ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Συμμετρικά και Ασύμμετρα Κρυπτοσυστήματα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της
ΦΩΣΚΟΛΟΥ ΜΑΡΙΑ ΘΗΡΕΣΙΑ
Α.Μ.: 09104027

Τριμελής επιτροπή: *Κουκουβίνος Χρήστος*
Καθηγητής Ε.Μ.Π
Παπαϊωάννου Αλέξανδρος (Επιβλέπων)
Αναπληρωτής Καθηγητής Ε.Μ.Π
Στεφανέας Πέτρος
Λέκτορας Ε.Μ.Π

ΑΘΗΝΑ, ΝΟΕΜΒΡΙΟΣ 2011

ΠΡΟΛΟΓΟΣ

Η παρακάτω διπλωματική εργασία αναφέρεται στην κρυπτογραφία και στα κρυπτοσυστήματα DES και AES. Ξεκινώντας από τις θεμελιώδεις έννοιες και την ορολογία της κρυπτογραφίας, προσεγγίζονται σταδιακά οι διάφορες τεχνικές της, οι αρχές σχεδιασμού και τα είδη κρυπτογράφησης. Έχει γίνει αναφορά σε μια πληθώρα μεθόδων κρυπτογράφησης και αποκρυπτογράφησης ξεκινώντας από την αρχαιότητα και φτάνοντας μέχρι τις ημέρες μας. Κύριο μέλημα της εργασίας είναι η ενασχόληση με τα block ciphers και πιο συγκεκριμένα η παρουσίαση των αλγορίθμων κρυπτογράφησης DES και AES, δίνοντας πληροφορίες για τα χαρακτηριστικά σχεδιασμού τους και για κάποιες επιθέσεις που έχουν διεξαχθεί εναντίον τους, καθώς και δύο εμπορικές εφαρμογές τους (το πρωτόκολλο Kerberos και το UMTS authentication πρωτόκολλο).

Το πρώτο κεφάλαιο αποτελεί ουσιαστικά μια πρώτη γνωριμία με την κρυπτογραφία μέσα από τις βασικές της έννοιες, κάνοντας συγχρόνως μια αναδρομή στην εξέλιξή της μέσα στο πέρασμα του χρόνου. Ταυτόχρονα, αναφέρονται οι κύριες κατηγορίες κρυπτοσυστημάτων και παρουσιάζονται κάποια χαρακτηριστικά παραδείγματα αλγορίθμων, δίνοντας έμφαση στους αλγόριθμους τμήματος.

Το δεύτερο κεφάλαιο ασχολείται ενδελεχώς με τον αλγόριθμο DES, παρουσιάζοντας τα γεγονότα που οδήγησαν στη δημιουργία του κι εκείνα που προκάλεσαν την αντικατάστασή του. Επιπρόσθετα, αναλύεται η δομή του, ο τρόπος λειτουργίας του και η κρυπτανάλυσή του. Το κεφάλαιο ολοκληρώνεται με χαρακτηριστική εφαρμογή του DES, το πρωτόκολο Kerberos.

Το τρίτο κεφάλαιο ξεκινάει με τη διαδικασία ανάδειξης του αλγορίθμου Rijndael ως AES και στη συνέχεια αναλύεται η δομή του, ο τρόπος λειτουργίας του και η κρυπτανάλυσή του. Επίσης, δίνεται ένα παράδειγμα για να γίνει πιο κατανοητή η διαδικασία της κρυπτογράφησης του AES. Κλείνοντας, περιγράφεται μια χαρακτηριστική εμπορική εφαρμογή του, τα συστήματα τρίτης γενιάς (UMTS).

Στο τέταρτο και τελευταίο κεφάλαιο γίνεται μια ανακεφαλαίωση καθώς και μια συνοπτική σύγκριση των κρυπτοσυστημάτων DES και AES.

Ολοκληρώνοντας το προλογικό αυτό σημείωμα, θεωρώ υποχρέωσή μου να ευχαριστήσω τον επιβλέποντα της διπλωματικής εργασίας, Αναπληρωτή Καθηγητή του Ε.Μ.Π, κύριο Αλέξανδρο Παπαϊωάννου για τη βοήθεια και την καθοδήγησή του κατά την εκπόνηση της διπλωματικής μου εργασία καθώς και τον μεταπτυχιακό φοιτητή Κόλλια Γρηγόρη για τις συμβουλές και το υλικό που μου έδωσε τα οποία με βοήθησαν σε μεγάλο βαθμό, να αντεπεξέλθω στις απαιτήσεις της εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1
Κρυπτογραφία και αλγόριθμοι

1.1 Εισαγωγή στην κρυπτογραφία

Η κρυπτογραφία ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" κι αποτελεί έναν κλάδο της επιστήμης της κρυπτολογίας, η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς την γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στην γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (Αντικειμενικοί σκοποί):

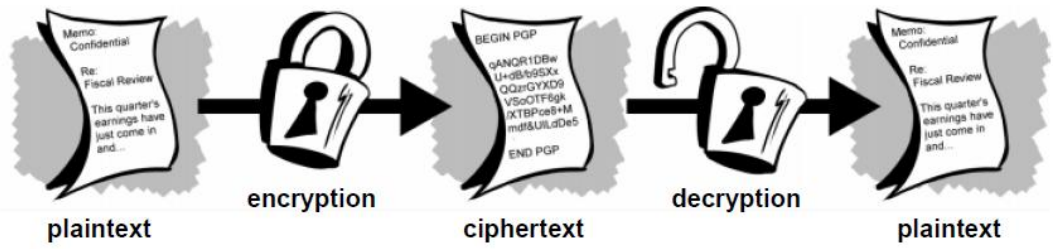
- **Εμπιστευτικότητα:** Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- **Ακεραιότητα:** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- **Μη απάρνηση:** Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- **Πιστοποίηση:** Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

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 το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (decryption)**.
- **Κρυπτογραφικός αλγόριθμος (cipher)** είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.
- **Αρχικό κείμενο (plaintext)** είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- **Κλειδί (key)** είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.
- **Κρυπτογραφημένο κείμενο (ciphertext)** είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού 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 της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

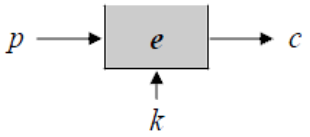
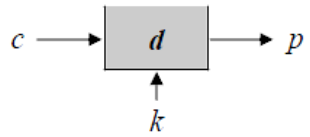
Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα:



Σχήμα 1.1 Διαδικασία κρυπτογράφησης - αποκρυπτογράφησης

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 εμπιστευτικότητα του 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 ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Οι διαδικασίες της κρυπτογραφήσεως και της αποκρυπτογραφήσεως μπορούν να παρασταθούν, ισοδυνάμως, είτε χρησιμοποιώντας μαθηματικές σχέσεις, είτε σχηματικώς, όπως φαίνεται στον επόμενο πίνακα.

	Μαθηματική παράσταση	Συμβολική παράσταση
Κρυπτογράφηση	$c = e_k(p)$	
Αποκρυπτογράφηση	$p = d_k(c)$	

p : Αρχικό κείμενο
c : Κρυπτοκείμενο
k : Κλειδί
e : Συνάρτηση κρυπτογραφήσεως
d : Συνάρτηση αποκρυπτογραφήσεως

Το κρυπτογραφημένο κείμενο αποτελεί το σημείο επέμβασης των πιθανών εισβολέων του συστήματος με σκοπό την αποκάλυψη κάποιου από τα συστατικά του συστήματος κρυπτογράφησης, συνήθως του κλειδιού, με σκοπό είτε την υποκλοπή του μηνύματος (αποκάλυψη του αρχικού κειμένου) είτε την αλλοίωσή του (παραγωγή νέου κρυπτογραφημένου μηνύματος που κατά την αποκρυπτογράφηση του από τον εξουσιοδοτημένο παραλήπτη θα προκύψει διαφορετικό μήνυμα από το αρχικό).

1.2 Ιδιότητες κλειδιών

Για να αποφεύγονται οι αποκαλούμενες επιθέσεις εκτενών αναζητήσεων πρέπει το πλήθος των πιθανών διαφορετικών συνδυασμών κλειδιών για έναν κρυπτογραφικό αλγόριθμο να είναι μεγάλο, καθώς σε περίπτωση που ο κρυπταναλυτής αποκτήσει ένα αντίστοιχο ζεύγος αρχικού και κρυπτογραφημένου κειμένου μπορεί προσπαθώντας με όλα τα πιθανά κλειδιά να δει ποιό ταιριάζει και να το χρησιμοποιήσει κατόπιν για να αποκρυπτογραφεί κι άλλα κρυπτογραφημένα κείμενα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Διαφορετικά, σε περίπτωση που απλά κατάφερε να υποκλέψει ένα κρυπτογραφημένο κείμενο, μπορεί να το αποκρυπτογραφήσει με διαφορετικούς συνδυασμούς κλειδιών μέχρι να βρει ένα αρχικό κείμενο που έχει λογική σημασία, οπότε τότε αποκτά, ουσιαστικά, και το σωστό κλειδί που στη συνέχεια μπορεί να το χρησιμοποιήσει για την αποκρυπτογράφηση και άλλων κρυπτογραφημένων κειμένων.

Τυπικά, τα κλειδιά είναι σειρές από bits και ως εκ τούτου η απαίτηση για μεγάλο πλήθος κλειδιών έχει την έννοια της χρήσης ολοένα και περισσότερων bits. Η χρήση 64 bits αποτελεί ένα τυπικό μήκος κλειδιού το οποίο παρέχει $2^{64} \cong 10^{19}$ διαφορετικά κλειδιά, που σημαίνει ότι αν είχαμε τη δυνατότητα να

δοκιμάζουμε ένα κλειδί ανά nanosecond, δηλαδή 1.000.000.000 κλειδιά ανά δευτερόλεπτο, θα χρειαζόμασταν περίπου 300 χρόνια για να δοκιμάσουμε όλους τους δυνατούς συνδυασμούς κλειδιών.

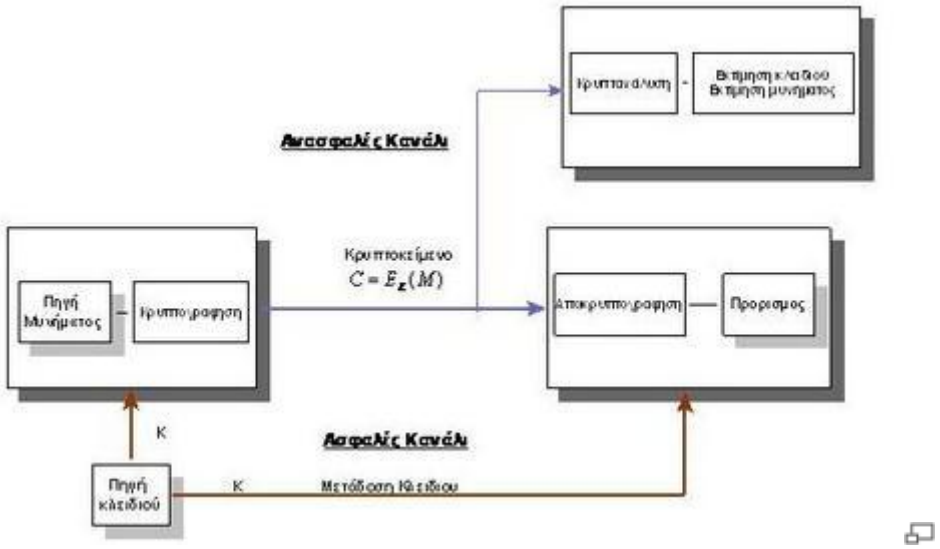
1.3 Βασικές έννοιες

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει την δυνατότητα σε 2 πρόσωπα, έστω τον Κώστα και την Βασιλική, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων.
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων.
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος.
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση.
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης.

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.



Σχήμα 1.2 Μοντέλο Τυπικού Κρυπτοσυστήματος

Το Σύστημα του Σχήματος λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους n από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις 2 τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.

1.4 Ιστορική Αναδρομή

1.4.1 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 $5^{ο}$ 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" (Εικόνα 1.3), 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.

Εικόνα 1.3 Η 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 14^{ο} 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 17^{ο} 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 σε 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 (Εικόνα 1.4), 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.

Εικόνα 1.4 Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που ανάσκαψε 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".

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

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20^{ου} 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 1.5).

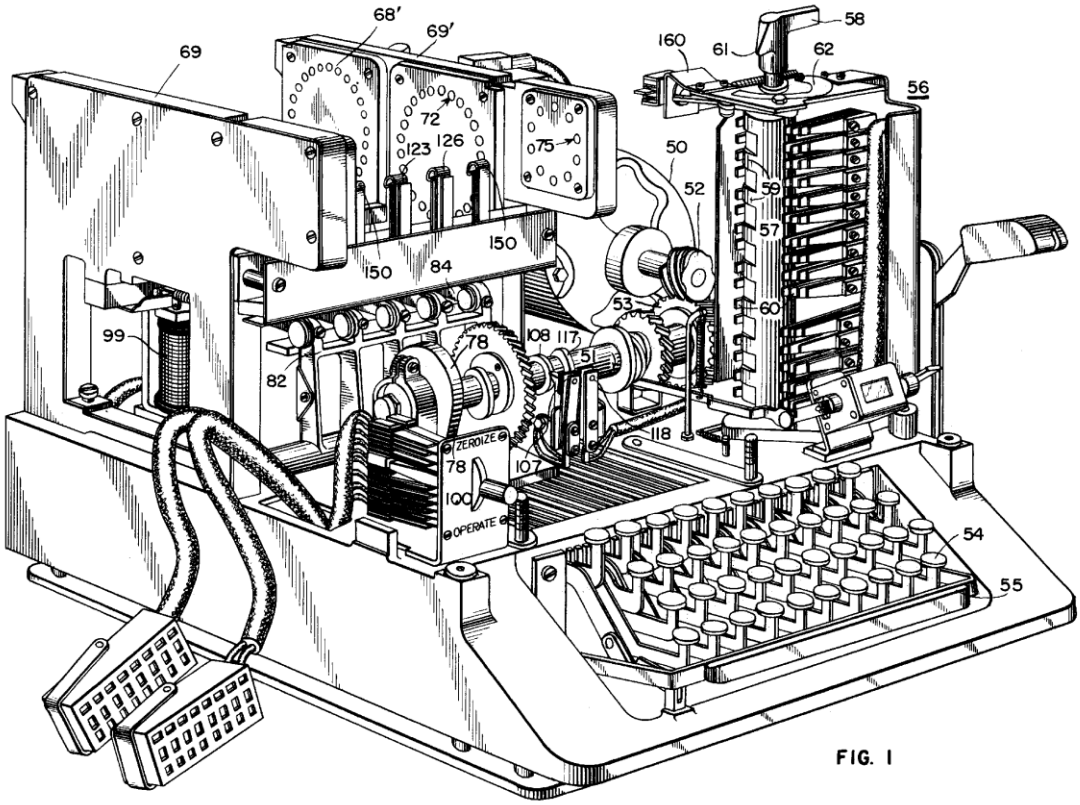
Εικόνα 1.5 Η μηχανή Enigma

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 βασίζονταν 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 στο περίφημο 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 αποκρυπτογράφησης 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 (Εικόνα 1.6). 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 Μ-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών Μ-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 προανήγγελλε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.



Εικόνα 1.6 Κρυπτομηχανή SIGABA

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.

1.4.3 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 επικοινωνίας. Το 1949 δημοσίευσε την εργασία "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 καθιέρωσαν 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 (δηλαδή 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 το NBS (National Bureau of Standards) υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν αντικατέστησε 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, ενσωματωμένοι 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 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. Η ανάγκη επομένως για αντικατάσταση του DES ήταν επιβλητική. Τα δεδομένα από τότε έχουν αλλάξει αρκετά. Αρκετές εταιρίες και επιχειρήσεις έχουν δημιουργήσει δικούς τους αλγόριθμους κρυπτογράφησης προκειμένου να διασφαλίσουν τα δεδομένα τους.

1.5 Εφαρμογές κρυπτογραφίας

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς. Τα κρυπτογραφικά συστήματα χρησιμοποιούνται για να παρέχουν :

- **Μυστικότητα (secrecy),**
- **Ακεραιότητα δεδομένων (data integrity),**
- **Αυθεντικοποίηση χρηστών (user authentication)**
- **Αδυναμία απάρνησης (non – repudiation).**

Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε hardware λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου. Η λογισμική κρυπτογραφία είναι φτηνότερη, πράγμα που την κάνει ευρέως αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια, δεν είναι το ίδιο γρήγορη με την εκτέλεση της σε hardware, αλλά η ολοένα αυξανόμενη ανάγκη για διασφάλιση των επικοινωνιών εδραίωσε την χρήση της.

Η κρυπτογραφία χρησιμοποιείται μεταξύ άλλων για:

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων

19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

Τέλος, για να κλείσουμε αυτή την ενότητα αναφέρουμε ότι η κρυπτογραφία και η κρυπτανάλυση βρίσκονται σε ένα συνεχή αγώνα δρόμου. Δεν υπάρχει αλγόριθμος κρυπτογράφησης που να μην σπάει (τουλάχιστον προς το παρόν και από αυτά που γνωρίζει 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 επίθεσης ωμής βίας να μην μπορεί κάποιος μη εξουσιοδοτημένος να αποκρυπτογραφήσει ένα κρυπτογραφημένο μήνυμα.

1.6 Προστασία

Η προοπτική να χρησιμοποιηθεί το Internet ως μέσο για τις ηλεκτρονικές συναλλαγές και την γενικότερη ανθρώπινη επικοινωνία οδήγησε στην τεράστια ανάπτυξη του διαδικτύου που παρακολουθούμε τα τελευταία χρόνια. Όμως, δεν προβλέφθηκε από τους σχεδιαστές του ο ορισμός μηχανισμών ασφάλειας για την προστασία των πληροφοριών που διακινούνται, αφού το διαδίκτυο σχεδιάστηκε για ενδοπανεπιστημιακή επικοινωνία και όχι γι’ αυτό που παρακολουθούμε και χρησιμοποιούμε σε παγκόσμια κλίμακα σήμερα. Για την προστασία των πληροφοριών που μεταδίδονται μέσω δικτύων ψηφιακών επικοινωνιών χρησιμοποιούνται σήμερα ευρέως συστήματα κρυπτογραφίας δημοσίου και μυστικού κλειδιού.

Βασικά θέματα προστασίας

Η διαδεδομένη χρήση του διαδικτύου σε εφαρμογές που περιλαμβάνουν επικοινωνίες ευαίσθητων δεδομένων εισάγει την ανάγκη για λύσεις στα προβλήματα ασφαλείας που υπάρχουν. Όλες οι επικοινωνίες μέσω Internet χρησιμοποιούν το πρωτόκολλο Transmission Control Protocol / Internet Protocol (TCP/IP). Το TCP/IP επιτρέπει να στέλνονται πληροφορίες από έναν Η/Υ σε έναν άλλο μέσω διαφόρων ενδιαμέσων Η/Υ και δικτύων. Αυτό σημαίνει ότι τρίτα μέρη μπορούν να παρεμβληθούν στην επικοινωνία με τους εξής τρόπους :

- Υποκλέπτοντας (Eavesdropping)
- Παραποιώντας (Tampering)
- Παραπλανώντας (Impersonation)
    - Σε επίπεδο προσώπου (Spoofing)
    - Σε επίπεδο οργανισμού (Misrepresentation)

Μια καλά σχεδιασμένη λύση σε αυτά τα προβλήματα αποτελεί η εκτεταμένη χρήση της κρυπτογραφίας που επιτρέπει για τις διακινούμενες πληροφορίες :

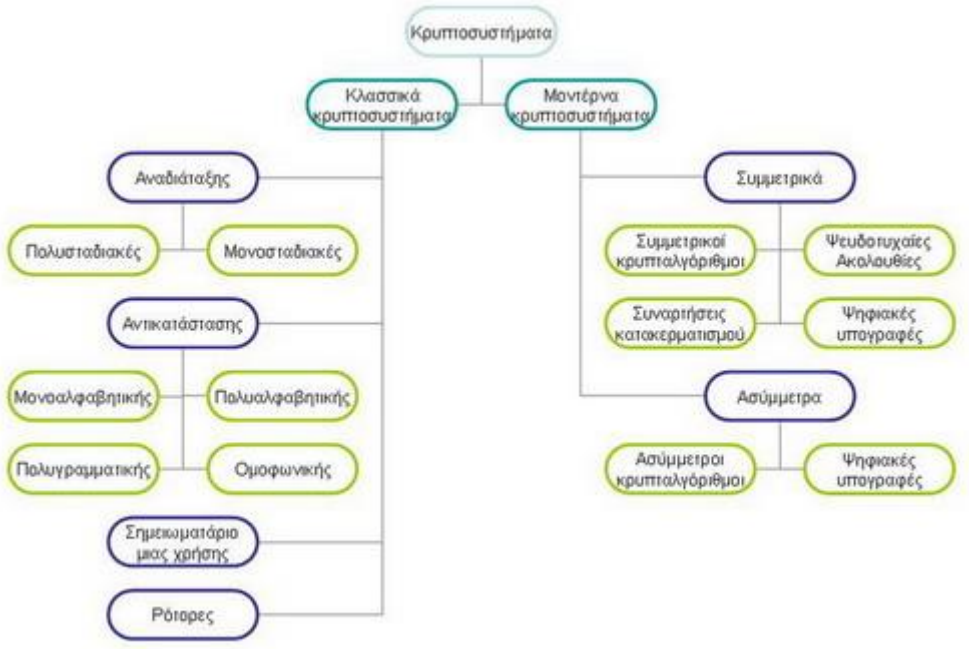
- Κρυπτογράφηση (encryption) και αποκρυπτογράφηση (decryption).
- Ανίχνευση αλλοιώσεων (tamper detection).

- Αυθεντικοποίηση του αποστολέα (authentication).
- Αδυναμία απάρνησης του αποστολέα (nonrepudiation).

Για την αντιμετώπιση αυτών των προβλημάτων αναπτύχθηκε η τεχνολογία των Υποδομών Δημοσίου Κλειδιού – ΥΔΚ (Public Key Infrastructure – PKI). Μια ΥΔΚ αποτελεί μια υποδομή ασφαλείας που ενσωματώνει τεχνολογίες όπως η κρυπτογράφηση δημοσίου κλειδιού, ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές, ώστε να διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των διακινουμένων δεδομένων, αλλά και η ταυτοποίηση και η ιδιότητα της μη απάρνησης για τα συναλλασσόμενα μέρη. Η ανάπτυξη μιας ΥΔΚ βασίζεται κυρίως στην κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography – PKC).

1.7 Κατηγορίες Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα χωρίζονται σε κατηγορίες ανάλογα με τα κλειδιά και τον τρόπο κρυπτογράφησης των μηνυμάτων. Οι δύο μεγαλύτερες κατηγορίες είναι τα Κλασικά Κρυπτοσυστήματα και τα Μοντέρνα. Στα σύγχρονα συστήματα συνήθως υιοθετείται μια μέθοδος ασύμμετρου – συμμετρικού όπου χρησιμοποιείται ασύμμετρο σύστημα για την μεταφορά του κλειδιού και μετά συμμετρικό σύστημα για την μεταφορά και κρυπτογράφηση – αποκρυπτογράφηση των δεδομένων. Με αυτό τον τρόπο εκμεταλλεύονται τα προτερήματα και των δύο συστημάτων.



Σχήμα 1.7 Μπλοκ ανάλυσης ειδών κρυπτοσυστήματος

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.

1.7.1 Κλασικά κρυπτοσυστήματα

Τα κλασικά κρυπτοσυστήματα χωρίζονται σε τέσσερις κατηγορίες:

- Αναδιάταξης
- Αντικατάστασης
- Σημειωματάριο μιας χρήσης
- Ρότορες

1.7.1.1 Αλγόριθμος του Καίσαρα

Χαρακτηριστικό παράδειγμα κρυπτοσυστήματος αντικατάστασης είναι ο αλγόριθμος του Καίσαρα. Σε αυτόν τον κρυπτογραφικό αλγόριθμο, το κλειδί αποτελεί μια μετάθεση των γραμμάτων της αλφαβήτου. Η κρυπτογράφηση περιλαμβάνει αντικατάσταση κάθε γράμματος με το αντίστοιχο γράμμα που προκύπτει από τη μετάθεση. Αντίστοιχα, η αποκρυπτογράφηση γίνεται με χρήση της αντίστροφης μετάθεσης.

Στον κρυπτογραφικό αλγόριθμο του Καίσαρα (Caesar cipher) το μήνυμα (αρχικό κείμενο) πρέπει να είναι μια ακολουθία από γράμματα. Κάθε γράμμα αντιστοιχίζεται με έναν αριθμό. Το κλειδί k είναι ένας αριθμός από το 1 ως το 25.

Κατά την κρυπτογράφηση το κλειδί k προστίθεται στον αριθμό κάθε γράμματος του μηνύματος και υπολογίζεται το υπόλοιπο της διαίρεσης του αθροίσματος με το πλήθος των γραμμάτων της αλφαβήτου (για το λατινικό αλφάβητο έχουμε modulo 26 αφού το πλήθος των γραμμάτων είναι 26). Έτσι, για παράδειγμα, εάν το κλειδί k είναι το 3, τότε το μήνυμα "SECURE" κρυπτογραφείται σε "VHFXUH". Πιο συγκεκριμένα για το γράμμα "S" προκύπτει το "V" γιατί το "S" έχει αντίστοιχο αριθμό το 18 και κρυπτογραφείται με τον υπολογισμό 18+3=21, οπότε 21mod26=21, που αντιστοιχεί στο γράμμα "V".

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Σχήμα 1.8 Πίνακας αντιστοίχησης γραμμάτων και αριθμών

Ο κρυπτογραφικός αλγόριθμος του Καίσαρα είναι ουσιαστικά ένας συνηθισμένος τύπος κρυπτογραφικού αλγορίθμου ροής. Η μοναδική διαφοροποίηση του έγκειται στο ότι λειτουργεί με υπολογισμό του modulo 26 και όχι του modulo 2. Είναι φανερό ότι είναι πολύ μικρή για να παρέχει ασφάλεια, καθώς αν ξαναδούμε τις απαιτήσεις της γεννήτριας παραγωγής κλειδιών ενός κρυπτογραφικού αλγορίθμου ροής θα δούμε ότι θέτοντας την ακολουθία κλειδοροής ίση με μια σταθερή τιμή παραβιάζονται όλα τα κριτήρια. Η περίοδος της ακολουθίας κλειδοροής είναι μόνο 1, η ακολουθία δεν είναι σίγουρα ψευδοτυχαία με οποιονδήποτε τρόπο μέτρησης και η γραμμική ισοδυναμία είναι επίσης 1, καθώς για την ακολουθία κλειδοροής s_i ισχύει ότι $s_i+1=s_i$.

Ο κρυπτογραφικός αλγόριθμος του Καίσαρα είναι πολύ εύκολο να σπάσει (κρυπταναλυθεί). Η μέθοδος της εκτεταμένης αναζήτησης θα δώσει αποτέλεσμα γιατί υπάρχουν μόνο 25 διαφορετικά κλειδιά, καθώς το σύνολο των κλειδιών είναι ίσο με το σύνολο των όλων των δυνατών μεταθέσεων των γραμμάτων, ίσο δηλαδή με το πλήθος των γραμμάτων του λατινικού αλφαβήτου.

Γενικότερα, παρά τον μεγάλο αριθμό κλειδιών, πράγμα που αποκλείει μια απλά επίθεση εξαντλητικής αναζήτησης (exhaustive search attack) , ένας κρυπτογραφικός αλγόριθμος απλής αντικατάστασης είναι εύκολο να σπάσει. Ένας λόγος είναι ότι σε κάθε φυσική γλώσσα τα γράμματα της αλφαβήτου παρουσιάζουν πολύ διαφορετικές συχνότητες εμφάνισης στις διάφορες προτάσεις π.χ. στα Ελληνικά το γράμμα Α είναι πολύ πιο συχνά επαναλαμβανόμενο σε σχέση με γράμματα όπως Ζ και το Ψ. Αυτή η πληροφορία συνδυαζόμενη με συχνότητες εμφάνισης συνδυασμών δύο ή τριών γραμμάτων μπορεί να χρησιμοποιηθεί για να εξαχθούν αντιστοιχίες μεταξύ του αρχικού και του κρυπτογραφημένου κειμένου, από τις οποίες είναι δυνατόν στη συνέχεια να προκύψει η τιμή του κλειδιού. Παραθέτουμε τον πίνακα με τη συχνότητα εμφάνισης κάθε γράμματος του λατινικού αλφαβήτου.

A	B	C	D	E	F	G	H	I	J	K	L	M
8%	1.5%	3%	4%	13%	2%	1.5%	6%	6.5%	0.5%	0.5%	3.5%	3%

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7%	8%	2%	0.2%	6.5%	6%	9%	3%	1%	1.5%	0.5%	2%	0.2%

1.7.1.2 Αλγόριθμος Vigenere

Ένας άλλος παρόμοιος κρυπτογραφικός αλγόριθμος είναι ο αλγόριθμος Vigenere. Σε αυτόν τα γράμματα αντιστοιχίζονται πάλι με τους αριθμούς από το 0 ως το 25, όπως ακριβώς και με τον κρυπτογραφικό αλγόριθμο του Καίσαρα. Όμως το μυστικό κλειδί, τώρα, δεν είναι ένας αριθμός, αλλά μια μικρή ακολουθία γραμμάτων, όπως για παράδειγμα μια λέξη.

Κατά την κρυπτογράφηση προστίθεται το αριθμητικό ισοδύναμο κάθε γράμματος του αρχικού κειμένου με το αριθμητικό ισοδύναμο ενός γράμματος του κλειδιού. Επειδή συνήθως το μήκος του αρχικού κειμένου είναι μεγαλύτερο από το μήκος του κλειδιού, τα γράμματα του κλειδιού ανακυκλώνονται και επαναλαμβάνεται η χρήση τους όσο χρειάζεται.

Αξίζει να σημειώσουμε ότι ο κρυπτογραφικός αλγόριθμος του Καίσαρα είναι μια ειδική περίπτωση του κρυπτογραφικού αλγορίθμου Vigenere για την περίπτωση που το μήκος της λέξης του κλειδιού είναι ίσο με 1. Έτσι για παράδειγμα, αν το κλειδί είναι η λέξη "SOS", η κρυπτογράφηση λειτουργεί ως εξής :

Αρχικό κείμενο	P	L	A	I	N	T	E	X	T
Κλειδοροή	S	O	S	S	O	S	S	O	S
Κρυπτογραφημένο κείμενο	H	Z	S	A	B	L	W	L	L

Όπως είναι φανερό, χρησιμοποιείται η ίδια αντιστοίχηση γραμμάτων αριθμών με τον κρυπτογραφικό αλγόριθμο του Καίσαρα. Αυτός ο αλγόριθμος ανήκει στην κατηγορία των αποκαλούμενων Κρυπτογραφικών Αλγορίθμων Πολυαλφαβητικής Αντικατάστασης (polyalphabetic substitution ciphers).

Ο κρυπτογραφικός αλγόριθμος Vigenere είναι και αυτός μια ειδική μορφή κρυπτογραφικού αλγορίθμου ροής. Ακριβώς όπως με τον κρυπτογραφικό αλγόριθμο του Καίσαρα, χρησιμοποιεί πρόσθεση με υπολογισμό του modulo 26 αντί για πρόσθεση με υπολογισμό του modulo 2 για να συνδυάσει το αρχικό κείμενο με την κλειδοροή. Η κλειδοροή είναι απλά η λέξη-κλειδί, η οποία επαναλαμβάνεται όσο χρειάζεται. Όμως πάλι παραβαίνει τους κανόνες των γεννητριών κλειδοροής. Η περίοδος της ακολουθίας κλειδοροής είναι φτωχές. Έτσι προκύπτει ότι φυσιολογικά ο κρυπτογραφικός αλγόριθμος Vigenere σπάει εύκολα.

