ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Τίτλος Διπλωματικής

Κρυπτογραφία - Περιγραφή Αλγορίθμων DES και AES

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μπέτα Βικέλντα-Ελένη

Επιβλέπων : Αλέξανδρος Παπαιωάννου

Αν. Καθηγητής ΕΜΠ

Εξετάστηκε από : Δ. Ρασσιάς**, Καθηγητής ΕΜΠ**

Β. Παπανικολάου**, Καθηγητής ΕΜΠ**

Αθήνα , Μάρτιος 2011

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Επιβλέπων : Αλέξανδρος Παπαιωάννου

Αν. Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ……

Αλ. Παπαιωάννου	Δ. Ρασσιάς	Β. Παπανικολάου
Αν. Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π

Περιεχόμενα

Περιεχόμενα 3
Abstract 5
Περίληψη 6
Κεφάλαιο 1 - Εισαγωγή 7
1.1. Εισαγωγή στην κρυπτογραφία 7
1.2. Ορολογία 8
1.3. Ιστορική Αναδρομή 10
1.3.1. Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.) 10
1.3.2. Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.) 14
1.3.3. Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. - Σήμερα) 16
1.4. Κρυπτογραφικοί αλγόριθμοι 18
1.5. Κατηγορίες Κρυπτογραφίας 21
1.5.1. Συμμετρική Κρυπτογραφία 21
1.5.2. Ασύμμετρη Κρυπτογραφία 22
1.6. Εφαρμογές κρυπτογραφίας 23
Κεφάλαιο 2 - Μαθηματικό υπόβαθρο 25
2.1. Θεμελιώδεις Έννοιες 25
2.2. Αριθμητική Υπολοίπων 27
2.3. Πεπερασμένα σώματα και πολυώνυμα 28
2.3.1. Βασικές έννοιες θεωρίας πολυωνύμων 28
2.3.2. Πολυώνυμα ορισμένα επί σωμάτων 28
2.3.3. Αναπαράσταση bytes με πολυώνυμα επί του $\boldsymbol{GF}(\mathbf{2})$ 29
2.3.4. Αναπαράσταση bytes με πολυώνυμα επί του $\boldsymbol{GF}(\mathbf{28})$ 30
Κεφάλαιο3 - Data Encryption Standard (DES) 33
3.1. Ιστορικά στοιχεία 33
3.2. Περιγραφή αλγορίθμου (DES) 35
3.2.1. Πίνακες Μεταθέσεων $\boldsymbol{IP}$ και $\boldsymbol{IP}-\mathbf{1}$ 36
3.2.2. Συνάρτηση DES (Feistel) 38
3.2.3. Συνάρτηση μετάθεσης κλειδιού. 41
3.3. Καταστάσεις Λειτουργίας κρυπταλγορίθμων τμήματος 44

3.3.1. Ηλεκτρονικό κωδικοβιβλίο (ECB) 44
3.3.2. Κρυπταλγόριθμος αλυσιδωτού τμήματος (CBC) 45
3.3.3. Κρυπταλγόριθμος ανάδρασης (CFB) 46
3.3.4. Ανάδραση Εξόδου (OFB) 47
3.3.5. Τρόπος λειτουργίας μετρητή (CTR) 48
3.4. Ασφάλεια DES 50
3.4.1. Brute force attack 50
3.4.2. Επιθέσεις ταχύτερες από την brute - force 52
Κεφάλαιο 4 – Advanced Encryption Standard (AES) 53
4.1. Ιστορικά στοιχεία 53
4.2. Περιγραφή αλγορίθμου (AES) 54
4.2.1. Μετασχηματισμός SubBytes 58
4.2.2. Μετασχηματισμός ShiftRows 61
4.2.3. Μετασχηματισμός MixColumns 61
4.2.4. Μετασχηματισμός AddRoundKey 63
4.3. Επέκταση κλειδιού 64
4.4. Ασφάλεια AES 67
Παράρτημα Α – Υπολογιστικό Παράδειγμα κρυπτογράφησης DES 68
Παράρτημα Β – Υπολογιστικό Παράδειγμα κρυπτογράφησης AES 75
Table of figures 82

Abstract

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). The symmetric cryptography is the classic method of cryptography. The main feature is the use of the same key for both encryption and for decryption processes. Part of symmetric cryptography are block ciphers such as DES and AES.

The DES was adopted as the national standard and formally published as FIPS-46 with the name of DES on January 15, 1977. The DES algorithm is designed to encrypt and decrypt 64-bits blocks using a 56-bits key which is expressed as 64-bits text. The general structure of the algorithm includes 16 identical processing steps. There is also an initial and a final permutation known as IP and IP-1, which are inverse functions. Before the main rounds, the block is divided into two 32-bit texts and processed sequentially. This method is known as Feistel function . The Feistel function ensures that decryption and encryption processes are similar. The key processes in the swap function key.

AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. Rijndael algorithm was selected to be most suitable for AES, which was developed by Belgian researchers Joan Daemen and Vincent Rijmen. The plain text is divided into blocks of 128 bits, while the key may have a length of 128, 192 or 256 bits, depending on the desired security level. The algorithm is AES-128 is the most prevalent and is supported by most hardware implementations. Both during the process of encryption and decryption process, each round consists of a series of transformations at byte level. In fact, there are used 4 types of transformations: SubBytes, ShiftRows, MixColums, AddRoundKey.

Linear and differential cryptanalysis methods are attacks that affect mainly the security of DES. Because DES has proven vulnerable to such attacks, AES was designed to be immune to such attacks.

Περίληψη

Η κρυπτογραφία είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης . Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Η συμμετρική κρυπτογραφία είναι η κλασική μέθοδος κρυπτογραφίας. Το κύριο χαρακτηριστικό της είναι η χρήση του ιδίου κλειδιού τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφησης. Υποκατηγορία συμμετρικής κρυπτογραφίας είναι οι κρυπταλγόριθμοι τμήματος όπως είναι ο DES και ο AES.

Ο DES υιοθετήθηκε ως Εθνικό Πρότυπο ενώ δημοσιεύτηκε επίσημα σαν έκδοση FIPS-46 με το όνομα DES στις 15 Ιανουαρίου του 1977. Ο αλγόριθμος DES έχει σχεδιαστεί με σκοπό να κρυπτογραφεί και να αποκρυπτογραφεί σύνολα δεδομένων που αποτελούνται από 64-bits με την βοήθεια ενός 56-bits κλειδιού που εκφράζεται σαν 64-bits κείμενο. Στην γενική δομή του αλγορίθμου συμμετέχουν 16 πανομοιότυπα στάδια επεξεργασίας. Υπάρχει, επίσης , μια αρχική και μια τελική μεταλλαγή που καλούνται IP και IP-1, οι οποίες είναι αντίστροφες συναρτήσεις. Πριν από τους κύριους γύρους, το block διαιρείται σε δύο 32-bit κομμάτια και επεξεργαζεται διαδοχικά. Αυτή η σταυροειδής διάταξη είναι γνωστή ως σχήμα Feistel. Η δομή Feistel εξασφαλίζει ότι η αποκρυπτογράφηση και η κρυπτογράφηση είναι παρόμοιες διαδικασίες. Το κλειδί επεξεργάζεται με την Συνάρτηση Μετάθεσης Κλειδιού.

Ο Advanced Encryption Standard (AES) εκδόθηκε από το National Institute of Standards and Technology (NIST) το 2001. Ως πρότυπο AES επελέγη ο αλγόριθμος Rijndael, που ανεπτύχθη από τους Βέλγους ερευνητές Joan Daemen και Vincent Rijmen. Το απλό κείμενο κατατέμνεται σε δέσμες (blocks) των 128 bits, ενώ το κλειδί μπορεί να έχει μήκος 128, 192 ή 256 bits, αναλόγως με το επιθυμητό επίπεδο ασφαλείας. Ο αλγόριθμος AES-128 είναι ο επικρατέστερος και υποστηρίζεται από τις περισσότερες hardware υλοποιήσεις. Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Για την ακρίβεια, χρησιμοποιούνται 4 τύποι μετασχηματισμών: SubBytes, ShiftRows, MixColums, AddRoundKey.

Η γραμμική και η διαφορική κρυπτανάλυση είναι μέθοδοι επιθέσεων που ανεπτύχθησαν για να προσβάλλουν, κυρίως, την ασφάλεια του DES. Επειδή ο DES απεδείχθη ευάλωτος στις επιθέσεις αυτές, η σχεδίαση του AES έγινε εξ αρχής με στόχο να είναι απρόσβλητος σε τέτοιες επιθέσεις.

Κεφάλαιο 1 - Εισαγωγή

1.1. Εισαγωγή στην κρυπτογραφία

Η κρυπτογραφία είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή τηςπληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς τηνγνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριοχαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασίαγινόταν πάνω στην γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνειχρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία τωνμαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας,υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

- *Εμπιστευτικότητα:*Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο σταεξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.

- *Ακεραιότητα:*Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.

- *Μη απάρνηση:*Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί νααρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

- *Πιστοποίηση:*Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τιςταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας μεδιαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

1.2. Ορολογία

Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται τοαρχικό μήνυμα ονομάζεται *αποκρυπτογράφηση* (decryption).

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

Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μίαδιεργασία κρυπτογράφησης.

Κλειδί (key) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στηνσυνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (Ciphertext) είναι το αποτέλεσμα της εφαρμογής ενόςκρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis) είναι μία επιστήμη που ασχολείται με το "σπάσιμο"κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί τηςκρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα:

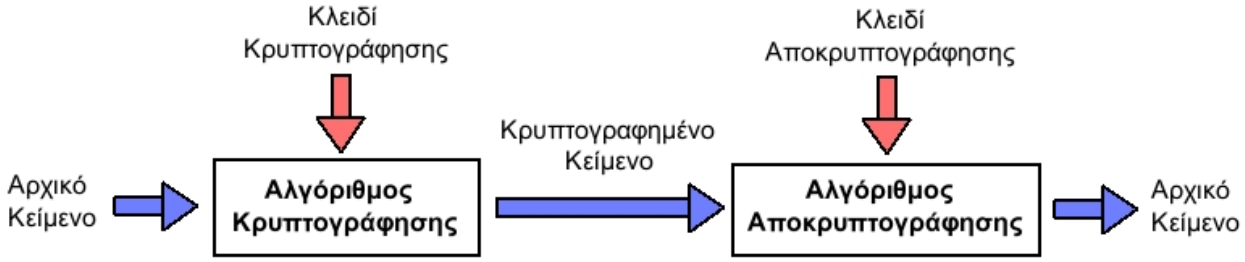

Fig 1 – Κρυπτογράφηση - Αποκρυπτογράφηση

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητατου κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης.Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει οεξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότεραμπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς.

Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

1.3. Ιστορική Αναδρομή

1.3.1.Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» (Σχήμα 2), ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Fig 2 –Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στην

στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Στην διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός Giovanni Batista Porta, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «De furtivis literarum notis», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος Vigenere, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

Ο C.Wheatstone, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους,

με τίτλο «Oedipus Aegyptiacus». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια σς ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής:

- 3000 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850 1450 π.Χ.: Γραμμική γραφή Α
- 1450 1200 π.Χ.: Γραμμική Γραφή Β

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού (Σχήμα 3), που ανακαλύφθηκε το 1908 στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Fig 3 –Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που άνεσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma.

Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

1.3.2.Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Εικόνα 4).

Fig 4 – Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως από την Γερμανία

Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση

της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με την βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Σχήμα 2.4). Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την

προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

1.3.3.Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (Mathematical Theory of Communication), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο

Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

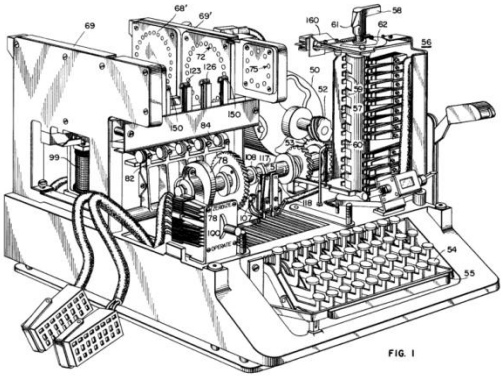

Fig 5 – Κρυπτό-μηχανή SIGABA

1.4. Κρυπτογραφικοί αλγόριθμοι

Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν, κατά κανόνα, (κρυπτογραφικά) κλειδιά, η τιμή των οποίων επηρεάζει την κρυπτογράφηση και την αποκρυπτογράφηση. Το σύνολο των δυνατών τιμών των κλειδιών λέγεται πεδίο τιμών (keyspace). Υπάρχουν δυοκατηγορίες κρυπτογραφικών αλγορίθμων: οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι. Οισυμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, και για αυτό το λόγο καλούνται επίσης αλγόριθμοι μυστικού κλειδιού ή αλγόριθμοι μονού κλειδιού. Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν ένα ζεύγος κρυπτογραφικών κλειδιών: το δημόσιο κλειδί για την κρυπτογράφηση και το ιδιωτικό για την αποκρυπτογράφηση.

Παραλλαγές

DES είναι το ακρωνύμιο των λέξεων Data Encryption Standard. Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1 που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στη νανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί.. Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

Triple-DES

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείταιδιαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

• DES-EEE3 (Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.

• DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.

• DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύοδιαφορετικά κλειδιά.

• DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο

κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο.Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφησηκαι τα τρία διαφορετικά κλειδιά.

DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

AES (Advanced Encryption Standard)

Τοακρωνύμιο AES προέρχεταιαπότηνφράση Advanced Encryption Standard. Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES.

DSS (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιοτου 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α.

Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

RC4, RC5

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.

Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA

Inc το1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και

μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

IDEA (International Data Encryption Algorithm)

Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, ηαποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχεισχεδιαστεί για να εύκολα εφαρμόσιμος τόσο hardware σε όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

Blowfish

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

1.5. Κατηγορίες Κρυπτογραφίας

Τα κρυπτοσυστήματα χωρίζονται σε 2 μεγάλες κατηγορίες τα *Κλασσικά Κρυπτοσυστήματα* και τα *Μοντέρνα Κρυπτοσυστήματα*.

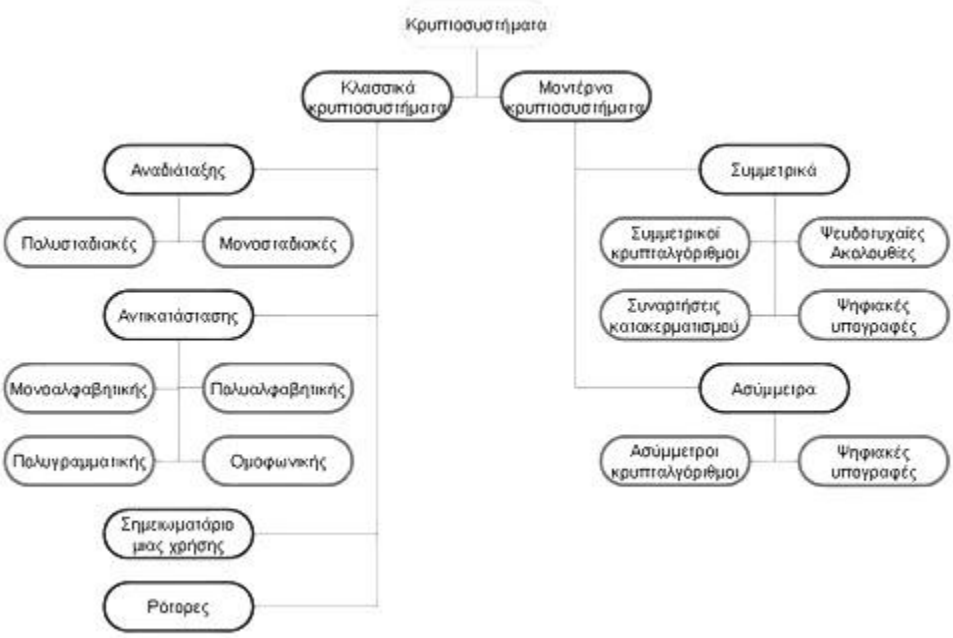

Fig 6 – Κατηγορίες κρυπτοσυστημάτων

Επιπροσθέτως, οι κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
- Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα.

1.5.1.Συμμετρική Κρυπτογραφία

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης ένα κοινό κλειδί (public key). Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τασυμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα απόένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Η συμμετρική κρυπτογραφία είναι η κλασική μέθοδος κρυπτογραφίας. Το κύριο χαρακτηριστικό της είναι η χρήση του ιδίου κλειδιού τόσο για την κρυπτογράφηση,

όσο και για την αποκρυπτογράφηση. Ο αλγόριθμος αποκρυπτογραφήσεως ακολουθεί την ίδια διαδικασία με τον αλγόριθμο κρυπτογραφήσεως, αλλά με αντίστροφη σειρά. Οι αλγόριθμοι συμμετρικής κρυπτογραφήσεως διακρίνονται σε κρυπταλγορίθμους ροής (stream ciphers) και κρυπταλγορίθμους τμήματος (block ciphers).

Γνωστοί κρυπταλγόριθμοι ροής είναι οι: RC4, VEST, Turing, SNOW, SEAL,ενώ, αντιστοίχως, γνωστοί κρυπταλγόριθμοι τμήματος είναι οι: DES ,AES, IDEA, Twofish, Hierocrypt, SHARK, BKSQ, MARS, RC6.

1.5.2.Ασύμμετρη Κρυπτογραφία

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι: ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο.

Στα σύγχρονα συστήματα συνήθως υιοθετείται μια μέθοδος ασύμμετρου – συμμετρικού όπου χρησιμοποιείται ασύμμετρο σύστημα για την μεταφορά τουκλειδιού και μετά συμμετρικό σύστημα για την μεταφορά και κρυπτογράφηση – αποκρυπτογράφηση των δεδομένων. Με αυτό τον τρόπο εκμεταλλεύονται ταπροτερήματα και των δύο συστημάτων.

1.6. Εφαρμογές κρυπτογραφίας

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώνταςπλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούςσκοπούς. Μερικοί από αυτούς είναι:

- Ασφάλεια συναλλαγών σε τράπεζες δίκτυα – ATM
- Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
- Σταθερή τηλεφωνία (cryptophones)
- Διασφάλιση Εταιρικών πληροφοριών
- Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
- Διπλωματικά δίκτυα (Τηλεγραφήματα)
- Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
- Ηλεκτρονική ψηφοφορία
- Ηλεκτρονική δημοπρασία
- Ηλεκτρονικό γραμματοκιβώτιο
- Συστήματα συναγερμών
- Συστήματα βιομετρικής αναγνώρισης
- Έξυπνες κάρτες
- Ιδιωτικά δίκτυα (VPN)
- World Wide Web
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
- Ασύρματαδίκτυα (Hipperlan, Bluetooth, 802.11x)
- Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
- Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

Τέλος, για να κλείσουμε αυτή την ενότητα αναφέρουμε ότι η κρυπτογραφία και κρυπτανάλυση βρίσκονται σε ένα συνεχή αγώνα δρόμου. Δεν υπάρχει αλγόριθμος κρυπτογράφησης που να μην σπάει (τουλάχιστον προς το παρόν και από αυτά πουγνωρίζει το ευρύ κοινό). Οι αλγόριθμοί που χρησιμοποιούνται είναι τόσο ισχυροί που να χρειάζεται πολύς χρόνος και υπολογιστική ισχύ μέχρι να αποκρυπτογραφηθεί το μήνυμα. Επίσης, γίνονται έρευνες για την χρήση διπλής κρυπτογράφησης έτσι ώστε ακόμα και με την χρήση brute force επίθεσης να μην μπορεί κάποιος μη εξουσιοδοτημένος να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα.

Κεφάλαιο 2 - Μαθηματικό υπόβαθρο

2.1. Θεμελιώδεις Έννοιες

Έστω οι αριθμοί $a \in Z$ και $b \in Z^*$. Ο α ονομάζεται *πολλαπλάσιο* του bεάν υπάρχει $k \in Z$ τέτοιο ώστε $a = k \cdot b$. Εάν $b \in N^*$ ο b καλείται *διαιρέτης ή παράγοντας* του α.

