μέθοδος της κρυπτογράφησης μυστικού κλειδιού. Όπως είδαμε κατά τη λειτουργία των διάφορων συμμετρικών αλγορίθμων, η ασφάλεια της κρυπτογράφησης μπορεί να τεθεί σε κίνδυνο αν τα κουτιά αντικατάστασης χρησιμοποιηθούν χωρίς την απαραίτητη συνέπεια. Αυτό συμβαίνει και στις περιπτώσεις αλγορίθμων όπου κατά τη λειτουργία τους οδηγούν την διαδικασία σε αντικαταστάσεις των S-boxes με κάποιες αλγεβρικές συναρτήσεις, διακινδυνεύοντας την ασφάλεια της κρυπτογράφησης. Γίνεται λοιπόν κατανοητό ότι πριν την λειτουργία κάποιου αλγόριθμου κρυπτογράφησης θα πρέπει να γίνεται αυστηρή και ενδελεχής μελέτη των ιδιοτήτων των κουτιών αντικατάστασης που θα χρησιμοποιηθούν τόσο κατά την κρυπτογράφηση όσο και κατά την διαδικασία της κρυπτανάλυσης και κυρίως να αποσαφηνιστούν πλήρως τα γραμμικά και διαφορικά τους χαρακτηριστικά.

Τα Strict avalanche και Output independence κριτήρια όπως και αυτά της μη γραμμικότητας, και της αμφίεσης είναι οι βασικές παράμετροι ασφαλείας που διατυπώθηκαν από τους Adams και Tavares και αποτελούν πλέον θεμελιώδεις κατασκευαστικούς περιορισμούς κατά την ανάπτυξη και σχεδιασμό των κουτιών αντικατάστασης ενός αλγορίθμου μυστικού κλειδιού. Η παρεχόμενη ασφάλεια των κουτιών αντικατάστασης αποτελεί διαρκές αντικείμενο επιστημονικής μελέτης, οι οποίες χρησιμοποιούν διάφορες τεχνικές και μεθόδους για να την επιτύχουν και να αποτρέψουν επιθέσεις αλγεβρικού, γραμμικού ή διαφορικού τύπου. Κάποιες από αυτές χρησιμοποιούν μεθόδους όπως την χρησιμοποίηση του μετασχηματισμού Fourier, τις αλυσίδες Markov, των εκθετών Gold και Kasami, των τεχνικών Maiorana - McFarland και Matrix Power και σειρά άλλων. Όπως αποδεικνύεται η XOR κατανομή αντιμετωπίζει ιδανικά τις επιθέσεις κρυπτανάλυσης και τα κουτιά αντικατάστασης που βασίζονται στις συναρτήσεις Bent διαθέτουν ισχυρά χαρακτηριστικά ασφαλείας. Ως καλύτερη λύση λοιπόν για την ασφάλεια των αλγορίθμων θεωρείται η κατασκευή κουτιών αντικατάστασης μεγέθους mxn όπου m ≤ n, τα οποία θα είναι bent-function-based και

θα επιτυγχάνουν σε σημαντικό βαθμό την ανθεκτικότητα των αλγορίθμων στην διαφορική κρυπτανάλυση.

Βιβλιογραφία

[01] Κωνσταντίνος Πατσάκης – Ευάγγελος Φούντας, Κρυπτογραφία και εφαρμογές, Εκδόσεις ΒΑΡΒΑΡΗΓΟΥ, 2009

[02] Alfred J. Menezes – Paul C. van Oorschot – Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1997.

[03] Dorothy Elizabeth Robling Denning, “Cryptography and Data Security”, Addison-Wesley, Publishing Company, 1982.

[04] V.V. Yaschenko, “Cryptography: An Introduction”, American Mathematical Society, 2002.

[05] Whitfield Diffie and Martin E. Hellman, “New Directions in Cryptography”, Invited Paper, 1976

[06] Federal Information Processing Standards Publication 46-3, “Data Encryption Standard”, U.S Department of Commerce/National Institute of Standards and Technology, 1999.

[07] X. Lai, “On the design and security of block ciphers”, ETH Series in Information Processing (J.L. Massey, ed.), Vol. 1, Hartung-Gorre Verlag Konstanz, Technische Hochschule (Zurich), 1992.