1.7.1.3 Αλγόριθμος σημειωματάριου μιας χρήσης

Ο κρυπτογραφικός αλγόριθμος του σημειωματάριου μιας χρήσης (The one-time pad cipher) ή αλγόριθμος του Vernam είναι μια ειδική παραλλαγή κρυπτογραφικού αλγορίθμου ροής. Η ψευδοτυχαία κλειδοροή αντικαθίσταται από μια τυχαία (μη επαναλαμβανόμενη) ακολουθία δυαδικών ψηφίων (bits) η οποία χρησιμοποιείται μόνο μια φορά (από αυτό προκύπτει και ο χαρακτηρισμός "μιας χρήσης"). Αν χρησιμοποιηθεί σωστά, ο αλγόριθμος αυτός αποδεδειγμένα δεν είναι δυνατόν να σπάσει (unbreakable).

Το μοναδικό πρόβλημα αφόρα τη διαχείριση των κλειδιών. Πριν να καταστεί δυνατή η κρυπτογραφημένη επικοινωνία, τα δυο μέρη (αποστολέας και παραλήπτης) πρέπει να συμφωνήσουν σε τόσο υλικό τυχαίων κλειδιών όσα και τα δεδομένα που θα μεταδοθούν.

1.7.1.4 Μέθοδος της σκυτάλης

Είναι μια μέθοδος κρυπτογραφίας που χρησιμοποιούνταν από τους αρχαίους Έλληνες. Η μέθοδος κρυπτογραφίας αυτή αποτελείται από μια σκυτάλη η οποία έχει τυλιγμένη γύρω της μια λωρίδα δέρματος. Το κλειδί στην μυστικότητα του μηνύματος είναι η διάμετρος του κυλίνδρου (σκυτάλης).

Για παράδειγμα έστω ότι θέλουμε να κρυπτογραφήσουμε το μήνυμα: "Help me I am under attack". Αφού τυλίξουμε μια λωρίδα δέρματος γύρω από τη σκυτάλη, γράφουμε το μήνυμά μας.

	H	E	L	P	M
E	I	A	M	U	
N	D	E	R	A	
T	T	A	C	K	

Ξετυλίγοντας το δέρμα, θα πάρουμε το εξής κρυπτογραφημένο μήνυμα: "HENTEIDTLAEAPMRCMUAK".

Η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο. Ο παραλήπτης του μηνύματος αφού τυλίξει τη λωρίδα δέρματος γύρω από μια σκυτάλη ιδίας διαμέτρου με αυτή του αποστολέα θα μπορέσει να διαβάσει το αρχικό κείμενο: "Help me I am under attack".

Σχήμα 1.9 Η μέθοδος της σκυτάλης

1.7.2 Μοντέρνα κρυπτοσυστήματα

Τα μοντέρνα κρυπτοσυστήματα χωρίζονται με βάση τα κλειδιά σε:

- **Μυστικού ή Συμμετρικού Κλειδιού (Symmetric Key)**, χρησιμοποιούν το ίδιο μυστικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.
- **Δημοσίου ή Ασύμμετρου Κλειδιού (Public or Asymmetric Key)**, χρησιμοποιούν διαφορετικό κλειδί για κρυπτογράφηση (δημόσιο κλειδί παραλήπτη) και διαφορετικό για αποκρυπτογράφηση (προσωπικό κλειδί παραλήπτη).

1.7.2.1 Συμμετρικά Κρυπτοσυστήματα

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

Σχήμα 1.10 Μοντέλο Συμμετρικού Κρυπτοσυστήματος

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- **Τμήματος (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.

Συμμετρικοί Κρυπταλγόριθμοι Τμήματος (Block Ciphers) :

- Data Encryption Standard
- 3-Way
- Blowfish
- CAST
- CMEA
- Triple-DES
- DEAL FEAL
- GOST
- IDEA
- LOKI
- Lucifer
- MacGuffin
- Twofish
- MARS
- MISTY
- MMB
- NewDES
- RC2
- RC5
- RC6
- REDOC

- Rijndael
- Safer
- Serpent
- SQUARE
- Skipjack
- Tiny Encryption Algorithm

Συμμετρικοί Κρυπταλγόριθμοι Ροής (Stream Ciphers) :

- ORYX
- RC4
- SEAL

Εκτός από τα συμμετρικά κρυπτοσυστήματα DES, Triple – DES και AES, τα οποία θα αναλύσουμε εκτενέστερα στη συνέχεια, αξίζει να αναφερθούν κάποιες πληροφορίες και για τους παρακάτω αλγορίθμους:

- **Αλγόριθμος IDEA (International Data Encryption Algorithm)**

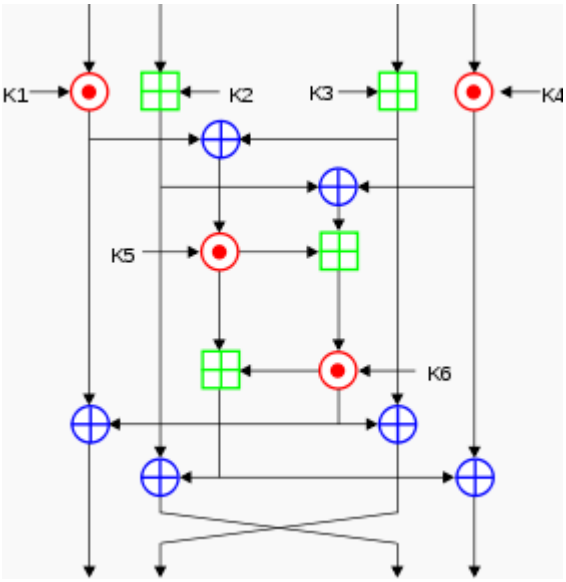
Ο αλγόριθμος International Data Encryption Algorithm – IDEA αποτελεί συμμετρικό κωδικοποιητή τμημάτων, που αναπτύχθηκε από τους X. Lai και J. Massey, στο Swiss Federal Institute of Technology, το 1991. Ο IDEA χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Ο IDEA διαφέρει από τον DES τόσο στη συνάρτηση F, όσο και στη συνάρτηση παραγωγής των υποκλειδιών. Για τη συνάρτηση F, ο IDEA δε χρησιμοποιεί S-boxes, αλλά στηρίζεται σε τρεις διαφορετικές μαθηματικές λειτουργίες: τη δυαδική πράξη XOR, τη δυαδική πρόσθεση ακεραίων των 16-bit και το δυαδικό πολλαπλασιασμό ακεραίων των 16-bit.

Οι συναρτήσεις συνδυάζονται με τρόπον ώστε να αναπτυχθεί ένας πολύπλοκος μετασχηματισμός που αναλύεται δύσκολα, ώστε να καθίσταται πολύ δύσκολη η διαδικασία κρυπτανάλυσης. Ο αλγόριθμος παραγωγής δευτερευόντων κλειδιών βασίζεται στη χρήση κυκλικών μετατοπίσεων, οι οποίες χρησιμοποιούνται με πολύπλοκο τρόπο για να παραχθούν συνολικά έξι δευτερεύοντα κλειδιά, για καθέναν από τους οκτώ γύρους του IDEA.

Παρόλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί 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.

Ο IDEA, που ήταν ένας από τους προτεινόμενους 128-bit αντικαταστάτες του DES, έχει υποβληθεί σε αξιοσημείωτη διερεύνηση και εμφανίζεται

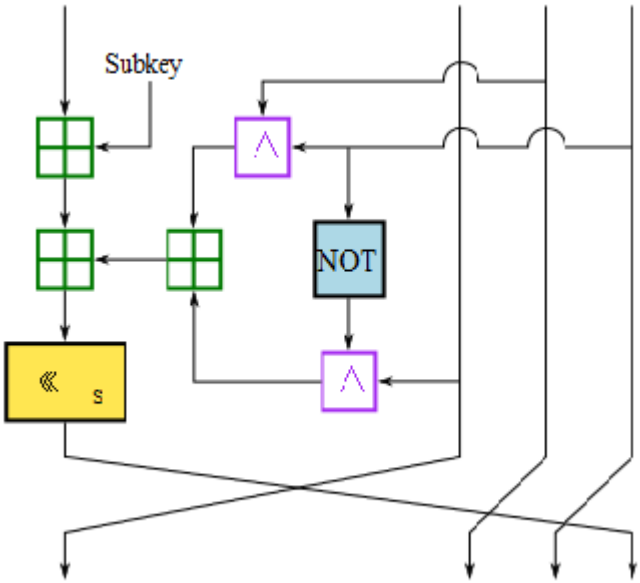
ανθεκτικός σε κρυπταναλυτικές επιθέσεις. Επίσης, χρησιμοποιείται στο προϊόν λογισμικού PGP ως μία από τις εναλλακτικές επιλογές, καθώς και σε διάφορα εμπορικά προϊόντα.



Σχήμα 1.11 Αλγόριθμος IDEA

- **Αλγόριθμος RC2**

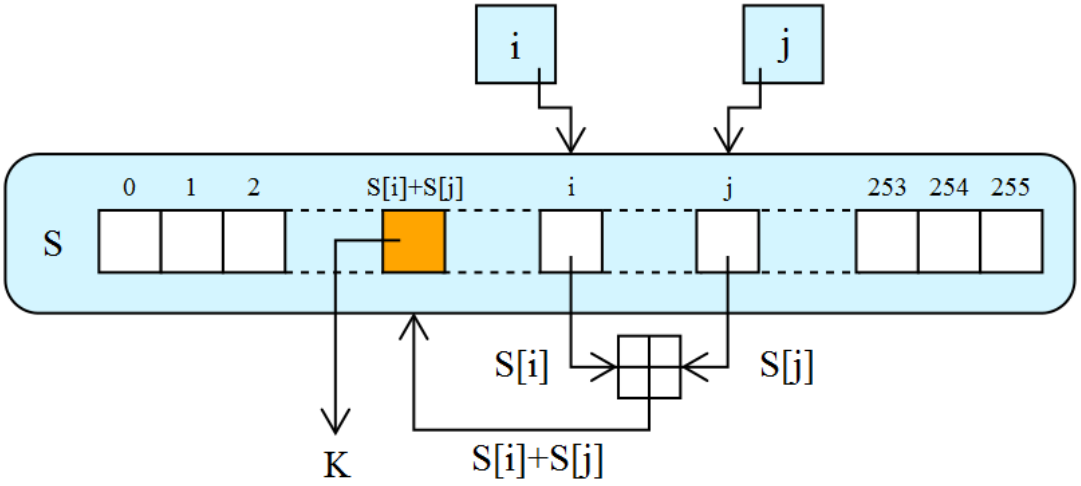
Ο κρυπτογραφικός αλγόριθμος RC2 αναπτύχθηκε από τον Ron Rivest της εταιρίας RSA Security το 1987. Είναι ένας κρυπταλγόριθμος τμήματος με μέγεθος block 64 bits που χρησιμοποιεί 18 γύρους σε δίκτυο Feistel. Βασικό χαρακτηριστικό του είναι ότι υποστηρίζει κλειδιά μεταβλητού μεγέθους από 8 έως 128 bits. Αν το μέγεθος του κλειδιού είναι μεγαλύτερο από 56 bit είναι ανεκτικότερος από τον κρυπτογραφικό αλγόριθμο DES.



Σχήμα 1.12 Αλγόριθμος RC2

➢ Αλγόριθμος RC4

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε από την Ron Rivest για λογαριασμό της RSA Inc το 1987 και δημοσιεύτηκε το 1994. Έχει μεταβλητό μήκος κλειδιού από 40 έως 2048 bits και λειτουργεί στο επίπεδο του byte. Χρησιμοποιεί 256 γύρους και 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.



Σχήμα 1.13 Αλγόριθμος RC4

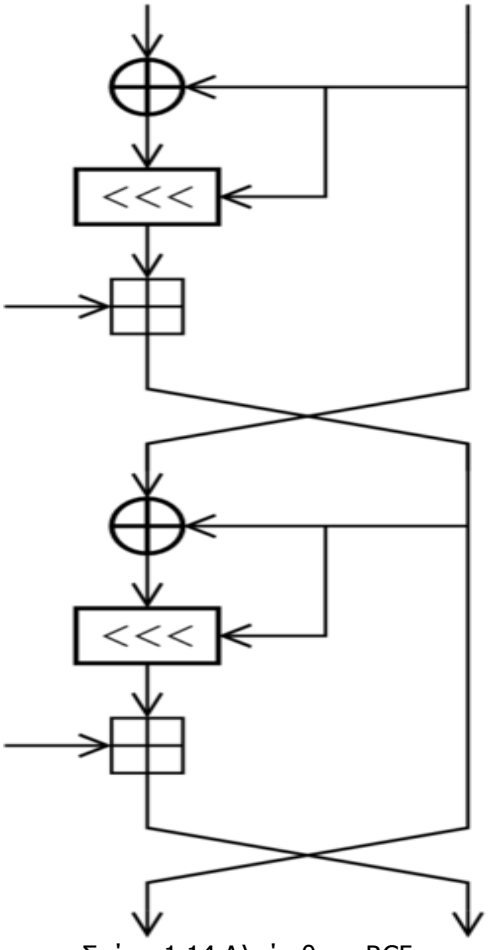
➢ Αλγόριθμος RC5

Ο RC5 αναπτύχθηκε το 1994 από τον R. Rivest, έναν από τους σχεδιαστές του αλγορίθμου δημοσίου κλειδιού RSA. Ο RC5 προσδιορίζεται στο RFC 2040 και σχεδιάστηκε για να υποστηρίζει τα ακόλουθα χαρακτηριστικά:

- Κατάλληλος για υλοποίηση σε υλικό ή λογισμικό: Ο RC5 χρησιμοποιεί μόνο βασικές υπολογιστικές λειτουργίες, που συνήθως περιλαμβάνονται στους μικροεπεξεργαστές.
- Ταχύς: Προκειμένου να επιτευχθεί υψηλή ταχύτητα, ο RC5 είναι ένας απλός αλγόριθμος που βασίζεται στη λέξη (word). Οι βασικές λειτουργίες του στηρίζονται σε πλήρεις λέξεις δεδομένων ανά στιγμή.
- Προσαρμόσιμος σε επεξεργαστές διαφορετικών μηκών λέξης: Ο αριθμός των δυαδικών ψηφίων σε μία λέξη αποτελεί παράμετρο του RC5, έτσι ώστε διαφορετικά μήκη λέξης παράγουν διαφορετικούς αλγορίθμους.
- Μεταβλητό μέγεθος block: Το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) ή 128 bits.

- Μεταβλητό μήκος γύρων: Ο αριθμός των γύρων αποτελεί δεύτερη παράμετρο του RC5 και παίρνει τιμές από 1 έως 255. Αυτή η παράμετρος επιτρέπει την εναλλαγή μεταξύ υψηλότερης ταχύτητας και υψηλότερης ασφάλειας.
- Μεταβλητό μήκος κλειδιού: Το μήκος κλειδιού αποτελεί την τρίτη παράμετρο του RC5 και παίρνει τιμές από 0 έως 2040 bits. Επίσης επιτρέπει την εναλλαγή μεταξύ υψηλότερης ταχύτητας και υψηλότερης ασφάλειας.
- Απλός: Η απλή δομή του RC5 υλοποιείται εύκολα και διευκολύνει τον υπολογισμό της ισχύος του αλγορίθμου.
- Χαμηλή απαίτηση μνήμης: Η χαμηλή απαίτηση μνήμης καθιστά τον αλγόριθμο RC5 κατάλληλο για αξιοποίηση σε έξυπνες κάρτες και άλλες συσκευές περιορισμένης μνήμης.
- Υψηλή ασφάλεια: Ο RC5 προορίζεται για να παρέχει υψηλή ασφάλεια με προσδιορισμό των κατάλληλων παραμέτρων.
- Περιστροφές εξαρτώμενες από τα δεδομένα: Ο RC5 ενσωματώνει τις περιστροφές, δηλαδή κυκλικές μετατοπίσεις δυαδικών ψηφίων, των οποίων ο αριθμός είναι στοιχείο εξαρτώμενο από τα δεδομένα. Το γεγονός αυτό ενισχύει τον αλγόριθμο ενάντια στην κρυπτανάλυση.

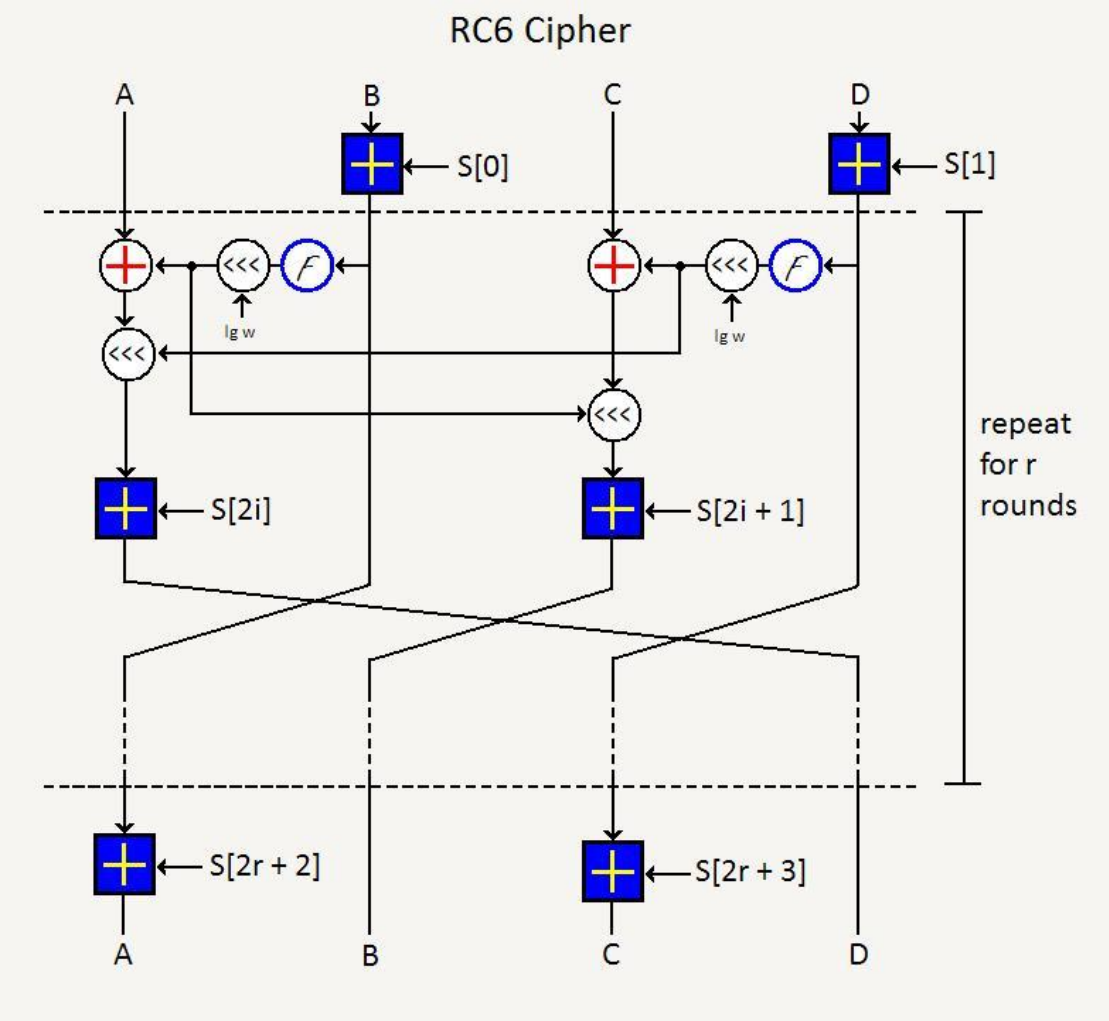
Ο RC5 χρησιμοποιείται σε διάφορα προϊόντα από την RSA Data Security, Inc.



Σχήμα 1.14 Αλγόριθμος RC5

➢ Αλγόριθμος RC6

Ο αλγόριθμος RC6 δημοσιεύτηκε το 1998 και περιλαμβάνει 20 κύκλους μετασχηματισμών. Σε όλους τους κύκλους διεξάγεται μεταβλητή περιστροφή δεδομένων και οι πράξεις που λαμβάνουν χώρα είναι πολλαπλασιασμός, πρόσθεση, XOR και πρόσθεση υποκλειδιών. Έχει μέγεθος τμήματος 128 bits και μέγεθος κλειδιού 128, 192 ή 256 bits.



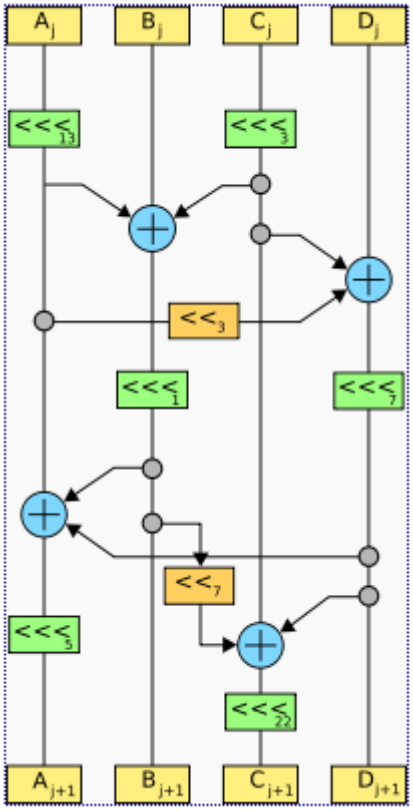
Σχήμα 1.15 Αλγόριθμος RC6

➢ Αλγόριθμος MARS

Ο αλγόριθμος MARS περιλαμβάνει 32 κύκλους μετασχηματισμών. Από αυτούς, μόνον οι 16 κύκλοι βασίζονται στο μυστικό κλειδί και οι πράξεις που λαμβάνουν χώρα είναι ο πολλαπλασιασμός, η πρόσθεση με κλειδιά των 32-bit και η ολίσθηση ή περιστροφή των δεδομένων. Οι υπόλοιποι 16 κύκλοι αξιοποιούν 8 S-boxes των 32 bit με πράξεις πρόσθεσης και XOR.

➢ Αλγόριθμος Serpent

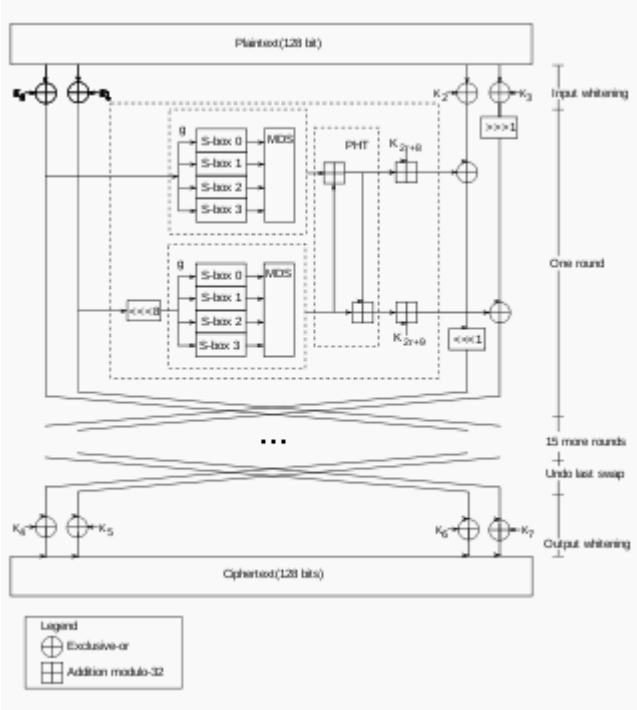
Ο αλγόριθμος Serpent περιλαμβάνει 32 κύκλους μετασχηματισμών. Στον αλγόριθμο προσδιορίζεται μία αρχική και μία τελική μετάθεση, οι οποίες διευκολύνουν εναλλακτικούς τρόπους λειτουργίας. Σε καθέναν από τους 32 κύκλους περιλαμβάνονται τρία επιμέρους επίπεδα μετασχηματισμών: η πράξη XOR με το υποκλειδί, 32 παράλληλες εφαρμογές ενός από τα 8 S-boxes και ένας γραμμικός μετασχηματισμός.



Σχήμα 1.16 Αλγόριθμος Serpent

➢ Αλγόριθμος Twofish

Ο αλγόριθμος Twofish περιλαμβάνει 16 κύκλους, σε καθέναν από τους οποίους εφαρμόζονται 4 S-boxes τα οποία εξαρτώνται από το μυστικό κλειδί. Τα επόμενα στάδια περιλαμβάνουν την αξιοποίηση σταθερών S-boxes, τη διενέργεια μετασχηματισμού pseudo-Hadamard, καθώς και την πρόσθεση του υποκλειδιού.



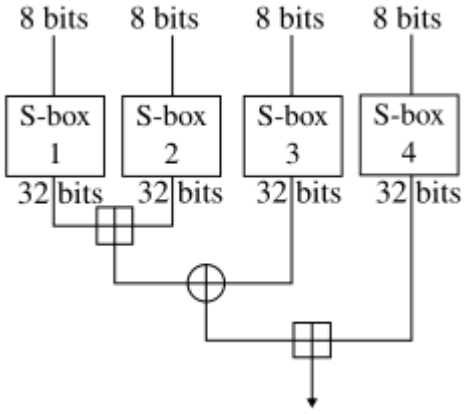
Σχήμα 1.17 Αλγόριθμος Twofish

➢ Αλγόριθμος Blowfish

Ο αλγόριθμος Blowfish αναπτύχθηκε το 1993 από τον επιφανή κρυπτογράφο B. Schneier και καθιερώθηκε ως μία από τις δημοφιλέστερες εναλλακτικές λύσεις του DES. Ο Blowfish δημιουργήθηκε ώστε να είναι εύκολος στην υλοποίηση και να παρουσιάζει μεγάλη ταχύτητα εκτέλεσης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθόλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος. Πρόκειται για ένα συνεπτυγμένο αλγόριθμο με μέγεθος block 64 bits που χρησιμοποιεί δίκτυο Feistel και που μπορεί να εκτελεστεί σε μνήμη μικρότερη από 5K. Ενδιαφέρον χαρακτηριστικό γνώρισμα του Blowfish αποτελεί το μήκος κλειδιού, το οποίο είναι μεταβλητό, μπορεί να λάβει τιμές έως 448 bits, αν και πρακτικά χρησιμοποιούνται κλειδιά των 128 bits. Ο Blowfish χρησιμοποιεί 16 γύρους.

Όπως ο αλγόριθμος DES, ο αλγόριθμος Blowfish χρησιμοποιεί S-boxes, XOR, καθώς και δυαδική πρόσθεση. Αντίθετα από τον DES που χρησιμοποιεί σταθερά S-boxes, ο Blowfish χρησιμοποιεί δυναμικά S-boxes που παράγονται ως συνάρτηση του κλειδιού. Στον Blowfish, τα υποκλειδιά και τα S-boxes παράγονται από την επανειλημμένη εφαρμογή του ίδιου του αλγορίθμου Blowfish στο κλειδί. Συνολικά απαιτούνται 521 εκτελέσεις του αλγορίθμου κρυπτογράφησης Blowfish για την παραγωγή των υποκλειδιών και των S-boxes. Απόρροια των χαρακτηριστικών αυτών είναι το συμπέρασμα ότι ο Blowfish δεν είναι κατάλληλος για εφαρμογές στις οποίες το μυστικό κλειδί αλλάζει συχνά.

Ο Blowfish περιλαμβάνεται στους καλύτερους συμβατικούς αλγορίθμους κρυπτογράφησης που έχουν εφαρμοστεί, αφού τα υποκλειδιά και τα S-boxes παράγονται από διαδικασία επανειλημμένων εφαρμογών του Blowfish στον εαυτό του. Οι επαναλήψεις αυτές τροποποιούν πλήρως τα δυαδικά ψηφία και καθιστούν την κρυπτανάλυση εξαιρετικά δύσκολη. Οι μέχρι σήμερα δημοσιεύσεις των προσπαθειών για κρυπτανάλυση του Blowfish δεν αναφέρουν πρακτικές αδυναμίες. Ο Blowfish χρησιμοποιείται, επίσης, σε διάφορες εμπορικές εφαρμογές.



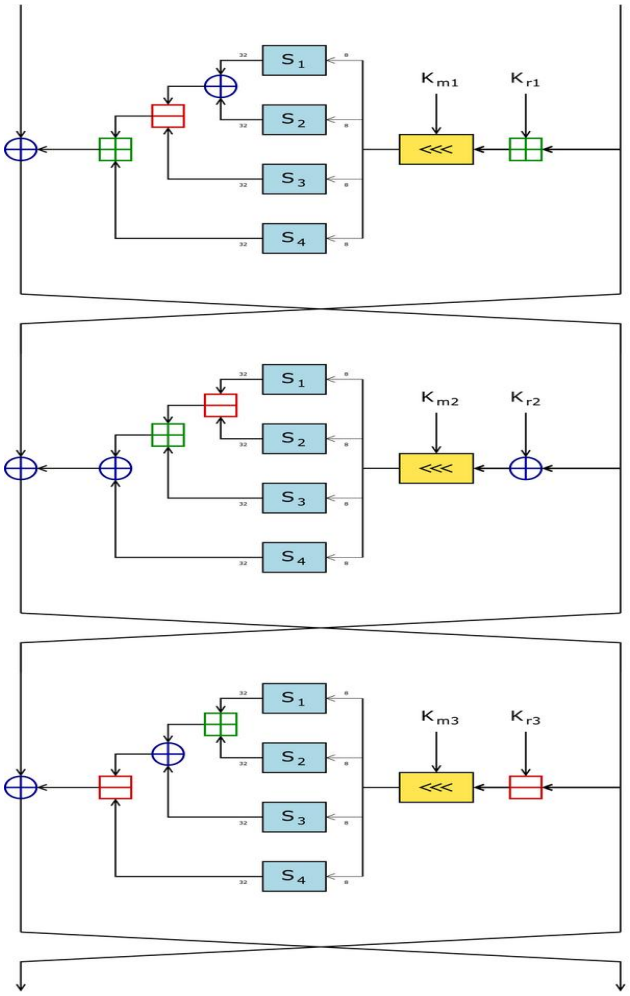
Σχήμα 1.18 Αλγόριθμος Blowfish

- **Αλγόριθμος CAST-128**

Το CAST αποτελεί μία διαδικασία σχεδίασης συμμετρικών αλγορίθμων κρυπτογράφησης, η οποία αναπτύχθηκε το 1996 από τους C. Adams και S. Tavares της εταιρίας Entrust Technologies. Ένας συγκεκριμένος αλγόριθμος που αναπτύχθηκε ως τμήμα του προγράμματος CAST είναι ο CAST-128 που ορίστηκε στο RFC 2144. Ο αλγόριθμος αυτός έχει μέγεθος τμήματος 64 bits, χρησιμοποιεί 12 ή 16 γύρους σε δίκτυο Feistel κι έχει μήκος κλειδιού που λαμβάνει τιμές από 40 bits έως 128 bits, με βήματα των 8 bits. Το CAST είναι το αποτέλεσμα μιας μακράς χρονικά διαδικασίας έρευνας και ανάπτυξης και έχει ενσωματώσει σειρά σχολίων από κρυπταναλυτές. Σε πρώτη φάση είχε χρησιμοποιηθεί σε διάφορα προϊόντα, συμπεριλαμβανομένου και του PGP.