Ένας αριθμός $a \in N^*$ με $a > 1$ ονομάζεται *πρώτος*εάν οι μόνοι διαιρέτες του είναι οι α και 1. Σύμφωνα με το *θεμελιώδες θεώρημα της Αριθμητικής*, κάθε φυσικός αριθμόςείναι δυνατόν να αναλυθεί σε γινόμενο πρώτων παραγόντων του, κατά μοναδικό τρόπο.

*Μέγιστος κοινός διαιρέτης (ΜΚΔ)*δύο (ή περισσοτέρων) ακεραίων αριθμών είναι ο μεγαλύτερος από τους κοινούς διαιρέτες. Αν δύο ακέραιοι αριθμοί έχουν ΜΚΔ το 1 ονομάζονται *πρώτοι μεταξύ τους*.

Θεώρημα διαιρέσεως: Για οποιουσδήποτε αριθμούς $a \in Z$ και$d \in N^*$ υπάρχουν μοναδικοί αριθμοί $q \in Z$ και $r \in N^*$, με $r < d$ ώστε:

$$a = q \cdot d + r$$

Τα q και r ονομάζονται *πηλίκο και υπόλοιπο*, αντιστοίχως και συμβολίζονται ως $a$div$d$ και $a$mod$d$.

Ως *πράξη* επί ενός μη κενού συνόλου S ορίζεται μία απεικόνιση $S \times S \rightarrow S$.

Σε ένα σύνολο είναι δυνατόν να ορισθούν διάφορες πράξεις. Το σύνολο μαζί με τις πράξεις που ορίζονται σε αυτό απαρτίζουν μία *αλγεβρική δομή*.

Αβελιανή ομάδα (Abelian group) ονομάζεται μία δομή αποτελούμενη από έναασύνολο G εφοδιασμένο με μία πράξη $*$, για την οποία ισχύουν οι εξής ιδιότητες:

1. $a * (b * c) = (a * b) * c \forall a, b, c \in G$ (προσεταιριστική ιδιότητα)
2. $\exists e \in G: a * e = a \forall a \in G$ (ουδέτερο στοιχείο)
3. $\exists a' \in G: a * a' = e \forall a \in G$ (συμμετρικό στοιχείο)
4. $a * b = b * a \forall a, b \in G$ (αντιμεταθετική ιδιότητα)

Εάν δεν ισχύει η 4η ιδιότητα, τότε η δομή $(G,*)$ ονομάζεται απλώς ομάδα.Δύο βασικές ιδιότητες των ομάδων είναι πως το ουδέτερο στοιχείο είναι μοναδικό και πως το συμμετρικό στοιχείο κάθε στοιχείου του συνόλου είναι επίσης μοναδικό.

Δακτύλιος (Ring) ονομάζεται μία δομή αποτελούμενη από ένα σύνολο R εφοδιασμένο με τις πράξεις $+$ (πρόσθεση) και o (πολλαπλασιασμός), για την οποία ισχύουν οι εξής ιδιότητες:

1. Η δομή $(R,+)$ είναι αβελιανή προσθετική ομάδα. (Ουδέτερο στοιχείο για την πρόσθεση είναι το 0)
2. Η πράξη o είναι προσεταιριστική.
3. Υπάρχει ουδέτερο στοιχείο για την πράξη o (1).
4. $a \circ (b + c) = a \circ c + b \circ c \; \forall a, b, c \in G$ (επιμεριστική ιδιότητα)

Ομομορφισμός (δακτυλίων) λέγεται μία απεικόνιση F μεταξύ των δακτυλίων R και $R'(F : R \to R')$ με ουδέτερα στοιχεία για την πράξη ο τα 1 και $1'$, αντιστοίχως, όταν:

1. $\mathrm{F(1) = 1'}$
2. $\mathrm{F(a + b) = F(a) + F(b)} \; \forall \mathrm{a, b} \in \mathrm{R}$
3. $\mathrm{F(a^{\circ}b) = F(a)^{\circ} F(b)} \forall \mathrm{a, b} \in \mathrm{R}$

Ισομορφισμός (δακτυλίων) λέγεται ο αμφιμονοσήμαντος $(1-1)$ ομομορφισμός, ο οποίος, λόγω της ιδιότητός του αυτής, είναι αντιστρέψιμος.

Δύο δομές $(S,\bullet)$ και $(S',*)$ θεωρούνται *ισομορφικές* όταν ισχύουν τα εξής:

1. Μεταξύ των συνόλων S και S' υπάρχει αμφιμονοσήμαντη $(1-1)$ αντιστοιχία.
2. Οι πράξεις $\bullet$ και $*$ διατηρούνται στην αντιστοιχία. Δηλαδή:
   Εάν για $s_1, s_2 \in S$, και $s'_1, s'_2 \in S'$, ισχύει $s_1 \leftrightarrow s'_1$ και $s_2 \leftrightarrow s'_2$,τότε $s_1 \bullet s_2 \leftrightarrow s'_1 * s'_2$.

Σώμα (field) ονομάζεται μία δομή αποτελούμενη από ένα σύνολο $F \neq \{0\}$ εφοδιασμένο με τις πράξεις + (πρόσθεση) και o (πολλαπλασιασμός), για την οποία ισχύουν οι εξής ιδιότητες:

1. Η δομή $(F,+,o)$ είναι αντιμεταθετικός δακτύλιος.
2. Για όλα τα μη μηδενικά στοιχεία του F υπάρχει συμμετρικό στοιχείο για την πράξη o .

Τάξη της εν λόγω δομής (ομάδαή δακτύλιος ή σώμα) ορίζεται ως το πλήθος των στοιχείων του συνόλου της.

Τα σώματα με πεπερασμένο αριθμό στοιχείων (πεπερασμένα σώματα) καλούνται *σώματα Galois (Galois Fields),* προς τιμήν του Γάλλου μαθηματικού Évariste Galois και συμβολίζονται ως $GF(m)$, όπου m η τάξη του σώματος. Τα σώματα αυτά παρουσιάζουν ιδιαίτερο ενδιαφέρον για την επιστήμη της κρυπτολογίας. Αποδεικνύεται ότι για να είναι μία αλγεβρική δομή σώμα Galois πρέπει η τάξη της να είναι n-οστήδύναμη $(n \in N^*)$ κάποιου πρώτου αριθμού $p(m = p^n)$, ο οποίος αποτελεί την χαρακτηριστική του σώματος. Για τον λόγο αυτό προτιμάται ο συμβολισμός $GF(p^n)$για τα πεπερασμένα σώματα. Αποδεικνύεται, επίσης, πως όλα τα σώματα Galois ιδίας τάξεως είναι ισομορφικές δομές.

2.2. Αριθμητική Υπολοίπων

Όταν δύο αριθμοί $a, b \in Z$ διαιρούμενοι με τον $n \in N^*$έχουν το ίδιο υπόλοιπο,ονομάζονται ισοϋπόλοιποι (ή ισοδύναμοι) ως προς modulo n.

$$a \equiv b(modn)$$

Στην αριθμητική υπολοίπων είναι δυνατόν να διαχωρίσουμε το σύνολο των ακεραίων σε *κλάσεις ισοδυναμίας*, αναλόγως με το υπόλοιπό τους κατά την διαίρεση με κάποιον φυσικό αριθμό. Η κλάση ισοδυναμίας ως προς modulo$n$ ($n \in N^*$) του $a \in Z$ ορίζεται ως εξής:

$$[a]_n = \{(a + k \cdot n), k \in Z\} = \{w \in Z: w \equiv a(mod\ n)\}$$

Κάθε κλάση αναπαρίσταται συνήθως με το μικρότερο μη αρνητικό στοιχείο της. Βάσει των ανωτέρω ορίζεται το σύνολο των ακεραίων modulo$n$:

$$Z_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

Ένα εξίσου σημαντικό σύνολο στην αριθμητική υπολοίπων είναι το σύνολο των κλάσεων ισοδυναμίας των σχετικώς πρώτων με τον n ακεραίων:

$$Z_n^* = \{[a]_n \in Z_n : \gcd(a, n) = 1\}$$

Αρχή της αριθμητικής υπολοίπων: Εάν $a_1, a_2 \in Z$, και $*$ η πράξη της προσθέσεως ή του πολλαπλασιασμού (η αφαίρεση θεωρείται ίδια πράξη με την πρόσθεση), τότε η αναγωγή $modn$ από τους ακεραίους στους ακεραίους modulo$n$ είναι ομοιομορφισμός. Δηλαδή:

$$(a_1 * a_2) mod\ n = [(a_1 mod\ n) * (a_2 mod\ n)] mod\ n$$

Οι πράξεις της προσθέσεως και του πολλαπλασιασμού στο σύνολο Z_n συμβολίζονται ως$+_n$ και$\times_n$, αντιστοίχως.

Η δομή $(Z_n, +_n)$καλείται προσθετική ομάδα modulo$n$ και αποδεικνύεται πως είναι μία πεπερασμένη αντιμεταθετική αβελιανή ομάδα, τάξεως n. Αντιθέτως, η δομή $(Z_n, \times_n)$δεν είναι ομάδα, όμως αποδεικνύεται ότι η δομή $(Z_n^*, \times_n)$είναι μία πεπερασμένη αντιμεταθετική αβελιανή ομάδα, η τάξη της οποίας είναι συνάρτηση του n και ονομάζεται πολλαπλασιαστική ομάδα modulo$n$.

Για έναν πρώτο αριθμό p, αποδεικνύεται πως η δομή $(Z_p, +_p, \times_p)$είναι σώμα και είναι ισοδύναμη έκφραση του $GF(p)$, αφού κάθε τάξη ορίζει μόνον ισομορφικές δομές. Στην περίπτωση αυτή ισχύει:

$$Z_p^* = Z_p - \{[0]_p\}$$

ενώ η τάξη της δομής $(Z_p, \times_p)$είναι $p - 1$.

2.3. Πεπερασμένα σώματα και πολυώνυμα

Τα πεπερασμένα σώματα της μορφής $GF(2^n)$, κυρίως τα $GF(2)$και $GF(2^8)$ παρουσιάζουν ιδιαίτερο ενδιαφέρον στην κρυπτολογία. Η δυνατότητα αναπαραστάσεως μεμονωμένων bytes (ή ομάδων τους) με τηνμορφή πολυωνύμων, ορισμένων επί των συγκεκριμένων πεπερασμένων σωμάτων, διευκολύνει την θεωρητική μελέτη κρυπτογραφικών αλγορίθμων, οι οποίοι βασίζονταισε διαδικασίες που ορίζονται σε επίπεδο byte, όπως ο AES.

2.3.1.Βασικές έννοιες θεωρίας πολυωνύμων

Πολυώνυμο βαθμού $n\ (n \in N)$επί του συνόλου $A \supseteq \{a_k, k = 1,2, \dots, n\}$ως προςτην μεταβλητή x, ορίζεται μία αλγεβρική παράσταση της μορφής:

$$P(x) = \sum_{k=0}^{n} a_k \cdot x^k$$

Στην άλγεβρα πολυωνύμων δεν ενδιαφέρει ο υπολογισμός του πολυωνύμου γιαδεδομένη τιμή της μεταβλητής, παρά οι συντελεστές του πολυωνύμου. Οι πράξειςτης προσθέσεως, αφαιρέσεως και του πολλαπλασιασμού μεταξύ πολυωνύμων ορί-ζονται πάντοτε, ενώ για να είναι δυνατή και η διαίρεση πρέπει το πολυώνυμο ναείναιορισμένο επί ενός σώματος.Αν έχουμε τα παρακάτω πολυώνυμα:

$$P(x) = \sum_{k=0}^{n} a_k \cdot x^k \kappa\alpha\iota\ Q(x) = \sum_{k=0}^{m} b_k \cdot x^k\ \mu\varepsilon\ m \leq n,$$

τότε *Πρόσθεση/Αφαίρεση*ορίζεται ως:

$$P(x) \pm Q(x) = \sum_{k=0}^{m} (a_k + b_k) \cdot x^k + \sum_{m+1}^{n} a_k \cdot x^k$$

και*Πολλαπλασιασμός*ορίζεται ως:

$$P(x) \cdot Q(x) = \sum_{k=0}^{m+n} c_k \cdot x^k, \quad \text{όπου}\ c_k = a_0 \cdot b_k + a_1 \cdot b_{k-1} + \cdots + a_k \cdot b_0$$
$$\mu\varepsilon\ a_k = 0, \forall k > n \kappa\alpha\iota b_k = 0, \forall k > m$$

2.3.2.Πολυώνυμα ορισμένα επί σωμάτων

Θεωρούμε πως οι συντελεστές ενός συνόλου πολυωνύμων είναι ορισμένοι επί ενός σώματος $(F, +, o)$. Το σύνολο των πολυωνύμων συμβολίζεται με $F[x]$, ενώ με$F[x]_n$ συμβολίζεται το σύνολο των πολυωνύμων βαθμού μικρότερου του n.Αποδεικνύεται ότι η δομή $(F[x], +, o)$ αποτελεί έναν αντιμεταθετικό δακτύλιο, ο οποίος χαρακτηρίζεται πολυωνυμικός δακτύλιος.

Για την διαίρεση $P(x)/Q(x)$ δύο πολυωνύμων βαθμών n και $m\,(m \leq n)$, αντιστοίχως, που ανήκουν σε έναν πολυωνυμικό δακτύλιο το θεώρημα της διαιρέσεως. Δηλαδή:

$$P(x) = q(x) \cdot Q(x) + r(x)$$

Ο βαθμός του $q(x)$ είναι $n - m$, ενώ ο βαθμός του $r(x)$ είναι μικρότερος του m.Εάν $r(x) = 0$, τότε το $Q(x)$ είναι *παράγοντας* του $P(x)$.

Ορίζεται *ΜΚΔ* μεταξύ πολυωνύμων, ως το μονοειδές πολυώνυμο με τον μεγαλύτερο βαθμό που είναι κοινός παράγοντας των πολυωνύμων. Ένα πολυώνυμο που δεν έχει παράγοντες στο σώμα στο οποίο το θεωρούμε, καλείται ανάγωγο ή πρώτο.

Εάν $C(x)$ και $m(x)$δεδομένα πολυώνυμα και $P(x)$τυχαίο πολυώνυμο, η κλάση ισοδυναμίας του $C(x)$ ως προς modulo $m(x)$ ορίζεται ως:

$$[C(x)]_{\mathrm{m(x)}} = \{P(x): P(x) mod m(x) = C(x)\}$$

Εάν ένα σύνολο πολυωνύμων είναι ορισμένο στο πεπερασμένο σώμα $F = GF(p)$, το οποίο είναι εφοδιασμένο με τις πράξεις$(+_p, \times_p)$, θα υπάρχουν $k = p^n$ κλάσεις ισοδυναμίας ως προς modulo$m(x)$, όπου n ο βαθμός του $m(x)$. Τότε:

$$\mathrm{F[x]_n} = \{[C_1(x)]_{\mathrm{m(x)}}, [C_2(x)]_{\mathrm{m(x)}}, \dots, [C_k(x)]_{\mathrm{m(x)}}\}$$

Αποδεικνύεται ότι εάν το $m(x)$ είναι ανάγωγο, το σύνολο$F[x]_n$, εφοδιασμένομε τις πράξεις$(+_p, \times_p)$συνιστά ένα πεπερασμένο σώμα τάξεως p^n, υπό τις εξής προϋποθέσεις:

1. Η αριθμητική επί των συντελεστών των πολυωνύμων πραγματοποιείται με χρήση των πράξεων $(+_p, \times_p)$.
2. Εάν το αποτέλεσμα του πολλαπλασιασμού πολυωνύμων είναι βαθμού μεγαλύτερου του $n - 1$, τότε γίνεται αναγωγή του αποτελέσματος modulo$m(x)$.

Δηλαδή, το αποτέλεσμα της αριθμητικής πολυωνύμων modulo$m(x)$ επί του$GF(p)$, όταν το $m(x)$ είναι ανάγωγο, είναι αναπαράσταση του $GF(p^n)$.

2.3.3.Αναπαράσταση bytes με πολυώνυμα επί του $GF(2)$

Ένα byte$b_7b_6b_5b_4b_3b_2b_1b_0$, όπου $b_i \in B = \{0,1\}$, $i = 0,1,\dots,7$ είναι δυνατόν να αναπαρασταθεί με ένα πολυώνυμο βαθμού 7 με συντελεστές $b_i \in B$. Δηλαδή:

$$b_7b_6b_5b_4b_3b_2b_1b_0 \leftrightarrow b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

Η δομή $(B, +_2, \times_2)$είναι ισοδύναμημε το $GF(2)$. Να σημειωθεί ότι $+_2 \equiv \oplus_{(XOR)}$.

Τον πολλαπλασιασμό με αναγωγή modulo κάποιο πολυώνυμο, στο εξής θα τον

συμβολίζουμε με $\otimes$, ενώ με $\times$ θα συμβολίζεται ο απλός πολλαπλασιασμός, άνευ αναγωγής.

για να είναι τα πολυώνυμα που αναπαριστούν bytes στοιχεία του $GF(28)$, πρέπει να ορισθεί στο σώμαατό ένα ανάγωγο πολυώνυμο βαθμού 8, για την αναγωγή των αποτελεσμάτων του πολλαπλασιασμού μεταξύ bytes. Στον κρυπταλγόριθμο AES θεωρείται, για τον λόγο αυτό, το εξής πολυώνυμο:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Ειδική μνεία πρέπει να γίνει στον πολλαπλασιασμό b(x)⊗x , καθώς η ευκολίαυπολογιστικής πραγματοποιήσεώς του απλοποιεί την διαδικασία υπολογισμού του πολλαπλασιασμού μεταξύ δύο byte. Ο πολλαπλασιασμός ενός byte επί x αντιστοιχεί στον πολλαπλασιασμό επί $02_{(16)}$.

$$b(x) \times x = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

Παρατηρούμε ότι το αποτέλεσμα της πράξεως $b(x) \times x$ είναι ένα πολυώνυμο βαθμού 8. Η αναγωγή του πολυωνύμου αυτού mod$m(x)$ ισοδυναμεί με την πράξη XOR μεταξύ $b(x) \times x$ και $m(x)$. Δηλαδή:

$$b(x) \otimes x = [b(x) \times x] \oplus m(x)$$

Τελικά:

$$b(x) \otimes x = b_6x^7 + b_5x^6 + b_4x^5 + (b_3 \oplus b_7)x^4 + (b_2 \oplus b_7)x^3 + b_1x^2 + (b_0 \oplus b_7)x + b_7$$

Η διαδικασία του πολλαπλασιασμού $b(x) \otimes x$είναι ι εξής:

1. Αριστερή ολίσθηση των bits του byte $b(x)$ κατά μία θέση και προσθήκη του 0 ως το τελευταίο bit.
2. Εάν το πρώτο αριστερά bit είναι 0, το αποτέλεσμα είναι τα 8 υπόλοιπα bits.
3. Εάν το πρώτο αριστερά bit είναι 1, το τελικό αποτέλεσμα προκύπτει από την πράξη XOR μεταξύ του αποτελέσματος της ολισθήσεως και του 100011011.

2.3.4.Αναπαράσταση bytes με πολυώνυμα επί του $\boldsymbol{GF(2^8)}$

Στον AES εμφανίζονται διανύσματα 4-bytes, τα οποία αναπαρίστανται με πολυώνυμα ορισμένα επί του $GF(2^8)$βαθμού 3.