[08] X. LAI, J.L. MASSEY, AND S. MURPHY, ‘’Markov ciphers and differential cryptanalysis’’, Advances in Cryptology – EUROCRYPT ’91 (lncs 547), 17-38, 1991

[09] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22.

[010] G. Blakley. "Safeguarding cryptographic keys." In Proceedings of AFIPS 1979, volume 48, pp.313–317.

[011] Shamir. "How to share a secret." In Communications of the ACM, volume 22, pp. 612–613,ACM.

[012] ΒΑΣΙΛΕΙΟΣ ΖΟΡΚΑΔΗΣ, Θεωρία Πληροφορίας και Κωδικοποίησης, 2002

[013] Adams, C. & Tavares, S. (1990). “The Structured Design of Cryptographically Good S-Boxes”, Journal of Cryptology 3(1), pp. 27–41.

[014] Biham, E. (1995) “On Matsui’s Linear Cryptanalysis”, Proceedings, EUROCRYPT 94, pp. 398-412.

[015] Παγκόσμιος Ιστός (www.wikipedia.com, www.bletchleypark.net, www.islab.demokritos.gr, www.securetrust.com/resources/cryptography-history).

[016] Biham, E. & Shamir, A. (1993). Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag.
[017] Heys, H. & Tavares, S. (1996). “Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis”, Journal of Cryptology 9(1), pp. 1–19.
[018] Webster, A. & Tavares, S. (1986). “On the Design of S-Boxes”, CRYPTO 85, Vol. LNCS 403 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 21-25, pp. 523–534.
[019] Πάγκαλος, Γ. & Μαυρίδης, Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, Ανικούλα.
[020] ΑΠΟΣΤΟΛΙΔΟΥ ΚΥΡΙΑΚΗ, ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ, 2008
[021] C. M. Adams and S.E. Tavares, Designing s-boxes resistant to differential cryptnalysis, Proceedings of 3rd Symposium on the State and Progress of Research in Cryptography, pp. 181-190, Rome, Italy, 1994.
[022] C. M. Adams and S.E. Tavares, The Use of Bent Sequences to Achieve Higher-Order Strict Avalanche Criterion in S-Box Design, Technical Report TR 90-013, Jan. 1994.
[023] K. Nyberg, Perfect nonlinear S-boxes, Advances in Cryptology - Proceedings of EUROCRYPT '91, Springer-Verlag, pp. 378-386, 1991.
[024] K. Nyberg, Linear Approximations of Block Ciphers, Advances in Cryp-tology - EUROCRYPT '94 (Lecture Notes in Computer Science,no. 950), Springer-Verlag, pp. 17-38, 1991.
[025] K. Nyberg. Linear approximation of block ciphers. In Advances in Cryptology — Eurocrypt ’94 (rump session), pages 439–44, Springer-Verlag,
[026] Δημόπουλος Δημητρίος, «Υπολογιστική Υλοποίηση Πρωτοκόλλου DES με εφαρμογές στην Κρυπτογράφηση Κειμένων», Θεσσαλονίκη, 2008
[027] L.R. Knudsen. Practically secure Feistel ciphers. In Proceedings of 1st Workshop on Fast Software Encryption, pages 211–221, Springer-Verlag, 1993.
[028] L. O’Connor. A unified markov approach to differential and linear cryptanalysis. In Advances in Cryptology — Asiacrypt ’94, pages 387–397
[029] Αμπατζόγλου Παντελής, “Κρυπτογράφηση και Ποιότητα Υπηρεσιών (Qos) σε Ad-hoc ασύρματα δίκτυα”, 2009
[030] Dawson, M. and S. Tavares. 1991. An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-Like Attacks. Advances in Cryptology -- EUROCRYPT '91. 353-367.
[031] Sivabalan, M, S. Tavares and L. Peppard. 1992. On the Design of SP Networks from an Information Theoretic Point of View. Advances in Cryptology -- CRYPTO '92. 260-279.
[032] Adams, C. 1992. On immunity against Biham and Shamir's "differential cryptanalysis." Information Processing Letters. 41: 77-80.