Το CAST χρησιμοποιεί σταθερά S-boxes, αλλά μόνον αυτά που είναι σημαντικά μεγαλύτερα των S-boxes που χρησιμοποιούνται στο DES. Τα S-boxes σχεδιάστηκαν προσεκτικά, ώστε να μην παρουσιάζουν γραμμικότητα στη σχέση εισόδου και εξόδου, συνεπώς να είναι ανθεκτικά σε κρυπταναλυτικές επιθέσεις. Η διαδικασία παραγωγής υποκλειδιών που χρησιμοποιείται στον CAST-128 είναι διαφορετική από αυτήν που υιοθετείται σε άλλους συμβατικούς αλγορίθμους κρυπτογράφησης τμημάτων. Οι σχεδιαστές του CAST προσπάθησαν να δημιουργήσουν υποκλειδιά με μεγαλύτερο βαθμό ανθεκτικότητας σε γνωστές κρυπταναλυτικές επιθέσεις. Θεωρήθηκε ότι η χρήση μη-γραμμικών S-boxes για παραγωγή κλειδιών από

το βασικό κλειδί, παρείχε αυτή την ισχύ. Αξιοσημείωτο χαρακτηριστικό γνώρισμα του CAST-128 αποτελεί η συνάρτηση κύκλου F, η οποία διαφέρει από γύρο σε γύρο, καθιστώντας τον αλγόριθμο κρυπταναλυτικά ανθεκτικότερο.



Σχήμα 1.19 Αλγόριθμος CAST-128

1.7.2.2 Ασύμμετρα κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Εφευρέθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman με σκοπό να παρέχει ένα τελείως διαφορετικό μοντέλο διαχείρισης των κρυπτογραφικών κλειδιών. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν διαμοιράζονται ένα μυστικό κλειδί αλλά αντιθέτως έχουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Όπως αναφέρθηκε προηγουμένως, ενώ η συμμετρική κρυπτογραφία μπορεί να εξασφαλίσει την εμπιστευτικότητα των δεδομένων, δε μπορεί να εγγυηθεί για την ταυτότητα του αποστολέα. Επιπλέον, παρόλο που τα δεδομένα μπορούν να μεταδοθούν με ασφάλεια μετά την κρυπτογράφηση, είναι δύσκολη η διανομή του μυστικού κλειδιού με ασφάλεια. Η ασύμμετρη

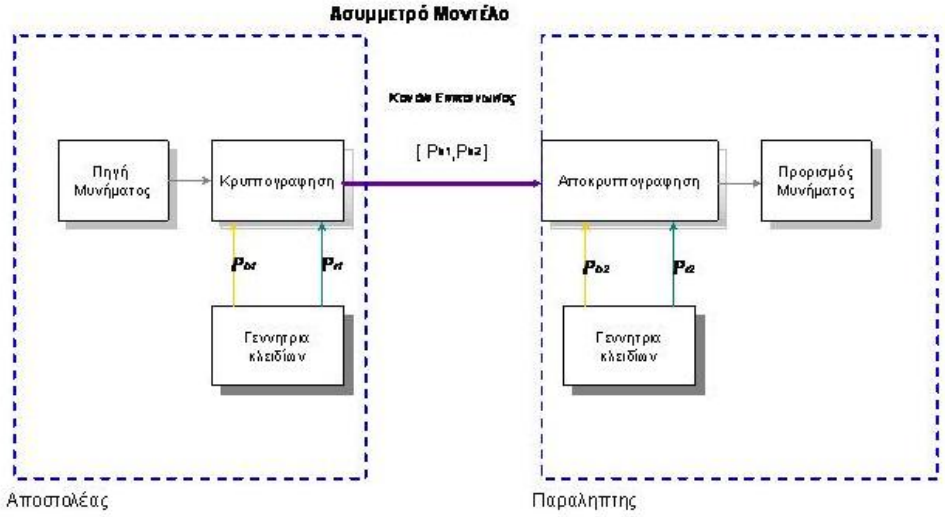
κρυπτογραφία (ή δημοσίου κλειδιού) αναλαμβάνει να λύσει πολλά από τα προβλήματα της συμμετρικής.

Η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική. Η ιδιωτική κλείδα δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνο που γνωρίζει την ιδιωτική κλείδα.

Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.



Σχήμα 1.20 Μοντέλο Ασύμμετρου Κρυπτοσυστήματος

Λίστα Ασύμμετρων Κρυπταλγορίθμων

- RSA
- Ανταλλαγή κλειδιού Diffie–Hellman
- DSA
- Paillier
- El Gamal
- Κρυπτογραφία ελλειπτικών καμπυλών (ECC)

Αξίζει να αναφερθούν κάποιες πληροφορίες και για τους παρακάτω αλγορίθμους δημοσίου κλειδιού:

➢ Αλγόριθμος RSA

Το πρώτο πραγματικά χρήσιμο σύστημα δημοσίου κλειδιού αναπτύχθηκε από τους Rivest, Shamir και Adleman (RSA) στα τέλη της δεκαετίας του 1970. Η ασφάλεια του συστήματος RSA βασίζεται στη δυσκολία εύρεσης παραγόντων (prime factors) πολύ μεγάλων αριθμών.

Για την απόκτηση ζεύγους κλειδιών RSA, ο χρήστης Α διαλέγει πρώτα δύο πολύ μεγάλους πρώτους αριθμούς p και q (μήκους τουλάχιστον 200 bits) και υπολογίζει τον προς δημοσίευση συντελεστή (modulus) :

$$n=p\times q.$$

Ο χρήστης Α επιλέγει ακόμη ένα (ιδιωτικό) εκθέτη κρυπτογράφησης (encryption exponent) e , τέτοιο ώστε:

$$\text{ΜΚΔ}(e,(p-1)*(q-1))=1,$$

όπου το ΜΚΔ σημαίνει "μέγιστος κοινός διαιρέτης", δηλαδή ότι το e δεν έχει κοινούς παράγοντες με τα (p −1) και (q −1) .

Το δημόσιο κλειδί αποτελείται από το ζεύγος αριθμών n και e. Το ιδιωτικό κλειδί υπολογίζεται κατόπιν, ως εξής:

$$d=e^{-1}(\mathrm{mod}(p-1)(q-1)),$$
$$\text{όπου } e\times d=1\mathrm{mod}(p-1)(q-1).$$

Ο χρήστης Α κοινοποιεί το ζεύγος (e,n), καθώς αυτό είναι πλέον το δημόσιο κλειδί του, αλλά κρατάει για δική του αποκλειστική χρήση τα d, p και q. Για την κρυπτογράφηση κάθε μηνύματος m, ο χρήστης Β το αναπαριστά ως ένα αριθμό m (όπου το μήκος του m είναι μικρότερο από το μήκος του n) και υπολογίζει τη σχέση:

$$c=m^{e}(\mathrm{mod}(n)).$$

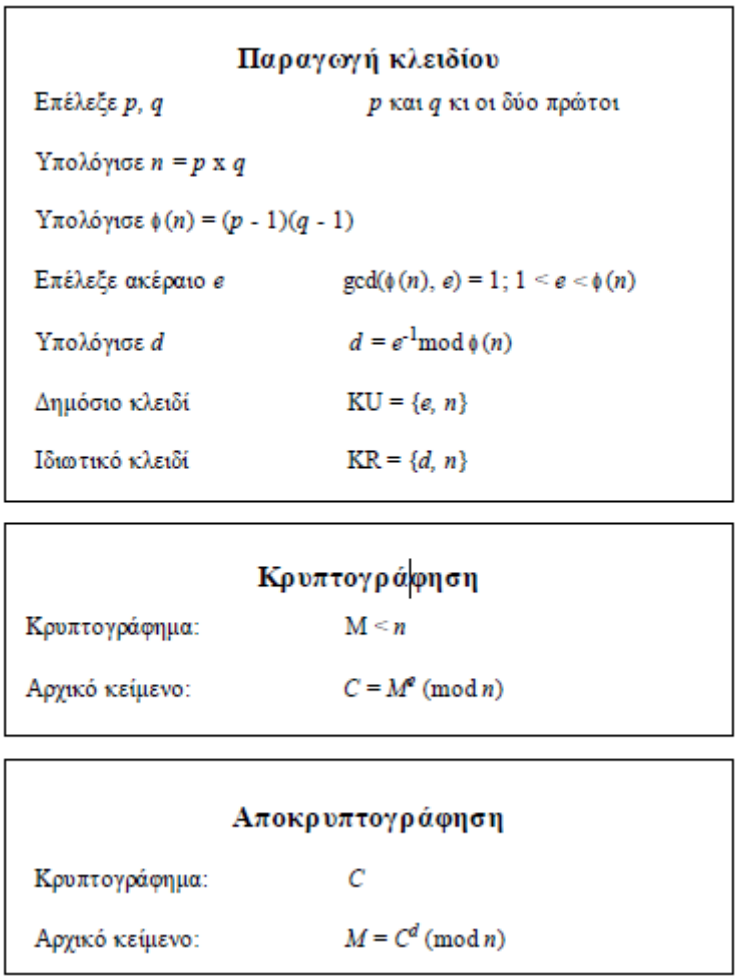
Αν το μήνυμα είναι πολύ μεγάλο, δηλαδή ο αριθμός των bits ξεπερνά τον αριθμό των bits του συντελεστή n, τότε το μήνυμα πρέπει να σπάσει σε τμήματα (blocks). Κάθε ένα από αυτά τα τμήματα κρυπτογραφείται σε κρυπτογραφημένα τμήματα c_i με το κλειδί κρυπτογράφησης (δημόσιο) και την ακόλουθη συνάρτηση :

$$c_i=m_i^{e}(\mathrm{mod}(n)).$$

Για την αποκρυπτογράφηση ο χρήστης Α χρησιμοποιεί το (προσωπικό) κλειδί αποκρυπτογράφησης και ακολουθεί την συνάρτηση :

$$m_i=c_i^{d}(\mathrm{mod}(n)).$$

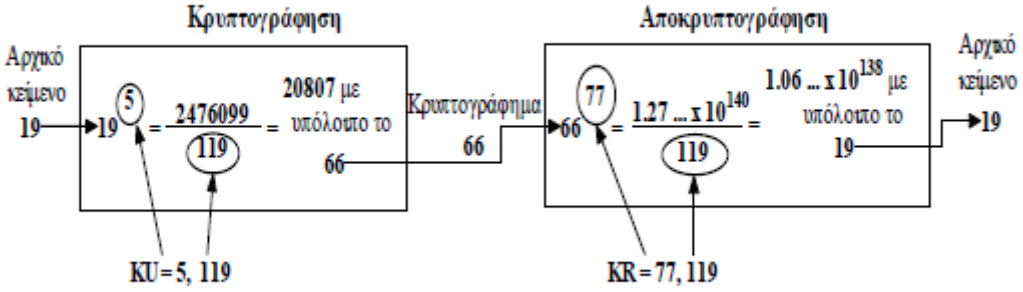
Μόνο ο χρήστης Α μπορεί να κάνει κάτι τέτοιο, αφού μόνο αυτός διαθέτει τον εκθέτη αποκρυπτογράφησης (decryption exponent) d.



Σχήμα 1.21 Αλγόριθμος RSA

Για να γίνει αντιληπτός ο αλγόριθμος RSA στη συνέχεια παραθέτουμε ένα παράδειγμα για τις ανάγκες του οποίου, τα κλειδιά δημιουργήθηκαν ως εξής:

1. Επιλέχθηκαν δύο πρώτοι αριθμοί, p=7 και q=17.
2. Υπολογίσθηκε η τιμή του n=pq=7*17=119.
3. Υπολογίσθηκε η τιμή του φ(n)=(p-1)(q-1)=96.
4. Επιλέχθηκε το e, το οποίο είναι πρώτος αριθμός ως προς το φ(n)=96 και μικρότερο του φ(n). Στην περίπτωση αυτή e=5.
5. Προσδιορίστηκε το d έτσι, ώστε de=1 mod 96 και d<96. Η σωστή τιμή του d είναι 77, γιατί 77*5=385=4*96+1.



Σχήμα 1.22 Παράδειγμα αλγορίθμου RSA

Με τη διαδικασία αυτή υπολογίσθηκε το δημόσιο κλειδί KU={5,119} και το ιδιωτικό κλειδί KR={77,119}. Το παράδειγμα παρουσιάζει τη χρήση αυτών των κλειδιών για ένα αρχικό κείμενο με M=19. Για την κρυπτογράφηση, το 19 υψώνεται στην 5η δύναμη δίνοντας αποτέλεσμα 2476099. Διαιρούμενο με το 119 δίνει υπόλοιπο 66. Άρα, $19^5 = 66 \bmod 199$ και το κρυπτογραφημένο κείμενο είναι C=66. Για την αποκρυπτογράφηση προκύπτει ότι $66^{77} = 19 \bmod 119$.

Υπάρχουν δύο πιθανές προσεγγίσεις με τις οποίες είναι δυνατόν να προκληθεί επιτυχημένη επίθεση στον RSA αλγόριθμο. Η πρώτη είναι η προσέγγιση της εξαντλητικής αναζήτησης: δοκιμάζονται όλα τα πιθανά ιδιωτικά κλειδιά. Έτσι, όσο μεγαλύτερο πλήθος bits χρησιμοποιείται για τα e,d τόσο πιο ασφαλής είναι ο αλγόριθμος. Παρόλα αυτά, επειδή απαιτούνται πολύπλοκοι υπολογισμοί τόσο κατά τη δημιουργία των κλειδιών όσο και κατά την κρυπτογράφηση και αποκρυπτογράφηση, όσο μεγαλύτερο είναι το μέγεθος των κλειδιών τόσο βραδύτερος θα είναι ο ρυθμός λειτουργίας του συστήματος.

Οι περισσότερες, όμως, συζητήσεις για την κρυπτανάλυση του RSA έχουν επικεντρωθεί στη διαδικασία ανεύρεσης δύο πρώτων αριθμών που να είναι παράγοντες του n. Για ένα μεγάλο αριθμό n, η διαδικασία αυτή αποτελεί δύσκολο πρόβλημα αλλά όχι σε τόσο μεγάλο βαθμό όσο ήταν τα προηγούμενα χρόνια. Για παράδειγμα, τον Ιανουάριο του 1977 οι σχεδιαστές του RSA ζήτησαν από τους αναγνώστες του επιστημονικού περιοδικού Scientific American να αποκρυπτογραφήσουν ένα κρυπτογραφημένο μήνυμα που είχαν δημοσιεύσει σε στήλη του περιοδικού. Μάλιστα, προσέφεραν αμοιβή 100 δολαρίων για μία μόνο πρόταση του αποκρυπτογραφημένου κειμένου, γεγονός που εκτιμούσαν πως δεν είναι δυνατό να συμβεί στα επόμενα 40 τετράκις εκατομμύρια χρόνια. Όμως τον Απρίλιο του 1994, μία ερευνητική ομάδα που εργαζόταν αξιοποιώντας την υπολογιστική ισχύ 1600 υπολογιστών στο Internet κέρδισε το βραβείο μετά από 8 μήνες προσπάθεια. Στην περίπτωση αυτή, χρησιμοποιήθηκε δημόσιο κλειδί μεγέθους 129 δεκαδικών ψηφίων (μήκος του n), δηλαδή περίπου 428 bits. Επιπλέον, το 1996 αναλύθηκε σε γινόμενο πρώτων παραγόντων ένας αριθμός 130 ψηφίων με 10 φορές

λιγότερες πράξεις από όσες είχαν απαιτηθεί κατά την ανάλυση του αριθμού με 129 ψηφία. Τα αποτελέσματα αυτά, βεβαίως, με κανένα τρόπο δε μειώνουν τις δυνατότητες του RSA. Απλώς σημαίνουν ότι πρέπει να χρησιμοποιούνται μεγαλύτερα μεγέθη κλειδιών. Ένα κλειδί μεγέθους 2048 bits θεωρείται ισχυρό για όλες τις σημερινές τυπικές εφαρμογές.

- **Ανταλλαγή Κλειδιού Diffie – Hellman**

Ο πρώτος αλγόριθμος για ασύμμετρο κρυπτοσύστημα δημοσιεύτηκε στην εργασία των Diffie - Hellman που όριζε την κρυπτογραφία με ασύμμετρο κρυπτοσύστημα και είναι γνωστός ως ανταλλαγή κλειδιών κατά Diffie-Hellman (Diffie-Helmann key exchange). Ένας σημαντικός αριθμός προϊόντων υιοθέτησε αυτή την τεχνική.

Σκοπός του αλγορίθμου είναι να καταστήσει εφικτή και ασφαλή μεταξύ δύο χρηστών την ανταλλαγή ενός μυστικού κλειδιού, το οποίο ακολούθως θα χρησιμοποιηθεί για κρυπτογράφηση μηνυμάτων. Ο αλγόριθμος περιορίζεται ακριβώς στην ανταλλαγή των κλειδιών.

Η αποτελεσματικότητά του αλγορίθμου Diffie-Hellman βασίζεται στη δυσκολία υπολογισμού διακριτών λογαρίθμων. Συνοπτικά, ο διακριτός λογάριθμος ορίζεται ως εξής: Αρχικά προσδιορίζεται μία αρχική (primitive) ρίζα ενός πρώτου αριθμού p τέτοιου, ώστε οι δυνάμεις του να παράγουν όλους τους ακέραιους από το 0 ως το p-1. Έτσι, αν a είναι μία ρίζα του πρώτου αριθμού p, τότε οι αριθμοί $a \bmod p$, $a^2 \bmod p$, …, $a^{p-1} \bmod p$ αποτελούν τους ακεραίους από το 1 έως το p-1 με κάποια μετάθεση.

Για οποιοδήποτε ακέραιο b και για μία αρχική ρίζα a ενός πρώτου αριθμού p, μπορεί να βρεθεί ένας μοναδικός πρώτος αριθμός i, τέτοιος, ώστε $b=a^i \bmod p$ όπου $0 \le i \le (p-1)$.

Ο εκθέτης i αναφέρεται ως ο διακριτός λογάριθμος ή δείκτης (index) του b για βάση a, mod p και συμβολίζεται $i=\text{ind}_{a,p}(b)$.

Με βάση τα παραπάνω μπορεί να οριστεί η ανταλλαγή κλειδιών κατά Diffie-Hellman, η οποία παρουσιάζεται συνοπτικά στο Σχήμα 1.23. Για αυτήν την τεχνική απαιτείται να υπάρχουν δύο δημοσίως γνωστοί αριθμοί. Ένας πρώτος αριθμός q και ένας ακέραιος a που είναι η αρχική ρίζα του q.

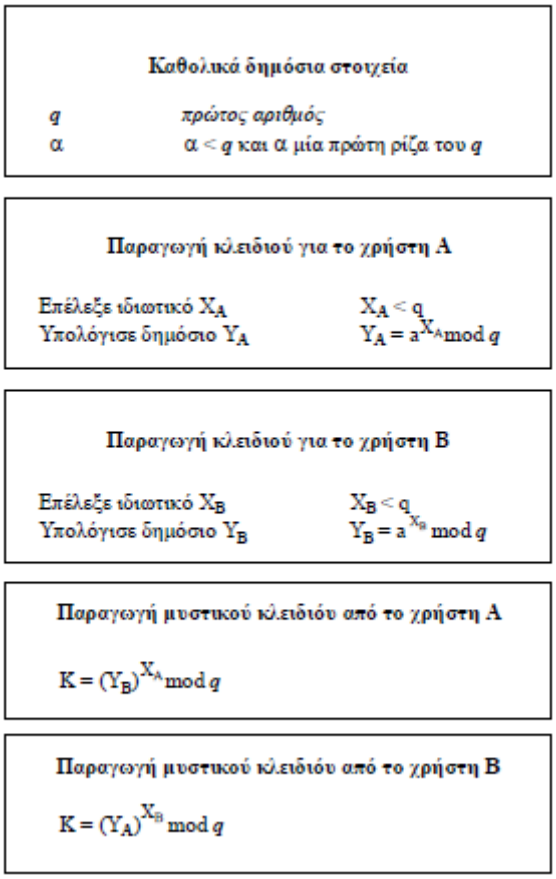
Έστω ότι οι A και B επιθυμούν να ανταλλάξουν ένα κλειδί. Ο A επιλέγει ένα τυχαίο ακέραιο X_A με $X_A<q$ και υπολογίζει το $Y_A=a^{X_A} \bmod q$. Ομοίως, ο B επιλέγει ανεξάρτητα από τον A έναν τυχαίο ακέραιο X_B με $X_B<q$ και υπολογίζει το $Y_B=a^{X_B} \bmod q$. Κάθε πλευρά κρατά μυστική την αντίστοιχη

τιμή του Χ, δηλαδή τα X_A, X_B και θέτει την αντίστοιχη ποσότητα Υ δημοσίως διαθέσιμη στην άλλη πλευρά. Ο Α υπολογίζει το κλειδί σύμφωνα με τη σχέση $K=(Y_B)^{X_A} \text{mod} q$, όπως επίσης και ο Β σύμφωνα με τη σχέση $K=(Y_A)^{X_B} \text{mod} q$. Όπως αποδεικνύεται παρακάτω, αυτές οι δύο σχέσεις παράγουν το ίδιο αποτέλεσμα:

$$
\begin{aligned}
K=(Y_B)^{X_A} \text{mod} q &= \\
&= (a^{X_B} \text{mod} q)^{X_A} \text{mod} q = \\
&= (a^{X_B})^{X_A} \text{mod} q = \\
&= a^{X_B X_A} \text{mod} q = \\
&= (a^{X_A})^{X_B} \text{mod} q = \\
&= (a^{X_A} \text{mod} q)^{X_B} \text{mod} q = \\
&= (Y_A)^{X_B} \text{mod} q
\end{aligned}
$$

Με τη διαδικασία αυτή, οι δύο πλευρές επιτυγχάνουν την ανταλλαγή ενός μυστικού κλειδιού. Εφόσον τα X_A και X_B είναι μυστικά, ένας επιτιθέμενος έχει μόνον τα ακόλουθα στοιχεία για να αποπειραθεί να κρυπταναλύσει τον αλγόριθμο: q, a, Y_A, Y_B. Έτσι είναι αναγκασμένος να υπολογίσει ένα διακριτό λογάριθμο, για να κατορθώσει να υπολογίσει το κλειδί. Για παράδειγμα, αν επιτεθεί στην πλευρά του Β θα πρέπει να υπολογίσει την ποσότητα $X_B=\text{ind}_{a,q}(Y_B)$. Ο επιτιθέμενος στη συνέχεια, θα μπορεί να υπολογίσει το κλειδί Κ με τον ίδιο τρόπο που το υπολογίζει και ο Β.

Η ασφάλεια της ανταλλαγής κλειδιού κατά Diffie-Hellman έγκειται στο γεγονός ότι ενώ είναι υπολογιστικά εύκολο να υπολογιστεί η ποσότητα $a^X \text{mod} q$, είναι πολύ δύσκολο να υπολογιστούν οι διακριτοί λογάριθμοι. Και για μεγάλους πρώτους αριθμούς το πρόβλημα θεωρείται ανέφικτο να επιλυθεί.



Σχήμα 1.23 : Ανταλλαγή κλειδιών κατά Diffie – Hellman

Ένα τυπικό αριθμητικό παράδειγμα περιλαμβάνει τα ακόλουθα βήματα:

Η ανταλλαγή κλειδιών βασίζεται στη χρήση του πρώτου αριθμού q=71 και μιας αρχικής ρίζας του 71, έστω την a=7. Οι Α και Β επιλέγουν ως ιδιωτικά κλειδιά, αντιστοίχως, X_A=5 και X_B=12. Τα δημόσια κλειδιά υπολογίζονται χωριστά από κάθε επικοινωνούντα ως ακολούθως:

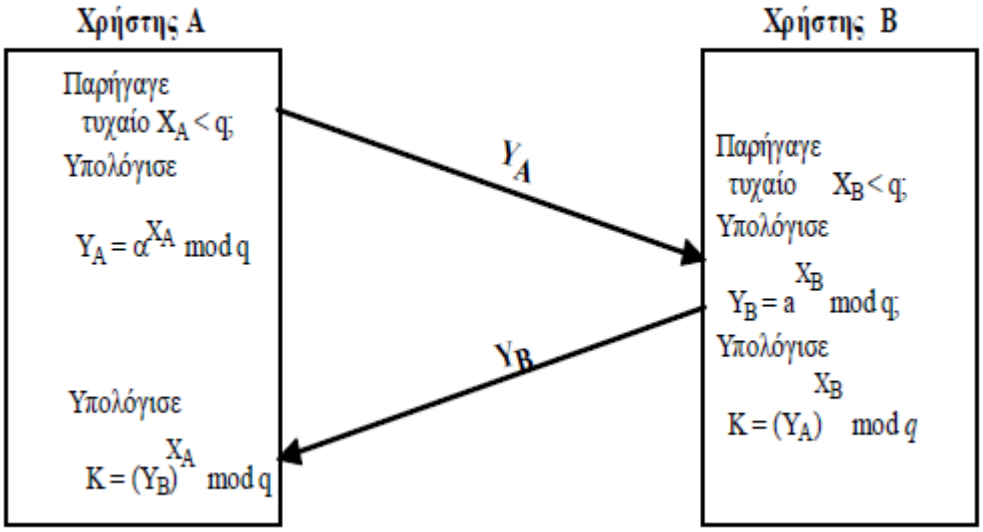
$$Y_A=7^5=51 \bmod 71$$
$$Y_B=7^{12}=4 \bmod 71$$

Μετά τον υπολογισμό των δημόσιων κλειδιών, κάθε πλευρά μπορεί να υπολογίσει το κοινό μυστικό κλειδί ως ακολούθως:

$$K=(Y_B)^{X_A} \bmod 71=4^5=30 \bmod 71$$
$$K=(Y_A)^{X_B} \bmod 71=51^{12}=30 \bmod 71$$

Από τη γνώση των {51, 4} ένας επιτιθέμενος δεν μπορεί εύκολα να υπολογίσει το κοινό μυστικό κλειδί 30.

Στο Σχήμα 1.24 παρουσιάζεται ένα απλό πρωτόκολλο που χρησιμοποιεί την τεχνική Diffie-Hellman. Έστω ότι ο Α επιθυμεί να εγκαταστήσει μία επικοινωνία με τον Β και χρησιμοποιεί ένα μυστικό κλειδί ώστε να κρυπτογραφεί τα μηνύματα σε αυτή τη σύνδεση. Ο Α μπορεί να παράγει ένα ιδιωτικό κλειδί $X_{A.}$ Στη συνέχεια υπολογίζει το Y_A και το στέλνει στον Β. Ο Β απαντά παράγοντας το μυστικό κλειδί X_B, υπολογίζοντας το Y_B και αποστέλλοντάς το στον Α. Και οι δύο χρήστες μπορούν πλέον να υπολογίσουν το κοινό μυστικό κλειδί Κ. Τα απαραίτητα δημόσια στοιχεία q και a θα πρέπει να είναι γνωστά από την αρχή. Εναλλακτικά, ο Α θα μπορούσε να διαλέξει τιμές για τα q και a και να τα συμπεριλάβει στο πρώτο μήνυμα.



Σχήμα 1.24: Παράδειγμα ανταλλαγής κλειδιών κατά Diffie - Hellman

- **Κρυπτογραφία Ελλειπτικής Καμπύλης – ECC**

Τα περισσότερα προϊόντα και πρότυπα, που χρησιμοποιούν ασύμμετρα κρυπτοσυστήματα για κρυπτογράφηση και ψηφιακή υπογραφή, χρησιμοποιούν τον αλγόριθμο RSA. Το πλήθος των bits που χρησιμοποιείται για ασφαλή χρήση του RSA έχει αυξηθεί σημαντικά τα τελευταία χρόνια και το γεγονός αυτό έχει επιβαρύνει τις αντίστοιχες εφαρμογές με σημαντικό επεξεργαστικό φόρτο. Το πρόβλημα εντείνεται σε περιβάλλον ιστοσελίδων εφαρμογών ηλεκτρονικού εμπορίου, όπου πραγματοποιούνται πολλές ασφαλείς δοσοληψίες. Τα τελευταία χρόνια έχει αρχίσει να αναπτύσσεται ένα ανταγωνιστικό σύστημα του RSA. Πρόκειται για την Κρυπτογραφία Ελλειπτικής Καμπύλης (Elliptic Curve Cryptography - ECC). Ήδη, το ECC κινείται στα πλαίσια προτυποποίησής του, αφού έχει συμπεριλάβει το πρότυπο για ασύμμετρα κρυπτοσυστήματα IEEE P1363.

Ο κύριος λόγος που καθιστά ελκυστικό το ECC συγκρινόμενο με τον αλγόριθμο RSA, είναι ότι προσφέρει το ίδιο επίπεδο ασφάλειας για μικρότερο πλήθος bits, μειώνοντας κατ' αυτόν τον τρόπο τον απαιτούμενο υπολογιστικό χρόνο και φόρτο εργασίας. Σύμφωνα με σχετικά πρόσφατες επιστημονικές ανακοινώσεις, έγινε κατορθωτό να κρυπταναλυθεί το ECC με μέγεθος κλειδιού 109 bits αξιοποιώντας αδιάκοπα την επεξεργαστική ισχύ 10.000 υπολογιστών επί 549 ημέρες. Στην παρούσα φάση ο αλγόριθμος θεωρείται ασφαλής αν το μέγεθος του κλειδιού διατηρεί μήκος τουλάχιστον 163 bits. Από την άλλη πλευρά, αν και η θεωρία του ECC ήταν γνωστή για αρκετό καιρό, μόλις πρόσφατα έχουν ξεκινήσει να εμφανίζονται προϊόντα που χρησιμοποιούν ECC. Το γεγονός αυτό δικαιολογεί το χαμηλό επίπεδο εμπιστοσύνης προς το ECC, σχετικά με το RSA.

Το ECC σε θεωρητική βάση είναι πιο δύσκολο να εξηγηθεί, συγκριτικά με τους αλγορίθμους RSA και Diffie-Hellman. Η αξιοποιηθείσα τεχνική βασίζεται στη χρήση ενός μαθηματικού μοντέλου, γνωστού ως ελλειπτική καμπύλη.

Εφαρμογές της κρυπτογραφίας δημοσίου κλειδιού

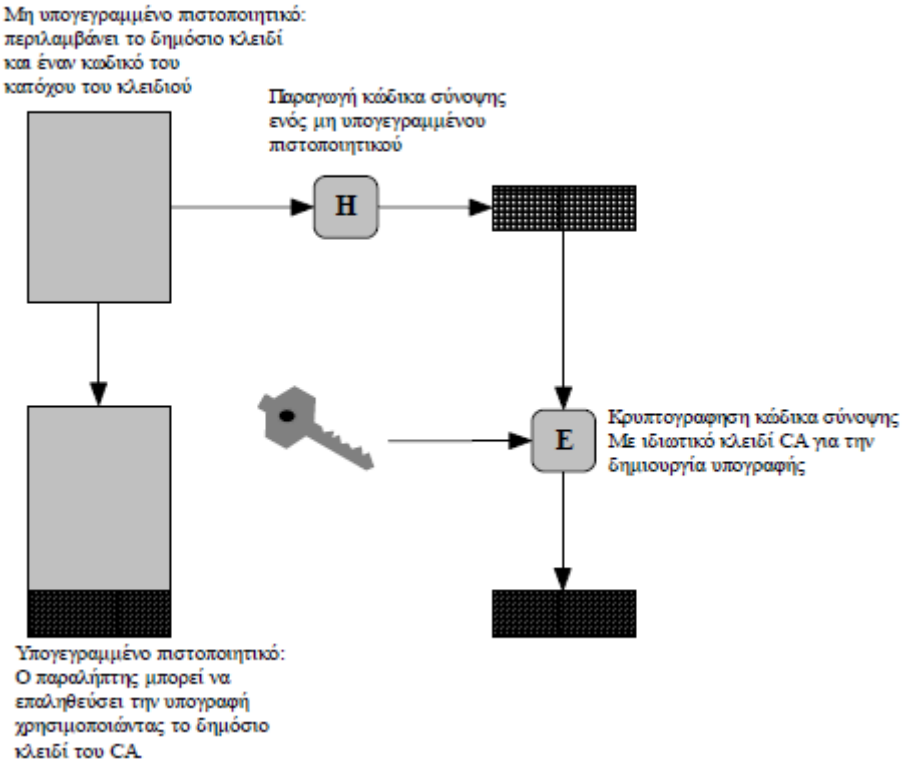
- **Ψηφιακές Υπογραφές**

Υποθέτουμε ότι ο Β επιθυμεί να αποστείλει ένα μήνυμα στον Α. Στις καταγραφείσες απαιτήσεις δεν περιλαμβάνεται πλέον η εμπιστευτικότητα του κειμένου, αλλά ο Α επιθυμεί να είναι σίγουρος για την προέλευση του κειμένου, δηλαδή απαιτείται αυθεντικοποίηση (authenticity) του αποστολέα του μηνύματος. Σε αυτή την περίπτωση, ο Β κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Όταν ο Α παραλάβει το κρυπτογραφημένο μήνυμα, το αποκρυπτογραφεί με το δημόσιο κλειδί του Β, εξασφαλίζοντας έτσι ότι το αρχικό μήνυμα έχει κρυπτογραφηθεί από τον Β. Κανένας άλλος δεν κατέχει και δε γνωρίζει το ιδιωτικό κλειδί του Β, συνεπώς, κανένας δεν μπορεί να δημιουργήσει κρυπτογραφημένο κείμενο το οποίο να αποκρυπτογραφείται με το δημόσιο κλειδί του Β. Έτσι, όλο το κρυπτογραφημένο κείμενο αποτελεί μία ψηφιακή υπογραφή (digital signature). Επιπλέον, είναι αδύνατον να αλλοιωθεί το μήνυμα χωρίς γνώση του ιδιωτικού κλειδιού του Β, οπότε εξασφαλίζεται αυθεντικοποίηση του αποστολέα, αλλά και ακεραιότητα των δεδομένων.