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0, a_i \epsilon\, GF(2^8), i = 0,1,2,3$$

Εαν $a(x)$ και $b(x)$πολυώνυμα ορισμένα επί του $GF(2^8)$βαθμού 3το αποτέλεσμα της πρόσθεσης $a(x) + b(x)$και του πολλαπλασιασμού $a(x) \times b(x)$προκύπτουν με την βοήθεια των $\otimes$ και $\oplus$. Έχουμε:

$$a(x) + b(x) = (a_3 \oplus b_3)x^3 + (a_2 \oplus b_2)x^2 + (a_1 \oplus b_1)x + (a_0 \oplus b_0)$$

και $\quad a(x) \times b(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$

όπου:

$$c_0 = a_0 \otimes b_0$$
$$c_1 = a_1 \otimes b_0 \oplus a_0 \otimes b_1$$
$$c_2 = a_2 \otimes b_0 \oplus a_1 \otimes b_1 \oplus a_0 \otimes b_2$$
$$c_3 = a_3 \otimes b_0 \oplus a_2 \otimes b_1 \oplus a_1 \otimes b_2 \oplus a_0 \otimes b_3$$
$$c_4 = a_3 \otimes b_1 \oplus a_2 \otimes b_2 \oplus a_1 \otimes b_3$$
$$c_5 = a_3 \otimes b_2 \oplus a_2 \otimes b_3$$
$$c_6 = a_3 \otimes b_3$$

Για να είναι το $c(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$διανυσμα 4-byteπρέπει να γίνει η αναγωγή του σε πολυώνυμο 4^{ου} βαθμού.Στον κρυπταλγόριθμο AES θεωρείται, για τον λόγο αυτό, το πολυώνυμο:

$$l(x) = x^4 + 1$$

Έτσι ώστε:

$$x^i mod(x^4 + 1) = x^{imod4}$$

Και υπολογίζοντας την αναγωγή:

$$[a(x) \times b(x)]\text{mod}l(x)$$

Προκύπτει: $a(x) \times b(x) = d_3x^3 + d_2x^2 + d_1x + d_0$

όπου:

$$d_0 = a_0 \otimes b_0 \oplus a_3 \otimes b_1 \oplus a_2 \otimes b_2 \oplus a_1 \otimes b_3$$
$$d_1 = a_1 \otimes b_0 \oplus a_0 \otimes b_1 \oplus a_3 \otimes b_2 \oplus a_2 \otimes b_3$$
$$d_2 = a_2 \otimes b_0 \oplus a_1 \otimes b_1 \oplus a_0 \otimes b_2 \oplus a_3 \otimes b_3$$
$$d_3 = a_3 \otimes b_0 \oplus a_2 \otimes b_1 \oplus a_1 \otimes b_2 \oplus a_0 \otimes b_3$$

Το οποίο εκφράζεται με μορφή πίνακα ως εξής:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Ειδικά αν $a(x) = x$ $(a_1 = 01_{(16)})$

$$d(x) = x \times b(x) \leftrightarrow \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} 00_{(16)} & 00_{(16)} & 00_{(16)} & 01_{(16)} \\ 01_{(16)} & 00_{(16)} & 00_{(16)} & 00_{(16)} \\ 00_{(16)} & 01_{(16)} & 00_{(16)} & 00_{(16)} \\ 00_{(16)} & 00_{(16)} & 01_{(16)} & 00_{(16)} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_3 \\ b_0 \\ b_1 \\ b_2 \end{bmatrix}$$

Δηλαδή ο πολλαπλασιασμός ενός πολυωνύμου επί του $GF(2^8)$ με x ισοδυναμεί με

κυκλική αναδιάταξη των συντελεστών του.

Το πολυώνυμο $l(x)$ δεν είναι ανάγωγο στο σώμα $GF(2^8)$, διότι $x^4 + 1 = (x + 1)^4$.Αυτό σημαίνει ότι ο πολλαπλασιασμός δεν είναι πάντοτε αντιστρέψιμος (δεν έχουν όλα τα πολυώνυμα συμμετρικό στοιχείο για την πράξη του πολλαπλασιασμού). Για να έχει ένα πολυώνυμο συμμετρικό στοιχείο πρέπει να μην διαιρείται με το $(x + 1)$. Στον AES ορίζεται, για τους ανωτέρω λόγους, μόνον πολλαπλασιασμός επί ένα συγκεκριμένο σταθερό πολυώνυμο, που καθιστά την πράξη αυτή αντιστρέψιμη.

Κεφάλαιο3 - Data Encryption Standard (DES)

Σε αυτό το κεφάλαιο, θα παρουσιαστούν τα θεμελιώδη στοιχεία του DES αλγορίθμου.

3.1. Ιστορικά στοιχεία

Τον Αύγουστο, του 1974, η IBM σε απάντηση στη δεύτερη προκήρυξη του Εθνικού Γραφείου Προτύπων (National Bureau of Standards, NBS), τώρα γνωστό ως Εθνικό Ίδρυμα Προτύπων & Τεχνολογίας (National Institute of Standards & Technology, NIST), υπέβαλε υποψηφιότητα για την ανάδειξη ενός κρυπτογραφικού αλγόριθμου, του οποίου στόχος ήταν ναπροστατεύσει τα στοιχεία κατά τη διάρκεια της μετάδοσης και της αποθήκευσης. Η IBM υπέβαλε ένα αλγόριθμο με το όνομα LUCIFER ο οποίος είχε μέγεθος κειμένου καθώς και μέγεθος κλειδιού 128 bits. Το NBS άρχισε την διαδικασία αξιολόγησης με τη βοήθεια της Υπηρεσίας ΕθνικήςΑσφάλειας (National Security Agency, NSA) από την οποία ζήτησε να διενεργήσει μια εξαντλητική τεχνική ανάλυση του αλγορίθμου. Επίσης κατά την διάρκεια αυτής της έρευνας, η IBM διαπραγματεύτηκε με το NBS τους όρους με βάση τους οποίους θα μπορούσε να διατεθεί αυτό το κατοχυρωμένο προϊόν της σε άλλους κατασκευαστές. Η συμφωνία τελικά επήλθε στις 13 Μαΐου 1975.

Τον Μάρτιο του 1975 δημοσιεύτηκε περιγραφή του αλγορίθμου προκειμένου να υπάρξουνσχόλια και προτάσεις από το ευρύ κοινό ενώ τον Αύγουστο της ίδιας χρονιάς δημοσιοποιήθηκε και ένα σχεδιάγραμμα του προτεινόμενου προτύπου. Τα σχόλια που ακολούθησαν ήταν ποικίλα. Πολλά από αυτά επικεντρωνόταν στους τρόπους χρησιμοποίησης και ενσωμάτωσης του συγκεκριμένου προτύπου σε διάφορες αρχιτεκτονικές υπολογιστών ενώ άλλα αναφέρονταν στην κρυπτογραφική δύναμη του αλγορίθμου. Μετά την διαδικασία αυτή ανταλλαγής απόψεων, η οποία διήρκησε περίπου 18 μήνες, στις 23 Νοεμβρίου του 1976 ο αλγόριθμος αυτός κρυπτογράφησης υιοθετήθηκε ως Εθνικό Πρότυπο ενώ δημοσιεύτηκε επίσημα σαν έκδοση FIPS-46 με το όνομα DES στις 15 Ιανουαρίου του 1977. Έξι μήνες αργότερα, στις 15 Ιουλίου του 1977, κατέστη υποχρεωτικός και όλες οι Εθνικές Υπηρεσίες, εκτός και εάν πρόβαλαν έναν αρκετά σοβαρό και βάσιμο λόγο, θα έπρεπε να συμμορφωθούν με τις προδιαγραφές του.

Ο αλγόριθμος DES σχεδιάστηκε με βάση κάποια συγκεκριμένα κριτήρια. Κατ’ αρχήν ο προτεινόμενοςαλγόριθμος θα έπρεπε να έχει εξαιρετικά υψηλό επίπεδο ασφαλείας το οποίο όμως δεν θα εξαρτάται από την μυστικότητα του κρυπταλγορίθμου ενώ οι προδιαγραφές του επιβάλλεται να είναι πλήρεις και διαφανείς. Να είναι κατάλληλο για ποικιλία εφαρμογών με χαμηλό κόστος υλοποίησης, να επιτρέπεται η εξαγωγή του (μία έκδοση του DES για εξαγωγή από τις ΗΠΑ είναι η Commercial Data Masking

Facility ή CDMF της IBM, η οποία χρησιμοποιεί ένα κλειδί των 40 bits) και τέλος να καθίσταται δυνατή η αξιολόγηση του.

Ωστόσο όλα αυτά τα κριτήρια ήταν καθαρά σε θεωρητικό επίπεδο, στην πράξη πολλά από αυτά τροποποιήθηκαν ή ακόμα και αγνοήθηκαν. Πρώτα απ' όλα ο DES είχε πολύ μικρότερο κλειδί γεγονός που από μόνο του τον καθιστούσε λιγότερο ασφαλή. Σε αυτό το γεγονός όμως ευθύνεταιαποκλειστικά η NSA των ΗΠΑ η οποία άσκησε πιέσεις για μικρό μήκος κλειδιού. Το κριτήριο διαφάνειας των προδιαγραφών ουσιαστικά αγνοήθηκε αφού τα κριτήρια σχεδιασμού των κουτιών αντικατάστασης που περιέχονται στη συνάρτηση γύρου του DES αποκαλύφθηκαν στα μέσα περίπου της δεκαετίας του `90 και τα κριτήρια σχεδιασμού τους περιείχαν ενδείξεις ότι η τεχνικήτης διαφορικής κρυπτανάλυσης που αποκαλύφθηκε στις αρχές της ίδιας δεκαετίας ήταν γνωστήπριν από 15 χρόνια. Αυτό αποδεικνύει εν' μέρει και η επιλογή των γύρων του δικτύου Feistel του DES η οποία έγινε έτσι ώστε ο αλγόριθμος να είναι ανθεκτικός σε περίπτωση διαφορικής κρυπτανάλυσης.

Ο DES είναι ο μοναδικός αλγόριθμος κρυπτογράφησης ο οποίος έχει υποστεί την μεγαλύτερη έρευνα ούτως ώστε να εξακριβωθεί η κρυπτογραφική του δύναμη. Οι απόπειρες κρυπτανάλυσης του DES είχαν σαν αποτέλεσμα την ανακάλυψη και καθιέρωση ποικίλων αρχών σχεδίασης των κρυπταλγορίθμων τμήματος.

3.2. Περιγραφή αλγορίθμου (DES)

Ο αλγόριθμος DES έχει σχεδιαστεί με σκοπό να κρυπτογραφεί και να αποκρυπτογραφεί σύνολα δεδομένων που αποτελούνται από 64-bitsμε την βοήθεια ενός 56-bits κλειδιού που εκφράζεται σαν 64-bits κείμενο. Το 8°, 16°, 24°…bitείναι καθορισμένα με τέτοιον τρόπο ώστε κάθε 8-άδα των bitsνα περιέχει μονό αριθμό από 1. Αυτό γίνεται για εντοπίζονται τυχών λάθηστακλειδιά. Η αποκρυπτογράφηση θα πρέπει να επιτυγχάνεται με την χρησιμοποίηση του ίδιου κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση, αλλά με αλλαγμένο το πρόγραμμα εφαρμογής των κλειδιών έτσι ώστε η διαδικασία αποκρυπτογράφησης να είναι η αντιστροφή της διαδικασίαςκρυπτογράφησης.

Η διαδικασία όπως δείχνει η εικόνα 2 ξεκινάει με ένα αρχικό 64-bits κείμενο εισόδου m(input) και διακρίνεται σε τρία στάδια:

1. Το αρχικό προς κρυπτογράφηση κείμενο υποβάλλεται σε μια μετάθεση (permutation) και μετατρέπεται στην μορφή $m_0 = IP_{(m)} = L_0R_0$, όπου L_0 τα πρώτα 32 bits του m_0(Left) και R_0 τα υπόλοιπα 32 bits του m_0 (Right).

2. Για$1 \leq i \leq 16$,εκτελούνται οι παρακάτω:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Όπου K_i, 48 bits κείμενο το οποίο προέρχεται από το κλειδί Κκαι fσυνάρτηση που θα αναλυθεί παρακάτω.

3. Αντιστρέφεται το αποτέλεσμα από $\mathrm{L_{16}R_{16}}$ σε $\mathrm{R_{16}L_{16}}$ και στη συνέχεια εφαρμόζεται η αντίστροφη διαδικασία $\mathrm{IP^{-1}}$ από την οποία προκύπτει το κρυπτογραφημένο κείμενο (ciphertext):

$$c = IP^{-1}(R_{16}L_{16})$$

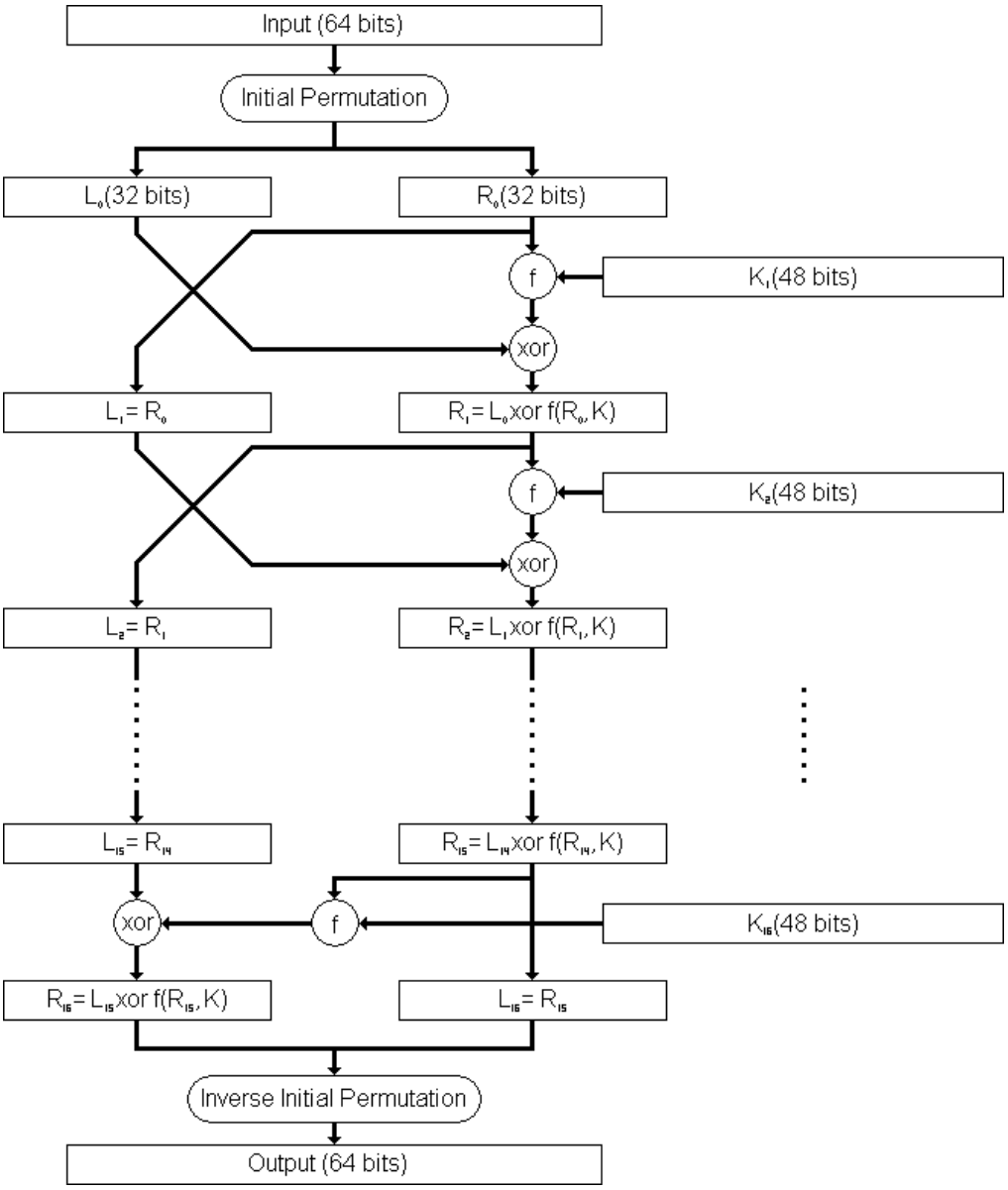

Fig 7 – Αλγόριθμος DES

Η αποκρυπτογράφηση γίνεται ακολουθώντας την ίδια διαδικασία με τα κλειδιά να έχουν αντίστροφη σειρά. Εάν δηλαδή κατά την κρυπτογράφηση το πρόγραμμα κλειδιού είναι$\{k_1, k_2, \ldots, k_{16}\}$, κατά την αποκρυπτογράφηση θα είναι $\{k_{16}, k_{15}, \ldots, k_1\}$.

3.2.1.Πίνακες Μεταθέσεων IP και IP^{-1}

Οι μεταθέσεις IP και IP^{-1} συμμετέχουν στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης DES. Ο λόγος που επιλέχθηκε η εξάρτηση αυτή των δύο μεταθέσεων δεν έχει να κάνει με την προσθήκη κάποιας επιπλέον ασφάλειας, αφού σε αυτές τις μεταθέσεις δεν παίρνει μέρος το κλειδί, αλλά για να μπορεί να

χρησιμοποιηθεί η ίδια διαδικασία και στην κρυπτογράφηση και στην αποκρυπτογράφηση. Επίσης, η ύπαρξη και μόνο των δύο αυτών μεταθέσεων προσδίδει την δυνατότητα αποθήκευσης τόσο του απλού κειμένου όσο και του κρυπτοκειμένου πριν και μετά την εφαρμογή του δικτύου Feistel.

Οι αριθμοί στους πίνακες δηλώνουν την σειρά των bits των m και $R_{16}L_{16}$ αντίστοιχα και η σειρά των αριθμών στους πίνακες δηλώνει την νέα θέση τους. Δηλαδή το 58-στο bit του m θα γίνει το 1ο bit του m_0 μετά την IP, το 50-στο θα γίνει το 2° κτλ.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Fig 8 – Πίνακες Μετάθεσης IP και IP^{-1}

3.2.2.Συνάρτηση DES (Feistel)

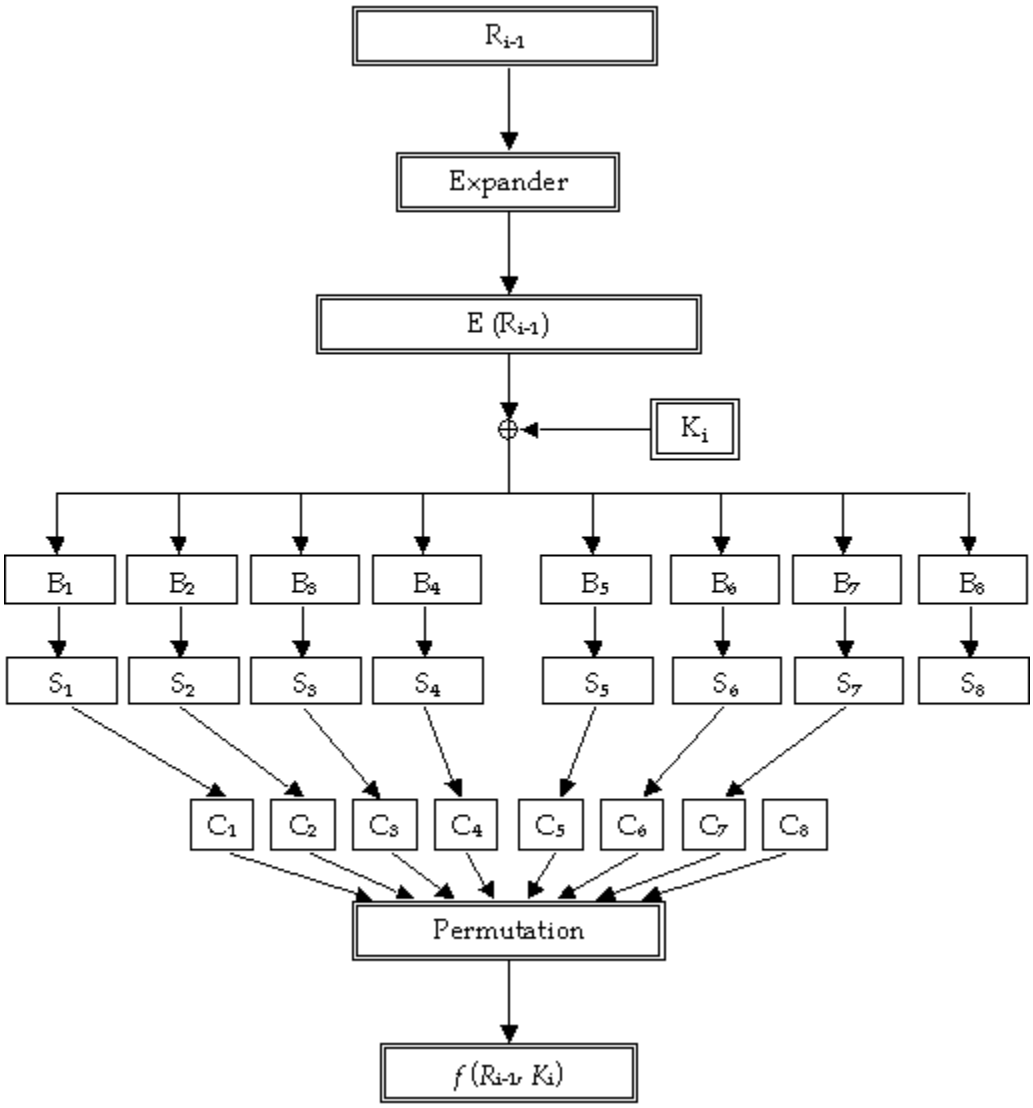

Fig 9 – Συνάρτηση DES $f(R_{i-1}, K_i)$

Η συνάρτηση $f(R_{i-1}, K_i)$ διακρίνεται στα εξής στάδια:

1. Το R υπόκειται σε διαδικασία επέκτασης $E(R)$ από 32 bits σε 48 bits (expansion) χρησιμοποιώντας τον ακόλουθο πίνακα.Οι αριθμοί στον πίνακα δηλώνουν την σειρά των bits του R και η σειρά των αριθμών στους πίνακες δηλώνει την νέα θέση τους σαν $E(R)$. Δηλαδή το 32° bit του Rθα είναι το 1°bit του $E(R)$.

$\boldsymbol{Expansion}$					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Fig 10 – Πίνακας Επέκτασης Μετάθεσης

2. Γίνεται υπολογισμός του $E(R) \oplus K_i$από το οποίο προκύπτει $B_1 B_2 \dots B_8$, όπου $B_j, 1 \leq j \leq 8$ blocks των 6 bits. Δηλαδή $B_j = b_{j1} b_{j2} b_{j3} b_{j4} b_{j5} b_{j6}$.Το πώς προκύπτει το K_i θα αναλυθεί παρακάτω.

3. Κάθε $B_j, 1 \leq j \leq 8$ είναι input για έναν πίνακα $S_j, 1 \leq j \leq 8$ (S-box).Το $b_{j1} b_{j6}$ καθορίζει την γραμμή του S_j ενώ το $b_{j2} b_{j3} b_{j4} b_{j5}$ καθορίζει την αντίστοιχη στήλη. Οι γραμμές και οι στήλες απαριθμούνται από 0 έως 3 και από 0 έως 15 αντίστοιχα. Από την διαδικασία αυτή προκύπτουν οκτώ 4-bit αποτελέσματα $C_1, C_2, \dots, C_8$.

$\boldsymbol{S_1}$															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$\boldsymbol{S_2}$															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2

7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Fig 11 – Πίνακες S-box

4. Το$C_1C_2 \dots C_8$κείμενο που προκύπτει από την προηγούμενη διαδικασία μετατίθεται με τη βοήθεια του παρακάτω πίνακα και το αποτέλεσμά του είναι το 32-bit $f(R, K_i)$.

Permutation			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Fig 12 – Πίνακας μετάθεσης

3.2.3.Συνάρτηση μετάθεσης κλειδιού.

Όπως προαναφέρθηκε η είσοδος κάθε γύρου εκτός από τα 32 bits δεδομένων απαιτεί και 48bits του κλειδιού. Το κλειδί K_i, με $1 \leq i \leq 16$, κάθε γύρου είναι διαφορετικό και προκύπτει από μια συγκεκριμένη διαδικασίαη οποία φαίνεται στο παρακάτω σχήμα κατά την οποία συμμετέχουν δύο συναρτήσεις μετάθεσης επιλογής (permutation choice) και διακρίνεται σε τρία στάδια:

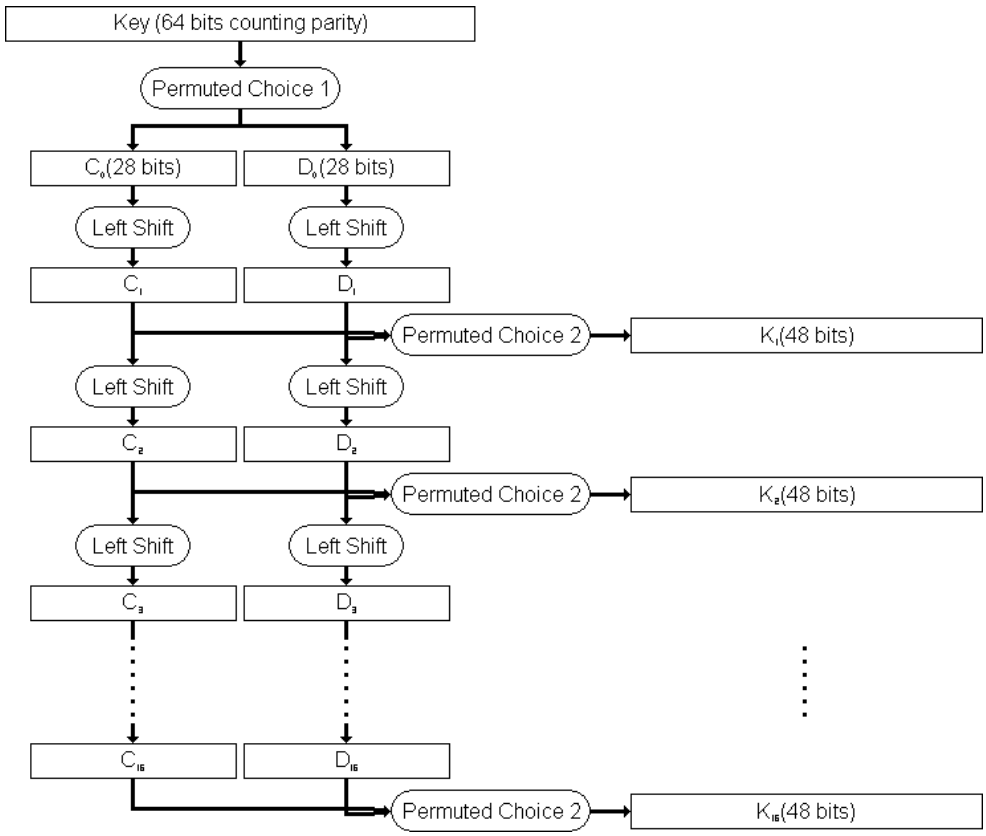

Fig 13 – Διαδικασία μετάθεσης κλειδιού

1. Ως *μετάθεση επιλογής* ορίζεται η μετάθεση κατά την οποία ορισμένα bits της εισόδου αγνοούνται και δεν εμφανίζονται στην έξοδο.
   Στην δική μας περίπτωση αγνοείται το τελευταίο bit κάθε 8-αδας bit (paritybit) του 64-bit K. Στην συνέχεια το αποτέλεσμα μετατίθεται από τον 1° πίνακα μετάθεσης επιλογής (permutationchoice - 1) από το οποίον προκύπτει το αποτέλεσμα C_0D_0. Το καθένα C_0 και D_0 περιέχουν από 28 bits.

Η πρώτη συνάρτηση επιλογής είναι η ακόλουθη:

$$PC-1: \{0,1\}64 \rightarrow \{0,1\}56$$

$\boldsymbol{PC-1}$						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22

14	6	61	53	45	37	29
21	13	5	28	20	12	4

Fig 14 – Πίνακας μετάθεσης επιλογής $PC-1$

2. Για κάθε γύρο $i, 1 \leq i \leq 16$,εκτελούνται οι παρακάτω:

$$C_i = LS_i(C_{i-1}) \text{ και } D_i = LS_i(D_{i-1}),$$

ΌπουLS_i αριστερή ολίσθηση του κατά 1 ή 2 θέσεις σύμφωνα με των παρακάτω πίνακα:

Γύρος	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Αρ.Ολισθήσεων	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3. Το κλειδί K_i, με $1 \leq i \leq 16$,προκύπτει σε κάθε γύρο χρησιμοποιώντας την δεύτερη μετάθεση επιλογής:

$$\mathrm{PC}-2: \{0,1\}56 \rightarrow \{0,1\}48,$$

κατά την οποία επιλέγονται 48 bits από το 56-bits κείμενο C_iD_i σύμφωνα με τον παρακάτω πίνακα:

$\boldsymbol{PC-2}$					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Fig 15 – Πίνακας μετάθεσης επιλογής $PC-2$

3.3. Καταστάσεις Λειτουργίας κρυπταλγορίθμων τμήματος

Ο αλγόριθμος DES είναι ένα παράδειγμα αλγορίθμων που κρυπτογραφούν και αποκρυπτογραφούν σύνολα δεδομένων (64-bits στην περίπτωση του DES).Οι τρόποι λειτουργίας είναι τρόποι διασύνδεσης κρυπταλγορίθμων τμήματος, με στόχο τηνπεραιτέρω αύξηση της κρυπτογραφικής δύναμης και την αποτελεσματικότερη απόκρυψη πιθανών υπολειμμάτων πληροφορίας του απλού κειμένου που μπορεί να υπάρχει στο κρυπτοκείμενο.

Υπάρχουν πέντε τυποποιημένοι τρόποι λειτουργίας καιαρκετοί μη τυποποιημένοι τρόποι λειτουργίας. Οι πέντε τρόποι λειτουργίας είναι:

- Κατάσταση λειτουργίας ηλεκτρονικού βιβλίου κωδικών (Electronic Codebook, ECB)
- Κατάσταση λειτουργίας αλυσιδωτής σύνδεσης τμημάτων κρυπτογραφίας (cipher block chaining, CBC).
- Κατάσταση λειτουργίας κρυπτογραφίας ανάδρασης (cipher feedback mode, CFB).
- Κατάσταση λειτουργίας ανάδρασης εξόδου (output feedback, OFB)
- Κατάσταση λειτουργίας μετρητή (CTR)

3.3.1.Ηλεκτρονικό κωδικοβιβλίο (ECB)

Ο τρόπος λειτουργίας ECB έγκειται στην διάσπαση μεγάλου κομματιούαπλού κειμένου/κρυπτοκειμένου σε μικρότερα κομμάτια, κατάλληλου μεγέθους, και επεξεργασία καθενός από αυτά ξεχωριστά. Η ονομασίατου τρόπου αυτού προέρχεται από την αναπαράσταση του κρυπτοσυστήματος ως ένα μεγάλοβιβλίο το οποίο περιέχει όλα τα ζεύγη απλού κειμένου και κρυπτοκειμένου για κάθε κλειδί. Η διαδικασία της κρυπτογράφησης/αποκρυπτογράφησης είναι η εξής:

$$C_j = E_k(P_j), j = 1,2, \dots, n$$

$$P_j = D_k(C_j), j = 1,2, \dots, n$$

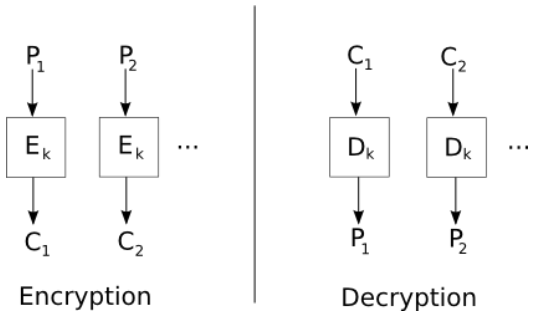

Fig 16 – ECB Mode

Η αναγκαία διάσπαση του απλού κειμένου είναι και το μειονέκτημα της ECB λειτουργίας. Για όμοια τμήματα του απλού κειμένου, τα αντίστοιχα κρυπτοκείμενα που προκύπτουν είναι επίσης όμοια. Αυτό καθιστά την ECB ακατάλληλη για τις εφαρμογές στις οποίες υπάρχουν επαναλαμβανόμενα μοτίβα δεδομένων. Για παράδειγμα, στα δίκτυα ηλεκτρονικών υπολογιστών, τα δεδομένα που ανταλλάσσονται μεταξύ των υπολογιστών βασίζονται σε πρωτόκολλα επικοινωνίας τα οποία χρησιμοποιούν τυποποιημένα μηνύματα. Έτσι κάποιος είναι σε θέση να αναγνωρίζει και να μαντεύει τα επαναλαμβανόμενα τμήματα του απλού κειμένου, τις στιγμές κατά τις οποίες γίνεται η αλλαγή του κλειδιού κρυπτογράφησης, και επίσης μπορεί να κατασκευάσει κομμάτια κρυπτοκείμενου και να τις διοχετεύσει στην ροή της πληροφορίας. Για αυτό τον λόγω οτρόπος λειτουργίας ECB δεν ενδείκνυται για τις ασφαλείς εφαρμογές.

3.3.2.Κρυπταλγόριθμος αλυσιδωτού τμήματος (CBC)

Μια μέθοδος για να μειωθεί η αδυναμία του ηλεκτρονικού κωδικοβιβλίου είναι ο κρυπταλγόριθμος αλυσιδωτού τμήματος (cipher block chaining CBC). Η κρυπτογράφηση ενός τμήματος του απλού κειμένου P_j εξαρτάται και από το προηγούμενο τμήμα P_{j-1} με την ακόλουθη σχέση κρυπτογράφησης:

$$C_j = E_k\,(P_j \oplus C_{j-1}),$$

Ενώ αντίστοιχα η αποκρυπτογράφηση:

$$P_j = D_k\,(C_j) \oplus C_{j-1},$$

όπου C_0 μια προκαθορισμένη αρχική τιμή.

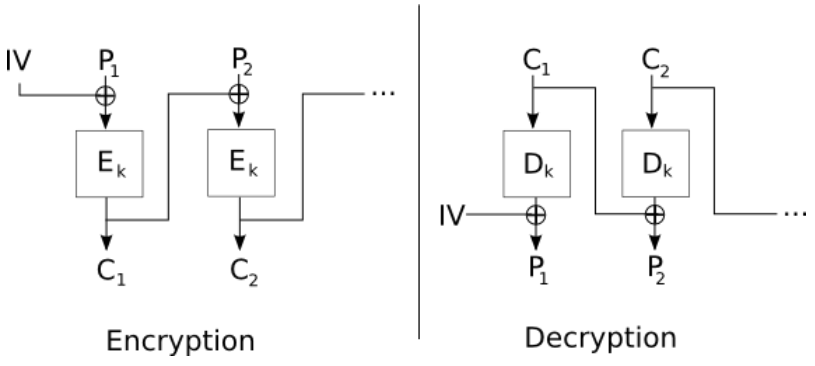

Fig 17 – CBD Mode

Μπορούμε να παρατηρήσουμε ότι η ποσότητα του κρυπτοκειμένου που

εφαρμόζεταιστην αποκλειστική διάζευξη είναι η ίδια τόσο στην πλευρά ένα κρυπτογράφησης, όσο καιστην πλευρά ένα αποκρυπτογράφησης και είναι αυτή που προκύπτει από την προηγούμενη κρυπτογράφηση.

Για να καθοριστεί πλήρως η κρυπτογράφηση ένα λειτουργίας CBC, θα πρέπει ναορισθούν η αρχική τιμή C_0. Στηνπερίπτωση ένα κρυπτογράφησης του πρώτου τμήματος P_1είναι:

$$C_1 = E_k (P_1 \oplus C_0),$$

που σημαίνει ότι απαιτείται η ποσότητα C_0. Αυτή η ποσότητα είναι το διάνυσμα αρχικοποίησης (initialization vectoror IV) η οποία θα πρέπει να είναι γνωστή τόσο κατά τη διαδικασία ένακρυπτογράφησης,όσο και κατά τη διαδικασία ένα αποκρυπτογράφησης.Αν και η εμπιστευτικότητα του δεν είναι υποχρεωτική, αποτελεί κοινή πρακτική να στέλνεται στον αποδέκτη μαζί με το πρώτο κείμενο C_1 κρυπτογραφημένο με ECB.

3.3.3.Κρυπταλγόριθμος ανάδρασης (CFB)

Ένα από τα προβλήματα με τους προηγούμενους μεθόδους ECBκαι CBC είναι ότι η κρυπτογράφηση ή αποκρυπτογράφηση δεν μπορούν να ξεκινήσουν μέχρι ένα ολοκληρωμένο 64-bits κείμενο είναι διαθέσιμο.

Στον κρυπταλγόριθμο ανάδρασης (CipherFeedBackor CFB) το κρυπτοκείμενο προκύπτει από την επανακρυπτογράφηση του προηγουμένου κρυπτοκειμένου, συνδυασμένο με αποκλειστική διάζευξη με το απλό κείμενο. Έτσι η κρυπτογράφηση ορίζεται ως εξής:

$$C_i = P_i \oplus E_k (C_{i-1}) \; i \geq 1$$

Ενώ κατά την αποκρυπτογράφηση ισχύει:

$$P_i = C_i \oplus E_k (C_{i-1}) \; i \geq 1$$

Ένα κρυπτοσύστημα σε λειτουργία CFB παρουσιάζεται στο ακόλουθο σχήμα:

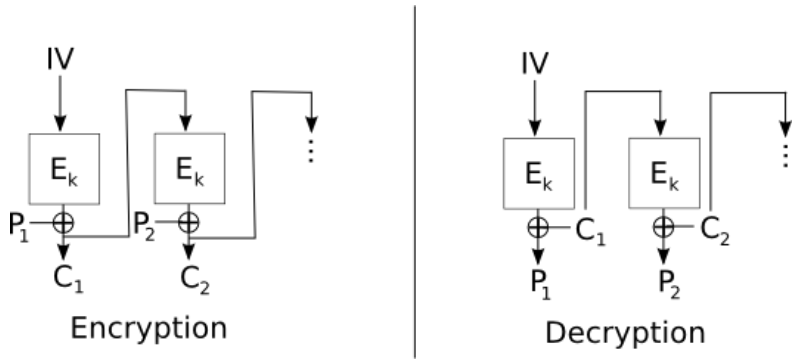

Fig 18 – CFB Mode

Η λειτουργία CFB μπορεί να θεωρηθεί ως κρυπταλγόριθμος ροής, όπου τα σύμβολα τουαπλού κειμένου είναι δυαδικές λέξεις μεγέθους n bits, που σημαίνει ότι το αλφάβητο του απλοκειμένου και του κρυπτοκειμένου αποτελείται από $2n$ σύμβολα. Επίσης σε ένα κρυπταλγόριθμο ροής, οι γεννήτριες της κλειδοροής του αποστολέα και του αποδέκτη θα πρέπει να παράγουν τηνίδια ακολουθία. Αυτό φαίνεται και από την πράξη αποκρυπτογράφησης, όπου ο κρυπταλγόριθμος τμήματος εφαρμόζεται σε λειτουργία κρυπτογράφησης και όχι αποκρυπτογράφησης.

Παρόμοια με την λειτουργία CBC, για την πλήρη εκτέλεση της CFB απαιτείται διάνυσμα αρχικοποίησης (initialization vectoror IV). Το διάνυσμα αυτό αποθηκεύεται στον καταχωρητή αποθήκευσης που τροφοδοτεί τον κρυπταλγόριθμο τμήματος. Η μετάδοσή του διανύσματος αρχικοποίησης δεν απαιτεί εμπιστευτικότητα. Αντίθετα, μπορεί να προηγηθεί του μηνύματος και να σταλεί κρυπτογραφημένο με το ίδιο το κρυπτοσύστημα της CFB. Οι δύο καταχωρητές αποθήκευσης μπορούν να έχουν μηδενικές τιμές κατά τη μετάδοση του διανύσματος αρχικοποίησης.

3.3.4.Ανάδραση Εξόδου (OFB)

Η κρυπτογράφηση πραγματοποιείται με την αποκλειστική διάζευξη του απλού κειμένου με την ακολουθία της κλειδοροής. Αντίστοιχα, η αποκρυπτογράφηση πετυχαίνετε με την αποκλειστική διάζευξη το κρυπτοκειμένου με την ακολουθία της κλειδοροής. Η διαδικασία δημιουργίας της κλειδοροής είναι ανεξάρτητη από το απλό κείμενο και το κρυπτοκείμενο. Θα μπορούσαμε να υποστηρίξουμε ότι η ασφάλεια της OFB είναι μικρότερη από την ασφάλεια των υπόλοιπων τριών τρόπων λειτουργίας και αυτό γιατί ο μόνος τρόπος διασύνδεσής του απλού κειμένου και του κρυπτοκειμένου είναι η πράξη της αποκλειστικής διάζευξης. Εφόσον η γεννήτρια κλειδοροής είναι μηχανή πεπερασμένων καταστάσεων, η κλειδοροή που παράγει θα είναι περιοδική. Επομένως υπάρχει κάποια χρονική στιγμή όπου η κλειδοροή εμφανίζει τα ίδια

κλειδιά. Αν ο αντίπαλος εντοπίσει την αρχή της περιόδου,τότε μπορεί να απομακρύνει την πληροφορία της κλειδοροής από το κρυπτοκείμενο με τον ακόλουθο τρόπο.