Ένα πρόβλημα που δημιουργείται σε αυτή την περίπτωση αφορά το χώρο αποθήκευσης: κάθε μήνυμα πρέπει να είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή για πρακτικούς λόγους. Πρέπει, επίσης, να φυλάσσεται ένα αντίγραφο σε κρυπτογραφημένη μορφή, ώστε η προέλευση και τα περιεχόμενα να μπορούν να προσδιοριστούν εύκολα σε περίπτωση αμφισβήτησης και διαφωνίας. Ένας εύκολος τρόπος για να επιτευχθούν τα ίδια αποτελέσματα, θα ήταν να κρυπτογραφηθεί μικρό τμήμα από bits, το οποίο θα αποτελεί συνάρτηση του κειμένου. Ένα τέτοιο

τμήμα ονομάζεται αυθεντικοποιητής (authenticator) και θα πρέπει να είναι αδύνατο να τροποποιηθεί το μήνυμα, χωρίς να αλλάξει ο αυθεντικοποιητής. Αν ο αυθεντικοποιητής κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα, τότε χαρακτηρίζεται ως ψηφιακή υπογραφή (digital signature). Η περίπτωση αυτή φαίνεται στο Σχήμα 1.25. Για τη δημιουργία μιας ψηφιακής υπογραφής ενός κειμένου από μία οντότητα, συνήθως κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα η σύνοψη του μηνύματος.

Θα πρέπει να τονιστεί ότι η ψηφιακή υπογραφή δεν προσφέρει εμπιστευτικότητα για το μήνυμα, αλλά αποτελεί υπηρεσία που ικανοποιεί απαιτήσεις ακεραιότητας μηνύματος, αυθεντικοποίησης αποστολέα και μη αποποίησης αποστολής μηνύματος.



Σχήμα 1.25: Ψηφιακές υπογραφές

- **Διαχείριση Δημόσιων Κλειδιών**

Η διανομή των δημόσιων κλειδιών αποτελεί ένα από τα σημαντικότερα προβλήματα του ασύμμετρου κρυπτοσυστήματος. Υπάρχουν δύο διαφορετικές περιπτώσεις στη διανομή των κλειδιών που παρουσιάζουν ιδιαίτερο ενδιαφέρον:

1. Η διανομή των δημόσιων κλειδιών.

2. Η χρήση του ασύμμετρου κρυπτοσυστήματος για τη διανομή μυστικών κλειδιών, δηλαδή των κλειδιών που χρησιμοποιούνται στο συμμετρικό κρυπτοσύστημα.

❖ Ψηφιακά Πιστοποιητικά

Για την αποτελεσματική λειτουργία του ασύμμετρου κρυπτοσυστήματος, το δημόσιο κλειδί πρέπει να μπορεί να είναι γνωστό σε όσους δυνητικά ενδιαφέρονται. Έτσι, υποθέτοντας ότι υπάρχει ένας ευρέως αποδεκτός αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης όπως ο RSA, οποιοσδήποτε μπορεί να αποστείλει το δημόσιο κλειδί του σε κάποιον άλλο ή να το μεταδώσει προς όλους. Η μέθοδος αυτή είναι αρκετά χρήσιμη, αλλά έχει μία σημαντική αδυναμία: την αδυναμία διασφάλισης της ακεραιότητας και της αυθεντικοποίησης του αποστολέα κατά την αποστολή του μηνύματος που περιέχει το δημόσιο κλειδί. Οποιοσδήποτε μπορεί να πραγματοποιήσει μία τέτοια μετάδοση. Με τον τρόπο αυτό, κάποιος Χ μπορεί να προσποιηθεί ότι είναι ο Α και να στείλει ένα δημόσιο κλειδί σε τρίτον ή να το μεταδώσει προς περισσότερες οντότητες. Μέχρι τη στιγμή που ο Α θα αντιληφθεί ότι βρίσκεται σε εξέλιξη μία απάτη, ο Χ θα έχει διαβάσει όλα τα κρυπτογραφημένα μηνύματα που προορίζονταν για τον Α, ενώ έχει τη δυνατότητα να υπογράφει και να αυθεντικοποιείται ως Α.

Λύση σε αυτό το πρόβλημα αποτελεί η χρήση του ψηφιακού πιστοποιητικού (digital certificate) ή απλώς πιστοποιητικού (certificate) δημοσίου κλειδιού. Συγκεκριμένα, ένα πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του χρήστη και έναν κωδικό (userID) του κατόχου του κλειδιού, υπογεγραμμένα ψηφιακά από μία Έμπιστη Τρίτη Οντότητα (Trusted Third Party - TTP), η οποία συνήθως αποκαλείται Πάροχος Υπηρεσιών Πιστοποίησης (Certification Service Provider - CSP). Ο χρήστης παρουσιάζει το δημόσιο κλειδί του στον CSP με έναν αξιόπιστο τρόπο και λαμβάνει ένα πιστοποιητικό που το περιέχει ή, στη γενική περίπτωση, ο CSP παράγει, αποθηκεύει, διανέμει και ανακαλεί, όταν απαιτείται, τα πιστοποιητικά. Οποιοσδήποτε επιθυμεί να χρησιμοποιήσει το δημόσιο κλειδί του χρήστη μπορεί να λάβει το πιστοποιητικό και να είναι σίγουρος για την ορθότητα του δημόσιου κλειδιού. Η διαδικασία αναπαρίσταται στο Σχήμα 1.25.

Το πιο διαδεδομένο σύστημα πιστοποιητικού είναι το πρότυπο ISO/ITU-T X.509, το οποίο χρησιμοποιείται σε πολλές περιπτώσεις, όπως στην ασφάλεια IP, στο TLS/SSL, στο SET, στο S/MIME κ.τ.λ.

❖ Διανομή Μυστικών Κλειδιών με Ασύμμετρο Κρυπτοσύστημα

Όπως αναφέρθηκε σε προηγούμενες παραγράφους, σε ένα συμμετρικό κρυπτοσύστημα προκειμένου να επικοινωνήσουν δύο χρήστες πρέπει να διαμοιράζονται τη γνώση ενός μυστικού κλειδιού. Για παράδειγμα, έστω ότι

ο Β θέλει να δημιουργήσει μία εφαρμογή που θα του παρέχει τη δυνατότητα να ανταλλάσσει μηνύματα με χρήση υπηρεσίας ηλεκτρονικού ταχυδρομείου με τον Α, χρησιμοποιώντας συμμετρικό κρυπτοσύστημα. Θα πρέπει να βρεθεί ένας τρόπος να αποστείλει ο Β στον Α το μυστικό κλειδί.

Ένας πολύ διαδεδομένος τρόπος είναι η αξιοποίηση ψηφιακού φακέλου (digital envelope), δηλαδή να χρησιμοποιήσει ο Β ασύμμετρο κρυπτοσύστημα για την αποστολή του μυστικού κλειδιού. Προφανώς απαιτείται η χρήση πιστοποιητικών και η λειτουργία PKI, ώστε να εξασφαλίζεται η αυθεντικότητα του αποστολέα Α και η ακεραιότητα του μηνύματος. Τα γενικά βήματα που θα πρέπει να ακολουθηθούν σε μία τέτοια περίπτωση είναι τα ακόλουθα:

- Ο Β ετοιμάζει το προς αποστολή μήνυμα.
- Ο Β κρυπτογραφεί το μήνυμα με συμβατικό κρυπτοσύστημα, χρησιμοποιώντας ένα μυστικό κλειδί που ο ίδιος δημιούργησε.
- Ο Β κρυπτογραφεί το μυστικό κλειδί με το δημόσιο κλειδί του Α.
- Ο Β επισυνάπτει το κρυπτογραφημένο κλειδί στο μήνυμα και το αποστέλλει στον Α.

Ο Α είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το μήνυμα και να αναγνώσει το αρχικό κείμενο. Αν ο Β έχει ανακτήσει το δημόσιο κλειδί του Α μέσω πιστοποιητικού από κάποια Έμπιστη Τρίτη Οντότητα, τότε ο Β είναι σίγουρος ότι το μυστικό κλειδί είναι ορθό.

1.7.2.3 Σύγκριση συμμετρικής και ασύμμετρης κρυπτογραφίας

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από

εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Γι' αυτό το λόγο, όπως προτείνεται και από το πρωτόκολλο SSL, χρησιμοποιείται η κρυπτογράφηση δημοσίου κλειδιού για την ανταλλαγή συμμετρικών κλειδιών και στη συνέχεια χρησιμοποιείται η συμμετρική κρυπτογράφηση για την ουσιαστική επικοινωνία. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (nonrepudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι.

Σ' αυτό το σημείο πρέπει να σημειώσουμε ότι η ανθεκτικότητα της κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών παρά από τους αλγορίθμους. Το μέγεθος των κλειδιών μετριέται όπως αναφέραμε και παραπάνω σε bits. Γενικά, κλειδιά μεγάλου μεγέθους παρέχουν ανθεκτικότερη κρυπτογράφηση. Για παράδειγμα, η κρυπτογράφηση 128 bit RS4 είναι 3078 φορές ανθεκτικότερη από την 40 bit RS4. διαφορετικοί αλγόριθμοι απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης. Για παράδειγμα ένας αλγόριθμος συμμετρικής κρυπτογράφησης με κλειδί μεγέθους 128 bits παρέχει ανθεκτικότερη κρυπτογράφηση από τον αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού RSA με το ίδιο μέγεθος κλειδιού. Γι' αυτό πρέπει να χρησιμοποιούμε κλειδί μεγέθους τουλάχιστον 512 bits προκειμένου η

κρυπτογράφηση RSA να θεωρείται ανθεκτική, ενώ οι συμμετρικοί αλγόριθμοι πετυχαίνουν το ίδιο επίπεδο ανθεκτικότητας με κλειδί μεγέθους 56 bits. Όμως ακόμη και αυτά τα επίπεδα ανθεκτικότητας αρχίζουν και αποδεικνύονται ευπαθή σε επιθέσεις.

1.8 Συμμετρικοί κρυπτογραφικοί αλγόριθμοι

Κρυπτογραφία μυστικού κλειδιού

Οι αλγόριθμοι συμμετρικής κρυπτογραφίας βασίζονται στη ύπαρξη ενός μόνο μυστικού κλειδιού που είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Αυτό το κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση του μηνύματος.

Η συμμετρική κρυπτογραφία εγγυάται την εμπιστευτικότητα (confidentiality) των δεδομένων αφού κρυπτογραφεί το μήνυμα με το μυστικό κλειδί. Το μήνυμα που παράγεται αποκρυπτογραφείται από τον παραλήπτη με τη βοήθεια του ίδιου κλειδιού, το οποίο πρέπει να μείνει μυστικό μεταξύ των δύο.

Παρόλο που η συμμετρική κρυπτογράφηση εγγυάται την εμπιστευτικότητα, δεν μπορεί να εγγυηθεί για το πώς θα γίνει η ανταλλαγή του κλειδιού. Για να είναι ασφαλής η επικοινωνία θα πρέπει με κάποιο ασφαλή τρόπο να γίνει η ανταλλαγή του μυστικού κλειδιού. Όταν ο αποστολέας και ο παραλήπτης δεν γνωρίζονται, όπως συμβαίνει στις περισσότερες ηλεκτρονικές συναλλαγές, θα πρέπει να υπάρχει ένα ασφαλές κανάλι επικοινωνίας για τη μεταφορά του κλειδιού. Συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν ήδη αναπτυχθεί και χρησιμοποιούνται σήμερα, με πιο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT.

Ένα ακόμη σημαντικό πρόβλημα αφορά την ταυτοποίηση μεταξύ του αποστολέα και του παραλήπτη. Το πρόβλημα της ταυτοποίησης στο ότι πολλοί άνθρωποι μπορεί να έχουν πρόβλημα στο κοινό κλειδί. Όταν κάποιος από αυτούς λάβει ένα κρυπτογραφημένο μήνυμα, ξέρει ότι ήρθε από κάποιον από αυτούς αλλά δεν μπορεί να αποδείξει ποιός πραγματικά του έστειλε το μήνυμα. Άρα χρειάζεται ένας τρόπος ώστε να μπορεί με μοναδικό τρόπο να ταυτοποιήσει τον αποστολέα. Αυτό το πρόβλημα μπορεί να το λύσει η κρυπτογραφία δημοσίου κλειδιού.

Το βασικό πλεονέκτημα των συμμετρικών αλγορίθμων είναι ότι οι χρήστες δεν καταλαβαίνουν κάποια σημαντική χρονική καθυστέρηση λόγω της διαδικασίας κρυπτογράφησης - αποκρυπτογράφησης. Αρκεί να διατηρείται μυστικό το κλειδί της κρυπτογράφησης. Η ασφάλεια των συμμετρικών συστημάτων κρυπτογράφησης εξαρτάται από την προφύλαξη της μυστικότητας των κλειδιών k(e) και k(d). Επομένως, υπάρχουν σημαντικά προβλήματα διαχείρισης των κλειδιών και ιδιαίτερα σε ότι αφορά την αρχική διανομή τους.

Μια άλλη σημαντική επίθεση, δεδομένου ότι ο κρυπτογραφικός αλγόριθμος είναι γνωστός, περιλαμβάνει τη δοκιμή όλων των δυνατών κλειδιών αποκρυπτογράφησης. Για αντιμετωπιστούν αυτού του είδους οι επιθέσεις, χρησιμοποιούνται κλειδιά με όσο το δυνατόν μεγαλύτερο πεδίο ορισμού, με όσο το δυνατόν μεγαλύτερο μήκος δηλαδή.

1.8.1 Αλγόριθμοι Ροής (Stream Ciphers)

Τα stream ciphers αποτελούν μια σημαντική κλάση τεχνικών συμμετρικής κρυπτογραφίας. Λειτουργούν σε μικρές μονάδες, συνήθως bits, του απλού μηνύματος (plaintext) και ο μετασχηματισμός αυτών των bits εξαρτάται από το χρόνο. Από τα πιο σημαντικά χαρακτηριστικά των stream ciphers είναι η ταχύτητα και η απλότητα. Με τον όρο απλότητα, εννοούμε ότι οι σχεδιαστές stream ciphers έχουν ως κύριο στόχο το σχεδιασμό ciphers τα οποία να έχουν ταχείς επιδόσεις όσον αφορά το software τμήμα ή να είναι "μικρά" στο hardware τμήμα. Τα χαρακτηριστικά αυτά έχουν σαν αποτέλεσμα την ευρεία χρήση των stream ciphers σε πολλές εφαρμογές. Παραδείγματα αποτελούν τα stream ciphers E0, A5/x και RC4 τα οποία χρησιμοποιούνται σε δίκτυα Bluetooth, 2g cellular telephony και 802.11a/b wireless networking αντίστοιχα.

Ένας κρυπτογραφικός αλγόριθμος ροής λειτουργεί ως εξής :

- Τα δεδομένα που πρόκειται να κρυπτογραφηθούν παριστάνονται ως μια ακολουθία από δυαδικά ψηφία (bits). Κατόπιν, ελέγχεται μια γεννήτρια κλειδοροής (key stream generator) που δέχεται ως είσοδο ένα μυστικό κλειδί k και παράγει στην έξοδο μια ψευδοτυχαία ακολουθία από bits που ονομάζεται κλειδοροή (key stream). Η γεννήτρια κλειδοροής είναι ένας ειδικός τύπος γεννήτριας ψευδοτυχαίων αριθμών.
- Στη συνέχεια, το αρχικό κείμενο κρυπτογραφείται με modulo 2 (XOR), δηλαδή προσθέτοντας την κλειδοροή στο αρχικό κείμενο. Η ακολουθία από bits που παράγεται με αυτόν τον τρόπο αποτελεί το κρυπτογραφημένο κείμενο (cipher text).

Επομένως ένας συμβολισμός του κρυπτογραφικού αλγόριθμου ροής θα μπορούσε να είναι :

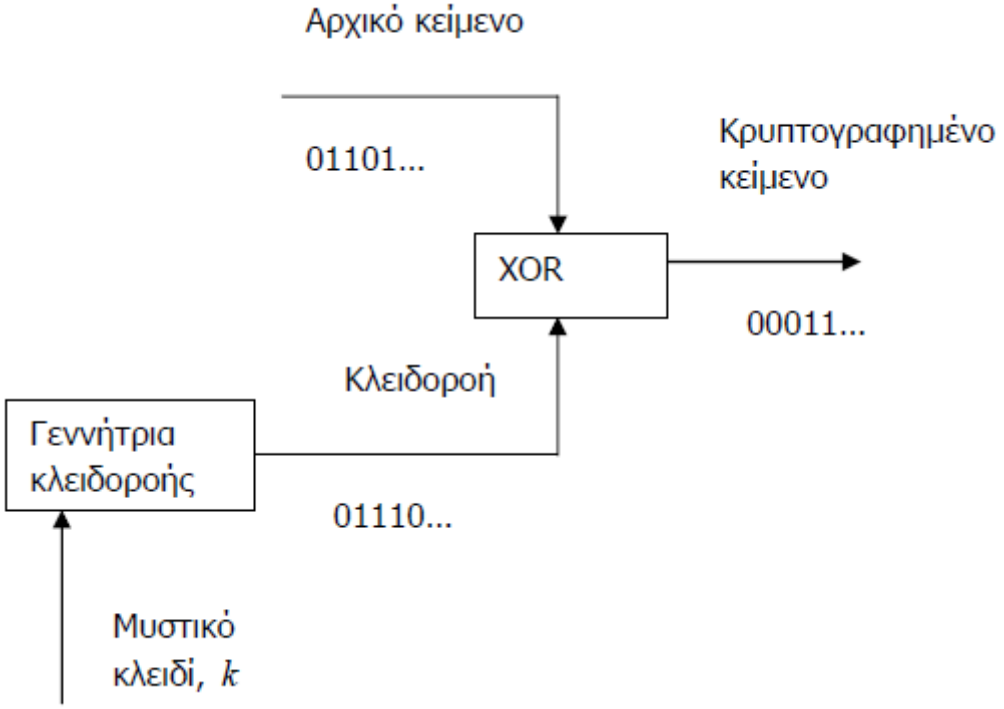
$$c_i=m_i \oplus s_i, \text{ για } i \geq 0,$$

όπου m_0, m_1, ... είναι τα bits του αρχικού κειμένου, s_0, s_1, ... είναι τα bits της κλειδοροής και c_0, c_1, … είναι τα bits του κρυπτογραφημένου κειμένου. Το σύμβολο $\oplus$ συμβολίζει την πράξη της αποκλειστικής διάζευξης (exclusive – or) μεταξύ των bits.

Αντίστοιχα για την αποκρυπτογράφηση ισχύει :

$$m_i=c_i \oplus s_i, \text{ για } i \geq 0.$$

Δηλαδή, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση ροής.



Οι κρυπτογραφικοί αλγόριθμοι ροής θεωρούνται σχετικά απλοί και εύκολα υλοποιήσιμοι.

Ιδιότητες της κλειδοροής

Για να είναι ασφαλής ένας κρυπτογραφικός αλγόριθμος ροής πρέπει η γεννήτρια κλειδοροής να διαθέτει τις παρακάτω ιδιότητες :

- Η ακολουθία πρέπει να έχει μεγάλη περίοδο επανάληψης. Πράγματι η ακολουθία είναι αναγκαστικά περιοδική, δηλαδή μετά από κάποιον αριθμό bits χρειάζεται να επαναλαμβάνεται ξεκινώντας από την αρχή, αφού παράγεται από κάποια συνάρτηση με βάση ένα κλειδί. Αν η περίοδος επανάληψης είναι πολύ μικρή τότε είναι δύσκολο να υπολογιστεί το ακριβές μέγεθος της περιόδου επιτρέποντας κατόπιν την αποκρυπτογράφηση του κρυπτογραφημένου κειμένου.
- Η ακολουθία πρέπει να είναι ψευδοτυχαία, δηλαδή να μοιάζει με μια πραγματικά τυχαία ακολουθία. Αυτό συνήθως επαληθεύεται με εφαρμογή ελέγχων τυχαιότητας (random tests), οι οποίοι ελέγχουν κατά πόσο είναι περίπου ίδιο το πλήθος των ψηφίων μηδέν (0) και των ψηφίων (1), ή ότι κάθε μηδενικό ψηφίο (0) ακολουθείται από ψηφίο ένα (1) τόσο συχνά όσο και το αντίστροφο.
- Η ακολουθία πρέπει να έχει μεγάλη γραμμική ισοδυναμία (linear equivalence). Οποιαδήποτε περιοδική ακολουθία δυαδικών ψηφίων (όπως μια ακολουθία κλειδοροής) μπορεί να παραχθεί με τη χρήση γραμμικών (linear) μεθόδων, για παράδειγμα με υπολογισμό κάθε

στοιχείου της ακολουθίας ως γραμμικό συνδυασμό των στοιχείων της ακολουθίας που προηγήθηκαν. Αν η ακολουθία μπορεί να παραχθεί από μια γραμμική αναδρομή (recurrence) χρησιμοποιώντας μόνο έναν μικρό αριθμό όρων, τότε λέμε ότι έχει μικρή γραμμική ισοδυναμία. Μια τέτοια ακολουθία έχει ως αποτέλεσμα έναν ανασφαλή κρυπτογραφικό αλγόριθμο.

Αυτές οι συνθήκες, όμως, δεν είναι αρκετές για να εγγυηθούν ασφάλεια. Γενικότερα, ένας κρυπτογραφικός αλγόριθμος κλειδοροής μπορεί να προσφέρει ένα καλό επίπεδο ασφαλείας όταν είναι δυνατό να διασφαλιστεί ότι ακόμα κι αν κανείς αποκτήσει οποιαδήποτε πληροφορία για κάποιο κομμάτι της ακολουθίας κλειδοροής είναι υπολογιστικά αδύνατο να συνάγει άλλα κομμάτια της ακολουθίας.

Οι μοντέρνοι κρυπτογραφικοί αλγόριθμοι ροής χρησιμοποιούν γεννήτριες κλειδοροών που παράγουν ψευδοτυχαίες ακολουθίες με πολύ μεγάλες περιόδους, για παράδειγμα 264 bits ή και περισσότερα. Υπάρχουν ακόμη και συσκευές (hardware) γεννητριών κλειδοροή που κατορθώνουν να τρέχουν σε πολύ μεγάλες ταχύτητες. Σήμερα οι υψηλές ταχύτητες μπορούν να επιτυγχάνονται ακόμη και με λογισμικό (software) παραγωγής κλειδοροών.

Η κρυπτογράφηση με αλγόριθμους ροής μπορεί να γίνεται πολύ γρήγορα, καθώς από τη μια η λειτουργία της κρυπτογράφησης είναι πολύ απλή και από την άλλη είναι δυνατή η υλοποίηση ασφαλών γεννητριών κλειδοροής που λειτουργούν με πολύ μεγάλες ταχύτητες.

Μια ενδιαφέρουσα ιδιότητα των κρυπτογραφικών αλγορίθμων ροής είναι ότι με αυτούς δεν πολλαπλασιάζονται τα λάθη μετάδοσης. Αυτό σημαίνει ότι όταν υπάρχει ένα λάθος bit στο κρυπτογραφημένο κείμενο, τότε μετά την αποκρυπτογράφηση μόνο ένα bit του αρχικού κειμένου θα είναι λάθος. Πέρα όμως από περιορισμό των λαθών μετάδοσης, οι κρυπτογραφικοί αλγόριθμοι ροής δεν παρέχουν από μόνοι τους κάποιου είδους προστασία ενάντια σε πιθανή μετατροπή του μηνύματος που μεταδίδεται. Αυτό σημαίνει ότι ο υποκλοπέας του μηνύματος μπορεί να αλλάξει ένα bit στο κρυπτογραφημένο κείμενο όντας σίγουρος ότι με αυτόν τον τρόπο θα αλλάξει μόνο το αντίστοιχο bit στο κείμενο που θα προκύψει από την αποκρυπτογράφηση του μηνύματος.

Ένα ακόμη μειονέκτημα είναι ότι αν το κλειδί χρησιμοποιηθεί δύο φορές θα δώσει την ίδια κλειδοροή. Αυτό αποτελεί κίνδυνο για την ασφάλεια και πρέπει να αποφεύγεται όσο γίνεται. Η συνηθισμένη λύση σε αυτό το πρόβλημα παρέχεται όταν αυτός που κάνει την κρυπτογράφηση (encryptor) :

- Παράγει ένα τυχαίο κλειδί μηνύματος ή συνόδου πριν αρχίσει την κρυπτογράφηση.
- Με αυτό το κλειδί μετατρέπει το μυστικό κλειδί που εισάγεται στη γεννήτρια κλειδοροής.
- Στέλνει το κλειδί μηνύματος ως πρόθεμα (prefix) του κρυπτογραφημένου κειμένου.

1.8.2 Αλγόριθμοι Τμήματος (Block Ciphers)

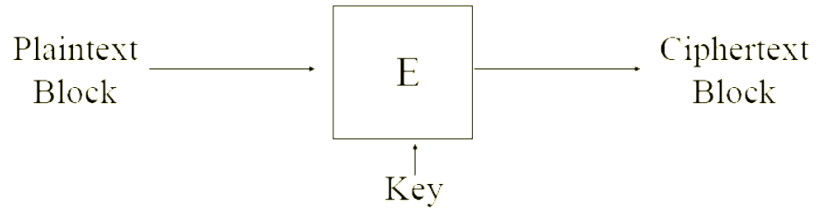
Τα block ciphers συμμετρικού κλειδιού είναι τα πιο διάσημα και σημαντικά στοιχεία σε πολλά κρυπτογραφικά συστήματα. Από μόνα τους προσφέρουν εμπιστευτικότητα (confidentiality) αλλά λόγω της προσαρμοστικότητάς τους συχνά χρησιμοποιούνται και για την κατασκευή γεννητριών παραγωγής ψευδοτυχαίων ακολουθιών, stream ciphers, συναρτήσεων κατακερματισμού (hash functions) και MACs (Message Authentication Codes). Επίσης μπορούν να χρησιμοποιηθούν ως βασικό στοιχείο σε τεχνικές αυθεντικοποίησης μηνύματος, σε μηχανισμούς ακεραιότητας μηνύματος, σε πρωτόκολλα αυθεντικοποίησης οντότητας και σε ψηφιακές υπογραφές. Παρόλο που προσφέρουν υψηλό επίπεδο ασφάλειας τα block ciphers δεν μπορούν να χρησιμοποιηθούν σε όλες τις εφαρμογές που απαιτούν κρυπτογραφικά συστήματα. Αυτό ισχύει κυρίως λόγω των απαιτήσεων ταχύτητας και περιορισμένης μνήμης ορισμένων εφαρμογών.

Στην εργασία αυτή θα παρουσιάσουμε κάποια βασικά χαρακτηριστικά των block ciphers, δύο γενικές κατηγορίες αυτών (Feistel και SP networks) και δύο από τα πιο γνωστά κρυπτοσυστήματα, το DES και το AES, εξετάζοντας την αρχιτεκτονική σχεδιασμού τους, το επίπεδο ασφάλειας που προσφέρουν και κάποιες γενικές τεχνικές κρυπτανάλυσης τους, ενώ στη συνέχεια θα περιγράψουμε κάποιες από τις εφαρμογές στις οποίες χρησιμοποιούνται, το πρωτόκολλο αυθεντικοποίησης Kerberos για το DES και τα 3g δίκτυα κινητής τηλεφωνίας για το AES.

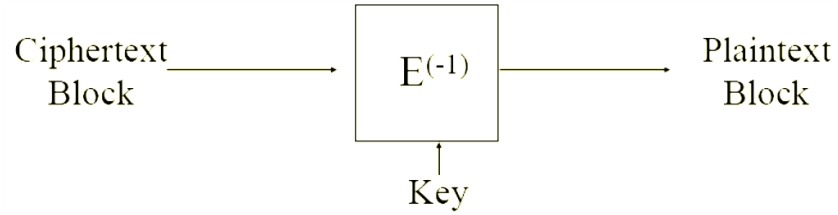
1.8.2.1 Βασικές έννοιες και ορισμοί

Τα block ciphers μπορεί να είναι συμμετρικού και δημόσιου κλειδιού. Επικεντρωνόμαστε στα block ciphers συμμετρικού κλειδιού. Το block cipher είναι μια συνάρτηση η οποία αντιστοιχεί τμήματα μήκους n-bits απλού κειμένου σε τμήματα μήκους n-bits κρυπτοκειμένου. Το n ονομάζεται μήκος τμήματος. Μπορεί να θεωρηθεί ως ένα απλό κρυπτοσύστημα αντικατάστασης με χαρακτήρες μεγάλου μεγέθους. Η συνάρτηση έχει ως παράμετρο το διάνυσμα-κλειδί k διάστασης n, $k \epsilon K$ όπου K είναι ένα υποσύνολο του συνόλου όλων των διανυσμάτων διάστασης n.

Ορισμός 1.1 Ένα n-bit block cipher είναι μια συνάρτηση $E:V_n x K \rightarrow V_n$ τέτοια ώστε για κάθε κλειδί $k \epsilon K$, το E(P, k) είναι μια αντιστρέψιμη αντιστοιχία (η συνάρτηση κρυπτογράφησης για το k) από το V_n στο V_n η οποία συμβολίζεται $E_k(P)$. Η αντίστροφη αντιστοιχία είναι η συνάρτηση αποκρυπτογράφησης η οποία συμβολίζεται $D_k(C)$. Η σχέση $C=E_k(P)$ συμβολίζει ότι το κρυπτοκείμενο C προκύπτει από την κρυπτογράφηση του απλού κειμένου P. Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζονται στα σχήματα 1.26 και 1.27 αντίστοιχα.