Η λειτουργία OFB παρουσιάζεται στο παρακάτω σχήμα:

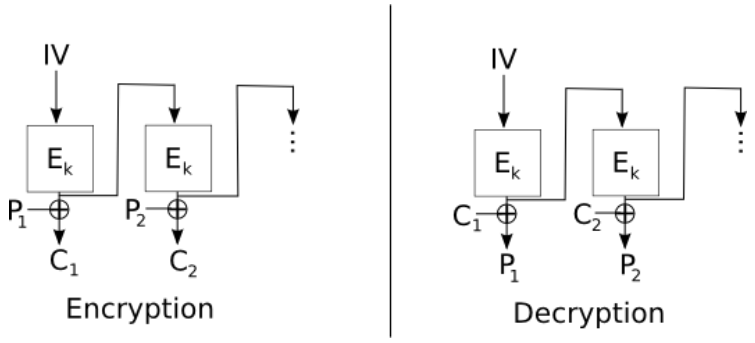

Fig 19 – OFB Mode

Έστω τα τμήματα του κρυπτοκειμένου c_i και c_j τα οποία προκύπτουν από την εφαρμογή ιδίων τμημάτων της κλειδοροής. Αν συνδυάσουμε τα κρυπτοκείμενα με αποκλειστική διάζευξηπροκύπτει ότι:

$$c_i + c_j = (p_i + k_i) + (p_j + k_i) = p_i + p_j$$

Δηλαδή, η κλειδοροή έχει εξαλειφθεί.Αν το απλό κείμενο είναι κάποια φυσική γλώσσα με υψηλή περίσσεια, τότε ο αντίπαλος μπορεί να εντοπίσει την περίοδο με στατιστικές μεθόδους. Στη συνέχεια,μπορεί να συνδυάζει με αποκλειστική διάζευξη απλά κείμενα της γλώσσας στα παραπάνω άθροισμα για να ξεχωρίσει τα και p_j. Επομένως στην περίπτωση της λειτουργίας OFB δεν υπάρχει η ίδια ελευθερία επιλογής κρυπταλγόριθμου τμήματος που υπάρχει στους υπόλοιπους τρόπους λειτουργίας. Ο κρυπταλγόριθμος τμήματος θα πρέπει από τη μια να έχει μεγάλη περίοδο, ενώ από την άλλη θαπρέπει να αλλάζει το κλειδί προτού ξεπεραστεί αυτή η περίοδος. Η αλλαγή του κλειδιού τουκρυπταλγόριθμου τμήματος θα έχει ως αποτέλεσμα η γεννήτρια κλειδοροής να μεταπίπτει σε άλλη ακολουθία κλειδοροής.

3.3.5.Τρόπος λειτουργίας μετρητή (CTR)

Η κατάσταση λειτουργίας μετρητή δεν χρησιμοποιεί τον αλγόριθμο απευθείας για την κρυπτογράφηση των δεδομένων. Αντίθετα, κρυπτογραφεί την τυχαία τιμή ενός μετρητή και στη συνέχεια εφαρμόζει την πράξη XOR ανάμεσα στο αποτέλεσμα της κρυπτογράφησης και τα δεδομένα. Με τον τρόπο αυτό προκύπτει το κρυπτογραφημένο κείμενο. Ο μετρητής γενικά αυξάνεται κατά 1 με κάθε διαδοχικό

μπλοκ που κρυπτογραφείται.

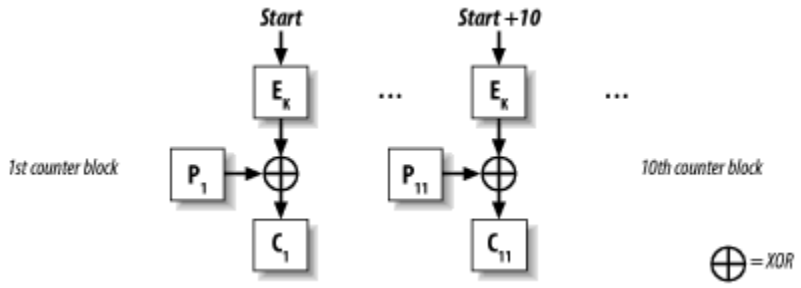

Fig 20 – CTR Mode

Επειδή ο μετρητής αλλάζει τιμή για κάθε μπλοκ αποφεύγεται το πρόβλημα που εμφανίζεται στην κατάσταση λειτουργίας ECB με τα επαναλαμβανόμενα μπλοκ. Ακόμα και αν δύο μπλοκ δεδομένων είναι πανομοιότυπα, θα συνδυαστούν με διαφορετική τιμή του μετρητή και θα προκύψει διαφορετικό αποτέλε-σμα για κάθε μπλοκ. Παρόλα αυτά, με τον τρόπο που παρουσιάζεται, η μέθοδος αυτή έχει ως αποτέλεσμα δύο ίδια, αλλά ξεχωριστά μηνύματα, να παρουσιάζουν το ίδιο αποτέλεσμα μετά την κρυπτογράφηση. Για το λόγο αυτό, στην πράξη, ο μετρητής δεν ξεκινάει από την τιμή 1. Τυπικά, αρχικοποιείται με μία τιμή η οποία αλλάζει για κάθε διαδοχικό μήνυμα (nonce).

Η αποκρυπτογράφηση είναι ακριβώς η ίδια διαδικασία με την κρυπτογράφηση, καθώς η εφαρμογή της πράξης XOR δύο φορές στα ίδια δεδομένα επιστρέφει τα αρχικά δεδομένα. Αυτό σημαίνει ότι οι διάφορες υλοποιήσεις πρέπει να υλοποιήσουν μόνο τον αλγόριθμο κρυπτογράφησης και όχι τον αλγόριθμο αποκρυπτογράφησης.

Για ορισμένες εφαρμογές, η κρυπτογράφηση μπορεί να πραγματοποιηθεί παράλληλα. Εφόσον όλες οι τιμές του μετρητή είναι γνωστές εκ των προτέρων, μπορούμε να έχουμε μία τράπεζα από μονάδες κρυπτογράφησης ώστε να κρυπτογραφήσουμε ολόκληρο το μήνυμα σε ένα μόνο πέρασμα. Αυτό δεν ισχύει για πολλές από τις υπόλοιπες καταστάσεις λειτουργίας.

Τέλος στην κατάσταση λειτουργίας μετρητή δεν παίζει ρόλο αν το μήνυμα δεν αποτελείται από ακριβή αριθμό μπλοκ. Απλά παίρνουμε το τελευταίο (μη συ-μπληρωμένο) μπλοκ και εφαρμόζουμε την πράξη XOR με την κρυπτογραφημένη τιμή του μετρητή, χρησιμοποιώντας μόνο τον αριθμό από bits που είναι αναγκαίος. Επομένως, το μήκος του κρυπτογραφημένου μηνύματος μπορεί να είναι το ίδιο ακριβώς με το αρχικό μήνυμα. Επειδή κάθε πράξη σε μπλοκ εξαρτάται από την κατάσταση του μετρητή από το προηγούμενο μπλοκ, η κα-τάσταση λειτουργίας μετρητή αποτελεί ουσιαστικά, κρυπτογράφηση ροής

(stream cipher).

3.4. Ασφάλεια DES

Ο DES θεωρείται πλέον ανασφαλής για πολλές εφαρμογές. Αυτό οφείλεται κυρίως στο μικρό μέγεθος του κλειδιού του, που έχει μήκος 56 bits. Τον Ιανουάριο του 1999 οι εταιρείες *Distributed.net* και *Electronic Frontier Foundation*, κατόπιν συνεργασίας, "έσπασαν" δημοσίως ένα κλειδί του DES μέσα σε 22 ώρες και 15 λεπτά. Υπάρχουν, επίσης, ορισμένα αναλυτικά αποτελέσματα που καταδεικνύουν θεωρητικές αδυναμίες στον κρυπταλγόριθμο, αν και είναι ανέφικτο να υλοποιηθούν στην πράξη. Θεωρείται πως ο αλγόριθμος είναι πρακτικά ασφαλής υπό τη μορφή του τριπλού DES (tripleDES), αν και υπάρχουν θεωρητικές αμφισβητήσεις. Τα τελευταία χρόνια ο κρυπταλγόριθμος DES έχει εκτοπιστεί από το Προηγμένο Πρότυπο Κρυπτογράφησης (AdvancedEncryptionStandard - AES).

Αν και οι περισσότερες πληροφορίες που έχουν δημοσιευθεί αφορούν στην κρυπτανάλυση του DES απ' ότι οποιουδήποτε άλλου blockcipher, η πρακτικότερη επίθεση μέχρι και σήμερα είναι ακόμα η προσέγγιση *bruteforce* (ωμής βίας). Είναι γνωστές διάφορες δευτερεύουσες κρυπταναλυτικές ιδιότητες και τρεις θεωρητικές επιθέσεις είναι δυνατές˙ που ακόμα κι αν έχουν μια θεωρητική πολυπλοκότητα μικρότερη από την επίθεση bruteforce, απαιτείται να φέρουν ιλιγγιώδες μέγεθος γνωστών ή προεπιλεγμένων plaintext και δεν αποτελούν, στην πράξη, πηγή ανησυχίας.

3.4.1. Brute force attack

Για οποιοδήποτε κρυπταλγόριθμο, η πιο βασική μέθοδος επίθεσης είναι η brute force, δοκιμάζοντας συνεχόμενα κάθε πιθανό κλειδί. Το μήκος του κλειδιού καθορίζει το πλήθος των πιθανών κλειδιών και ως εκ τούτου την δυνατότητα πραγματοποίησης αυτής της προσέγγισης. Τέθηκαν από νωρίς ερωτήσεις για την επάρκεια του μήκους κλειδιού του DES, πριν ακόμα υιοθετηθεί ως πρότυπο. Το μικρό μήκος κλειδιού ήταν αυτό που, στην ουσία, υπαγόρευση την ανάγκη για την αντικατάσταση του αλγόριθμου, παρά η θεωρητική κρυπτανάλυση. Είναι γνωστό ότι η NSA ενθάρρυνε, αν δεν έπεισε, την IBM για να μειώσει το μήκος του κλειδιού από τα 128 στα 64 μπιτς και από εκεί σε 56 μπιτς. Αυτό λαμβάνεται συχνά ως ένδειξη ότι η NSA σκέφτηκε ότι θα ήταν σε θέση να "σπάσει" κλειδιά αυτού του μήκους ακόμη και στα μέσα της δεκαετίας του '70.

Στον ακαδημαϊκό κόσμο έγιναν διάφορες προηγμένες προτάσεις για μια μηχανή που θα αποσκοπούσε στο να "σπάει" τον DES. Το 1977, οι Diffie και Hellman πρότειναν μια μηχανή που θα στοίχιζε, κατ' εκτίμηση, 20 εκατομμύρια δολάρια, η οποία θα μπορούσε να βρει ένα κλειδί DES σε μία και μόνο ημέρα. Μέχρι το 1993, ο Wiener

είχε προτείνει μια μηχανή αναζήτησης κλειδιού με κοστολόγηση 1 εκατομμύριο δολάρια, που θα έβρισκε ένα κλειδί μέσα σε 7 ώρες. Εντούτοις, καμία από αυτές τις πρόωρες προτάσεις δεν εφαρμόστηκε· τουλάχιστον καμία εφαρμογή δεν αναγνωρίστηκε δημόσια. Η ευπάθεια του DES επιδείχθηκε πρακτικά προς το τέλος της δεκαετίας του '90. Το 1997, η εταιρεία RSA Security υποστήριξε μια σειρά διαγωνισμών με βραβείο $10.000 στην πρώτη ομάδα που θα "έσπαζε" ένα μήνυμα, το οποίο είχε κρυπτογραφηθεί με τον DES. Τον διαγωνισμό κέρδισε το πρόγραμμα DESCHALL, που δημιουργήθηκε από τους Rocke Verser, Matt Curtin, και Justin Dolske, χρησιμοποιώντας ιδανικούς κύκλους χιλιάδων υπολογιστών σε ολόκληρο το Διαδίκτυο. Η δυνατότητα πραγματοποίησης του "σπασίματος" του DES καταδείχθηκε γρήγορα το 1998 όταν φτιάχτηκε μια ρουτίνα "σπασίματος" του DES από την EFF (Electronic Frontier Foundation), μια ομάδα αστικών δικαιωμάτων του Κυβερνοχώρου, με κόστος περίπου $250,000. Το κίνητρό τους ήταν να δείξουν ότι ο DES ήταν το ίδιο εύθραυστος στην πράξη όπως και στην θεωρία. Δείχνοντάς τους μία φυσική μηχανή που μπορεί να "σπάσει" τον DES σε μερικές ημέρες είναι ο μόνος τρόπος να πειστούν μερικοί άνθρωποι ότι δεν μπορούν να εμπιστευθούν την ασφάλειά τους στον DES.

Η μηχανή εμφάνισε ένα κλειδί με χρήση brute force σε κάτι περισσότερο από 2 ημέρες. Περίπου στον ίδιο χρόνο ένας πληρεξούσιος του αμερικανικού Υπουργείου Δικαιοσύνης ανήγγελλε ότι ο DES δεν ήταν δυνατό να παραβιαστεί.

Η μόνη άλλη επιβεβαιωμένη μηχανή που "έσπαζε" τον DES ήταν η μηχανή COPACOBANA (σύντμηση του βέλτιστου κόστους και παράλληλα ενός code breaker) που δημιουργήθηκε πιο πρόσφατα από τις ομάδες των πανεπιστημίων του Μπόχουμ και του Κίελου της Γερμανίας. Αντίθετα από τη μηχανή της EFF, η COPACOBANA αποτελείται από εμπορικά διαθέσιμα, ανασχηματισμένα ολοκληρωμένα κυκλώματα. 120 αυτών των FPGAs του τύπου XILINX Spartan3-1000 τρέχουν σε παράλληλη σύνδεση. Ομαδοποιούνται σε 20 DIMM ενότητες, που κάθε μια περιέχει 6 FPGAs. Η χρήση των ανασχηματισμένων υλικών κάνει την μηχανή να βρισκει εφαρμογή και σε άλλες λειτουργίες για "σπάσιμο" κωδικών. Η Εικόνα 5 δείχνει μία πλήρη μηχανή COPACOBANA. Μια από τις πιό ενδιαφέρουσες πτυχές COPACOBANA είναι ο παράγοντας του κόστους της. Μια μηχανή μπορεί να κατασκευαστεί με κόστος περίπου $10.000. Η μείωση κόστους από έναν, κατά προσέγγιση, παράγοντα της τάξης του 25% από αυτή της μηχανής της EFF είναι ένα εντυπωσιακό παράδειγμα για τη συνεχή βελτίωση του ψηφιακού υλικού. Κατά ενδιαφέροντα τρόπο, ο νόμος του Moore προβλέπει μια βελτίωση της τάξης περίπου 32%, δεδομένου ότι περίπου οκτώ έτη έχουν μεσολαβήσει μεταξύ του σχεδιασμού των δύο μηχανών, πράγμα το οποίο επιτρέπει περίπου πέντε διπλασιασμούς της ισχύος των υπολογιστών (ή 5 μειώσεις τις τάξεως του 50% του κόστους για τον ίδιο υπολογισμό).

3.4.2.Επιθέσεις ταχύτερες από την brute - force

Υπάρχουν τριων ειδών επιθέσεις που είναι γνωστό οτι μπορούν να "σπάσουν" ΚΑΙ τους δέκα έξι γύρους του DES με λιγότερη πολυπλοκότητα από μια αναζήτηση brute force:

- Η Διαφορική Κρυπτανάλυση (Differential Cryptanalysis – DC)
- Η Γραμμική Κρυπτανάλυση (Linear Cryptanalysis - LC) και τέλος
- Η επίθεση του Davie (Davies' Attack)

Εντούτοις, οι επιθέσεις είναι θεωρητικές και είναι αδύνατο να εφαρμοστούν στην πράξη. Τέτοιου είδους επιθέσεις καλούνται μερικές φορές Certificational Weaknesses

Κεφάλαιο 4 – Advanced Encryption Standard (AES)

Σε αυτό το κεφάλαιο, θα παρουσιαστούν τα θεμελιώδη στοιχεία του Advanced Encryption Standard (AES) αλγορίθμου.

4.1. Ιστορικά στοιχεία

Στις αρχές της δεκαετίας του 1990 η ραγδαία αύξηση της υπολογιστικής ισχύος, σε συνδυασμό με την μείωση του κόστους των υπολογιστικών συστημάτων, κατέστησε τον DES ευάλωτο σε κρυπταναλυτικές επιθέσεις. Ως προσωρινό μέτρο δημιουργήθηκε μία ασφαλέστερη παραλλαγή του DES, ο triple-DES, ο οποίος εξακολουθούσε να είναι ευάλωτος, παρ' ότι ασφαλέστερος του DES. Υπό τις συνθήκες αυτές, εκρίθη απαραίτητη η υιοθέτηση ενός νέου κρυπτογραφικού προτύπου.

Τον Ιανουάριο του 1997, το «Εθνικό Ινστιτούτο Προτύπων & Τεχνολογίας» των ΗΠΑ (National Institute of Standards and Technology, NIST) προκήρυξε διεθνή διαγωνισμό για την υιοθέτηση του νέου κρυπτογραφικού προτύπου εμπορικής (μη κυβερνητικής) χρήσεως, του AES. Για πρώτη φορά στα χρονικά της σύγχρονης κρυπτογραφίας οι διαδικασίες αξιολογήσεως και επιλογής των υποψηφίων προτάσεων θα ήταν ανοικτές.

Τον Σεπτέμβριο του 1997 δημοσιοποιήθηκαν η τελική προκήρυξη, καθώς και οι προδιαγραφές που έπρεπε να πληροί ο AES. Οι βασικότερες ήταν:

1. Ο αλγόριθμος έπρεπε να είναι συμμετρικός, τμήματος (block cipher).
2. Η πλήρης σχεδίαση θα έπρεπε να δημοσιοποιηθεί.
3. Ο αλγόριθμος έπρεπε να υποστηρίζει μήκη κλειδιών 128, 192 και 256 bits.
4. Έπρεπε να είναι εφικτή – και σχετικώς απλή – η υλοποίηση του αλγορίθμου τόσο με λογισμικό (software), όσο και με υλικό (hardware).
5. Η χρήση του αλγορίθμου θα ήταν ελεύθερη, χωρίς να απαιτείται κάποια συγκεκριμένη άδεια χρήσεως.

Κατετέθησαν 15 συνολικώς προτάσεις οι οποίες θα υπεβάλλοντο σε δύο γύρους αξιολογήσεων. Ο πρώτος γύρος ξεκίνησε με το Α΄ συνέδριο για το πρότυπο AES (Αύγουστος 1998) και κατέληξε στην απόρριψη των 5 εκ των 15 υποψηφίων προτάσεων. Τον Μάρτιο του 1999 ξεκίνησε ο δεύτερος γύρος με το Β΄ συνέδριο για το πρότυπο AES για να καταλήξουμε στην απόρριψη άλλων 5 προτάσεων, τον Αύγουστοτου 1999. Τελικώς από τις 5 εναπομείνασες προτάσεις ως πρότυπο AES επελέγη ο αλγόριθμος Rijndael, που ανεπτύχθη από τους Βέλγους ερευνητές Joan Daemen και Vincent Rijmen. Η επίσημη ανακοίνωση της επιλογής του Rijndael έγινε στις 2 Οκτωβρίου 2000.

4.2. Περιγραφή αλγορίθμου (AES)

Ο *Advanced Encryption Standard* (AES) εκδόθηκε από το *National Institute of Standards and Technology* (NIST) το 2001. Ο αλγόριθμος AES είναι ένας επαναληπτικός κρυπταλγόριθμος τμήματος και ανήκει στην οικογένεια των συμμετρικών αλγόριθμων κρυπτογραφίας, όπου και ο αποστολέας και ο παραλήπτης συμφωνούν σε ένα κοινό μυστικό κλειδί για την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης. Το απλό κείμενο κατατέμνεται σε δέσμες (blocks) των 128 bits (16 bytes), ενώ το κλειδί μπορεί να έχει μήκος 128, 192 ή 256 bits (16, 24 ή 32 bytes), αναλόγως με το επιθυμητό επίπεδο ασφαλείας. Ο αλγόριθμος AES-128 είναι ο επικρατέστερος και υποστηρίζεται από τις περισσότερες hardware υλοποιήσεις. Η διαφοροποίηση του AES σε σχέση προς το αρχικό πρότυπο Rijndael, το οποίο υπεστήριζε μεταβλητά μήκη τόσο για το κλειδί, όσο και για τα τμήματα του απλού κειμένου. Τα μήκη αυτά μπορούσαν να λάβουν οποιαδήποτε τιμή, πολλαπλάσια του 32, μεταξύ 128 και 256 (σε bits).

Άρα το πρότυπο AES ορίζει ότι τα μπλοκ που επεξεργάζεται ο αλγόριθμος έχουν μέγεθος 128 bits και αυτό ορίζεται από την ποσότητα $Nb = 4$, που συμβολίζει τον αριθμό των 32-bit λέξεων στο μπλοκ. Από την άλλη, τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση, μπορούν να έχουν μήκος 128, 192 ή 256 bits. Η μεταβλητή Nk συμβολίζει τον αριθμό των 32-bit λέξεων που μπορεί να περιλαμβάνει ένα κλειδί και κατά συνέπεια μπορεί να πάρει τις τιμές 4, 6 και 8.

Ανάλογα με το μήκος κλειδιού που θα επιλεχθεί για την κρυπτογράφηση, ο αλγόριθμος ορίζει έναν αριθμό από γύρους επεξεργασίας που απαιτούνται για την ολοκλήρωση της. Η μεταβλητή Nr χρησιμοποιείται για να δηλώσει το πλήθος των γύρων. Αν χρησιμοποιηθεί μήκος κλειδιού 128 bits τότε απαιτούνται 10 γύροι επεξεργασίας. Για μήκη κλειδιού ίσα με 192 και 256 bits απαιτούνται αντίστοιχα 12 και 14 γύροι.

Να σημειωθεί ότι οι παραπάνω συνδυασμοί μήκους μπλοκ, μήκους κλειδιού και γύρων επεξεργασίας είναι αυτοί που ορίζονται αυστηρά στο πρότυπο AES. Ο αλγόριθμος κρυπτογράφησης Rijndael στον οποίο βασίζεται ο AES δίνει την δυνατότητα πραγματοποίησης περισσότερων συνδυασμών. Έτσι, καταλαβαίνει κανείς ότι ο AES ουσιαστικά ορίζει ένα υποσύνολο του αλγορίθμου Rijndael.

Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Για την ακρίβεια, χρησιμοποιούνται 4 τύποι μετασχηματισμών :

1. ένας μετασχηματισμός αντικατάστασης bytes χρησιμοποιώντας κάποιον σχετικό πίνακα αντικατάστασης (SubBytes)
2. ένας μηχανισμός ολίσθησης των bytes της State κατά διαφορετικά offsets (ShiftRows)

3. μια διαδικασία ανάμειξης των bytes της State (MixColums)
4. μια πρόσθεση ενός κλειδιού στην State (AddRoundKey)

Στον AES, το απλό κείμενο (Plain Text), το κρυπτοκείμενο (Cipher Text) και το κλειδί (Key) αναπαρίστανται ως πίνακες 4 γραμμών, κάθε στοιχείο των οποίων αποτελείται από ένα byte.

Εαν το 128 bit κείμενο εισόδου ειναι:

$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \dots, a_{3,3}$ όπου τα$a_{i,j}$, $0 \leq i, j \leq 3$ παριστάνουν ένα byte,

Ο πίνακας που δημιουργείται είναι ο ακόλουθος:

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$$

Πολλαπλασιασμός στο $GF(2^8)$. Είναι ο πολλαπλασιασμός μεταξύ πολυωνύμων modulo ένα irreducible πολυώνυμο βαθμού 8. Irreducible ονομάζεται ένα πολυώνυμο αν διαιρείται μονάχα από τον εαυτό του και την μονάδα. Το πολυώνυμο που έχει επιλεχθεί για το AES είναι το :

$$m_{(x)} = x^8 + x^4 + x^3 + x + 1$$

Η modulo πράξη εξασφαλίζει ότι το πολυώνυμο που θα προκύψει θα είναι ένα δυαδικό πολυώνυμο βαθμού μικρότερου του 8, άρα θα μπορεί να αναπαρασταθεί από ένα byte. Να σημειωθεί ότι το ουδέτερο στοιχείο της πράξης είναι το $\{01\}$ και ότι το σύμβολο που χρησιμοποιείται για να διακρίνει την πράξη αυτή από έναν κοινό αριθμητικό πολλαπλασιασμό είναι το$\otimes$.

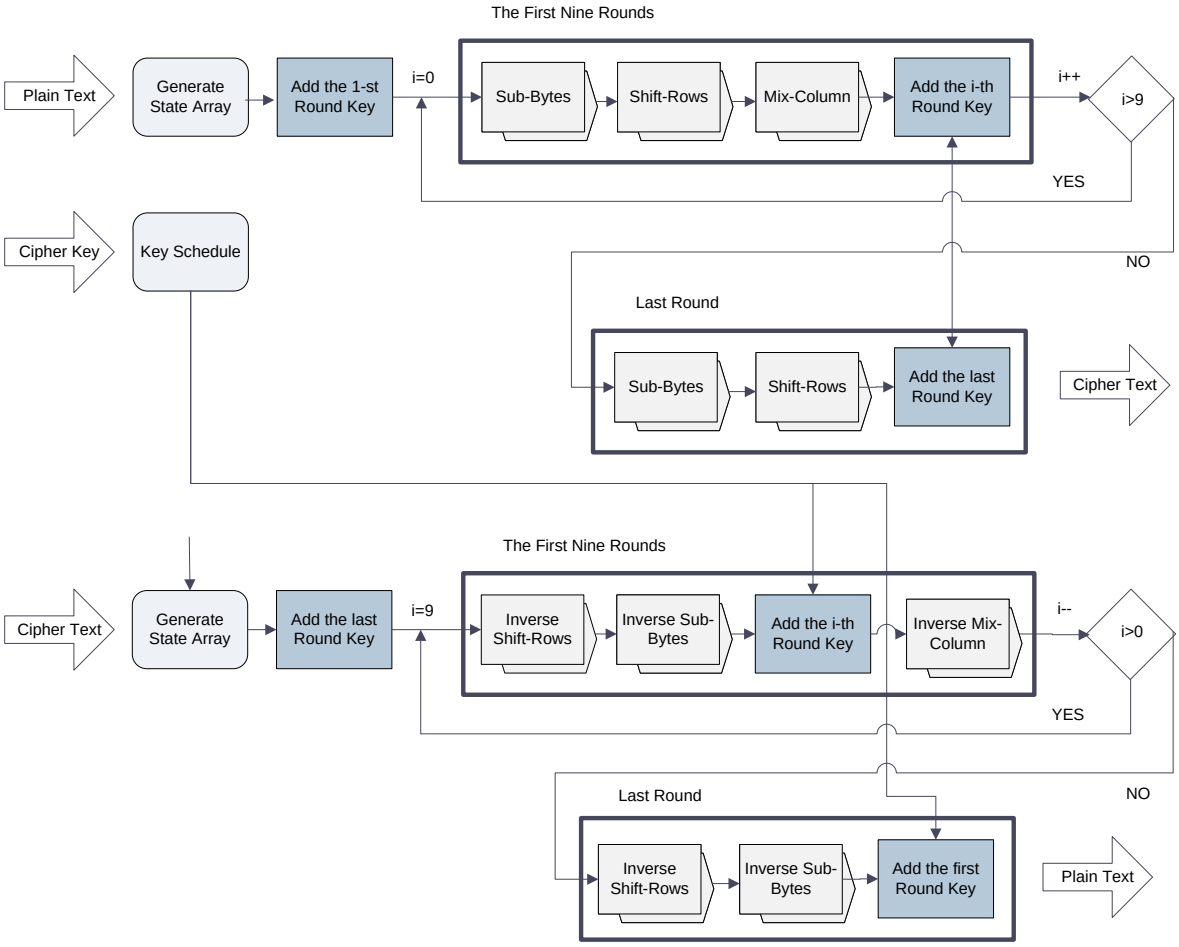

Fig 21 – Structure of Basic AES algorithm (Nr=10)

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])

begin

        byte state[4,Nb]

        state = in

        AddRoundKey(state, w[0, Nb-1])

        for round = 1 step 1 to Nr−1

                SubBytes(state)

                ShiftRows(state)

                MixColumns(state)

                AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])

        end for

        SubBytes(state)

        ShiftRows(state)

        AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

        out = state

end
```

Fig 22 – Ψευδοκώδικαςκρυπτογράφησης AES

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])

begin

        byte state[4,Nb]

        state = in

        AddRoundKey(state, w[Nr*Nb,(Nr+1)*Nb-1])

        for round = Nr−1 step -1 downto 1

                InvShiftRows(state)

                InvSubBytes(state)

                AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])

                InvMixColumns(state)

        end for

        InvShiftRows(state)

        InvSubBytes(state)

        AddRoundKey(state, w[0, Nb-1])

        out = state

end
```

Fig 23 – Ψευδοκώδικαςαποκρυπτογράφησης AES

Αυτό που πρέπει να διευκρινιστεί είναι η έννοια της πρόσθεσης στον AES αλγόριθμο. Τα bytes της πληροφορίας κατά την επεξεργασία τους λαμβάνονται ως πολυώνυμα. Έτσι, η πράξη της πρόσθεσης είναι ουσιαστικά μια διαδικασία πρόσθεσης πολυωνύμων. Η πρόσθεση μεταξύ πολυωνύμων πραγματοποιείται με την πρόσθεση των συντελεστών των αντίστοιχων όρων (δυνάμεων) των πολυωνύμων. Η πρόσθεση γίνεται modulo-2, δηλαδή μέσω μιας XOR πράξης. Να υπενθυμισθεί ότι η XOR πράξη μεταξύ δύο bits (συμβολίζεται με $\oplus$) έχει τον εξής πίνακα αληθείας :

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 0 &= 1 \\ 1 \oplus 1 &= 0 \end{aligned}$$

Η δεικτοδότηση των bits και των bytes στα μπλοκ και στα κλειδιά γίνεται σύμφωνα με τον παρακάτω πίνακα:

Σειρά εισόδου bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	...
Αριθμός Byte	0								1								2								...
Σειρά bit στο byte	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	...

Fig 24 – Δεικτοδότηση bits και bytes

4.2.1.Μετασχηματισμός SubBytes

Αποτελεί έναν μη γραμμικό μετασχηματισμό όπου κάθε byte αντικαθίσταται σύμφωνα με έναν πίνακα αντικατάστασης (S-Box) διαστάσεων 16x16. Κάθε στοιχείο του πίνακα εισόδου μετατρέπεται σε 8 bitμορφή abcdefgh. Το στοιχείο του πίνακα αντικατάστασης που ανήκει στην 'abcd' γραμμή και στην'efgh' στήλη είναι η τιμή αντικατάστασης.Αν για παράδειγμα το στοιχείο εισόδου είναι το 10001011 και η αρίθμηση των γραμμών/στηλών είναι 0-15, ο μετασχηματισμός ψάχνει την 8 $(2^3 + 0^2 + 0^1 + 0^0)$ γραμμή και την 11 $(2^3 + 0^2 + 2^1 + 2^0)$ στήλη. Η τιμή αντικατάστασης είναι το 61 με δυαδική μορφή 111101.

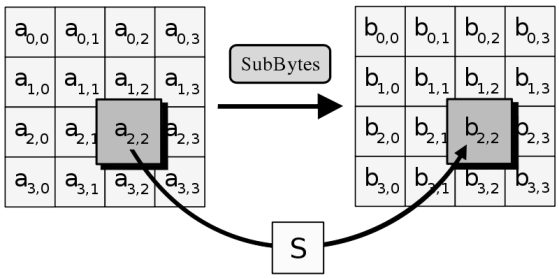

Fig 25 – Μετασχηματισμός SubBytes

Μαθηματικά περιγράφεται ως:

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \xrightarrow{SubBytes} \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}, \; b_{i,j} = S(a_{i,j}), \; 0 \le i,j \le 3$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
1	202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
2	183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
3	4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
4	9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
5	83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
6	208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
7	81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
8	205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
9	96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
10	224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
11	231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
12	186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
13	112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
14	225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
15	140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Fig 26 – S-Box Πίνακας αντικατάστασης δεκαδικής μορφής

Ουσιαστικά τα βήματα του μετασχηματισμού είναι τα εξής:

1. Παίρνουμε τον πολλαπλασιαστικό αντίστροφο στο πεπερασμένο πεδίο $GF(2^8)$με το στοιχείο $\{00\}$ να αντιστοιχίζεται στον εαυτό του.
2. Εφαρμόζουμε τον ακόλουθο μετασχηματισμό ($GF(2)$):

$$b_i = a_i \oplus a_{(i+4)mod8} \oplus a_{(i+5)mod8} \oplus a_{(i+6)mod8} \oplus a_{(i+7)mod8} \oplus c_i$$

για $0 \le i \le 7$, όπου a_i είναι το i-οστό bit του byte ($a_7a_6a_5a_4a_3a_2a_1a_0$) , καιc_i είναι το i-οστό bit του byte c με την τιμή $\{63\}$ or $\{01100011\}$.

```
SubBytes(a7a6a5a4a3a2a1a0)

external FieldInv, BinaryToField, FieldToBinary

z ← BinaryToField(a7a6a5a4a3a2a1a0)

if z ≠ 0

then z ← FieldInv(z)

(a7a6a5a4a3a2a1a0) ← FieldToBinary(z)

(c7c6c5c4c3c2c1c0) ← (01100011)

for i ← 0 to 7

do bi ← (ai + a(i+4)mod8 + a(i+5)mod8 + a(i+6)mod8 + a(i+7)mod8 + ci) mod 2

return (b7b6b5b4b3b2b1b0)
```

Fig 27 – Ψευδοκώδικας SubBytes

Ο μετασχηματισμός InvSubBytes όπως δηλώνει και το όνομα του, είναι ο αντίστροφος του μετασχηματισμού αντικατάστασης bytes της κρυπτογράφησης. Έτσι, στην περίπτωση αυτή, αντί για το S-Box πίνακα χρησιμοποιείται ο αντίστροφος του (inverse S-Box).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	82	9	106	213	48	54	165	56	191	64	163	158	129	243	215	251
1	124	227	57	130	155	47	255	135	52	142	67	68	196	222	233	203
2	84	123	148	50	166	194	35	61	238	76	149	11	66	250	195	78
3	8	46	161	102	40	217	36	178	118	91	162	73	109	139	209	37
4	114	248	246	100	134	104	152	22	212	164	92	204	93	101	182	146
5	108	112	72	80	253	237	185	218	94	21	70	87	167	141	157	132
6	144	216	171	0	140	188	211	10	247	228	88	5	184	179	69	6
7	208	44	30	143	202	63	15	2	193	175	189	3	1	19	138	107
8	58	145	17	65	79	103	220	234	151	242	207	206	240	180	230	115
9	150	172	116	34	231	173	53	133	226	249	55	232	28	117	223	110
10	71	241	26	113	29	41	197	137	111	183	98	14	170	24	190	27
11	252	86	62	75	198	210	121	32	154	219	192	254	120	205	90	244
12	31	221	168	51	136	7	199	49	177	18	16	89	39	128	236	95
13	96	81	127	169	25	181	74	13	45	229	122	159	147	201	156	239
14	160	224	59	77	174	42	245	176	200	235	187	60	131	83	153	97
15	23	43	4	126	186	119	214	38	225	105	20	99	85	33	12	125

Fig 28 – S-Box Πίνακας αντίστροφης αντικατάστασης δεκαδικής μορφής

4.2.2.Μετασχηματισμός ShiftRows

Αποτελεί βήμα αλληλομετάθεσης όπου κάθε γραμμή απότονπίνακα εισόδου ολισθαίνει κυκλικά για ένα συγκεκριμένο αριθμό θέσεων.

Γραμμή πίνακα	1	2	3	4
Θέσεις ολισθήσεως	0	1	2	3

Μαθηματικά περιγράφεται ως:

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \xrightarrow{ShiftRows} \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{bmatrix}$$

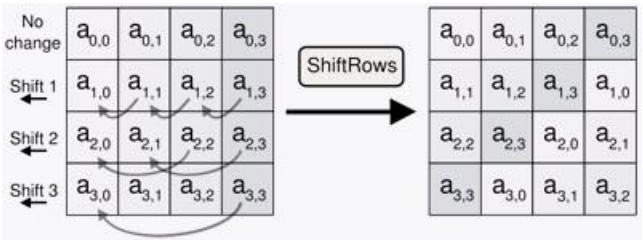

Fig 29 – ShiftRows Step

Ο μετασχηματισμός InvShiftRows είναι ο αντίστροφος του μετασχηματισμού ShiftRows της κρυπτογράφησης και περιγράφεται από την σχέση:

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \xrightarrow{InvShiftRows} \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,3} & a_{1,0} & a_{1,1} & a_{1,2} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,0} \end{bmatrix}$$

4.2.3.Μετασχηματισμός MixColumns

Ο μετασχηματισμός εφαρμόζεται σε κάθε στήλη του State καιαναπαριστά ένα γραμμικό μετασχηματισμό βασισμένο στα 4 bytes τηςστήλης.

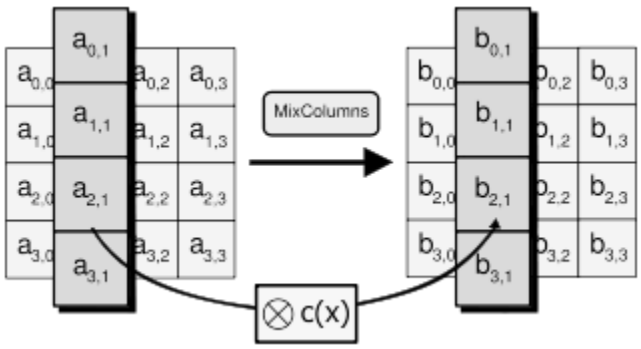

Fig 30 – MixColumns Step

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} = [A_0 A_1 A_2 A_3]$$

Ένα διάνυσμα $\alpha(x)_\iota = [\alpha_0, \alpha_1, \alpha_2, \alpha_3]^T$θεωρείται ως ένα πολυώνυμο 3ου βαθμού, ορισμένο επί του $GF(2^8)$. Άρα:

$$\alpha(x)_i = a_{3,i} \cdot x^3 + a_{2,i} \cdot x^2 + a_{1,i} \cdot x + a_{0,i}$$

Επειδή το πολυώνυμο $l(x) = x^4 + 1$ που χρησιμοποιείται για την αναγωγή των αποτελεσμάτων του πολλαπλασιασμού στο$GF(2^8)$,δεν είναι ανάγωγο στο σώμα αυτό, στην συνάρτηση MixColumns ο πολλαπλασιασμός πραγματοποιείται επί το σταθερό πολυώνυμο:

$$c(x) = \{03\}_{(16)} \cdot x^3 + \{01\}_{(16)} \cdot x^2 + \{01\}_{(16)} \cdot x + \{02\}_{(16)}$$

το οποίο δεν έχει κοινούς παράγοντες με το $l(x)$. Έτσι ο πολλαπλασιασμός καθίσταται αντιστρέψιμος.