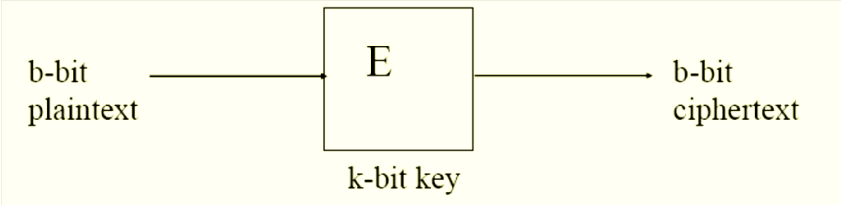


Σχήμα 1.26 Κρυπτογράφηση απλού κειμένου



Σχήμα 1.27 Αποκρυπτογράφηση κρυπτοκειμένου

Οι δύο σημαντικότερες παράμετροι των block ciphers είναι το μήκος του block και το μήκος του κλειδιού. Τα περισσότερα κρυπτοσυστήματα αυτού του είδους έχουν μήκος block b=64 ή 128 και μήκος κλειδιού k=64 ή 128 ή 192 ή 256. Όμως τα block ciphers μπορούν να θεωρηθούν ως μια αντιμετάθεση η οποία εξαρτάται από το κλειδί (key-dependent permutation) καθώς χρησιμοποιούν ένα μικρό σύνολο από αντιμεταθέσεις εξαρτώμενες από τον αριθμό των πιθανών κλειδιών. Συγκεκριμένα, έστω ότι $\#P=\#C=2^b$ και $\#K=2^k$. Η διαδικασία κρυπτογράφησης τότε είναι:



Τότε ο αριθμός των πιθανών αντιμεταθέσεων b-bit blocks είναι $(2^b)!$, αλλά τελικά περιορίζεται από το κλειδί k και είναι 2^k. Επομένως για ένα "καλό" block cipher θα πρέπει να ισχύουν οι εξής ιδιότητες:

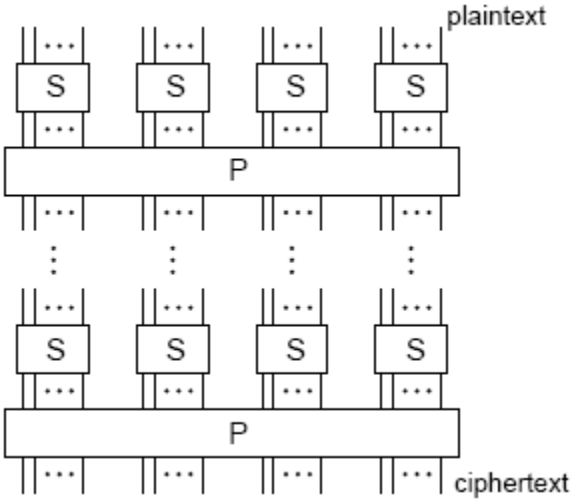
- Το κλειδί επιλέγει μια τυχαία αντιμετάθεση
- Συγγενικά κλειδιά δίνουν μη-συγγενικές αντιμεταθέσεις

ώστε να είναι ανθεκτικό σε επιθέσεις κάθε είδους (ciphertext-only, known plaintext και chosen-plaintext/ciphertext).

Το 1949 ο Shannon εισήγαγε τις έννοιες σύγχυση (Confusion) και διάχυση (Diffusion). Η σύγχυση ορίζεται ως η λειτουργία η οποία κάνει τη σχέση μεταξύ κλειδιού και κρυπτοκειμένου όσο το δυνατόν πολυπλοκότερη ενώ η διάχυση ορίζεται ως η λειτουργία η οποία διαχέει την επιρροή των bits του απλού κειμένου έτσι ώστε τα bits του κρυπτοκειμένου εξαρτώνται από ολόκληρο το απλό κείμενο. Η σύγχυση συνήθως δίνεται από τη χρήση μιας

αντικατάστασης η οποία ονομάζεται S-Box και η διάχυση δίνεται από τη χρήση μιας αντιμετάθεσης.

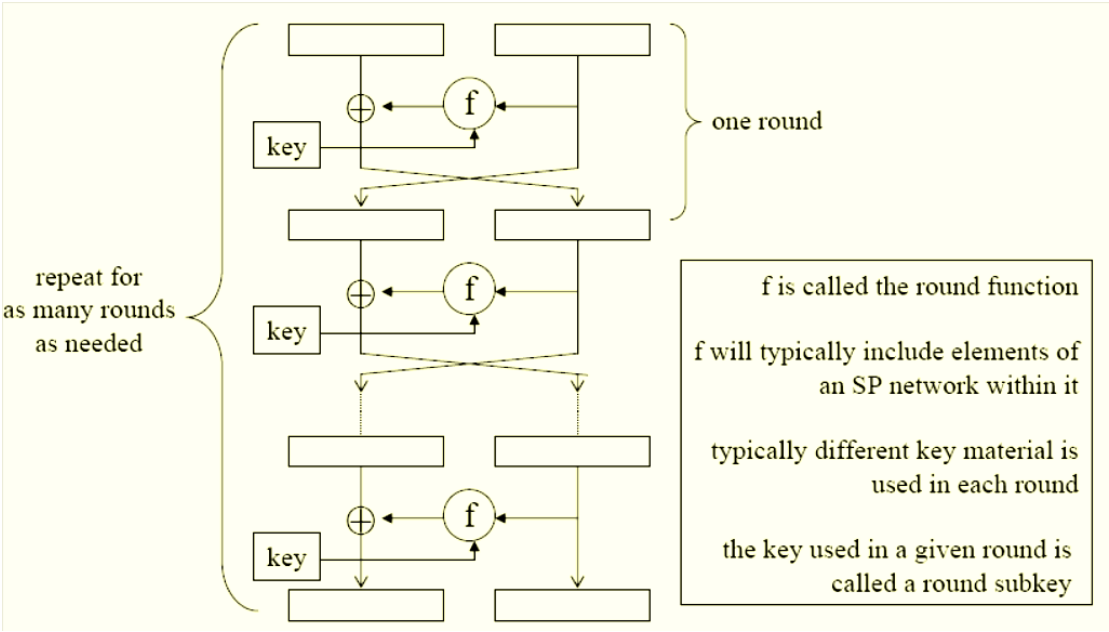
Ορισμός 1.2 Ένα SP-network είναι ένα επαναλαμβανόμενο κρυπτοσύστημα το οποίο αποτελείται από έναν αριθμό από γύρους. Κάθε γύρος αποτελείται από αντικαταστάσεις και αντιμεταθέσεις. Η αντικατάσταση η οποία καλείται και S-Box αντικαθιστά l-bits με ένα άλλο σύνολο από l-bits ενώ η αντιμετάθεση, αντιμεταθέτει τα bits.



Σχήμα 1.28 SP-network

Η λογική του σχεδιασμού των SP-networks είναι ότι οι αντικαταστάσεις και οι αντιμεταθέσεις χρησιμοποιούνται με τέτοιο τρόπο ώστε το τελικό κρυπτοσύστημα, μετά από ένα καθορισμένο αριθμό γύρων, είναι πιο ασφαλές από ότι σε κάθε γύρο ξεχωριστά.

Η άλλη μεγάλη κατηγορία block ciphers είναι τα Feistel ciphers. Στα κρυπτοσυστήματα τύπου Feistel, το κείμενο χωρίζεται σε δύο μέρη και αφού το κάθε ένα επιδέχεται διαφορετικές τροποποιήσεις στη συνέχεια συνδυάζονται με τέτοιο τρόπο ώστε το ένα χρησιμοποιείται για να "ενημερώσει" (update) το άλλο. Οι τροποποιήσεις σε κάθε γύρο γίνονται μέσω της συνάρτησης f η οποία είναι συνήθως ένα SP-network. Το κύριο χαρακτηριστικό του δικτύου Feistel είναι ότι η συνάρτηση f μπορεί να είναι οποιαδήποτε συνάρτηση ακόμα και αν δεν είναι αντιστρέψιμη. Η δομή του Feistel είναι τέτοια ώστε ο κάθε γύρος είναι αντιστρέψιμος ακόμα και αν η συνάρτηση f δεν είναι. Όλα τα παραπάνω μπορούν να φανούν αναλυτικά στο παρακάτω σχήμα.



Σχήμα 1.29 Feistel cipher

Η συνάρτηση f όπως ήδη αναφέραμε συνήθως είναι ένα SP-network. Αυτό είναι που θα δώσει στο κρυπτοσύστημα την απαιτουμένη Σύγχυση και διάχυση. Στη θεωρία ένας τρόπος να κατασκευάσει κάποιος ένα "καλό" block cipher είναι με το να επιλέξει για συνάρτηση f μια τυχαία συνάρτηση (Αν η f είναι τυχαία συνάρτηση που αντιστοιχεί n-bits σε n-bits, τότε η δομή του Feistel δίνει μια τυχαία συνάρτηση που αντιστοιχεί 2n-bits σε 2n-bits) και να χρησιμοποιήσει τουλάχιστον 3 γύρους ώστε να είναι ανθεκτικό σε συγκεκριμένους τύπους επιθέσεων. Στη πράξη όμως είναι απαραίτητο να χρησιμοποιούνται διαφορετικά μέρη του κλειδιού σε κάθε γύρο (στη διαδικασία κρυπτογράφησης). Επομένως υπάρχει η ανάγκη για ένα Πρόγραμμα κλειδιού.

1.8.2.2 Μέθοδοι Λειτουργίας (Modes of operation)

Μια μέθοδος λειτουργίας είναι ένας προτεινόμενος τρόπος να χρησιμοποιηθεί ένα block cipher για να κρυπτογραφήσει ένα string από bits, γνωστό και ως μήνυμα ή απλό κείμενο και να παράγει το κρυπτοκείμενο. Μια τέτοια μέθοδος είναι απαραίτητη καθώς τα block ciphers προσφέρουν τρόπο να κρυπτογραφούμε ένα string n-bits και όχι αυθαίρετου μήκους. Ακόμα και όταν κρυπτογραφούμε string n-bits μία μέθοδος λειτουργίας θα αποτρέψει τη διαρροή πληροφορίας που προκύπτει από επαναλαμβανόμενα n-bit στο απλό κείμενο.

Τέσσερις μέθοδοι λειτουργίας ονόματι Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) και Cipher Feedback (CFB) έγιναν πρότυπες μέθοδοι στις Η.Π.Α. το 1980. Αυτές οι μέθοδοι περιγράφηκαν κυρίως για χρήση με το κρυπτοσύστημα DES αλλά αργότερα εφαρμόστηκαν και σε άλλα block ciphers. Οι τέσσερις μέθοδοι λειτουργίας αρχικά καθορίστηκαν στο Αμερικάνικο πρότυπο μεθόδων λειτουργίας, το NBS FIPS

Pub.81, και στη συνέχεια έγιναν κρατικό πρότυπο στις Η.Π.Α., το ANSI X3.106 το 1983. Το τελευταίο δεν είναι πλέον διαθέσιμο καθώς αντικαταστάθηκε από ένα πρότυπο του διεθνούς οργανισμού ISO.

1.8.2.2.1 Μέθοδοι Γεμίσματος (Padding Methods)

Όλες οι μέθοδοι που θα παρουσιάσουμε προϋποθέτουν ότι το απλό κείμενο θα χωριστεί σε τμήματα καθορισμένου μήκους π.χ. j-bits. Αυτό γίνεται εύκολα με το να θέσουμε τα πρώτα j-bits του απλού κείμενου να ορίζουν το πρώτο τμήμα, τα επόμενα j-bits να ορίζουν το δεύτερο τμήμα κ.ο.κ. Αυτό όμως σημαίνει ότι το τελευταίο τμήμα θα πρέπει να έχει ακριβώς j-bits δηλαδή το μήκους όλου του απλού κειμένου να είναι πολλαπλάσιο του j. Για να λυθεί αυτό το πρόβλημα, τα δύο επικοινωνούντα μέλη θα πρέπει να συμφωνήσουν σε μια μέθοδο γεμίσματος. Μια τέτοια μέθοδος προσθέτει τον απαραίτητο αριθμό bits σύμφωνα με τη συμφωνημένη φόρμουλα ώστε το τελικό μήνυμα να έχει μήκος πολλαπλάσιο του j.

1.8.2.2.1.1 Zero Padding

Η διαγραφή του γεμίσματος από τον παραλήπτη είναι στοιχειώδης αν η δομή των δεδομένων είναι τέτοια ώστε ο παραλήπτης μπορεί εύκολα να καταλάβει το τέλος του string των δεδομένων. Κυρίως αυτό συμβαίνει σε περιπτώσεις όπου τα μηνύματα που ανταλλάσσονται είναι καθορισμένου μήκους. Αλλιώς, θα πρέπει να χρησιμοποιηθεί ένα "special" string, το οποίο δεν εμφανίζεται πουθενά αλλού στο μήνυμα, για να δείχνει το τέλος των δεδομένων. Σε αυτή τη περίπτωση μπορεί να χρησιμοποιηθεί οποιαδήποτε μέθοδος γεμίσματος με την πιο απλή να είναι η πρόσθεση του ελάχιστου αριθμού από μηδενικά στο τέλος του μηνύματος ώστε το padded string να έχει μήκος πολλαπλάσιο του j.

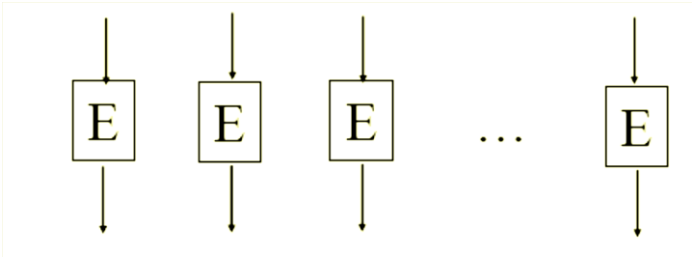
1.8.2.2.1.2 Unambiguous Padding

Μια μέθοδος γεμίσματος μπορεί να σχεδιαστεί έτσι ώστε η διαγραφή του γεμίσματος από τον παραλήπτη να γίνεται εύκολα ανεξάρτητα από το string δεδομένων. Μια τέτοια μέθοδος είναι η Unambiguous Padding όπου προτείνει την προσθήκη ενός 1 στο τέλος του μηνύματος, ακολουθούμενο από τον ελάχιστο αριθμό από μηδενικά ώστε το padded string να έχει μήκος πολλαπλάσιο του j. Αν ο παραλήπτης γνωρίζει ότι έχει χρησιμοποιηθεί αυτή η μέθοδος, η αφαίρεση του γεμίσματος είναι κάτι το τετριμμένο.

Το μειονέκτημα της μεθόδου αυτής είναι ότι μερικές φορές θα έχει ένα παραπάνω block σε σχέση με την Zero Padding. Αυτό γίνεται στις περιπτώσεις όπου το τελευταίο block έχει j-1 bits οπότε η μέθοδος θα προσθέσει ένα 1 και ένα ολόκληρο b-bit block με μηδενικά.

1.8.2.2.2 Electronic Codebook (ECB) Mode

Για να χρησιμοποιηθεί αυτή η μέθοδος, το απλό κείμενο θα πρέπει να έχει τη μορφή ακολουθίας n-bit blocks δηλαδή P_1, P_2, …, P_q (για να το φέρουμε σε αυτή τη μορφή, μπορεί να χρειαστεί μια μέθοδος γεμίσματος). Τότε το κρυπτοκείμενο ορίζεται να είναι η ακολουθία από τα blocks C_1, C_2, …, C_q όπου $C_i=e^K(P_i)$ για κάθε i ($1\leq i\leq q$). Η διαδικασία κρυπτογράφησης φαίνεται στο ακόλουθο σχήμα.



Σχήμα 1.30 ECB Mode

Η διαδικασία αποκρυπτογράφησης λειτουργεί ανάλογα. Ισχύει δηλαδή $P_i=d_K(C_i)$ για κάθε i ($1\leq i\leq q$).

Ιδιότητες: Στην ECB mode, ίδια blocks απλού κειμένου καταλήγουν σε ίδια block κρυπτοκειμένου. Αυτό είναι πρόβλημα όταν κρυπτογραφούνται μεγάλα μηνύματα αφού η πιθανότητα να υπάρχουν δύο ίδια block είναι μεγάλη. Για παράδειγμα, αν το απλό κείμενο είναι ένα κείμενο στο Αγγλικά τροποποιημένο σε δυαδική μορφή, τότε η πιθανότητα να υπάρχουν δύο ίδια blocks είναι αρκετά μεγάλη αφού επαναλαμβανόμενες λέξεις και φράσεις είναι κάτι το συνηθισμένο.

Επίσης, η χρήση αυτής της μεθόδου έχει σαν αποτέλεσμα την εμφάνιση ενός φαινομένου που ονομάζεται εξάπλωση σφάλματος (error propagation). Έτσι αν 1 απλό bit έχει σφάλμα κατά την μετάδοση του μηνύματος, κατά την αποκρυπτογράφηση θα είναι λάθος 1 ολόκληρο block.

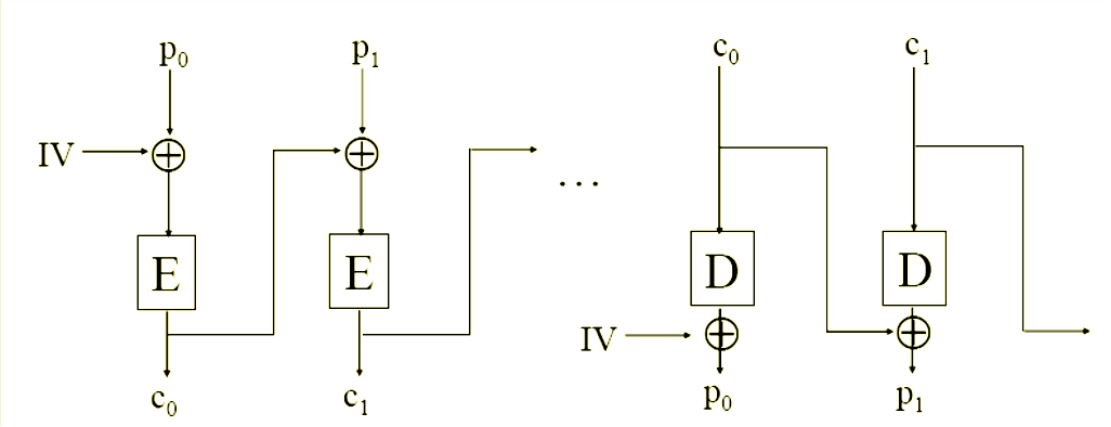
1.8.2.2.3 Cipher Block Chaining (CBC) Mode

Όπως και στην ECB, έτσι και στην CBC το απλό κείμενο πρέπει να "γεμιστεί" με κάποια από τις μεθόδους γεμίσματος ώστε να έχει μήκος πολλαπλάσιο του n και να χωριστεί σε μια ακολουθία τμημάτων n-bits: P_0, P_1, …, P_q. Επίσης μια Αρχική τιμή (IV) πρέπει να επιλεγεί. Τότε η κρυπτογράφηση (σχήμα 1.31(α)) περιέχει τον υπολογισμό τμημάτων κρυπτοκειμένου C_0, C_1, …, C_q ως εξής:

$$C_0=e_K(P_0\oplus IV) \text{ και } C_i=e_K(P_i\oplus C_{i-1}),\ (i>1)$$

Η αποκρυπτογράφηση (σχήμα 1.31 (β)) λειτουργεί ως εξής:

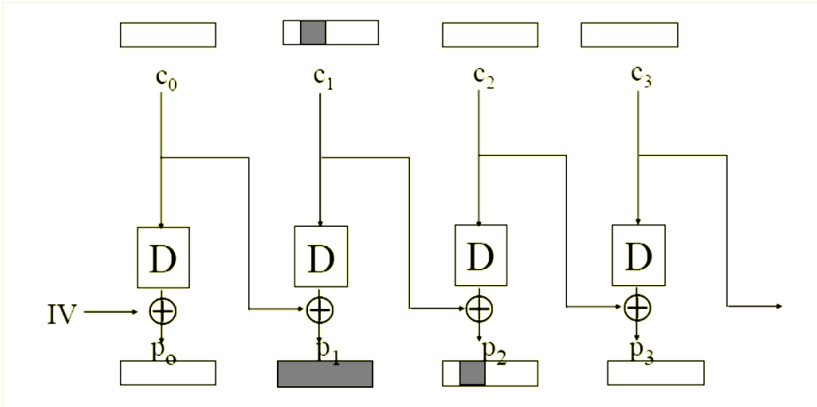
$$P_0=d_K(C_0)\oplus IV \text{ και } P_i=d_K(C_i)\oplus C_{i-1},\ (i>1)$$



Σχήμα 1.31 (α)Κρυπτογράφηση, (β) Αποκρυπτογράφηση στην CBC Mode

Ιδιότητες: Στην CBC mode, αν η IV είναι η ίδια για κάθε μήνυμα, τότε η κρυπτογράφηση του ίδιου κειμένου καταλήγει στο ίδιο κρυπτοκείμενο. Επομένως οι χρήστες θα πρέπει να χρησιμοποιούν διαφορετικές IV για κάθε μήνυμα και αν γίνεται να τις κρατούν κρυφές. Η διαχείριση των IVs είναι ένα δύσκολο ζήτημα αλλά δεν θα επεκταθούμε περισσότερο σε αυτό.

Το πλεονέκτημα της συγκεκριμένης μεθόδου έναντι της ECB είναι ότι , ίδια blocks απλού κειμένου δεν καταλήγουν σε ίδια block κρυπτοκειμένου. Τέλος, όσον αφορά την εξάπλωση σφάλματος (error propagation) και αυτή η μέθοδος παρουσιάζει το φαινόμενο αυτό. Πιο συγκεκριμένα, αν υποθέσουμε ότι το block κρυπτοκειμένου C_1 έχει σφάλμα μετάδοσης σε 1-bit, τότε επειδή κατά την αποκρυπτογράφηση το block απλού κειμένου P_1 εξαρτάται από δύο blocks κρυπτοκειμένου ($P_1=d_K(C_1)\oplus C_0$) καταλήγουμε ότι το P_1 θα έχει τυχαίο αριθμό bits που είναι λάθος. Επίσης το block απλού κειμένου P_2 θα έχει και αυτό σφάλμα κατά 1-bit, αφού ($P_2=d_K(C_2)\oplus C_1$) και το C_1 είναι λάθος. Αυτά φαίνονται αναλυτικά και στο σχήμα 1.32 όπου τα blocks που περιέχουν λάθη απεικονίζονται με πιο έντονο χρώμα.



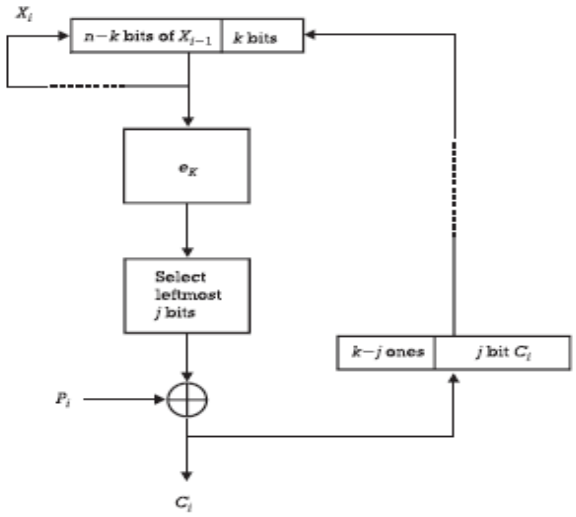
Σχήμα 1.32 Εξάπλωση σφάλματος στην CBC mode

1.8.2.2.4 Cipher Feedback (CFB) Mode

Η CFB mode μπορεί να χρησιμοποιηθεί και ως βασικό δομικό στοιχείο για την κατασκευή γεννήτριας παραγωγής keystream για ένα self-synchronous stream

cipher. Για τη χρήση της μεθόδου αρχικά πρέπει να ορίσουμε δύο παραμέτρους: το k , (1≤k≤n) το οποίο ορίζει το μέγεθος της feedback μεταβλητής και το j , (1≤j≤k) που ορίζει τον αριθμό των bits του απλού κειμένου που κρυπτογραφούνται σε κάθε block. Στη πράξη, το πιο διαδεδομένο σχήμα είναι αυτό όπου j=k=8 .

Η CFB λειτουργεί ως εξής: Το απλό κείμενο διαιρείται σε μια σειρά από blocks μήκους j-bits, τα P_1, P_2, …, P_q, όπου το P_q περιέχει t≤j bits. Οι υπολογισμοί κάνουν χρήση και των μεταβλητών X_i (1≤i≤q) όπου καθεμία είναι μήκους n-bits. Επίσης χρησιμοποιεί και αρχική τιμή IV.



Σχήμα 1.33 8-bit CFB Mode

Κρυπτογράφηση: Αρχικά ορίζουμε X_1=IV. Για i=1, 2, …, q γίνονται οι παρακάτω υπολογισμοί:

$$C_i=P_i\oplus(e_K(X_i\vert_j))$$
και
$$X_{i+1}=(X_i\Vert 1^{k-j}\Vert C_i)\vert^n$$

Στο τελευταίο βήμα, δηλαδή για i=q, ο πρώτος υπολογισμός γίνεται $C_q=P_q\oplus(e_K(X_q\vert_t))$ καθώς το P_q μπορεί να περιέχει t≤j bits ενώ η δεύτερη πράξη δεν γίνεται καθόλου.

Αποκρυπτογράφηση: Αρχικά ορίζουμε X_i=IV. Για i=1, 2, …, q γίνονται οι παρακάτω υπολογισμοί:

$$P_i=C_i\oplus(e_K(X_i\vert_j))$$
και
$$X_{i+1}=(X_i\Vert 1^{k-j}\Vert C_i)\vert^n$$

Όπως και στη διαδικασία κρυπτογράφησης, έτσι και στη διαδικασία αποκρυπτογράφησης, στο τελευταίο βήμα η δεύτερη πράξη δεν γίνεται καθόλου.

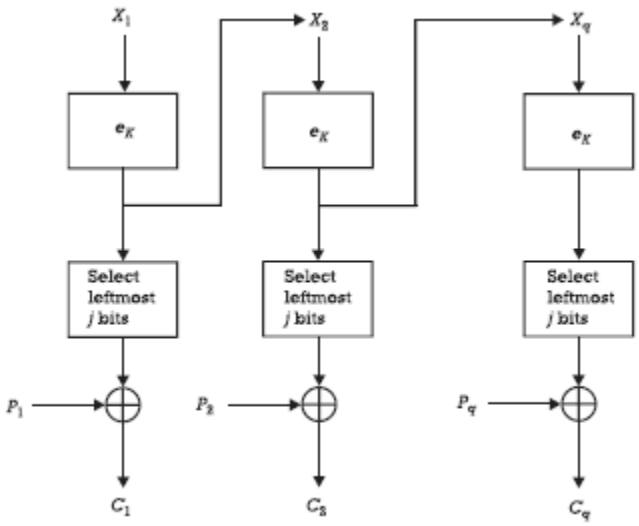
Ιδιότητες: Όπως και στην CBC mode, έτσι και στην CFB, αν η IV είναι η ίδια για κάθε μήνυμα, τότε η κρυπτογράφηση του ίδιου κειμένου καταλήγει στο ίδιο κρυπτοκείμενο. Επομένως οι χρήστες θα πρέπει να χρησιμοποιούν διαφορετικές IV για κάθε μήνυμα και αν γίνεται να τις κρατούν κρυφές.

Όσον αφορά την εξάπλωση σφάλματος (error propagation) και αυτή η μέθοδος παρουσιάζει το φαινόμενο αυτό. Πιο συγκεκριμένα, αν υποθέσουμε ότι το block κρυπτοκειμένου C_i έχει σφάλμα μετάδοσης σε 1-bit, τότε επειδή κατά την αποκρυπτογράφηση το block απλού κειμένου P_i εξαρτάται από δύο blocks κρυπτοκειμένου ($P_i=C_i\oplus(e_K(X_i\vert_j))$) καταλήγουμε ότι ένα τουλάχιστον block απλού κειμένου, το P_i, θα έχει τυχαίο αριθμό bits που είναι λάθος.

1.8.2.2.5 Output Feedback (OFB) Mode

Η OFB, μπορεί να χρησιμοποιηθεί και ως βασικό δομικό στοιχείο για την κατασκευή γεννήτριας παραγωγής keystream για ένα synchronous stream cipher. Για τη χρήση της μεθόδου αρχικά πρέπει να ορίσουμε τη παράμετρο j, ($1\le j\le k$) που ορίζει τον αριθμό των bits του απλού κειμένου που κρυπτογραφούνται σε κάθε block.

Η OFB λειτουργεί ως εξής: Πριν την εφαρμογή της κρυπτογράφησης, το απλό κείμενο διαιρείται σε μια σειρά από blocks. Αν το μήνυμα αποτελείται από (q-1)j+t bits ($1\le t\le j$) τότε το απλό κείμενο διαιρείται σε μια σειρά από blocks μήκους j-bits, τα P_1, P_2, …, P_q, όπου το P_q περιέχει $t\le j$ bits. Οι υπολογισμοί κάνουν χρήση και των μεταβλητών X_i ($1\le i\le q$) όπου καθεμία είναι μήκους n-bits. Επίσης χρησιμοποιεί και αρχική τιμή IV.



Σχήμα 1.34 OFB Mode

Κρυπτογράφηση: Αρχικά ορίζουμε X_1=IV. Για i=1, 2, …, q-1 γίνονται οι παρακάτω υπολογισμοί:

$$C_i = P_i \oplus (e_K(X_i \mid_j))$$
και
$$X_{i+1} = e_K(X_i)$$

Και στο τελευταίο βήμα, δηλαδή για i=q, έχουμε $C_q = P_q \oplus (e_K(X_q \mid_t))$.

Αποκρυπτογράφηση: Αρχικά ορίζουμε X_1=IV. Για i=1,2, …, q-1 γίνονται οι παρακάτω υπολογισμοί:

$$P_i = C_i \oplus (e_K(X_i \mid_j))$$
και
$$X_{i+1} = e_K(X_i)$$

Και στο τελευταίο βήμα, δηλαδή για i=q, έχουμε $P_q = C_q \oplus (e_K(X_q \mid_t))$.

Ιδιότητες: Όπως και στις δύο προηγούμενες μεθόδους, έτσι και στην OFB, αν η IV είναι η ίδια για κάθε μήνυμα, τότε η κρυπτογράφηση του ίδιου κειμένου καταλήγει στο ίδιο κρυπτοκείμενο. Επομένως οι χρήστες θα πρέπει να χρησιμοποιούν διαφορετικές IV για κάθε μήνυμα και αν γίνεται να τις κρατούν κρυφές.

Όσον αφορά την εξάπλωση σφάλματος (error propagation) αυτή η μέθοδος δεν παρουσιάζει το φαινόμενο αυτό. Πιο συγκεκριμένα, αν υποθέσουμε ότι το block κρυπτοκειμένου C_i έχει σφάλμα μετάδοσης σε 1-bit, τότε το block απλού κειμένου P_i θα έχει σφάλμα σε 1-bit.

Στα επόμενα κεφάλαια θα παρουσιάσουμε αναλυτικά δύο από τα πιο γνωστά block ciphers, το DES και το AES, τα οποία ανήκουν στις κατηγορίες που μόλις παρουσιάσαμε. Το DES είναι ένα Feistel cipher ενώ το AES είναι ένα "καθαρό" SP-network. Πιο συγκεκριμένα θα εξετάσουμε την αρχιτεκτονική σχεδιασμού τους, το επίπεδο ασφάλειας που προσφέρουν και κάποιες γενικές τεχνικές κρυπτανάλυσης τους και στη συνέχεια θα περιγράψουμε κάποιες από τις εφαρμογές στις οποίες χρησιμοποιούνται, το πρωτόκολλο αυθεντικοποίησης Kerberos για το DES και τα 3g δίκτυα κινητής τηλεφωνίας για το AES.

Κεφάλαιο 2
Data Encryption Standard

2.1 Ιστορική Αναδρομή

Ο DES είναι ο κρυπταλγόριθμος ο οποίος είχε επιλεγεί ως επίσημο Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών (Federal Information Processing Standard - FIPS) για τις Ηνωμένες Πολιτείες το 1976. Ο DES στη συνέχεια χρησιμοποιήθηκε διεθνώς. Ο αλγόριθμος αρχικά ήταν αμφισβητούμενος, με απόρρητα τα στοιχεία του σχεδιασμού του και ένα σχετικά μικρού μήκους κλειδί. Υπήρχαν υποψίες πως η δημιουργία του DES αποσκοπούσε στη δημιουργία backdoor (κερκόπορτας) για την παραβίαση της ασφάλειας της Υπηρεσίας Εθνικής Ασφάλειας (NSA) των Ηνωμένων Πολιτειών. Ο DES υπέστη έντονη ακαδημαϊκή διερεύνηση και αποτέλεσε το κίνητρο για την κατανόηση των κρυπταλγόριθμων συμμετρικού κλειδιού (block ciphers) και την ανάλυσή τους.

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 (triple DES), αν και υπάρχουν θεωρητικές αμφισβητήσεις. Τα τελευταία χρόνια ο κρυπταλγόριθμος DES έχει εκτοπιστεί από το Προηγμένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Standard - AES).

Η προέλευση του DES βρίσκεται στις αρχές της δεκαετίας του 1970. Το 1972, μετά την ολοκλήρωση μελέτης για την ασφάλεια των υπολογιστών της κυβέρνησης, το γραφείο προτύπων των Η.Π.Α., γνωστό ως NBS (National Bureau of Standards) - που τώρα ονομάζεται NIST (National Institute of Standards and Technology) - επισήμανε την ανάγκη για ένα κυβερνητικό πρότυπο με το οποίο θα μπορούσαν να κρυπτογραφηθούν μη απόρρητες, ευαίσθητες πληροφορίες. Στις 15 Μαΐου του 1973, μετά από διαβούλευση με την NSA, η NBS κάνει προτάσεις για έναν κρυπταλγόριθμο που θα ανταποκρίνεται σε κριτήρια αυστηρού σχεδιασμού. Εντούτοις, καμία από τις προτάσεις που υποβλήθηκαν δεν αποδείχθηκε κατάλληλη. Δημοσιεύθηκε μια δεύτερη πρόταση εκδήλωσης ενδιαφέροντος στις 27 Αυγούστου του 1974. Αυτή τη φορά, η IBM υπέβαλε έναν αλγόριθμο, ο οποίος κρίθηκε αποδεκτός: Ήταν κρυπταλγόριθμος που αναπτύχθηκε κατά τη διάρκεια της περιόδου 1973-1974 βασιζόμενος σε κάποιον προϋπάρχοντα. Αυτός ήταν ο κρυπταλγόριθμος "Lucifer", τον οποίο δημιούργησε ο Χορστ Φάιστελ (Horst

Feistel). Η ομάδα της IBM συνέχισε τον σχεδιασμό και την ανάλυση κρυπταλγόριθμων με τη βοήθεια των Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith και Bryart Tuckerman.

2.1.1 Η ανάμειξη της NSA στο σχεδιασμό

Στις 17 Μαρτίου του 1975 ο προτεινόμενος DES δημοσιεύθηκε στον Ομοσπονδιακό κατάλογο (Federal Register). Ζητήθηκαν δημόσια σχόλια και, στο έτος που ακολούθησε, δύο ανοικτά εργαστήρια κλήθηκαν για να συζητήσουν τα προτεινόμενα πρότυπα. Υπήρξε κριτική από διάφορα μέλη, ανάμεσα στους οποίους ήταν και οι πρωτοπόροι στην κρυπτογραφία δημοσίου κλειδιού Μάρτιν Χέλμαν (Martin Hellman) και Ουίτφιλντ Ντίφι (Whitfield Diffie), οι οποίοι ανέφεραν μικρότερο μήκος κλειδιού για τον DES καθώς και τα μυστήρια "S-boxes" ως στοιχεία ανάρμοστης παρέμβασης από την NSA. Η υποψία ήταν ότι ο αλγόριθμος ήταν συγκεκαλυμμένα αποδυναμωμένος από την Κεντρική Υπηρεσία Πληροφοριών (CIA) έτσι, ώστε μόνον αυτή να μπορεί εύκολα να διαβάσει τα κρυπτογραφημένα μηνύματα. Ο Άλαν Κόνχαϊμ (Alan Konheim), ένας από τους σχεδιαστές του DES, ανέφερε στα σχόλιά του: "Στείλαμε τα s-boxes στην Ουάσιγκτον. Επέστρεψαν και ήταν όλα διαφορετικά."

Η Επιτροπή Αντικατασκοπείας της Γερουσίας των ΗΠΑ (United States Senate Select Committee on Intelligence) αναθεώρησε τις ενέργειες της NSA, ώστε να καθορίσει εάν υπήρξε οποιαδήποτε ανάρμοστη συμμετοχή. Στην αταξινόμητη περίληψη των συμπερασμάτων της, που δημοσιεύθηκε το 1978, η Επιτροπή έγραψε: "Στην ανάπτυξη του DES, η NSA έπεισε την IBM ότι ένα μειωμένο μήκος κλειδιού ήταν ικανοποιητικό. Έμμεσα βοηθούμενη στην ανάπτυξη των δομών S-box και διαβεβαίωσαν ότι ο τελικός αλγόριθμος DES ήταν ό, τι καλύτερο διέθεταν, απαλλαγμένος από οποιαδήποτε στατιστική ή μαθηματική αδυναμία."

Εν τούτοις, η Επιτροπή ανακάλυψε και ανέφερε, επίσης, ότι: "Η NSA δεν πείραξε το σχέδιο του αλγορίθμου από καμιά άποψη. Η IBM εφηύρε και σχεδίασε τον αλγόριθμο, έλαβε όλες τις σχετικές αποφάσεις αναγνωρίζοντας την αξία του αλγόριθμου και συμφώνησε ότι το μέγεθος του κλειδιού ήταν περισσότερο από επαρκές για όλες τις εμπορικές εφαρμογές, για τις οποίες προοριζόταν ο DES."

Ένα άλλο μέλος της ομάδας DES, ο Walter Tuchman, αναφέρεται πως είπε: "Αναπτύξαμε τον αλγόριθμο DES εξ ολοκλήρου μέσα στην IBM χρησιμοποιώντας IBMers. Η NSA δεν δικτύωσε ούτε ένα καλώδιο!"

Ορισμένες από τις υποψίες σχετικά με τις κρυφές αδυναμίες στα S-boxes είχαν εξαλειφθεί το 1990, με την ανεξάρτητη ανακάλυψη και την ανοικτή δημοσίευση της Διαφορικής Κρυπτανάλυσης από τους Eli Biham και Adi Shamir. Τα S-boxes του DES ήταν πολύ πιο ανθεκτικά στην επίθεση απ' ότι αν

είχαν επιλεγεί τυχαία, γεγονός που υποδηλώνει έντονα ότι η IBM γνώριζε για την τεχνική που εφαρμόζονταν στη δεκαετία του 1970. Αυτή ήταν πράγματι η υπόθεση, το 1994, όταν ο Don Coppersmith δημοσίευσε τον αυθεντικό σχεδιασμό των κριτηρίων για τα S-boxes. Σύμφωνα με τον Steven Levi, οι ερευνητές της IBM Watson ανακάλυψαν διαφορικές κρυπταναλυτικές επιθέσεις το 1974 και ζητήθηκε από την NSA να κρατήσει την τεχνική μυστική. Ο Coppersmith εξηγεί την απόρρητη απόφαση της IBM λέγοντας πως: "Αυτό συνέβη επειδή η Διαφορική κρυπτανάλυση μπορεί να αποτελέσει ένα πολύ ισχυρό εργαλείο, που μπορεί να χρησιμοποιηθεί εναντίον πολλών συστημάτων-σχημάτων και υπήρχε ανησυχία ότι τέτοιες πληροφορίες στο δημόσιο τομέα θα μπορούσαν να επηρεάσουν δυσμενώς την εθνική ασφάλεια."

Ο Levy ανέφερε στον Walter Tuchman: "Μας ζητήθηκε να σφραγιστούν όλα τα εμπιστευτικά μας έγγραφα... Πρέπει όντως να βάλουμε έναν αριθμό για κάθε ένα έγγραφο και να τα κλειδώσουμε σε χρηματοκιβώτια, επειδή θεωρήθηκαν απόρρητα έγγραφα της Αμερικανικής κυβέρνησης. Μου είπαν να το κάνω και έτσι το έκανα."

Ο Shamir σχολίασε πως, σε αντίθεση με το τι πιστεύουν μερικοί άνθρωποι, δεν υπάρχουν ενδείξεις χειραγώγησης του DES, έτσι ώστε ο βασικός σχεδιασμός να εξασθενήσει.

Η άλλη κριτική - ότι το μήκος του κλειδιού ήταν πολύ μικρό - ενισχύεται από το γεγονός ότι η αιτιολογία που δόθηκε από την NSA για τη μείωση του μήκους του κλειδιού από τα 64 bits στα 56 bits ήταν ότι τα υπόλοιπα 8 bits θα μπορούσαν να χρησιμεύσουν ως bits ισοτιμίας (parity), πράγμα που έμοιαζε αληθοφανές. Ήταν ευρέως πιστευτό ότι η απόφαση της NSA τροποποιήθηκε λόγω της πιθανότητας να είναι σε θέση (η NSA) να κάνει επιτυχείς επιθέσεις τύπου "brute force" σε κλειδί της τάξης μεγέθους των 56 bits αρκετά χρόνια πριν από τον υπόλοιπο κόσμο.

2.1.2 Ο αλγόριθμος DES ως πρότυπο

Παρά τις επικρίσεις, ο DES εγκρίθηκε ως ομοσπονδιακό πρότυπο τον Νοέμβριο του 1976 και δημοσιεύθηκε στις 15 Ιανουαρίου του 1977 ως FIPS PUB 46 και η χρήση του ήταν επιτρεπτή σε όλα τα μη απόρρητα δεδομένα. Στη συνέχεια επιβεβαιώθηκε ως πρότυπο το 1983, το 1988 (αναθεωρήθηκε ως FIPS-46-1), το 1993 (ως FIPS-46-2) και πάλι το 1999 (ως FIPS-46-3). Ο τελευταίος ορισμός ήταν ο Triple DES. Στις 26 Μαΐου του 2002 ο DES τελικά εκτοπίστηκε από τον Advanced Encryption Standard (AES) κατόπιν δημόσιου διαγωνισμού. Στις 19 Μαΐου του 2005 ο FIPS 46-3 είχε επισήμως αποσυρθεί, αλλά το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) ενέκρινε τον Triple DES στο έτος 2003 για τις ευαίσθητες πληροφορίες της κυβέρνησης. Μια άλλη θεωρητική επίθεση, η γραμμική κρυπτανάλυση, δημοσιεύθηκε το 1994, αλλά ήταν μια επίθεση brute force το

1998 που αναπαράστησε και απέδειξε ότι μπορεί κάποιος να επιτεθεί στον DES και τονίστηκε η ανάγκη για αντικατάσταση του αλγόριθμου. Αυτές και άλλες μέθοδοι κρυπτανάλυσης εξετάζονται λεπτομερώς.

Η εισαγωγή του DES θεωρείται ότι ήταν καταλύτης για την ακαδημαϊκή μελέτη της κρυπτογραφίας, ιδιαίτερα των μεθόδων που "σπάνε" block κρυπταλγόριθμους, σύμφωνα με αναδρομή στο NIST για τον DES.

Μπορεί να ειπωθεί ότι το "αρχικό άλμα" του DES ξεπέρασε τις στρατιωτικές μελέτες και την ανάπτυξη των αλγορίθμων κρυπτογράφησης. Στην δεκαετία του 1970 υπήρχαν πολύ λίγοι κρυπτογράφοι, εκτός εκείνων των στρατιωτικών ή των μυστικών οργανώσεων, και ελάχιστη ήταν η ακαδημαϊκή έρευνα της κρυπτογραφίας. Υπάρχουν τώρα πολλοί δραστήριοι ακαδημαϊκοί κρυπτολόγοι και τμήματα μαθηματικών με ισχυρά προγράμματα στην κρυπτογραφία και την ασφάλεια των πληροφοριών και των εμπορικών εταιρειών και συμβούλων. Μια γενεά κρυπταναλυτών έχει αναλύσει εξονυχιστικά τον αλγόριθμο DES προσπαθώντας να τον "σπάσουν". Ανέφεραν πως ο DES έκανε περισσότερα για να γαλβανίσει τον τομέα της κρυπτανάλυσης από οτιδήποτε άλλο γιατί έτσι υπήρχε ένας αλγόριθμος για μελέτη. Ένα εκπληκτικό μερίδιο της ανοιχτής βιβλιογραφίας στην κρυπτογραφία κατά τη δεκαετία του 1970 και του 1980 ασχολήθηκε με τον DES και ο DES είναι πρότυπο ενάντια σε όλους τους αλγόριθμους συμμετρικού κλειδιού μετά από σύγκριση.

2.1.3 Χρονολογικά

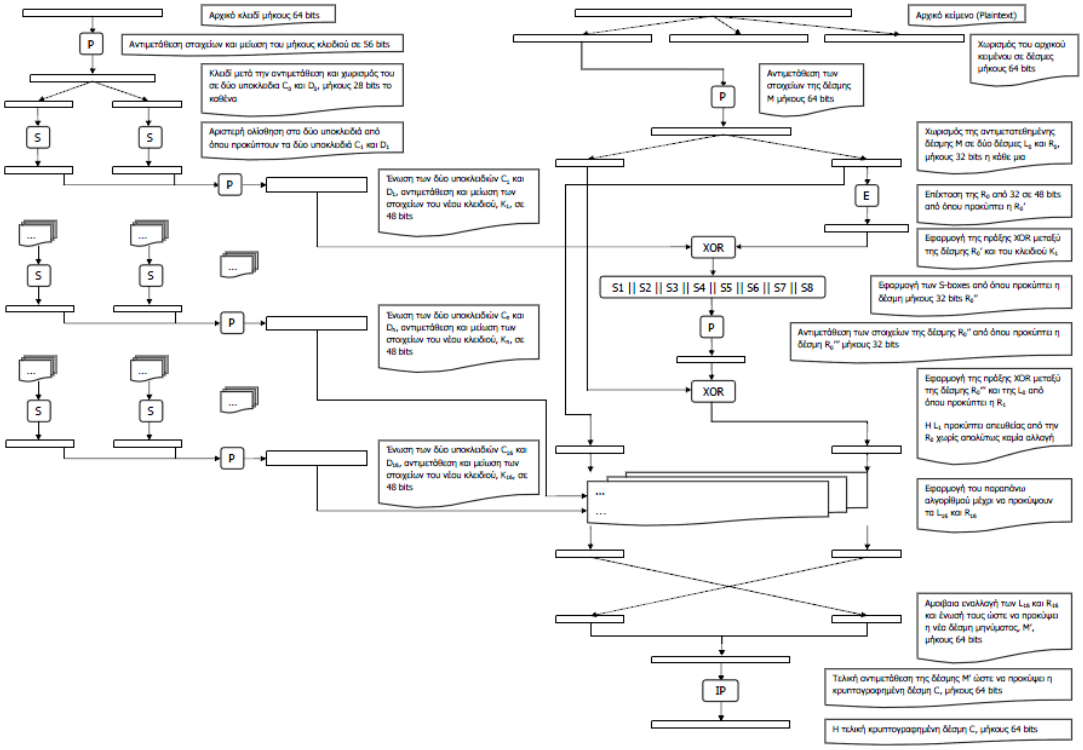
Ημερομηνία	Γεγονότα
15/05/1973	Η NBS δημοσιεύει το πρώτο αίτημα για έναν τυποποιημένο αλγόριθμο κρυπτογράφησης
27/08/1974	Η NBS δημοσιεύει ένα δεύτερο αίτημα για τους αλγόριθμους κρυπτογράφησης
17/03/1975	Ο DES δημοσιεύεται στον ομοσπονδιακό κατάλογο για σχόλια
08/1976	Δημιουργία του πρώτου εργαστηρίου για το DES
09/1976	Δεύτερο εργαστήριο για το DES
11/1976	Ο DES εγκρίνεται ως πρότυπο
15/01/1977	Ο DES δημοσιεύεται ως ένα πρότυπο του FIPS, το FIPS PUB 46
1983	Ο DES επιβεβαιώνεται για πρώτη φορά
1986	Το Videocipher II, ένα δορυφορικό σύστημα TV που χρησιμοποιείται από τη HBO, ανακατεύεται στα συστήματα που βασίζονται στο DES
22/01/1988	Ο DES επιβεβαιώνεται για δεύτερη φορά ως FIPS 46-1, εκτοπίζοντας το FIPS PUB 46
07/1990	Οι Biham και Shamir ανακαλύπτουν πάλι τη διαφορική κρυπτανάλυση και την εφαρμόζουν σε ένα κρυπτοσύστημα είδους DES 15 κύκλων
1992	Οι Biham και Shamir αναφέρουν την πρώτη θεωρητική επίθεση με λιγότερη πολυπλοκότητα από τη brute force, τη

	διαφορική κρυπτανάλυση. Εντούτοις, απαιτεί 2^{47} μη ρεαλιστικά προεπιλεγμένα plaintexts
30/12/1993	Ο DES επιβεβαιώνεται για τρίτη φορά ως FIPS 46-2
1994	Η πρώτη πειραματική κρυπτανάλυση του DES εκτελείται χρησιμοποιώντας γραμμική κρυπτανάλυση (Matsui, 1994)
06/1997	Το πρόγραμμα DESCHALL "σπάει" για πρώτη φορά μπροστά σε κοινό ένα μήνυμα που κρυπτογραφήθηκε με το DES
07/1998	Οι EFF ως DES crackers (Deep Crack) σπάνε ένα κλειδί του DES σε 56 ώρες
01/1999	Μαζί η Deep Crack και η distributed.net σπάνε ένα κλειδί του DES σε 22 ώρες και 15 λεπτά
25/10/1999	Ο DES επιβεβαιώνεται για τέταρτη φορά ως FIPS 46-3, που διευκρινίζει την προτιμημένη χρήση του triple DES με ενιαίο DES που επιτρέπεται μόνο στα κληρονομικά συστήματα
26/11/2001	Το AES δημοσιεύεται σε FIPS 197
26/05/2002	Το πρότυπο AES γίνεται αποτελεσματικό
26/07/2004	Η απόσυρση του FIPS 46-3 (και μερικών σχετικών προτύπων) προτείνεται στον ομοσπονδιακό κατάλογο
19/05/2005	Το NIST αποσύρει το FIPS 46-3
15/03/2007	Η παράλληλη μηχανή COPACOBANA (βασισμένη σε FPGA) του πανεπιστημίου του Μπόχουμ και του Κιέλου της Γερμανίας, σπάνε το DES σε 6,4 ημέρες με κόστος υλικού $10.000

2.2 Γενικές πληροφορίες για τον DES

Ο αλγόριθμος DES είναι ο πιο ευρέως διαδεδομένος αλγόριθμος κρυπτογράφησης στον κόσμο. Για πολλά χρόνια και μεταξύ πολλών ανθρώπων η έννοια της δημιουργίας "μυστικού κώδικα" και ο DES ήταν συνώνυμα. Παρά το γεγονός ότι η Electronic Frontier Foundation επένδυσε 220.000 δολάρια στο να κατασκευάσει ένα σύστημα το οποίο σπάει μηνύματα κρυπτογραφημένα σε DES, ο DES θα παραμένει το κυρίαρχο πρότυπο κρυπτογράφησης στις κυβερνητικές επικοινωνίες και διατραπεζικές συναλλαγές για αρκετά χρόνια ακόμα με μια νέα μορφή του, τον triple-DES.

Παρακάτω περιγράφεται ο τρόπος λειτουργίας του DES. Πρέπει να σημειωθεί ότι πολλοί άλλοι σύγχρονοι αλγόριθμοι κρυπτογράφησης βασίζονται πάνω στον DES και κατανοώντας κάποιος τον τρόπο λειτουργίας του DES δεν θα αντιμετωπίσει προβλήματα στο να κατανοήσει και τους υπολοίπους.



Σχήμα 2.1 Σχηματική παρουσίαση του τρόπου λειτουργίας του DES

2.3 Χαρακτηριστικά του DES

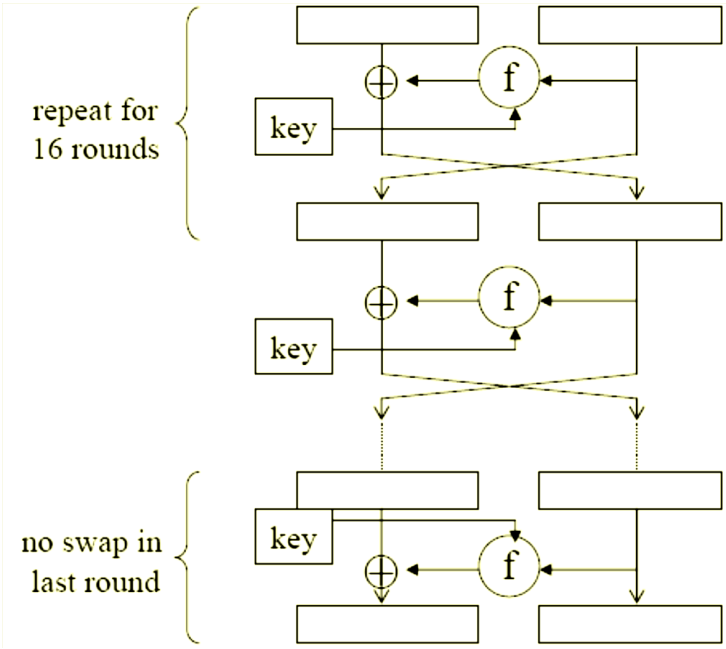
Ο DES είναι αρχετυπικός block cipher, δηλαδή, ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, που λαμβάνει μια σειρά από bits απλού κειμένου (plaintext bits) σταθερού μήκους και την μετατρέπει, μέσω μιας σειράς πολύπλοκων ενεργειών, σε μια άλλη σειρά bits, το κρυπτοκείμενο (ciphertext) με το ίδιο μήκος. Στην περίπτωση του DES το μέγεθος μπλοκ (block size: Η σειρά των bits σταθερού μήκους) είναι 64 bits. Ο DES χρησιμοποιεί, επίσης, ένα κλειδί για να προσαρμόσει την μετατροπή, ώστε η αποκρυπτογράφηση να μπορεί, υποθετικά, να πραγματοποιηθεί μόνο από εκείνους που γνωρίζουν το συγκεκριμένο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Το κλειδί φαινομενικά αποτελείται από 64 bits. Ωστόσο, στην πραγματικότητα μόνο 56 από αυτά χρησιμοποιήθηκαν από τον αλγόριθμο. Τα υπόλοιπα 8 bits χρησιμοποιούνται αποκλειστικά για τον έλεγχο της ισοτιμίας (parity) και στη συνέχεια απορρίπτονται (αυτά καλούνται parity bits), εξ ου και αναφέρεται συνήθως ως κλειδί μήκους 56 bits.

Για να γίνει πιο κατανοητό θα δώσουμε ένα παράδειγμα. Ο DES δουλεύει με bits. Κάθε τετράδα bits αποτελεί έναν δεκαεξαδικό αριθμό. Το δυαδικό 0001 αντιστοιχεί στο δεκαεξαδικό 1, το δυαδικό 1000 το δεκαεξαδικό 8 και το δυαδικό 1111 το δεκαεξαδικό F. Έτσι αν θεωρήσουμε το μη κρυπτογραφημένο κείμενο 8787878787878787 και το κρυπτογραφήσουμε με το κλειδί 0E329232EA6D0D73 θα λάβουμε το κρυπτογραφημένο μήνυμα 0000000000000000. Αν αποκρυπτογραφήσουμε το κρυπτογραφημένο αυτό μήνυμα με το μυστικό κλειδί 0E329232EA6D0D73 το αποτέλεσμα που θα

λάβουμε θα είναι το αρχικό μη κρυπτογραφημένο μήνυμα 8787878787878787.

Αυτό το παράδειγμα είναι επιδέξια κατασκευασμένο και μεθοδικό γιατί το μη κρυπτογραφημένο μήνυμα έχει μήκος ακριβώς 64 bits. Το ίδιο θα συνέβαινε και αν το αρχικό μήνυμα είχε μήκος πολλαπλάσιο των 64 bits, συνθήκη, όμως, που δεν ικανοποιείται από τα περισσότερα μηνύματα που πρόκειται να κρυπτογραφηθούν.

Όπως οι άλλοι block αλγόριθμοι κρυπτογράφησης, έτσι και ο DES από μόνος του δεν είναι ασφαλής τρόπος κρυπτογράφησης αλλά, αντίθετα, πρέπει να χρησιμοποιηθεί με ειδικό τρόπο λειτουργίας (mode of operation). Είναι ένα κρυπτοσύστημα τύπου Feistel που χρησιμοποιεί μήκος block 64 bits, κλειδί μήκους 56 bits, έχει 16 γύρους και σε κάθε γύρο εφαρμόζονται αντικαταστάσεις και αντιμεταθέσεις. Έχει σχεδιαστεί για εφαρμογές με περιορισμένους πόρους όπως κατανάλωση ρεύματος και πολυπλοκότητα πυλών (good hardware performance) ενώ δεν είναι κατάλληλο για εφαρμογές όπου υπάρχουν απαιτήσεις για υψηλές ταχύτητες παραγωγής. Για παράδειγμα ένα πρόγραμμα που έχει υλοποιηθεί στη γλώσσα προγραμματισμού C++ σε υπολογιστή Pentium 4 (2.1 GHz) "τρέχει" τις κρυπτογραφικές πράξεις με ταχύτητα 88 Mbits/sec ενώ σε μια hardware εφαρμογή όπως ASIC οι κρυπτογραφικές πράξεις γίνονται με ταχύτητα 1280 Mbits/sec. Η γενική δομή του DES φαίνεται παρακάτω:



Σχήμα 2.2 Δομή του DES

Παρατήρηση: Στην αρχή και στο τέλος της βασικής δομής του Feistel network προστίθεται μια αντιμετάθεση IP και η αντίστροφή της IP^{-1}. Η IP εφαρμόζεται στο απλό κείμενο πριν από το πρώτο γύρο, πριν καν αυτό χωριστεί στα δύο τμήματα ενώ η IP^{-1} εφαρμόζεται μετά το τέλος του $16^{ου}$ γύρου. Η χρησιμοποίηση αυτών των αντιμεταθέσεων δεν προσφέρει καθόλου

στην ασφάλεια της δομής παρά μόνο διευκολύνει στις hardware υλοποιήσεις (στο τρόπο που θα γίνει η φόρτωση των δεδομένων). Για το κρυπτοσύστημα DES η αρχική αντιμετάθεση IP δίνεται στο παρακάτω πίνακα. Σύμφωνα με τον πίνακα αυτό, το bit που βρίσκεται για παράδειγμα στη θέση 58, η IP το στέλνει στη θέση 1.

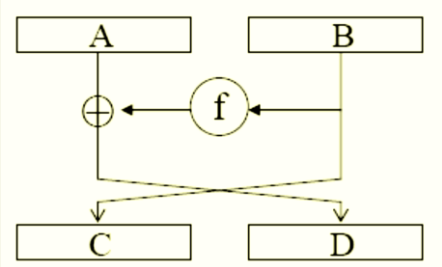
IP								IP^{-1}							
58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27
61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

Σχήμα 2.3 Αρχική Αντιμετάθεση του DES

2.4 Ανάλυση της δομής του DES

Υπάρχουν 16 πανομοιότυπα στάδια επεξεργασίας, που καλούνται γύροι. Υπάρχει, επίσης ,μια αρχική και μια τελική μετάθεση που καλούνται IP και FP (ή IP^{-1}) αντίστοιχα, οι οποίες είναι αντίστροφες συναρτήσεις (η IP "ανατρέπει" τη δράση του FP και αντίστροφα). Η IP και η FP δεν έχουν σχεδόν καμία κρυπτογραφική σημασία, αλλά συμπεριλήφθηκαν, προφανώς, προκειμένου να διευκολύνουν τα block φόρτωσης μέσα και έξω από το υλικό των μέσων της δεκαετίας του 1970, καθώς επίσης και για να κάνουν τον DES να "τρέχει" πιο αργά σε λογισμικό.

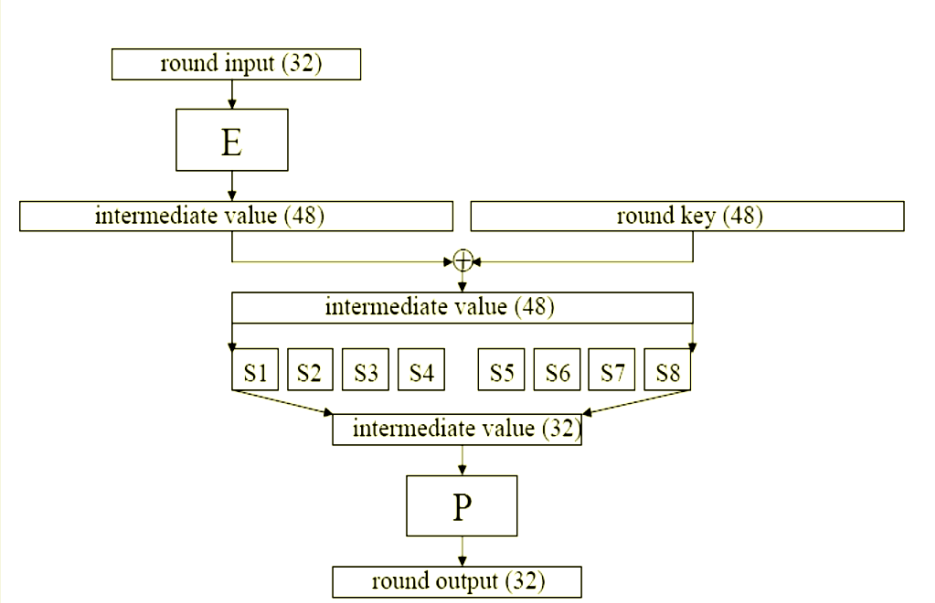
Μετά την εφαρμογή της IP, το απλό κείμενο χωρίζεται σε δύο τμήματα των 32 bits (βλέπε σχήμα 2.4). Κατά την κρυπτογράφηση, γίνονται οι εξής πράξεις: C=B και D=f(B)⊕A. Αυτό ολοκληρώνει ένα γύρο ενός Feistel network. Αυτή η σταυροειδής διάταξη εξασφαλίζει ότι η αποκρυπτογράφηση και η κρυπτογράφηση είναι παρόμοιες διαδικασίες. Η μόνη διαφορά είναι ότι τα υποκλείδια ή δευτερεύοντα κλειδιά (subkeys) εφαρμόζονται σε αντίστροφη διάταξη, όταν εκτελείται η πράξη της αποκρυπτογράφησης. Το υπόλοιπο του αλγορίθμου είναι ίδιο. Αυτό απλοποιεί πολύ την εφαρμογή, ιδιαίτερα στο υλικό, δεδομένου ότι δεν υπάρχει καμία ανάγκη για ξεχωριστούς αλγορίθμους κρυπτογράφησης και αποκρυπτογράφησης. Η F συνάρτηση αναμιγνύει το μισό τμήμα του block μαζί με ένα μέρος από το κλειδί. Η έξοδος από την συνάρτηση F συνδυάζεται έπειτα με το άλλο μισό του block και τα ήμισυ ανταλλάσσονται πριν από τον επόμενο κύκλο. Η διαδικασία αυτή επαναλαμβάνεται 15 φορές. Στον $16^{ο}$ και τελευταίο γύρο, δεν έχουμε εναλλαγή (δηλαδή το B πάει στο D και το A στο C). Κατά την αποκρυπτογράφηση, οι πράξεις που λαμβάνουν χώρα είναι οι εξής: B=C και A=D⊕f(C).