Μαθηματικά περιγράφεται ως:

$$b(x) = c(x) \otimes \alpha(x) \leftrightarrow \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} \{02\}_{(16)} & \{03\}_{(16)} & \{01\}_{(16)} & \{01\}_{(16)} \\ \{01\}_{(16)} & \{02\}_{(16)} & \{03\}_{(16)} & \{01\}_{(16)} \\ \{01\}_{(16)} & \{01\}_{(16)} & \{02\}_{(16)} & \{03\}_{(16)} \\ \{03\}_{(16)} & \{01\}_{(16)} & \{01\}_{(16)} & \{02\}_{(16)} \end{bmatrix} \otimes \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Για την αντίστροφη διαδικασία InvMixColumns πρέπει να υπολογισθεί το σταθερό πολυώνυμο $c'(x)$, τέτοιο ώστε:

$$c(x) \otimes c'(x) = 1 \leftrightarrow c'(x) = c^{-1}(x)(mod(x^4 + 1))$$

Τελικά:

$$c(x) = \{0B\}_{(16)} \cdot x^3 + \{0D\}_{(16)} \cdot x^2 + \{09\}_{(16)} \cdot x + \{0E\}_{(16)}$$

$$a(x) = c'(x) \otimes b(x) \leftrightarrow \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} \{0E\}_{(16)} & \{0B\}_{(16)} & \{0D\}_{(16)} & \{09\}_{(16)} \\ \{09\}_{(16)} & \{0E\}_{(16)} & \{0B\}_{(16)} & \{0D\}_{(16)} \\ \{0D\}_{(16)} & \{09\}_{(16)} & \{0E\}_{(16)} & \{0B\}_{(16)} \\ \{0B\}_{(16)} & \{0D\}_{(16)} & \{09\}_{(16)} & \{0E\}_{(16)} \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

4.2.4.Μετασχηματισμός AddRoundKey

Ο μετασχηματισμός αυτός επιβάλει την πρόσθεση της τιμής της ποσότητας roundkey στα bytes των στηλών του πίνακα State. Επειδή κάθε τιμή του roundkey αποτελείται από Nb λέξεις, επιλέγεται κάθε φορά η επιθυμητή λέξη. Η πράξη αυτή υλοποιείται σαν απλή XOR πράξη ανάμεσα στα bits των ποσοτήτων (bitwise XOR). Η πράξη αυτή μεταφράζεται μαθηματικά στην εξής σχέση:

$$[b_{0,i}, b_{1,i}, b_{2,i}, b_{3,i}] = [a_{0,i}, a_{1,i}, a_{2,i}, a_{3,i}] \oplus [W_{round+Nb+i}], 0 \leq \mathrm{i} < Nb$$

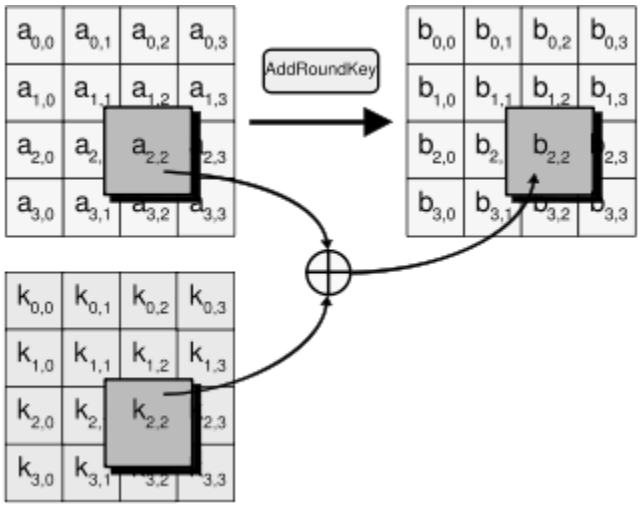

Fig 31 – AddRoundKey Step

4.3. Επέκταση κλειδιού

Η επέκταση κλειδιού ειναι μια διαδικασία κατά την οποία από τα bytestou αρχικού κλειδιού $k_i, 0 \leq i < 4 \cdot Nk$ προκύπτουν τα bytestou επεκταμένου κλειδιού w_i, $0 \leq i < Nb(Nr+1)$. Η επέκταση κλειδιού είναι μία αναδρομική διαδικασία. Η διαδικασία γίνεται πολυπλοκότερη όταν $Nk > 6$. Βασικός παράγων στην επέκταση κλειδιού είναι η ενσωμάτωση σε αυτήν μη γραμμικότητος, η οποία επιτυγχάνεται με την χρησιμοποίηση της συναρτήσεως SubBytes.

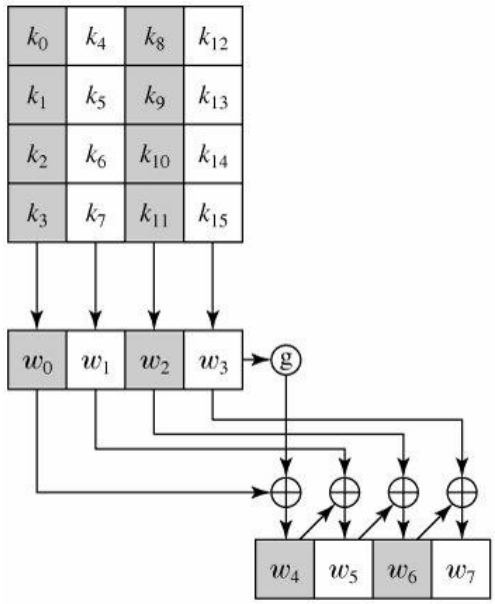

Fig 32 – Επέκταση κλειδιού

Στην επέκταση κλειδιού συμμετέχουν, για την απαλοιφή πιθανών συμμετριών κάποιες σταθερές, οι οποίες ονομάζονται σταθερές γύρου (round constants ή RCon) και ορίζονται αναδρομικώς ως εξής:

$$RCon_{[1]} = x^0 = 01_{(16)}$$

$$RCon_{[2]} = x^1 = 02_{(16)}$$

Για $i > 2$

$$RCon_{[i]} = x^{i-1} = x \otimes RCon_{[i-1]} = 02_{(16)} \otimes RCon_{[i-1]}$$

Λόγω του τρόπου χρήσεως των σταθερών γύρου στην επέκταση κλειδιού,οι δυνατές τιμές των σταθερώνγύρου είναι οι:

i	$RCon_{[i]}$ HEX	$RCon_{[i]}$ DEC
1	01	1
2	02	2
3	04	4
4	08	8
5	10	16
6	20	32
7	40	64
8	80	128
9	1B	27
10	36	54

Fig 33 – Πίνακας $RCon_{[i]}$

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)

begin

        word temp

        i = 0

        while (i < Nk)

                w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])

                i = i+1

        end while

        i = Nk

        while (i < Nb * (Nr+1)]

                temp = w[i-1]

                if (i mod Nk = 0)

                        temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]

                else if (Nk > 6 and i mod Nk = 4)

                        temp = SubWord(temp)

                end if

                w[i] = w[i-Nk] xor temp

                i = i + 1

        end while

end
```

Fig 34 – Ψευδοκώδικας Επέκτασης κλειδιού

Στον αλγόριθμο επέκτασης κλειδιού φαινονται να συμμετέχουν οι παρακάτω

συναρτήσεις:

Η διαδικασία *SubWord()* εκτελεί ουσιαστικά την ίδια διαδικασία με την συνάρτηση SubByte μόνο που αυτή την φορά προσδιορίζεται η αντίστοιχη τιμή μιας ολόκληρης λέξης, δηλαδή 4 bytes, μέσω του πίνακα S-box. Είναι, τελικά, σαν να εκτελείται διαδοχικά 4 φορές η συνάρτηση *SubByte().*

Η συνάρτηση *RotWord()* δέχεται ως είσοδο μια λέξη και ολισθαίνει κυκλικά τα bytes που την αποτελούν. Αν για παράδειγμα, δοθεί σαν είσοδος μια λέξη $[a_0, a_1, a_2, a_3]$ τότε σαν έξοδο έχουμε την λέξη $[a_1, a_2, a_3, a_0]$.

Σημειώνουμε ότι η διαδικασία επέκτασης κλειδιού για τον 256-bit AES είναι διαφέρει από της αντίστοιχες 128- /192-bit ($Nk = 8$). Αν $Nk = 8$ και $i - 4$ πολλαπλάσιο του Nk τότε Η διαδικασία *SubWord()* εφαρμόζεται στο $w[i-1]$ πριν την XOR.

4.4. Ασφάλεια AES

Η γραμμική και η διαφορική κρυπτανάλυση είναι μέθοδοι επιθέσεων που ανεπτύχθησαν για να προσβάλλουν, κυρίως, την ασφάλεια του DES. Επειδή ο DES απεδείχθη ευάλωτος στις επιθέσεις αυτές, η σχεδίαση του AES έγινε εξ αρχής με στόχο να είναι απρόσβλητος σε τέτοιες επιθέσεις.

Σημείο συγκρίσεως	**DES**	**AES**
Τύπος κρυπταλγορίθμου	Δίκτυο Feistel	SPN με κλειδί
Αριθμός γύρων	16	10 / 12 / 14
Διαφοροποίηση τελικού γύρου	ΟΧΙ	ΝΑΙ
Αρχικός μετασχηματισμός	ΝΑΙ	ΝΑΙ
Τελικός μετασχηματισμός	ΝΑΙ	ΟΧΙ
Μήκος τμήματος κειμένου	64 bits	128 bits
Μήκος κλειδιού	56 bits	128/192/256 bits
Ευάλωτα σημεία	• Αδύναμα & ημιαδύναμα κλειδιά • Ευπρόσβλητος σε γραμμική και διαφορική κρυπτανάλυση	κανένα εως τώρα

Fig 35 – Πίνακας Συνοπτικής Συγκρισης DES-AES

Μέχρι τον Μαϊο του 2009 οι μόνη δημοσιοποιημένη επιτυχής προσπάθεια ενάντια στον πλήρες αλγόριθμό AES είναι η *επίθεση πλευρικού καναλιού* σε ορισμένες εφαρμογές του AES.

Επίθεση πλευρικού καναλιού (side channel attack) είναι οποιαδήποτε επίθεση που βασίζεται σε πληροφορίες που αποκτήθηκαν από τη *πρακτική εφαρμογή* ενός κρυπτογραφικού συστήματος, παρά μιας επίθεσης ωμής βιας (σύγριση με 2^{128} πίθανά κλειδιά για το AES-128) ή κάποιας θεωρητικής αδυναμίας των αλγορίθμων. Για παράδειγμα, πληροφορίες χρονισμού, κατανάλωση ενέργειας, ηλεκτρομαγνητικές διαρροές ή ακόμη και ήχου μπορεί να παρέχουν μια επιπλέον πηγή πληροφοριών που μπορεί να αξιοποιηθεί για να «σπάσει» το σύστημα. Ορισμένες επιθέσεις side-channel απαιτούν τεχνική γνώση της εσωτερικής λειτουργίας του συστήματος στο οποίο υλοποιείται η κρυπτογράφηση. Οι πιο ισχυρές επιθέσεις πλευρικού καναλιού που βασίζεται σε στατιστικές μεθόδους για πρώτη φορά από τον Paul Kocher.

Παράρτημα Α – Υπολογιστικό Παράδειγμα κρυπτογράφησης DES

Στο παράρτημα αυτό θα αναλυθεί ένα παραδειγμα κρυπτογράφησης DES ενός 64-bit block χρησιμοποιώντας ένα 56-bit κλειδί το οποίο θα μετατραπεί σε 64-bit.

Input Message (Hex): 3f 2d 0c 09 02 0b 0e ff

56-bit κλειδί (Hex): 3a 72 61 b1 44 3d af

56-bitκλειδί (bit): 00111010 01110010 01100001 10110001 01000100 00111101 10101111

Χωρίζεται σε 8 δεσμες των 7 bits:

0011101 0011100 1001100 0011011 0001010 0010000 1111011 0101111

Προστίθεται το bit 0 ή 1 στο τέλος κάθε δέσμης τέτοιο ώστε το σύνολο των 1 σε κάθε δέσμη να είναι μονός αριθμός και έτσι προκύπτει το αρχικό κλειδί:

00111011 00111000 10011000 00110111 00010101 00100000 11110111 01011110

	Decimal	Hex
Input	63 45 12 9 2 11 14 255	3f 2d 0c 09 02 0b 0e ff
56-bit key	62 88 48 64 33 67 255	3a 72 61 b1 44 3d af
64-bit Key	59 56 152 55 21 32 247 94	3b 38 98 37 15 20 f7 5e

Inputbits: 00111111 00101101 00001100 00001001 00000010 00001011 00001110 11111111

Keybits: 00111011 00111000 10011000 00110111 00010101 00100000 11110111 01011110

CD[0]: 0100010 0110000 0001101 0111101 1100100 1110110 0010000 1111111

CD[1]: 1000100 1100000 0011010 1111010 1001001 1101100 0100001 1111111

KS[1]: 010111 000000 100001 001100 010101 011000 111101 001111

CD[2]: 0001001 1000000 0110101 1110101 0010011 1011000 1000011 1111111

KS[2]: 010100 010010 110111 110000 011001 001001 011111 001100

CD[3]: 0100110 0000001 1010111 1010100 1001110 1100010 0001111 1111100

KS[3]: 110101 001110 010010 000101 110110 001011 010011 101111

CD[4]: 0011000 0000110 1011110 1010001 0111011 0001000 0111111 1110010

KS[4]: 010100 111000 011100 000110 011011 101101 111010 101001

CD[5]: 1100000 0011010 1111010 1000100 1101100 0100001 1111111 1001001

KS[5]: 011010 001001 000010 100111 000110 100111 110101 111011

CD[6]: 0000000 1101011 1101010 0010011 0110001 0000111 1111110 0100111

KS[6]: 101100 011000 000001 101110 101011 111101 100100 110000

CD[7]: 0000011 0101111 0101000 1001100 1000100 0011111 1111001 0011101

KS[7]: 101000 000100 001010 110010 110000 010110 111101 110010

CD[8]: 0001101 0111101 0100010 0110000 0010000 1111111 1100100 1110110

KS[8]: 101101 000001 101100 110100 111111 011000 101000 011100

CD[9]: 0011010 1111010 1000100 1100000 0100001 1111111 1001001 1101100

KS[9]: 001000 101101 110101 000010 100100 111000 011001 111100

CD[10]: 1101011 1101010 0010011 0000000 0000111 1111110 0100111 0110001

KS[10]: 011010 000110 000101 010111 110110 011011 111110 000100

CD[11]: 0101111 0101000 1001100 0000011 0011111 1111001 0011101 1000100

KS[11]: 001001 011100 010100 011001 001110 000110 011010 111101

CD[12]: 0111101 0100010 0110000 0001101 1111111 1100100 1110110 0010000

KS[12]: 010001 110000 000110 110011 011110 110111 100010 000111

CD[13]: 1110101 0001001 1000000 0110101 1111111 0010011 1011000 1000011

KS[13]: 101111 111000 100010 010001 101001 100110 000110 111011

CD[14]: 1010100 0100110 0000001 1010111 1111100 1001110 1100010 0001111

KS[14]: 000111 110010 001010 001010 101001 110011 101101 000111

CD[15]: 1010001 0011000 0000110 1011110 1110010 0111011 0001000 0111111

KS[15]: 001110 100001 010010 011100 111101 101000 001111 110010

CD[16]: 0100010 0110000 0001101 0111101 1100100 1110110 0010000 1111111

KS[16]: 000100 010111 110010 000001 110101 111110 000101 001110

L[0]: 10000000 10000001 11000111 10101011

R[0]: 10000000 10000011 11101111 11110001

Round 1

E : 110000 000001 010000 000111 111101 011111 111110 100011

KS : 010111 000000 100001 001100 010101 011000 111101 001111

ExorKS: 100111 000001 110001 001011 101000 000111 000011 101100

Sbox: 0010 0011 0100 1111 1010 0010 0000 1110

P : 11001001 01100011 01010010 11100000

L[i]: 10000000 10000011 11101111 11110001

R[i]: 01001001 11100010 10010101 01001011

Round 2

E : 101001 010011 111100 000101 010010 101010 101001 010110

KS : 010100 010010 110111 110000 011001 001001 011111 001100

ExorKS: 111101 000001 001011 110101 001011 100011 110110 011010

Sbox: 0110 0011 0100 0101 0111 0011 1000 0000

P : 11100000 00100101 11110010 10000001

L[i]: 01001001 11100010 10010101 01001011

R[i]: 01100000 10100110 00011101 01110000

Round 3

E : 001100 000001 010100 001100 000011 111010 101110 100000

KS : 110101 001110 010010 000101 110110 001011 010011 101111

ExorKS: 111001 001111 000110 001001 110101 110001 111101 001111

Sbox: 1010 1110 1110 0110 0000 1011 0011 0100

P : 01010010 11101001 00110111 00110100

L[i]: 01100000 10100110 00011101 01110000

R[i]: 00011011 00001011 10100010 01111111

Round 4

E : 100011 110110 100001 010111 110100 000100 001111 111110

KS : 010100 111000 011100 000110 011011 101101 111010 101001

ExorKS: 110111 001110 111101 010001 101111 101001 110101 010111

Sbox: 1110 0100 0010 0100 1101 1001 0000 1011

P : 00111001 10000110 10111010 00010100

L[i]: 00011011 00001011 10100010 01111111

R[i]: 01011001 00100000 10100111 01100100

Round 5

E : 001011 110010 100100 000001 010100 001110 101100 001000

KS : 011010 001001 000010 100111 000110 100111 110101 111011

ExorKS: 010001 111011 100110 100110 010010 101001 011001 110011

Sbox: 1010 0101 1001 0000 0101 1001 0010 1100

P : 00111100 10000100 01100111 00110000

L[i]: 01011001 00100000 10100111 01100100

R[i]: 00100111 10001111 11000101 01001111

Round 6

E : 100100 001111 110001 011111 111000 001010 101001 011110

KS : 101100 011000 000001 101110 101011 111101 100100 110000

ExorKS: 001000 010111 110000 110001 010011 110111 001101 101110

Sbox: 0010 1010 1011 1001 0000 0111 0001 0010

P : 11000110 00101010 00100011 01001100

L[i]: 00100111 10001111 11000101 01001111

R[i]: 10011111 00001010 10000100 00101000

Round 7

E : 010011 111110 100001 010101 010000 001000 000101 010001

KS : 101000 000100 001010 110010 110000 010110 111101 110010

ExorKS: 111011 111010 101011 100111 100000 011110 111000 100011

Sbox: 0000 0011 1001 0110 0100 1011 0000 0001

P : 01010100 01100100 01111001 00000000

L[i]: 10011111 00001010 10000100 00101000

R[i]: 01110011 11101011 10111100 01001111

Round 8

E : 101110 100111 111101 010111 110111 111000 001001 011110

KS : 101101 000001 101100 110100 111111 011000 101000 011100

ExorKS: 000011 100110 010001 100011 001000 100000 100001 000010

Sbox: 1111 1011 0010 1111 0111 1001 0110 0010

P : 11110000 11011110 11110110 11000110

L[i]: 01110011 11101011 10111100 01001111

R[i]: 01101111 11010100 01110010 11101110

Round 9

E : 001101 011111 111010 101000 001110 100101 011101 011100

KS : 001000 101101 110101 000010 100100 111000 011001 111100

ExorKS: 000101 110010 001111 101010 101010 011101 000100 100000

Sbox: 0111 1000 1010 1011 1101 0011 0010 0111

P : 10100001 01101110 10101111 01100110

L[i]: 01101111 11010100 01110010 11101110

R[i]: 11010010 10000101 00010011 00101001

Round 10

E : 111010 100101 010000 001010 100010 100110 100101 010011

KS : 011010 000110 000101 010111 110110 011011 111110 000100

ExorKS: 100000 100011 010101 011101 010100 111101 011011 010111

Sbox: 0100 1000 0101 1110 0011 1000 1111 1011

P : 00111110 01011011 10011100 11000001

L[i]: 11010010 10000101 00010011 00101001

R[i]: 01010001 10001111 11101110 00101111

Round 11

E : 101010 100011 110001 011111 111101 011100 000101 011110

KS : 001001 011100 010100 011001 001110 000110 011010 111101

ExorKS: 100011 111111 100101 000110 110011 011010 011111 100011

Sbox: 1100 1001 1101 0011 1111 0111 0110 0001

P : 10100101 11111101 11101101 10001000

L[i]: 01010001 10001111 11101110 00101111

R[i]: 01110111 01111000 11111110 10100001

Round 12

E : 101110 101110 101111 110001 011111 111101 010100 000010

KS : 010001 110000 000110 110011 011110 110111 100010 000111

ExorKS: 111111 011110 101001 000010 000001 001010 110110 000101

Sbox: 1101 1010 0110 1101 1110 0010 1000 1101

P : 11001001 10101101 10011000 11100111

L[i]: 01110111 01111000 11111110 10100001

R[i]: 10011000 00100010 01110110 11001000

Round 13

E : 010011 110000 000100 000100 001110 101101 011001 010001

KS : 101111 111000 100010 010001 101001 100110 000110 111011

ExorKS: 111100 001000 100110 010101 100111 001011 011111 101010

Sbox: 0101 0110 1001 0010 0111 1100 0110 1100

P : 01111100 01010100 10000101 10111010

L[i]: 10011000 00100010 01110110 11001000

R[i]: 00001011 00101100 01111011 00011011

Round 14

E : 100001 010110 100101 011000 001111 110110 100011 110110

KS : 000111 110010 001010 001010 101001 110011 101101 000111

ExorKS: 100110 100100 101111 010010 100110 000101 001110 110001

Sbox: 1000 0111 0111 0010 1011 0100 1101 1111

P : 01101111 11010011 01001000 10111101

L[i]: 00001011 00101100 01111011 00011011

R[i]: 11110111 11110001 00111110 01110101

Round 15

E : 111110 101111 111110 100010 100111 111100 001110 101011

KS : 001110 100001 010010 011100 111101 101000 001111 110010

ExorKS: 110000 001110 101100 111110 011010 010100 000001 011001

Sbox: 1111 0100 0011 0100 0000 0011 1101 0000

P : 00000110 10110000 10110010 00010111

L[i]: 11110111 11110001 00111110 01110101

R[i]: 00001101 10011100 11001001 00001100

Round 16

E : 000001 011011 110011 111001 011001 010010 100001 011000

KS : 000100 010111 110010 000001 110101 111110 000101 001110

ExorKS: 000101 001100 000001 111000 101100 101100 100100 010110

Sbox: 0111 0011 1101 0101 0111 1100 1011 1110

P : 11111110 00000111 11010111 10101011

L[i]: 00001101 10011100 11001001 00001100

R[i]: 00001001 11110110 11101001 11011110

LR[16] 00001001 11110110 11101001 11011110 00001101 10011100 11001001 00001100

Output 11001100 00010001 10110011 11101111 00110001 00010100 00011101 00111101

Παράρτημα Β – Υπολογιστικό Παράδειγμα κρυπτογράφησης AES

Στο παράρτημα αυτό θα αναλυθεί ένα παραδειγμα κρυπτογράφησης AES ενός 64-bit block χρησιμοποιώντας ένα 128-bit κλειδί.

Input bits: a9 d1 c7 c5 aa 53 83 1f 1f bc 42 5c 9f b6 12 41

Key bits: 30 b7 3f 49 70 ce d2 f5 97 45 57 42 1a 06 3f 0d

Input bits:

a9	aa	1f	9f
d1	53	bc	b6
c7	83	42	12
c5	1f	5c	41

Key bits:

30	70	97	1a
b7	ce	45	06
3f	d2	57	3f
49	f5	42	0d

Επέκταση κλειδιού:

w[0] = 30 70 97 1a
w[1] = b7 ce 45 06
w[2] = 3f d2 57 3f
w[3] = 49 f5 42 0d
RotWord()= f5 42 0d 49
SubWord()= e6 2c d7 3b
^ Rcon()= e7 2c d7 3b

w[4] = d7 5c 40 21
w[5] = 60 92 05 27
w[6] = 5f 40 52 18
w[7] = 16 b5 10 15
RotWord()= b5 10 15 16
SubWord()= d5 ca 59 47
^ Rcon()= d7 ca 59 47

w[8] = 00 96 19 66
w[9] = 60 04 1c 41
w[10] = 3f 44 4e 59
w[11] = 29 f1 5e 4c
RotWord()= f1 5e 4c 29
SubWord()= a1 58 29 a5
^ Rcon()= a5 58 29 a5

w[12] = a5 ce 30 c3
w[13] = c5 ca 2c 82

```
w[14] =   fa 8e 62 db
w[15] =   d3 7f 3c 97
RotWord()=  7f 3c 97 d3
SubWord()=  d2 eb 88 66
 ^ Rcon()=  da eb 88 66

w[16] =   7f 25 b8 a5
w[17] =   ba ef 94 27
w[18] =   40 61 f6 fc
w[19] =   93 1e ca 6b
RotWord()=  1e ca 6b 93
SubWord()=  72 74 7f dc
 ^ Rcon()=  62 74 7f dc

w[20] =   1d 51 c7 79
w[21] =   a7 be 53 5e
w[22] =   e7 df a5 a2
w[23] =   74 c1 6f c9
RotWord()=  c1 6f c9 74
SubWord()=  78 a8 dd 92
 ^ Rcon()=  58 a8 dd 92

w[24] =   45 f9 1a eb
w[25] =   e2 47 49 b5
w[26] =   05 98 ec 17
w[27] =   71 59 83 de
RotWord()=  59 83 de 71
SubWord()=  cb ec 1d a3
 ^ Rcon()=  8b ec 1d a3

w[28] =   ce 15 07 48
w[29] =   2c 52 4e fd
w[30] =   29 ca a2 ea
w[31] =   58 93 21 34
RotWord()=  93 21 34 58
SubWord()=  dc fd 18 6a
 ^ Rcon()=  5c fd 18 6a

w[32] =   92 e8 1f 22
w[33] =   be ba 51 df
w[34] =   97 70 f3 35
w[35] =   cf e3 d2 01
RotWord()=  e3 d2 01 cf
SubWord()=  11 b5 7c 8a
 ^ Rcon()=  0a b5 7c 8a

w[36] =   98 5d 63 a8
w[37] =   26 e7 32 77
w[38] =   b1 97 c1 42
w[39] =   7e 74 13 43
RotWord()=  74 13 43 7e
SubWord()=  92 7d 1a f3
 ^ Rcon()=  a4 7d 1a f3

w[40] =   3c 20 79 5b
w[41] =   1a c7 4b 2c
w[42] =   ab 50 8a 6e
w[43] =   d5 24 99 2d
```

```
Initial state  a9 d1 c7 c5
               aa 53 83 1f
               1f bc 42 5c
               9f b6 12 41

Round Key  30 b7 3f 49
           70 ce d2 f5
           97 45 57 42
           1a 06 3f 0d
Round 1  99 66 f8 8c
         da 9d 51 ea
         88 f9 15 1e
         85 b0 2d 4c
After SubBytes  ee 33 41 64
                57 5e d1 87
                c4 99 59 72
                97 e7 d8 29
After ShiftRows  ee 33 41 64
                 5e d1 87 57
                 59 72 c4 99
                 29 97 e7 d8
After MixColumns  55 eb 33 70
                  90 8b e4 a2
                  79 a4 67 69
                  7c c3 55 c9
Round Key  d7 60 5f 16
           5c 92 40 b5
           40 05 52 10
           21 27 18 15
Round 2  82 8b 6c 66
         cc 19 a4 17
         39 a1 35 79
         5d e4 4d dc
After SubBytes  13 3d 50 33
                4b d4 49 f0
                12 32 96 b6
                4c 69 e3 86
After ShiftRows  13 3d 50 33
                 d4 49 f0 4b
                 96 b6 12 32
                 86 4c 69 e3
After MixColumns  51 5b d0 6a
                  87 22 f4 10
                  61 d7 3f 22
                  60 20 c0 f1
Round Key  00 60 3f 29
           96 04 44 f1
           19 1c 4e 5e
           66 41 59 4c
Round 3  51 3b ef 43
         11 26 b0 e1
         78 cb 71 7c
         06 61 99 bd
After SubBytes  d1 e2 df 1a
                82 f7 e7 f8
                bc 1f a3 10
                6f ef ee 7a
```

```
After ShiftRows  d1 e2 df 1a
                 f7 e7 f8 82
                 a3 10 bc 1f
                 7a 6f ef ee
After MixColumns  62 92 e5 58
                  a0 68 04 ca
                  f5 94 6e 8f
                  c8 14 fb 74
Round Key  a5 c5 fa d3
           ce ca 8e 7f
           30 2c 62 3c
           c3 82 db 97
Round 4  c7 57 1f 8b
         6e a2 8a b5
         c5 b8 0c b3
         0b 96 20 e3
After SubBytes  c6 5b c0 3d
                9f 3a 7e d5
                a6 6c fe 6d
                2b 90 b7 11
After ShiftRows  c6 5b c0 3d
                 3a 7e d5 9f
                 fe 6d a6 6c
                 11 2b 90 b7
After MixColumns  36 72 c9 1b
                  ba 3b 10 1b
                  28 82 e9 b8
                  b7 a8 13 c1
Round Key  7f ba 40 93
           25 ef 61 1e
           b8 94 f6 ca
           a5 27 fc 6b
Round 5  49 c8 89 88
         9f d4 71 05
         90 16 1f 72
         12 8f ef aa
After SubBytes  3b e8 a7 c4
                db 48 a3 6b
                60 47 c0 40
                c9 73 df ac
After ShiftRows  3b e8 a7 c4
                 48 a3 6b db
                 c0 40 60 47
                 ac c9 73 df
After MixColumns  c2 bc fb 7d
                  5c bc a2 7f
                  07 8b 99 eb
                  86 49 1f 6e
Round Key  1d a7 e7 74
           51 be df c1
           c7 53 a5 6f
           79 5e a2 c9
Round 6  df 1b 1c 09
         0d 02 7d be
         c0 d8 3c 84
         ff 17 bd a7
After SubBytes  9e af 9c 01
                d7 77 ff ae
```

ba 61 eb 5f
16 f0 7a 5c
After ShiftRows 9e af 9c 01
77 ff ae d7
eb 5f ba 61
5c 16 f0 7a
After MixColumns 09 16 80 7b
0a bd fe 6d
c0 d4 56 9a
9d 66 50 41
Round Key 45 e2 05 71
f9 47 98 59
1a 49 ec 83
eb b5 17 de
Round 7 4c f4 85 0a
f3 fa 66 34
da 9d ba 19
76 d3 47 9f
After SubBytes 29 bf 97 67
0d 2d 33 18
57 5e f4 d4
38 66 a0 db
After ShiftRows 29 bf 97 67
2d 33 18 0d
f4 d4 57 5e
db 38 66 a0
After MixColumns 0a dc 2c 27
af 86 38 3f
81 77 8b 2d
0f 4d 21 a1
Round Key ce 2c 29 58
15 52 ca 93
07 4e a2 21
48 fd ea 34
Round 8 c4 f0 05 7f
ba d4 f2 ac
86 39 29 0c
47 b0 cb 95
After SubBytes 1c 8c 6b d2
f4 48 89 91
44 12 a5 fe
a0 e7 1f 2a
After ShiftRows 1c 8c 6b d2
48 89 91 f4
a5 fe 44 12
2a a0 e7 1f
After MixColumns 6f dd dd b5
52 3c 79 08
7b 19 40 23
9d a3 bd b5
Round Key 92 be 97 cf
e8 ba 70 e3
1f 51 f3 d2
22 df 35 01
Round 9 fd 63 4a 7a
ba 86 09 eb
64 48 b3 f1
bf 7c 88 b4

After SubBytes 54 fb d6 da
f4 44 01 e9
43 52 6d a1
08 10 c4 8d
After ShiftRows 54 fb d6 da
44 01 e9 f4
6d a1 43 52
8d 08 10 c4
After MixColumns 84 47 c4 3e
e6 09 ca 1b
46 bb 89 dd
d4 a6 eb 40
Round Key 98 26 b1 7e
5d e7 97 74
63 32 c1 13
a8 77 42 43
After SubBytes 9c ef 9d 09
ea 28 4c a8
3f a7 52 8b
10 3e d3 7b
After ShiftRows 9c ef 9d 09
28 4c a8 ea
52 8b 3f a7
7b 10 3e d3
Output a0 f5 36 dc
08 8b f8 ce
2b c0 b5 3e
20 3c 50 fe

	Αρχή γύρου					SubBytes					ShiftRows					MixColumns					Κλειδί γύρου			
Input	30	70	97	1a																	30	b7	3f	49
	b7	ce	45	06																	70	ce	d2	f5
	3f	d2	57	3f																	97	45	57	42
	49	f5	42	0d																	1a	06	3f	0d
0	99	66	f8	8c		ee	33	41	64		ee	33	41	64		55	eb	33	70		d7	60	5f	16
	da	9d	51	ea		57	5e	d1	87		5e	d1	87	57		90	8b	e4	a2		5c	92	40	b5
	88	f9	15	1e		c4	99	59	72		59	72	c4	99		79	a4	67	69		40	05	52	10
	85	b0	2d	4c		97	e7	d8	29		29	97	e7	d8		7c	c3	55	c9		21	27	18	15
1	82	8b	6c	66		13	3d	50	33		13	3d	50	33		51	5b	d0	6a		00	60	3f	29
	cc	19	a4	17		4b	d4	49	f0		d4	49	f0	4b		87	22	f4	10		96	04	44	f1
	39	a1	35	79		12	32	96	b6		96	b6	12	32		61	d7	3f	22		19	1c	4e	5e
	5d	e4	4d	dc		4c	69	e3	86		86	4c	69	e3		60	20	c0	f1		66	41	59	4c
2	51	3b	ef	43		d1	e2	df	1a		d1	e2	df	1a		62	92	e5	58		a5	c5	fa	d3
	11	26	b0	e1		82	f7	e7	f8		f7	e7	f8	82		a0	68	04	ca		ce	ca	8e	7f
	78	cb	71	7c		bc	1f	a3	10		a3	10	bc	1f		f5	94	6e	8f		30	2c	62	3c
	6	61	99	bd		6f	ef	ee	7a		7a	6f	ef	ee		c8	14	fb	74		c3	82	db	97

	Αρχή γύρου					SubBytes					ShiftRows					MixColumns					Κλειδί γύρου			
3	c7	57	1f	8b		c6	5b	c0	3d		c6	5b	c0	3d		36	72	c9	1b		7f	ba	40	93
	6e	a2	8a	b5		9f	3a	7e	d5		3a	7e	d5	9f		ba	3b	10	1b		25	ef	61	1e
	c5	b8	0c	b3		a6	6c	fe	6d		fe	6d	a6	6c		28	82	e9	b8		b8	94	f6	ca
	0b	96	20	e3		2b	90	b7	11		11	2b	90	b7		b7	a8	13	c1		a5	27	fc	6b
4	49	c8	89	88		3b	e8	a7	c4		3b	e8	a7	c4		c2	bc	fb	7d		1d	a7	e7	74
	9f	d4	71	05		db	48	a3	6b		48	a3	6b	db		5c	bc	a2	7f		51	be	df	c1
	90	16	1f	72		60	47	c0	40		c0	40	60	47		07	8b	99	eb		c7	53	a5	6f
	12	8f	ef	aa		c9	73	df	ac		ac	c9	73	df		86	49	1f	6e		79	5e	a2	c9
5	df	1b	1c	09		9e	af	9c	01		9e	af	9c	01		09	16	80	7b		45	e2	05	71
	0d	02	7d	be		d7	77	ff	ae		77	ff	ae	d7		0a	bd	fe	6d		f9	47	98	59
	c0	d8	3c	84		ba	61	eb	5f		eb	5f	ba	61		c0	d4	56	9a		1a	49	ec	83
	ff	17	bd	a7		16	f0	7a	5c		5c	16	f0	7a		9d	66	50	41		eb	b5	17	de
6	4c	f4	85	0a		29	bf	97	67		29	bf	97	67		0a	dc	2c	27		ce	2c	29	58
	f3	fa	66	34		0d	2d	33	18		2d	33	18	0d		af	86	38	3f		15	52	ca	93
	da	9d	ba	19		57	5e	f4	d4		f4	d4	57	5e		81	77	8b	2d		07	4e	a2	21
	76	d3	47	9f		38	66	a0	db		db	38	66	a0		0f	4d	21	a1		48	fd	ea	34
7	c4	f0	05	7f		1c	8c	6b	d2		1c	8c	6b	d2		6f	dd	dd	b5		92	be	97	cf
	ba	d4	f2	ac		f4	48	89	91		48	89	91	f4		52	3c	79	08		e8	ba	70	e3
	86	39	29	0c		44	12	a5	fe		a5	fe	44	12		7b	19	40	23		1f	51	f3	d2
	47	b0	cb	95		a0	e7	1f	2a		2a	a0	e7	1f		9d	a3	bd	b5		22	df	35	01
8	fd	63	4a	7a		54	fb	d6	da		54	fb	d6	da		84	47	c4	3e		98	26	b1	7e
	ba	86	09	eb		f4	44	01	e9		44	01	e9	f4		e6	09	ca	1b		5d	e7	97	74
	64	48	b3	f1		43	52	6d	a1		6d	a1	43	52		46	bb	89	dd		63	32	c1	13
	bf	7c	88	b4		08	10	c4	8d		8d	08	10	c4		d4	a6	eb	40		a8	77	42	43
9						9c	ef	9d	09		9c	ef	9d	09										
						ea	28	4c	a8		28	4c	a8	ea										
						3f	a7	52	8b		52	8b	3f	a7										
						10	3e	d3	7b		7b	10	3e	d3										
	a0	f5	36	dc																				
	08	8b	f8	ce																				
	2b	c0	b5	3e																				
	20	3c	50	fe																				

Table of figures

Fig 1 – Κρυπτογράφηση - Αποκρυπτογράφηση 8
Fig 2 –Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση 10
Fig 3 –Ο Δίσκος της Φαιστού 13
Fig 4 – Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως από την Γερμανία 14
Fig 5 – Κρυπτό-μηχανή SIGABA 17
Fig 6 – Κατηγορίες κρυπτοσυστημάτων 21
Fig 7 – Αλγόριθμος DES 36
Fig 8 – Πίνακες Μετάθεσης $\mathbf{IP}$ και $\boldsymbol{IP}-\mathbf{1}$ 37
Fig 9 – Συνάρτηση DES $\boldsymbol{fRi}-\mathbf{1},\boldsymbol{Ki}$ 38
Fig 10 – Πίνακας Επέκτασης Μετάθεσης 39
Fig 11 – Πίνακες S-box 41
Fig 12 – Πίνακας μετάθεσης 41
Fig 13 – Διαδικασία μετάθεσης κλειδιού 42
Fig 14 – Πίνακας μετάθεσης επιλογής $\boldsymbol{PC}-\mathbf{1}$ 43
Fig 15 – Πίνακας μετάθεσης επιλογής $\boldsymbol{PC}-\mathbf{2}$ 43
Fig 16 – ECB Mode 44
Fig 17 – CBD Mode 45
Fig 18 – CFB Mode 47
Fig 19 – OFB Mode 48
Fig 20 – CTR Mode 49
Fig 21 – Structure of Basic AES algorithm (Nr=10) 56
Fig 22 – Ψευδοκώδικαςκρυπτογράφησης AES 57
Fig 23 – Ψευδοκώδικαςαποκρυπτογράφησης AES 57
Fig 24 – Δεικτοδότηση bits και bytes 58
Fig 25 – Μετασχηματισμός SubBytes 58
Fig 26 – S-Box Πίνακας αντικατάστασης δεκαδικής μορφής 59
Fig 27 – Ψευδοκώδικας SubBytes 60
Fig 28 – S-Box Πίνακας αντίστροφης αντικατάστασης δεκαδικής μορφής 60
Fig 29 – ShiftRows Step 61
Fig 30 – MixColumns Step 62
Fig 31 – AddRoundKey Step 63
Fig 32 – Επέκταση κλειδιού 64
Fig 33 – Πίνακας $\boldsymbol{RConi}$ 65
Fig 34 – Ψευδοκώδικας Επέκτασης κλειδιού 65
Fig 35 – Πίνακας Συνοπτικής Συγκρισης DES-AES 67

Βιβλιογραφία

[1] FIPS Publication 197, the Advanced Encryption Standard (AES), U.S. DoC/NIST,November, 2001.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] NIST Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Morris Dworkin
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[3] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, DATA ENCRYPTION STANDARD (DES), FIPS PUB 46-3, FEDERAL INFORMATION, PROCESSING STANDARDS PUBLICATION, 1999
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[4] Joan Daemen, Vincent Rijmen, AES Proposal:Rijndael, 2003
http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

[5] FIPS PUB 46-2, Supersedes FIPS PUB 46-1, DATA ENCRYPTION STANDARD (DES), Federal Information, Processing Standards Publication 46-2, 1988
http://www.itl.nist.gov/fipspubs/fip46-2.htm

[6] The DES Algorithm Illustrated, by J. Orlin Grabbe
http://orlingrabbe.com/des.htm

[7]Trappe W. and Washington L. "Introduction to Cryptography with coding Theory" , Pearson education international, 2006

[8]Stinson D., "Cryptography. Theory and Practice", third edition, Chapman and Hall, 2006

[9]Koukouvinos H. and Papaioannou A. "Cryptography", 2007

[10] http://en.wikipedia.org/