Σχήμα 2.4 Ένας γύρος ενός Feistel network

2.4.1 Round function f

Μέχρι στιγμής έχουμε απλώς αναφέρει ότι σε κάθε γύρο, το δεξί τμήμα B του απλού κειμένου περνάει από μια συνάρτηση f χωρίς να επεκταθούμε περισσότερο στις διαδικασίες που περιέχονται σε αυτή τη συνάρτηση f η οποία αποτελείται από τέσσερα στάδια, την επέκταση, την ανάμειξη κλειδιών, την αντικατάσταση και τέλος τη μεταλλαγή. Συγκεκριμένα, τα 32 bits απλού κειμένου που αποτελούν input στη συνάρτηση f αρχικά υπόκεινται μια επέκταση μέσω μιας συνάρτησης επέκτασης E (Expansion function). Το αποτέλεσμα είναι η επέκταση των 32 bits σε 48 ώστε να μπορέσει να γίνει η XOR με το round key, το οποίο όπως θα δούμε αναλυτικότερα στη συνέχεια είναι και αυτό μήκους 48 bits. Ο πιο συνηθισμένος τρόπος επέκτασης είναι η μερική επανάληψη όπου τα μισά bits επαναλαμβάνονται. Το επόμενο βήμα είναι η ανάμειξη κλειδιών, κατά την οποία εισάγεται ένα υποκλειδί μέσω μιας XOR το οποίο δίνει μια τιμή που ονομάζεται intermediate value και είναι μήκους 48 bits. Στη συνέχεια, η intermediate value χωρίζεται σε 8 τμήματα των 6 bits για να αποτελέσει είσοδο στη συνάρτηση αντικατάστασης (S-Boxes). Τα S-Boxes, που παρέχουν τον πυρήνα της ασφάλειας του DES και χωρίς αυτά ο κρυπταλγόριθμος θα ήταν γραμμικός και κοινότοπα εύθραυστος, αντιστοιχούν 6 - bits→4-bits , επομένως παράγουν μια "intermediate value 2" μήκους 32-bits, η οποία κατά το στάδιο της μεταλλαγής περνάει σε μια συνάρτηση αντιμετάθεσης P. Το αποτέλεσμα όλων αυτών των διαδικασιών ονομάζεται round output, είναι μήκους 32 bits και είναι η τιμή η οποία θα γίνει XOR με το δεξί τμήμα του απλού κειμένου (δηλαδή το A σύμφωνα με το σχήμα 2.4). Η εναλλαγή της αντικατάστασης από τα S-boxes και τη μεταλλαγή των bits από το P-box και την E-επέκταση (expansion), παρέχει τη λεγόμενη "σύγχυση και διάχυση" αντίστοιχα, μια έννοια που προσδιορίστηκε από τον Claude Shannon τη δεκαετία του 1940 ως απαραίτητη προϋπόθεση για ασφαλή και πρακτικό πλέον κρυπταλγόριθμο. Όλα τα παραπάνω φαίνονται λεπτομερώς παρακάτω:



Σχήμα 2.5 Η round function f

2.4.2 S-Boxes

Τα S-Boxes συνήθως είναι look-up tables που για το DES έχουν 16 στήλες και 4 γραμμές (βλέπε σχήμα 2.6). Οι γραμμές είναι 4 αντιμεταθέσεις, οι π_0, π_1, π_2, π_3.Το input στο S-Box είναι ένα string μήκους 6 bits π.χ. το 001101. Σε αυτό το string, τα δύο εξωτερικά bits (το πρώτο και το τελευταίο) δείχνουν τη γραμμή του πίνακα και τα 4 εσωτερικά bits δείχνουν τη στήλη. Στο παράδειγμά μας και για το S-Box 5 που δείχνουμε στο σχήμα 2.5, έχουμε 01=1 άρα πρώτη σειρά και 0110=6 άρα στην έκτη στήλη. Στη θέση αυτή του πίνακα είναι το στοιχείο 13 το οποίο είναι ίσο με 1101 σε δυαδική μορφή. Άρα τελικά το input 001101 στο S-Box 5 του DES, θα γίνει 1101.

S-Box 5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
π_0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
π_1	14	1	2	12	4	7	13	1	5	0	15	10	3	9	8	6
π_2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
π_3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Σχήμα 2.6 Το S-Box 5 του DES

Τα S-Boxes αποτελούν βασικό στοιχείο για τα κρυπτοσυστήματα του Feistel καθώς είναι τα μόνα μη-γραμμικά στοιχεία και επομένως οι περισσότερες επιθέσεις επικεντρώνονται σε αυτά. Για το λόγο αυτό ο σχεδιασμός του πρέπει να είναι προσεκτικός και να ακολουθεί κάποια κριτήρια. Για παράδειγμα, τα S-Boxes για το DES σύμφωνα με τον Coppersmith πρέπει να ακολουθούν τα παρακάτω κριτήρια:

- $Hwt(x_1 \oplus x_2)=1 \Rightarrow Hwt(y_1 \oplus y_2) \geq 2$
- $(x_1 \oplus x_2)=001100 \Rightarrow Hwt(y_1 \oplus y_2) \geq 2$
- $(x_1 \oplus x_2)=11??00 \Rightarrow Hwt(y_1 \oplus y_2) \geq 1$

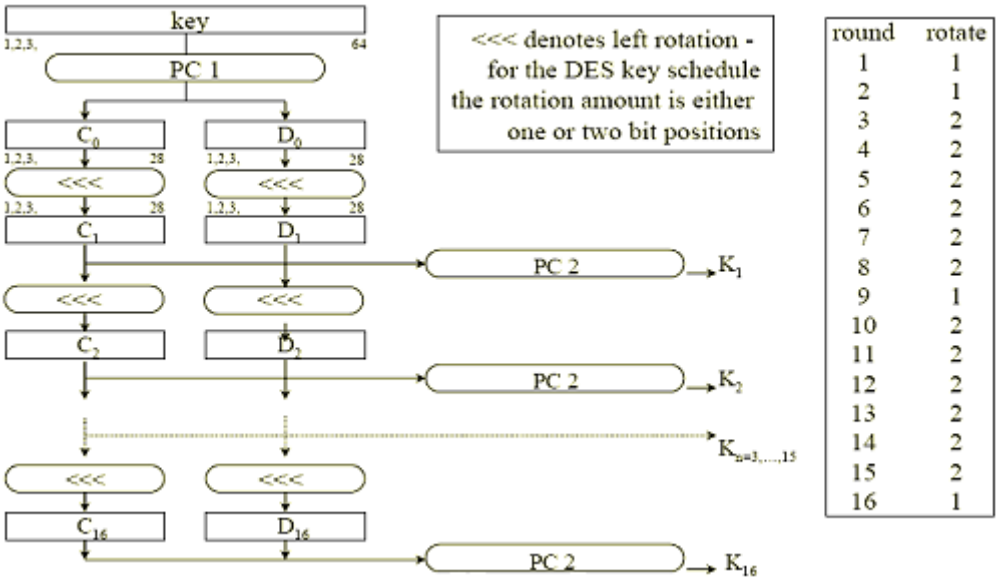
- $\text{Prob}[y_1 \oplus y_2)=a \mid x_1 \oplus x_2=b] \leq 0.25$ για $b \neq 0$

Τα κριτήρια αυτά μαζί με κάποιες ιδιότητες της συνάρτησης αντιμετάθεσης P κάνουν το κρυπτοσύστημα DES ανθεκτικό σε ένα είδος επίθεσης που ονομάζεται διαφορική κρυπτανάλυση (Differential cryptanalysis). Η συγκεκριμένη επίθεση παρουσιάζεται λεπτομερώς στη συνέχεια. Τα κριτήρια της συνάρτησης αντιμετάθεσης P είναι τα εξής:

- Τα output bits ενός S-Box επηρεάζουν 6 S-Boxes.
- Δύο output bits δεν επηρεάζουν το ίδιο S-Box.
- Δύο output bits επηρεάζουν δύο εσωτερικά bits.
- Τα δύο άλλα output bits θα επηρεάσουν δύο εξωτερικά bits.
- Αν ένα output bit του S-Box A επηρεάσει ένα εσωτερικό bit του S-Box B, τότε ένα output bit του S-Box B δεν μπορεί να επηρεάσει ένα εσωτερικό bit του S-Box A.

2.4.3 Πρόγραμμα Κλειδιού

Τέλος, παρουσιάζουμε το Πρόγραμμα Κλειδιού του DES. Όπως έχουμε ήδη αναφέρει, το DES χρησιμοποιεί κλειδί μήκους 64-bits από τα οποία 56-bits είναι αυτά που χρησιμοποιούνται στην ουσία καθώς τα 8 είναι parity bits.



Σχήμα 2.7 Πρόγραμμα Κλειδιού του DES

Επομένως, σύμφωνα και με το Πρόγραμμα Κλειδιού που παρουσιάζεται στο σχήμα 2.7, η συνάρτηση αντιμετάθεσης PC 1 (βλέπε σχήμα 2.8) αφαιρεί αυτά τα parity bits και στη συνέχεια τα 56-bits κλειδιού χωρίζονται σε δύο τμήματα των 28-bits (τα C_0 και D_0 στο σχήμα). Το κάθε τμήμα υπόκεινται σε "αριστερή περιστροφή" κατά μια ή δύο θέσεις. Αξίζει να σημειωθεί ότι οι περιστροφές δεν είναι κάθε φορά οι ίδιες για την αποφυγή κάποιων επιθέσεων που ονομάζονται "related key attacks". Μετά την περιστροφή, τα τμήματα C_1 και

D_1 συνδυάζονται και αποτελούν το κλειδί για τον πρώτο γύρο ενώ ταυτόχρονα υπόκεινται και σε άλλη περιστροφή ώστε να παράγουν και το κλειδί για τον δεύτερο γύρο κ.ο.κ. Ο συνδυασμός των τμημάτων C_1 και D_1 γίνεται μέσω της συνάρτησης PC2 (βλέπε σχήμα 2.8) η οποία προσθέτει και κάποια bits ώστε να παράγει κλειδί 48-bits. Τα 24 bits προέρχονται από το αριστερό μισό και τα υπόλοιπα 24 από το δεξί μισό. Οι περιστροφές σημαίνουν ότι ένα διαφορετικό σύνολο από bits χρησιμοποιείται σε κάθε υποκλειδί. Κάθε bit χρησιμοποιείται σε περίπου 14 από τα 16 υποκλειδιά.

PC1							PC2					
57	49	41	33	25	19	9	14	17	11	24	1	5
1	58	50	42	34	26	18	3	28	15	6	21	10
10	2	59	43	43	35	27	23	19	12	4	26	8
19	11	3	60	52	44	36	16	7	27	20	13	2
63	55	47	39	31	23	15	41	52	31	37	47	55
7	62	54	46	38	30	22	30	40	51	45	33	48
14	6	61	53	45	37	29	44	49	39	56	34	53
21	13	5	28	20	12	4	46	42	50	36	29	32

Σχήμα 2.8 Οι συναρτήσεις PC1 και PC2

Το πρόγραμμα κλειδιού για την αποκρυπτογράφηση είναι παρόμοιο, δηλαδή τα υποκλειδιά είναι σε αντίστροφη διάταξη έναντι αυτή της κρυπτογράφησης. Αν, δηλαδή, κατά την κρυπτογράφηση το πρόγραμμα κλειδιού είναι {k1, k2, k3 ... k16}, τότε το πρόγραμμα κλειδιού της αποκρυπτογράφησης θα είναι {k16 ... k3, k2, k1}. Πέραν αυτής της αλλαγής, η διαδικασία είναι η ίδια όπως για την κρυπτογράφηση.

2.5 Αδύναμα κλειδιά του DES

Ο αλγόριθμος DES έχει κάποια κλειδιά τα οποία ονομάζονται ασθενή-αδύναμα (weak) κλειδιά και κάποια άλλα τα οποία ονομάζονται ημιασθενή (semi-weak) κλειδιά. Η χρήση αυτών των κλειδιών έχει σαν αποτέλεσμα ο DES κατά τη διαδικασία της κρυπτογράφησης να συμπεριφέρεται όπως ακριβώς συμπεριφέρεται στη διαδικασία της αποκρυπτογράφησης.

Όπως ήδη γνωρίζουμε, το κλειδί των 56 bit σπάει σε 16 υποκλειδιά σύμφωνα με τον αλγόριθμο. Το πρόβλημα που δημιουργείται με τα ασθενή κλειδιά είναι ότι τα 16 υποκλειδιά που προκύπτουν από το αρχικό κλειδί, είναι ίδια. Παραθέτουμε τώρα, τις περιπτώσεις κατά τις οποίες προκύπτει ασθενές κλειδί:

1. Όταν έχουμε εναλλασσόμενους άσσους και μηδενικά (0101010101010101).
2. Όταν έχουμε εναλλασσόμενα "F" και "E" (FEFEFEFEFEFEFEFE).
3. Το κλειδί : E0E0E0E0F1F1F1F1.
4. Το κλειδί : 1E1E1E1E0F0F0F0F.

Χρησιμοποιώντας τα παραπάνω κλειδιά τα υποκλειδιά που προκύπτουν, ανάλογα με την περίπτωση, είναι μηδενικά, άσσοι ή εναλλασσόμενα μηδενικά

και άσσοι. Έτσι αν χρησιμοποιήσουμε τη διαδικασία της κρυπτογράφησης δύο φορές με το ίδιο κλειδί, θα πάρουμε το αρχικό κείμενο:

$$E_K(E_K(M))=M.$$

Με αντίστοιχο τρόπο λειτουργούν και τα ημιασθενή κλειδιά με τη διαφορά ότι τα ημιασθενή κλειδιά δουλεύουν ως ζεύγη. Αν δηλαδή κρυπτογραφήσουμε δύο φορές ένα αρχικό κείμενο με ένα ζεύγος ημιασθενών κλειδιών θα πάρουμε το αρχικό κείμενο:

$$E_{K1}(E_{K2}(M))=M.$$

Τα ζεύγη των ημιασθενών κλειδιών είναι τα παρακάτω:

1. 011F011F010E010E και 1F011F010E010E01.
2. 01E001E001F101F1 και E001E001F101F101.
3. 01FE01FE01FE01FE και FE01FE01FE01FE01.
4. 1FE01FE00EF10EF1 και E01FE01FF10EF10E.
5. 1FFE1FFE0EFE0EFE και FE1FFE1FFE0EFE0E.
6. E0FEE0FEF1FEF1FE και FEE0FEE0FEF1FEF1.

Σε αυτό το σημείο πρέπει να τονίσουμε ότι το πλήθος των προβληματικών κλειδιών του DES είναι πάρα πολύ μικρό και συνεπώς οι πιθανότητες να χρησιμοποιηθούν είναι ελάχιστες. Είναι πολύ βασικό για την ανθεκτικότητα του αλγορίθμου και κάθε αλγορίθμου, τα ασθενή κλειδιά να είναι γνωστά από την αρχή καθώς αν δεν τα γνωρίζουν ούτε οι σχεδιαστές του αλγορίθμου τότε υπάρχει σοβαρό κενό ασφαλείας στον αλγόριθμο. Αν οι σχεδιαστές γνωρίζουν τα ασθενή κλειδιά, μπορούν να ξεπεράσουν αυτό το εμπόδιο κατά την υλοποίηση του αλγορίθμου.

2.6 Κρυπτανάλυση του DES

Το DES κυρίως λόγω της ευρείας χρήσης του σε πολλές εφαρμογές έχει υποστεί αρκετές επιθέσεις. Οι φόβοι των περισσότερων για αδυναμίες του DES δεν έχουν επαληθευτεί ακόμα και σήμερα. Το μόνο μειονέκτημα πλέον του κρυπτοσυστήματος αυτού είναι η εξαντλητική μέθοδος (exhaustive key search) ή επίθεση ωμής βίας (brute-force), η οποία με τα σημερινά δεδομένα και λόγω του σχετικά μικρού μήκους κλειδιού (56- bits) είναι υπολογιστικά δυνατή. Επίσης, υπάρχουν τρία ακόμα είδη επιθέσεων που θεωρητικά μπορούν να σπάσουν και τους δέκα έξι γύρους του DES με λιγότερη πολυπλοκότητα από μια αναζήτηση brute force, αλλά είναι αδύνατο να εφαρμοστούν στην πράξη. Τέτοιου είδους επιθέσεις καλούνται μερικές φορές Certificational Weaknesses και είναι:

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

2.6.1 Εξαντλητική Μέθοδος (Exhaustive Key Search) ή επίθεση ωμής βίας (Brute-force)

Η brute-force attack (επίθεση ωμής βίας) αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Τέτοιου είδους επιθέσεις, οι οποίες χρησιμοποιούν όλα τα δυνατά κλειδιά, μπορούν πάντοτε να πραγματοποιηθούν. Συχνά, όμως, ο επιτιθέμενος ξεκινά την επίθεση χρησιμοποιώντας πιο "πιθανά", κατά την άποψή, του κλειδιά, προσπαθώντας με αυτό τον τρόπο να βρει το κλειδί πιο γρήγορα. Πρακτικά, η αναζήτηση σταματά μόλις βρεθεί το κλειδί, χωρίς να χρειαστεί περαιτέρω ενημέρωση της λίστας κλειδιών.

Στην ακαδημαϊκή βιβλιογραφία η μέθοδος brute-force είναι μέτρο ασφάλειας ενός αλγόριθμου κρυπτογράφησης. Ένας αλγόριθμος κρυπτογράφησης θεωρείται "σπασμένος" αν υπάρχει αλγόριθμος κρυπτανάλυσης, ο οποίος μπορεί να βρει το κλειδί με μικρότερη πολυπλοκότητα από τη μέθοδο brute-force, ανεξαρτήτως εάν αυτή η προσπάθεια υπολογισμού είναι εφικτή στην πράξη.

Συνήθως, το μήκος των κρυπτογραφικών κλειδιών επιλέγεται με τρόπο τέτοιο, ώστε να απαιτείται υπερβολικά μεγάλος χρόνος υπολογισμών (με βάση τις τρέχουσες υπολογιστικές δυνατότητες) και άρα να μην έχει χρηστική αξία μία τέτοιου είδους επίθεση. Ωστόσο, πολλά υπολογιστικά συστήματα έχουν κατά καιρούς γίνει στόχος brute force attack, με περισσότερο γνωστά τα συστήματα του Πενταγώνου και αστυνομικών αρχών των ΗΠΑ.

Η εξαντλητική μέθοδος για ένα στοιχείο σε δυαδική μορφή μήκους 56-bits, όπως το κλειδί του DES παίρνει χρόνο $O(2^{55})$. Αυτό μπορεί να μειωθεί στο μισό, δηλαδή σε χρόνο $O(2^{54})$, εκμεταλλευόμενοι μια ιδιότητα του DES η οποία ονομάζεται συμπληρωματικότητα (βλέπε ορισμό 2.1). Αν υποθέσουμε ότι ο αντίπαλος γνωρίζει δύο ζεύγη απλού κειμένου – κρυπτοκειμένου, τα (p,c)και (p*,d), τότε σύμφωνα με την ιδιότητα της συμπληρωματικότητας έχουμε ότι $d^*=DES_{k^*}(p)$ και $d=DES_k(p^*)$. Επομένως δοκιμάζοντας ένα trial key k' και κάνοντας δύο δοκιμές ($DES_{k'}=c$ ή $DES_{k'}=d^*$) ο αντίπαλος μπορεί να ανακαλύψει το σωστό κλειδί σε χρόνο $O(2^{54})$.

Ορισμός 2.1 Έστω $x^*=x\oplus 11\ldots 1$ το συμπληρωματικό στοιχείο ενός στοιχείου x. Εάν $DES_k(m)=c$ τότε $DES_{k^*}(m^*)=c^*$.

Η πρώτη επίθεση έχει καταγραφεί το 1977 από τους Diffie και Hellman η οποία βρήκε το κλειδί σε 20 ώρες ενώ η τελευταία έγινε το 1999. 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 "έσπαγε" 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. Η επίθεση του 1999 βρήκε το κλειδί σε 3 μέρες αλλά το κόστος της ήταν κατά πολύ μειωμένο σε σχέση με αυτή των Diffie και Hellman. Στην επίθεση αυτή χρησιμοποιήθηκε ένα DES Cracker ενώ 62% της υπολογιστικής δύναμης ήταν κατανεμημένο μέσω του διαδικτύου σε κάποιες εκατοντάδες υπολογιστές. Αναλυτικά οι επιθέσεις με τα κόστη και τα αποτελέσματά τους παρουσιάζονται στο πίνακα 2.9:

	Year	Cost	Time
Diffie+Hellman	1977	$20,000,000	20 hours
Wiener	1993	$1,000,000	7 hours
BSA	1995	$300,000	6 hours
Wiener	1998	$1,000,000	70 min.
Distributed.net	1997	≈ $0	140 days
EFF	1998	$250,000	9 days
Distributed.net+EFF	1999	$250,000	3 days

Πίνακας 2.9 Επιθέσεις κατά του DES

Η μόνη άλλη επιβεβαιωμένη μηχανή που "έσπαγε" 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 βρίσκει εφαρμογή και σε άλλες λειτουργίες για "σπάσιμο" κωδικών. Μια από τις πιο 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).

2.6.2 Διαφορική Κρυπτανάλυση (Differential Cryptanalysis)

Η διαφορική κρυπτανάλυση είναι μια επίθεση τύπου επιλεγμένου απλού κειμένου (chosen plaintext attack) δηλαδή τα δεδομένα που πρέπει να γνωρίζει ο αντίπαλος είναι ζεύγη απλού κειμένου τα οποία πρέπει να διαλέξει. Συνήθως οι επιθέσεις αυτές χρειάζονται μεγάλη ποσότητα δεδομένων για να υλοποιηθούν. Στη διαφορική κρυπτανάλυση, ο αντίπαλος ορίζει μια σχέση (συνήθως XOR) μεταξύ ζευγών απλού κειμένου για την οποία το αποτέλεσμα είναι γνωστό. Για παράδειγμα η σχέση $p \oplus p' = d$ μας δίνει την γνωστή διαφορά d μεταξύ των ποσοτήτων p και p΄. Η επίθεση συνεχίζεται με τον αντίπαλο να προσπαθεί να βρει (x, x΄) τέτοια ώστε να ισχύει η σχέση $x \oplus x' = e$ (όπου e γνωστή ποσότητα) με μεγάλη πιθανότητα.

Στη συνέχεια ορίζονται τα χαρακτηριστικά μονοπάτια για κάθε παράγοντα του κρυπτοσυστήματος, τα οποία είναι μονοπάτια διαφορών. Συνδυάζοντας τα χαρακτηριστικά μονοπάτια όλων των παραγόντων, καταλήγουμε σε χαρακτηριστικά μονοπάτια του κάθε γύρου. Επειδή τα χαρακτηριστικά μονοπάτια είναι επαναλαμβανόμενα, τελικά θα έχουμε χαρακτηριστικά μονοπάτια για πολλούς γύρους. Αυτό τελικά μας οδηγεί στο προσδιορισμό ενός διαφορικού. Διαφορικό ονομάζεται η συλλογή χαρακτηριστικών μονοπατιών και καθορίζεται στην αρχή και στο τέλος του κρυπτοσυστήματος.

Η επίθεση τώρα ολοκληρώνεται με την επιλογή ενός trial key και έλεγχο για να δούμε αν είναι το σωστό. Πιο συγκεκριμένα, για ένα κρυπτοσύστημα με r γύρους, ο αντίπαλος κατασκευάζει ένα διαφορικό r-1 γύρων. Έστω ότι η επίθεση άρχισε με ένα ζεύγος απλού κειμένου (p, p΄). Μετά τους r-1 γύρους, θα έχουμε το διαφορικό $x \oplus x'$ που ισχύει με πιθανότητα P ενώ το κρυπτοκείμενο είναι το (c,c΄). Επομένως ισχύει ότι: $c=E_k(x)$ και $c'=E_k(x')$. Ή ισοδύναμα $x=E_k^{-1}(c)$ και $x'=E_k^{-1}(c')$. Συνδυάζοντας τις δύο τελευταίες εξισώσεις, έχουμε:

$$e=x \oplus x' = E_k^{-1}(c) \oplus E_k^{-1}(c').$$

Άρα ο αντίπαλος υπολογίζει τη σχέση $E_k^{-1}(c) \oplus E_k^{-1}(c')$ για κάθε trial key και αν $k = k^*$ τότε $E_k^{-1}(c) \oplus E_k^{-1}(c') = e$ με πιθανότητα P ενώ αν $k \neq k^*$ τότε $E_k^{-1}(c) \oplus E_k^{-1}(c') \neq e$ με τυχαία πιθανότητα.

Για το DES, ο υπολογισμός των πιθανοτήτων βασίζεται στα S-Boxes. Για κάθε S-Box κατασκευάζεται ένας πίνακας 64x16 με στοιχεία $N_i(a,b) = \#\left\{x \in Z_2^6 \mid S_i(x) \oplus S_i(x \oplus a) = b\right\}$. Η πιθανότητα υπολογίζεται ως $2^{-6} N_i(a,b)$. Η μέγιστη τιμή για το $N_i(a,b)$ είναι 16 και το καλύτερο

χαρακτηριστικό μονοπάτι ισχύει με πιθανότητα $\frac{1}{234}$. Μετά από 14 γύρους, έχουμε 2^{-55}. Η χρονική πολυπλοκότητα της επίθεσης είναι αντιστρόφως ανάλογη της πιθανότητας του χαρακτηριστικού μονοπατιού, άρα για το DES η διαφορική επίθεση θέλει χρόνο $O(2^{55})$ που είναι ανάλογο του χρόνου της εξαντλητικής μεθόδου.

2.6.3 Γραμμική Κρυπτανάλυση (Linear Cryptanalysis)

Η Γραμμική κρυπτανάλυση είναι μια επίθεση τύπου γνωστού απλού κειμένου (known plaintext attack) όπου ο αντίπαλος προσπαθεί να βρει πιθανές γραμμικές σχέσεις μεταξύ ενός υποσυνόλου από απλά κείμενα και ενός υποσυνόλου από state bits πριν εφαρμοστούν οι αντικαταστάσεις στο τελευταίο γύρο. Για τα μη-γραμμικά στοιχεία του κρυπτοσυστήματος, ο αντίπαλος βρίσκει προσεγγίσεις που είναι αληθείς με πιθανότητα $\frac{1}{2}+\varepsilon$.

Συνδυάζοντας τις προσεγγίσεις για κάθε στοιχείο του κρυπτοσυστήματος, βρίσκουμε προσεγγίσεις για ένα γύρο και συνδυάζοντας αυτές τελικά βρίσκουμε προσεγγίσεις για όλο το κρυπτοσύστημα. Σύμφωνα με το piling-up Lemma οι προσεγγίσεις αυτές θα ισχύουν με πιθανότητα $\frac{1}{2}+2^{n-1}\varepsilon_1\cdot\varepsilon_2\cdots\varepsilon_n$. Από όλες τις προσεγγίσεις τελικά παίρνουμε πληροφορία για ένα bit κλειδιού. Το συνολικό μέγεθος δεδομένων που χρειάζεται ο αντίπαλος είναι ανάλογο του $\frac{1}{\varepsilon^2}$.

Το DES, κυρίως λόγω των κριτηρίων που ικανοποιούν τα S-Boxes και η συνάρτηση αντιμετάθεσης P, είναι ανθεκτικό ενάντια στη Γραμμική Κρυπτανάλυση. Η καλύτερη επίθεση περιέχει 5 γραμμικές προσεγγίσεις και έχει συνολικό Bias 2^{-49}. Άρα το μέγεθος των δεδομένων που χρειάζεται η επίθεση είναι 2^{49} το οποίο θεωρείται ακατάλληλο στη πράξη για να υλοποιηθεί η επίθεση.

2.6.4 Η επίθεση του Davies (Davies' Attack)

Η επίθεση Davies είναι μια γνωστή plaintext επίθεση βασισμένη στη μη ομοιόμορφη κατανομή των αποτελεσμάτων δύο παρακείμενων S-box. Λειτουργεί συγκεντρώνοντας πολλά γνωστά ζευγάρια plaintext / ciphertext και υπολογίζοντας την εμπειρική κατανομή ορισμένων χαρακτηριστικών. Έχοντας στη διάθεση μας ικανοποιητικό αριθμό γνωστών plaintexts μπορούμε να βρούμε κάποια bits από το κλειδί έτσι ώστε τα υπόλοιπα να βρεθούν μέσω της επίθεσης ωμής βίας. Ο αριθμός των bits του κλειδιού που θα βρεθούν, ο αριθμός των απαιτούμενων plaintexts και η πιθανότητα επιτυχίας είναι όλα αλληλένδετα. Για παράδειγμα, μια επίθεση μπορεί να βρει 24 bits του κλειδιού

γνωρίζοντας 2^{52} plaintexts με 53% ποσοστό επιτυχίας. Η επίθεση δημιουργήθηκε αρχικά το 1987 από τον Donald Davies, ενώ το 1994, ο Eli Biham και ο Alex Biryukov έκαναν σημαντικές βελτιώσεις στην τεχνική.

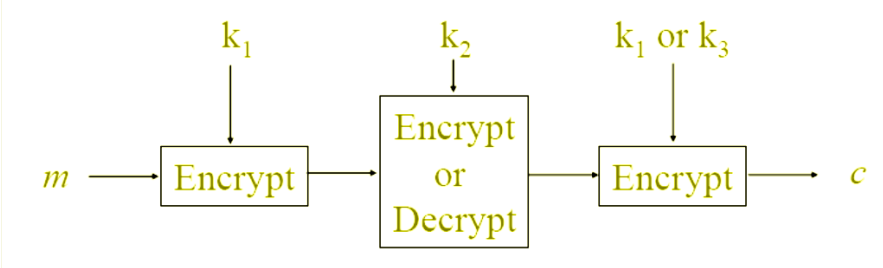
2.7 Triple-DES

Κυρίως εξαιτίας της επίθεσης ωμής βίας του 1999, το DES δεν θεωρείται πλέον ασφαλές και πολλοί ήταν αυτοί που προσπάθησαν να βρουν κάτι καινούργιο το οποίο θα ήταν ο αντικαταστάτης του DES σε εμπορικές εφαρμογές. Οι καλύτερες εναλλακτικές λύσεις είναι το Triple-DES (3DES) και το AES.

Το TDES ή TDEA ή συνηθέστερα 3DES προτάθηκε αρχικά από τον W. Tuchman και το 1985 προτυποποιήθηκε στο ANSI X9.17, ώστε να χρησιμοποιηθεί σε οικονομικές εφαρμογές. Το TDES ακολούθησε τον αλγόριθμο 2DES, ο οποίος δεν αξιοποιήθηκε ευρέως αφού θεωρήθηκε ευάλωτος στις κρυπταναλυτικές επιθέσεις τύπου ενδιάμεσου (man-in-the-middle attack). Το 1999, με τη δημοσίευση του ως FIPS PUB 46-3, το TDES ενσωματώθηκε ως τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES. Το FIPS 46-3 περιλαμβάνει τις ακόλουθες οδηγίες για το TDES:

- Το TDES αποτελεί τον εγκεκριμένο συμβατικό αλγόριθμο κρυπτογράφησης ως FIPS.
- Το DES, που χρησιμοποιεί μοναδικό κλειδί των 56-bit, επιτρέπεται στα συστήματα διαχείρισης δικτύων για επίτευξη συμβατότητας προς τα κάτω. Τα νέα συστήματα, όμως, πρέπει να υποστηρίζουν το TDES.
- Οι κυβερνητικές οργανώσεις των ΗΠΑ που χρησιμοποιούν DES ενθαρρύνονται για τη μετάβαση σε TDES.
- Είναι αναμενόμενο ότι το TDES και το Advanced Encryption Standard – AES θα συνυπάρξουν ως FIPS εγκεκριμένοι αλγόριθμοι, μέχρι την οριστική μετάβαση στο AES.

Το Triple-DES δεν είναι τίποτα άλλο παρά 3 συστήματα DES σε σειρά. Η έξοδος δηλαδή του πρώτου συστήματος είναι η είσοδος του δευτέρου του οποίου η έξοδος είναι η είσοδος του τρίτου. Προφανώς αποδίδει καλύτερη κρυπτογράφηση διότι πρέπει να υποκλαπούν 3 κλειδιά και όχι ένα. Είναι προφανές ότι είναι ένα κρυπτοσύστημα τύπου Feistel που χρησιμοποιεί μήκος block 64 bits, κλειδί μήκους 56 ή 112 ή 168 bits κι έχει 48 γύρους. Η κύρια δομή του φαίνεται στο σχήμα 2.10:



Σχήμα 2.10 Η δομή του Triple-DES

Υπάρχουν τρεις διαφορετικές εκδοχές αναλόγως με το τι επιλογή κλειδιού αποφασίζει να ακολουθήσει ο χρήστης. Στην πρώτη περίπτωση που είναι κι η πιο ασφαλής υπάρχουν τρία ανεξάρτητα κλειδιά και το συνολικό μήκος είναι 168 bits, δηλαδή 3 x 56. Στη δεύτερη περίπτωση υπάρχουν δύο ανεξάρτητα κλειδιά K_1 και K_2 ενώ ταυτόχρονα ισχύει $K_3=K_1$. Το συνολικό μήκος κλειδιού είναι 112 bits, δηλαδή 2 x 56. Τέλος, υπάρχει κι η τρίτη περίπτωση στην οποία και τα τρία κλειδιά είναι ίδια $K_1=K_2=K_3$. Το συνολικό μήκος είναι 56 bits, όσο δηλαδή και σε ένα κρυπτοσύστημα DES.Η επικρατέστερη εκδοχή είναι να γίνει αποκρυπτογράφηση στο δεύτερο βήμα και να χρησιμοποιηθούν 2 κλειδιά αντί για 3. Το κρυπτοσύστημα αυτό συμβολίζεται EDE_2 και είναι το πιο συχνά χρησιμοποιούμενο για δύο λόγους:

1. Το τρίτο κλειδί προσφέρει παραπάνω επίπεδο ασφάλειας αλλά και τα 2 κλειδιά με τα σημερινά δεδομένα είναι αρκετά ασφαλή.
2. Λόγω της αποκρυπτογράφησης στο δεύτερο βήμα, το Triple-DES είναι συμβατό με το DES άρα δεν χρειάζεται να αλλαχθεί το chip σε καμία από τις εφαρμογές που μέχρι τώρα χρησιμοποιούσαν το DES.

Ο TDES αποτελεί έναν εξαιρετικό αλγόριθμο, ο οποίος επειδή προέρχεται από τον DES παρουσιάζει την ίδια ρωμαλεότητα με αυτόν σε κρυπταναλυτικές επιθέσεις. Επιπλέον, με μήκος κλειδιού 168-bit οι επιθέσεις τύπου εξαντλητικής αναζήτησης είναι πρακτικά ατελέσφορες. Συνεπώς ο TDES αναμένεται ότι θα αξιοποιείται ολοένα και περισσότερο τα επόμενα χρόνια, μέχρι την ολοκληρωτική μετάβαση στις επερχόμενες υλοποιήσεις του AES.

2.8 Πρωτόκολλο Kerberos

Το πρωτόκολλο Kerberos είναι ένα πρωτόκολλο αυθεντικοποίησης σχεδιασμένο από τους Needham και Schroeder. Ξεκίνησε ως project στο Πανεπιστήμιο MIT της Μασαχουσέτης με το όνομα Athena και πλέον έχει γίνει πρότυπο RFC. Τα Requests for Comments (RFC) είναι μια σειρά κειμένων (εγγράφων) και σημειώσεων για την τεχνική και την οργάνωση που διέπουν το Internet. Τα επίσημα έγγραφα προδιαγραφών της ακολουθίας πρωτοκόλλου διαδικτύου που καθορίζονται από την Ομάδα Εργασίας Εφαρμοσμένης Μηχανικής διαδικτύου (Internet Engineering Task Force, IETF) και την Ομάδα Οδήγησης Εφαρμοσμένης Μηχανικής διαδικτύου (Internet Engineering Steering Group, IESG) καταγράφονται και δημοσιεύονται ως πρότυπα RFCs. Κατά συνέπεια, η διαδικασία δημοσιεύσεων RFC παίζει έναν σημαντικό ρόλο στη διαδικασία προτύπων διαδικτύου.

Στη συνέχεια θα παρουσιάσουμε το πρωτόκολλο Kerberos αλλά θα ξεκινήσουμε την περιγραφή μας από ένα πολύ βασικό στάδιο δίνοντας πληροφορίες για την υπηρεσία αυθεντικοποίησης και την σημαντικότητά της ως βασικό συστατικό στην προσφορά πιο σύνθετων υπηρεσιών ασφάλειας.

2.8.1 Βασικές Έννοιες και Ορισμοί

Ορισμός 2.2 Πρωτόκολλο είναι μια σειρά από κανόνες για ανταλλαγή μηνυμάτων μεταξύ δύο οντοτήτων μέσω ενός δικτύου.

Ορισμός 2.3 Όταν οι συμμετέχοντες δρουν ειλικρινά, τότε πετυχαίνουν το επιθυμητό σκοπό του πρωτοκόλλου (π.χ. η οντότητα Α αυθεντικοποιεί επιτυχώς την οντότητα Β). Το πρωτόκολλο αυτό ονομάζεται ασφαλές πρωτόκολλο όπου ο αντίπαλος (παθητικός ή ενεργός) δεν μπορεί να υπερνικήσει τον αντικειμενικό σκοπό.

Για τα παρακάτω, θα θεωρούμε ότι η Alice και ο Bob επιθυμούν να αυθεντικοποιήσουν ο ένας τον άλλο ή να μοιραστούν ένα κλειδί. Σε πιο περίπλοκα πρωτόκολλα, θα αναμειγνύεται και ο Trend, μια TTP (Trusted Third Party) που είναι έμπιστη οντότητα και από την Alice και από τον Bob. Ακόμα έχουμε και δύο ειδών αντιπάλους, την Eve η οποία μπορεί να κλέβει μηνύματα και την Mallory η οποία είναι ενεργός αντίπαλος που μπορεί να διαβάσει, να τροποποιήσει, να διαγράψει, να επαναλάβει και να προσθέσει μηνύματα σε ένα δίκτυο. Μπορεί ακόμα να αρχίσει ένα στιγμιότυπο ενός πρωτοκόλλου καθώς και να πάρει το ρόλο κάποιας άλλης οντότητας σε ένα στιγμιότυπο ενός πρωτοκόλλου αλλά δεν μπορεί για παράδειγμα να μαντέψει σωστά ένα τυχαίο αριθμό που έχει διαλέξει μια άλλη οντότητα ούτε να αντιστρέψει μια hash function.

Για να ανακεφαλαιώσουμε, στα παρακάτω θεωρούμε ότι η Alice, ο Bob και ο Trend είναι εφοδιασμένοι με ιδανικούς κρυπτογραφικούς μηχανισμούς (ψηφιακές υπογραφές, κρυπταλγορίθμους, hash functions, MACs) και επικοινωνούν μέσω ενός αναξιόπιστου δικτύου. Ο σκοπός είναι να χρησιμοποιήσουν αυτούς τους κρυπτογραφικούς μηχανισμούς ώστε να σχεδιάσουν ένα ασφαλές πρωτόκολλο (που προσφέρει δηλαδή υπηρεσίες ασφάλειας).

Πιο συγκεκριμένα, θα επικεντρωθούμε σε μια υπηρεσία ασφάλειας που ονομάζεται αυθεντικοποίηση. Η υπηρεσία αυτή χωρίζεται σε αυθεντικοποίηση οντότητας (entity authentication) και αυθεντικοποίηση προέλευσης των δεδομένων (data origin authentication). Η αυθεντικοποίηση οντότητας χωρίζεται περαιτέρω σε ετεροβαρής αυθεντικοποίηση (unilateral authentication) και αμφοτεροβαρής αυθεντικοποίηση (mutual authentication). Η αυθεντικοποίηση πετυχαίνεται με ανταλλαγή κρυπτογραφικών μηνυμάτων το οποίο ονομάζεται πρωτόκολλο αυθεντικοποίησης.

Ορισμός 2.4 Αυθεντικοποίηση οντότητας (entity authentication): η επιβεβαίωση ότι η οντότητα στο άλλο άκρο του καναλιού επικοινωνίας είναι αυτή που ισχυρίζεται ότι είναι σε μια συγκεκριμένη χρονική στιγμή (π.χ. σε ζωντανή επικοινωνία Voice over IP).

Ορισμός 2.5 Ετεροβαρής αυθεντικοποίηση (unilateral authentication): Αυθεντικοποίηση οντότητας η οποία προσφέρει σε μια οντότητα την επιβεβαίωση της ταυτότητας της άλλης αλλά όχι και αντίστροφα (π.χ. SSL).

Ορισμός 2.6 Αμφοτεροβαρής αυθεντικοποίηση (mutual authentication): Αυθεντικοποίηση οντότητας η οποία προσφέρει και στις δύο οντότητες την επιβεβαίωση της ταυτότητας της άλλης.

2.8.2 Παραδείγματα Πρωτοκόλλων Αυθεντικοποίησης

Υπάρχουν δύο βασικές κατηγορίες μηχανισμών που προσφέρουν αυθεντικοποίηση. Στη πρώτη κατηγορία είναι τα PIN και τα passwords τα οποία προσφέρουν ευπαθή αυθεντικοποίηση (weak authentication) και δεν είναι κατάλληλα για ανοικτά δίκτυα. Στην άλλη κατηγορία είναι τα πρωτόκολλα πρόκληση-απάντηση (Challenge-Response) όπου μια οντότητα αποδεικνύει την ταυτότητά της παρουσιάζοντας γνώση ενός μυστικού χωρίς όμως να αποκαλύπτει το μυστικό.

Στη συνέχεια παραθέτουμε ορισμένα παραδείγματα πρωτοκόλλων αυθεντικοποίησης και αναλύοντάς τα θα καταλάβουμε το λόγο ύπαρξης κάποιων στοιχείων στο πρωτόκολλο που μας ενδιαφέρει, το Kerberos.

Παράδειγμα 2.1 Ετεροβαρής Αυθεντικοποίηση με χρήση κρυπτογράφησης.

$$A \rightarrow B: \text{"Hi Bob I am Alice"}$$
$$B \rightarrow A: R \text{ (challenge)}$$
$$A \rightarrow B: \{R \| B\}_K \text{ (response)}$$

Σχήμα 2.11 Πρωτόκολλο ετεροβαρούς αυθεντικοποίησης με χρήση κρυπτογράφησης

Ανάλυση του Πρωτοκόλλου

Για το παραπάνω πρωτόκολλο υποθέτουμε ότι ο Bob και η Alice μοιράζονται ένα κοινό μυστικό κλειδί K . Στο βήμα 1 Η Alice αρχίζει την επικοινωνία στέλνοντας το μήνυμα "Hi Bob I am Alice". Στο βήμα 2, Ο Bob στέλνει στην Alice την πρόκληση R και στο βήμα 3 η Alice απαντάει στον Bob με το μήνυμα $\{R \| B\}_K$ το οποίο περιλαμβάνει το R, συνδεδεμένο με το id του Bob (B) και όλο αυτό κρυπτογραφημένο με το κοινό κλειδί K . Για την ασφάλεια του πρωτοκόλλου μπορούν να γίνουν οι εξής παρατηρήσεις:

- Η Eve βλέπει μόνο το R και το $\{R \| B\}_K$. Επειδή έχουμε τέλεια κρυπτογράφηση, δεν μπορεί να πάρει πληροφορία για το κλειδί K .
- Ο Bob παίρνει την πρόκλησή (challenge) του R πίσω, σαν απάντηση (response) που μόνο η Alice μπορεί να κατασκευάσει (λόγω του K).

Άρα είναι σίγουρος για την προέλευση (origin) και την ακεραιότητα (integrity) του μηνύματος.

- Αλλά η Mallory μπορεί εύκολα να υποδυθεί τον Bob. Επομένως η Alice δεν αυθεντικοποιεί τον Bob. Έχουμε δηλαδή ετεροβαρή αυθεντικοποίηση.

Επίσης, στο παραπάνω πρωτόκολλο αυθεντικοποίησης μπορεί να διεξαχθεί μια επίθεση (Replay Attack) αν η πρόκληση (challenge) R είναι "προβλέψιμη". Συγκεκριμένα, στο πρωτόκολλο του σχήματος 2.11 το R στο βήμα 5 είναι προβλέψιμο (αφού είναι το ίδιο) άρα η οντότητα M(A) μπορεί εύκολα να υποδυθεί την οντότητα A.

$$A \rightarrow M(B): \text{"Hi Bob I am Alice"}$$
$$M(B) \rightarrow A: R$$
$$A \rightarrow M(B): \{R \| B\}_K$$
$$M(A) \rightarrow B: \text{"Hi Bob I am Alice"}$$
$$B \rightarrow M(A): R$$
$$M(A) \rightarrow B: \{R \| B\}_K$$

Σχήμα 2.12 Replay Attack

Η παραπάνω επίθεση μας δείχνει ότι δεν αρκεί η επιβεβαίωση της προέλευσης (origin) και η επιβεβαίωση της ακεραιότητας (integrity) του μηνύματος. Τα πρωτόκολλα χρειάζεται να έχουν μηχανισμούς ελέγχου της φρεσκάδας (freshness) του μηνύματος και της ζωντάνιας (liveness) του συμμετέχοντα.

Ορισμός 2.7 Φρεσκάδα (freshness) ονομάζεται η σιγουριά ότι το μήνυμα δεν έχει χρησιμοποιηθεί νωρίτερα και ότι δημιουργήθηκε μέσα σε ένα αποδεκτό χρονικό περιθώριο (timeframe).

Ορισμός 2.8 Ζωντάνια (liveness) ονομάζεται η σιγουριά ότι το μήνυμα έχει σταλεί από ένα συμμετέχοντα μέσα σε ένα αποδεκτό χρονικό περιθώριο (timeframe).

Ο τρόπος για να παράγουμε φρεσκάδα (freshness) είναι η χρήση Nonce (Number Used Once) ή η χρήση Time Stamp. Το καθένα έχει πλεονεκτήματα και μειονεκτήματα και η επιλογή για το πιο θα χρησιμοποιηθεί, εξαρτάται από την εκάστοτε εφαρμογή.

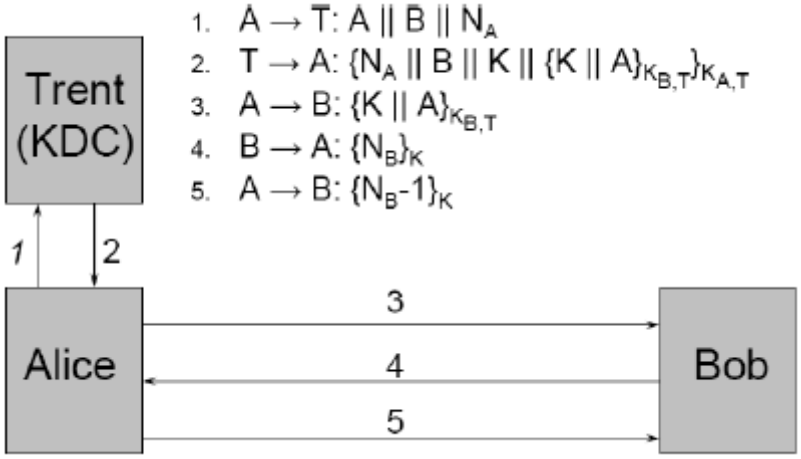
Παράδειγμα 2.2 Αμφοτεροβαρής αυθεντικοποίηση με χρήση ψηφιακών υπογραφών.

$$B \rightarrow A: R_B$$
$$A \rightarrow B: R_A, S_A\{R_A \| R_B \| B\}$$
$$B \rightarrow A: S_B\{R_B \| R_A \| A\}$$

Σχήμα 2.13 Πρωτόκολλο Αμφοτεροβαρούς αυθεντικοποίησης με χρήση ψηφιακών υπογραφών

Για το παραπάνω πρωτόκολλο υποθέτουμε ότι ο Bob έχει αυθεντικοποιημένη έκδοση του δημοσίου κλειδιού επαλήθευσης της Alice. Το πρωτόκολλο προσφέρει αυθεντικοποίηση και στις δύο οντότητες (Αμφοτεροβαρής αυθεντικοποίηση) λόγω των ψηφιακών υπογραφών (αφού πρώτα επαληθευτούν) και των Nonces R_A και R_B.

Η αυθεντικοποίηση οντότητας επιτυγχάνεται για μια συγκεκριμένη χρονική στιγμή ενώ στις περισσότερες εφαρμογές οι χρήστες επιθυμούν οι υπηρεσίες ασφάλειας (εμπιστευτικότητα, ακεραιότητα) να προσφέρονται για μια μεγαλύτερη χρονική περίοδο. Για το λόγο αυτό χρησιμοποιούνται authenticated session key establishment πρωτόκολλα στα οποία εκτός από αυθεντικοποίηση των οντοτήτων γίνεται και ανταλλαγή ενός session key. Το πιο γνωστό παράδειγμα τέτοιου είδους πρωτοκόλλου είναι το πρωτόκολλο Needham-Schroeder (σχήμα 2.14). Το πρωτόκολλο αυτό κάνει χρήση μιας TTP η οποία ονομάζεται Key Distribution Centre (KDC) και προσφέρει στους χρήστες αυθεντικοποίηση και ανταλλαγή του session key. Για τα παρακάτω υποθέτουμε ότι ο κάθε χρήστης μοιράζεται ένα long term key με το KDC. $K_{A,T}$ είναι το κλειδί που μοιράζεται το KDC με την Alice και
$K_{B,T}$ είναι το κλειδί που μοιράζεται το KDC με τον Bob.



Σχήμα 2.14 Το πρωτόκολλο Needham-Schroeder

Ανάλυση του πρωτοκόλλου

- Κατά την αποστολή των μηνυμάτων 1 και 2 υπάρχει επικοινωνία μεταξύ της Alice και του KDC. Ο KDC δίνει στην Alice το session key και αυθεντικοποιεί τον εαυτό του. Freshness έχουμε λόγω του Nonce N_A και Data origin authentication έχουμε λόγω του ότι το μήνυμα 2 είναι κρυπτογραφημένο με το κλειδί $K_{A,T}$. Άρα από τη σχέση (I) συνεπάγεται ότι έχουμε Liveness.
- Κατά την αποστολή των μηνυμάτων 3,4 και 5 υπάρχει επικοινωνία μεταξύ της Alice και του Bob. Στο μήνυμα 3, ο Bob μαθαίνει ότι η TTP πιστεύει ότι η Alice θέλει να επικοινωνήσει μαζί του με το κλειδί K. Τέλος, τα μηνύματα 4 και 5 αποτελούν ένα challenge-response πρωτόκολλο όπου η Alice θα αυθεντικοποιηθεί στον Bob.

Πλεονεκτήματα

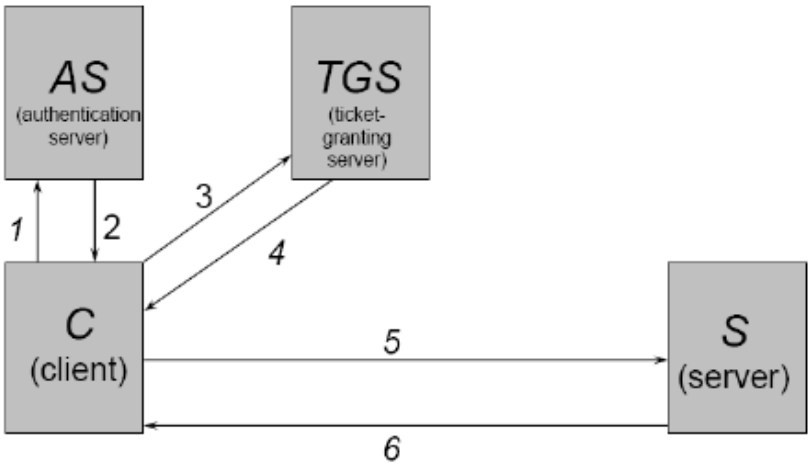
1. Λειτουργικότητα Αποθήκευσης Κλειδιού: Το KDC αποθηκεύει μόνο n κλειδιά.
2. Κάθε χρήστης αποθηκεύει ένα μόνο κλειδί (και όχι n-1).
3. Χρήση μόνο συμμετρικής κρυπτογραφίας (άρα μεγαλύτερη αποδοτικότητα.
4. Ο Bob μπορεί να είναι off-line στα βήματα 1 και 2 ενώ ο Trend μπορεί να είναι off-line στα βήματα 3,4 & 5.
5. Η Alice μπορεί να πάρει το κλειδί από τον Trend, να το αποθηκεύσει και να το χρησιμοποιήσει αργότερα με τον Bob.

Μειονεκτήματα

1. Το KDC είναι μοναδικό σημείο αποτυχίας από πλευράς ασφάλειας και διαθεσιμότητας.
2. Πιθανό υπολογιστικό και επικοινωνιακό "φρακάρισμα" στο KDC.
3. Απαίτηση για on-line έμπιστο server αφού η TTP γνωρίζει όλα τα κλειδιά (session και long term keys).
4. Αν κάποιος από τους χρήστες δεν διαχειριστεί καλά τα long term keys τότε καταρρέει η ασφάλεια όλου του πρωτοκόλλου αφού ο οποιοσδήποτε αντίπαλος μπορεί να υποδυθεί τον χρήστη.

2.8.3 Ανάλυση του Πρωτοκόλλου Kerberos

Το πρωτόκολλο Kerberos είναι ένα πρωτόκολλο αυθεντικοποίησης το οποίο κάνει χρήση δύο TTP ενώ data origin authentication προσφέρεται με χρήση κρυπτογράφησης συμμετρικού κλειδιού. Σχεδιάστηκε από τους Needham και Schroeder αν και την ίδια περίοδο ήταν project στο πανεπιστήμιο M.I.T. με το όνομα Athena. Έχει υλοποιηθεί σε software (Kerberos V5 Release 1.3.5) ενώ μια έκδοσή του χρησιμοποιείται στα Windows 2000 (κατά την secure attention sequence Ctrl+Alt+Del). Στη συνέχεια παραθέτουμε λεπτομερή περιγραφή του Kerberos.



Σχήμα 2.15 Το πρωτόκολλο Kerberos

Το Kerberos κάνει χρήση δύο TTPs, των Authentication Server (AS) και Ticket Granting Server (TGS). Ο Authentication Server (AS) προσφέρει αμφοτεροβαρή αυθεντικοποίηση (mutual authentication) με τον χρήστη, στο στάδιο που ο χρήστης κάνει login, βασιζόμενο σε long term keys (που υποθέτουμε εξ' αρχής ότι μοιράζεται με κάθε χρήστη) και σε δεύτερο στάδιο, εφοδιάζει το χρήστη με ένα ticket granting ticket και ένα short term key. Ο Ticket Granting Server (TGS) προσφέρει αυθεντικοποίηση (mutual authentication) με τον χρήστη βασιζόμενο στο short term key και στο ticket granting ticket και σε δεύτερη φάση εφοδιάζει το χρήστη με tickets τα οποία δίνουν πρόσβαση σε οποιουσδήποτε servers απαιτούν αυθεντικοποίηση από εκεί και πέρα.

Η ιδέα της χρήσης δύο TTPs είναι ότι ο χρήστης χρειάζεται να φορτώσει το long term key του για ελάχιστο χρόνο. Το κλειδί αυτό χρησιμοποιείται μόνο στο στάδιο του login για αμφοτεροβαρή αυθεντικοποίηση με τον AS. Αφού εφοδιαστεί με το short term key και το ticket granting ticket, ο χρήστης μπορεί πλέον να αφήσει το long term key του ανενεργό. Αυτό ελαχιστοποιεί το ρίσκο της έκθεσης του long term key στο αναξιόπιστο δίκτυο.

1. $C \rightarrow AS: C \| TGS \| from \| to \| N_C$
2. $AS \rightarrow C: C \| \{K_{C,TGS} \| C \| from \| to\}_{K_{AS,TGS}} \| \{K_{C,TGS} \| N_C \| from \| to \| TGS\}_{K_{AS,C}}$
3. $C \rightarrow TGS: S \| from \| to \| N'_C \| \{K_{C,TGS} \| C \| from \| to\}_{K_{AS,TGS}} \| \{C \| T_1\}_{K_{C,TGS}}$
4. $TGS \rightarrow C: C \| \{K_{C,S} \| C \| from \| to\}_{K_{TGS,S}} \| \{K_{C,S} \| N_C \| from \| to \| S\}_{K_{C,TGS}}$
5. $C \rightarrow S: \{K_{C,S} \| C \| from \| to\}_{K_{TGS,S}} \| \{C \| T_2\}_{K_{C,S}}$
6. $S \rightarrow C: \{T_2\}_{K_{C,S}}$

Σχήμα 2.16 Διάταξη και σχήμα των μηνυμάτων του Kerberos

Ανάλυση του Πρωτοκόλλου

Client↔AS. Κατά την ανταλλαγή των μηνυμάτων 1 και 2, ο χρήστης (Client) και ο AS χρησιμοποιούν το long term key $K_{AS,C}$ το οποίο προέρχεται από το password του χρήστη για να αυθεντικοποιήσουν ο ένας τον άλλο. Μετά και την λήψη του μηνύματος 2, ο χρήστης έχει εφοδιαστεί με το short term key $K_{C,TGS}$ και το ticket granting ticket:

$$\{K_{C,TGS} \| C \| from \| to\}_{K_{AS,TGS}}.$$

Αυτά επιτρέπουν στο χρήστη να μιλήσει στον TGS στο επόμενο βήμα. Μπορούμε να παρατηρήσουμε ότι το παραπάνω ticket περιέχει το short term key $K_{C,TGS}$ ενώ είναι κρυπτογραφημένο με το κλειδί $K_{AS,TGS}$ που μοιράζονται οι δύο servers. Με αυτό το τρόπο, ο TGS εφοδιάζεται με το short term key $K_{C,TGS}$ ενώ υπάρχει η βεβαιότητα ότι ο χρήστης δεν μπορεί να διαβάσει το περιεχόμενο του ticket granting ticket αφού δεν γνωρίζει το κλειδί $K_{AS,TGS}$. Τέλος, αξίζει να σημειωθεί ότι η χρονική διάρκεια του short term key $K_{C,TGS}$

είναι 10 ώρες. Μετά το πέρας των 10 ωρών, χρειάζεται ξανά αυθεντικοποίηση του χρήστη.

Client↔TGS. Κατά την ανταλλαγή των μηνυμάτων 3 και 4, ο χρήστης (Client) και ο TGS χρησιμοποιούν το short term key $K_{C,TGS}$ το οποίο και οι δύο εφοδιάστηκαν από τον AS για να αυθεντικοποιήσουν ο ένας τον άλλο. Πιο συγκεκριμένα, ο χρήστης στο μήνυμα 3 στέλνει αιτήματα για πρόσβαση στον server S μαζί με το ticket granting ticket και ένα μήνυμα για να αυθεντικοποιήσει τον εαυτό του στον TGS. Ο TGS ελέγχει την αξιοπιστία και τη διάρκεια ζωής του time stamp (για freshness) και στη συνέχεια υπολογίζει το δικό του αντίγραφο για το κλειδί $K_{C,TGS}$ (από το ticket granting ticket). Τώρα ο TGS μπορεί να αυθεντικοποιήσει τον χρήστη. Αν οι έλεγχοι αυτοί είναι εντάξει, ο TGS διανέμει στο χρήστη το session key $K_{C,S}$ και ένα ticket για να του δώσει πρόσβαση στον server S. Το ticket αυτό είναι κρυπτογραφημένο με το κλειδί $K_{TGS,S}$ που μοιράζονται ο TGS και ο S και είναι γνωστό μόνο σε αυτούς και έχει χρονική διάρκεια 5 λεπτά. Τέλος, ο TGS στέλνει και ένα μήνυμα για να αυθεντικοποιήσει τον εαυτό του στον χρήστη.

Client↔S. Κατά την ανταλλαγή των μηνυμάτων 5 και 6, ο χρήστης (Client) και ο S χρησιμοποιούν το short term key $K_{C,S}$ το οποίο και οι δύο εφοδιάστηκαν από τον TGS για να αυθεντικοποιήσουν ο ένας τον άλλο. Πιο συγκεκριμένα, ο χρήστης στο μήνυμα 5 στέλνει το ticket και ένα μήνυμα για να αυθεντικοποιήσει τον εαυτό του στον S. Ο S ελέγχει την αξιοπιστία και τη διάρκεια ζωής του time stamp (για freshness) και στη συνέχεια υπολογίζει το δικό του αντίγραφο για το κλειδί $K_{C,S}$ (από το ticket). Τώρα ο S μπορεί να αυθεντικοποιήσει τον χρήστη. Αν οι έλεγχοι αυτοί είναι εντάξει, τότε ο S παραχωρεί πρόσβαση στον χρήστη. Εναλλακτικά μπορεί να στείλει και το μήνυμα 6 για να αυθεντικοποιήσει τον εαυτό του στο χρήστη.

Το Kerberos χρησιμοποιεί συμμετρική κρυπτογραφία μέσω της οποίας γίνεται πιο λειτουργικό σε θέματα αποδοτικότητας. Συγκεκριμένα η Έκδοση 5 (όπως και αυτή που είναι στο πρότυπο RFC 1510) χρησιμοποιούν τον αλγόριθμο DES μαζί με μία hash function (MD4 ή MD5), ενώ το Release 1.2 του Kerberos V5 χρησιμοποιεί τον αλγόριθμο Triple-DES (3DES). Παρόλα αυτά υπάρχουν κάποια ζητήματα στις μέχρι τώρα εκδόσεις του πρωτοκόλλου. Αρχικά, λόγω της χρήσης time stamps (για την παραγωγή freshness), χρειάζονται συγχρονισμένα ρολόγια ανάμεσα σε όλους τους συμμετέχοντες, πράγμα το οποίο είναι δύσκολο στην υλοποίηση καθώς επίσης και αποθήκευση σε αρχεία των μέχρι τώρα ληφθέντων μηνυμάτων για την αποφυγή replay attacks (παράδειγμα 2.1) που αυξάνει την πολυπλοκότητα μνήμης. Ακόμα επειδή το long term key ανάμεσα σε χρήστη και AS στηρίζεται στην εισαγωγή του password του χρήστη, το σύστημα είναι ευπαθές σε επιθέσεις κατά των passwords (π.χ. guessing). Για το πρόβλημα αυτό διάφορες λύσεις έχουν προταθεί όπως αυτή της Microsoft για χρήση κρυπτογραφίας δημοσίου κλειδιού για την προστασία των μηνυμάτων μεταξύ χρήστη- AS που έχει υλοποιηθεί στο πρωτόκολλο SSL (Secure Sockets Layer).

Κεφάλαιο 3
Advanced Encryption Standard

3.1 Ιστορική Αναδρομή

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο το DES δεν θεωρούταν πλέον ασφαλές και έπρεπε να αντικατασταθεί άμεσα. Αν η ασφάλεια αποτελούσε το μοναδικό κριτήριο επιλογής του αλγορίθμου, τότε ο TDES θα ήταν μία εξαιρετικά κατάλληλη επιλογή για έναν τυποποιημένο αλγόριθμο κρυπτογράφησης για τα επόμενα χρόνια. Όμως, κύριο μειονέκτημα του TDES αποτελεί το γεγονός ότι ο αλγόριθμος είναι σχετικά αργός σε υλοποιήσεις με χρήση λογισμικού. Το σύστημα DES σχεδιάστηκε για υλοποίηση με χρήση υλικού τη δεκαετία του '70 και δε φαίνεται να παράγει αποδοτικό κώδικα λογισμικού. Ο TDES, που περιλαμβάνει τρεις φορές περισσότερους γύρους από τον DES, είναι προφανώς πολύ βραδύτερος. Επιπλέον μειονέκτημα αποτελεί η απαίτηση των DES και TDES για χρησιμοποίηση τμημάτων μεγέθους 64 bits. Για γενικότερους λόγους αποδοτικότητας και ασφάλειας, είναι επιθυμητό μεγαλύτερο μέγεθος τμήματος. Κατά συνέπεια ο TDES δε μπορεί να θεωρηθεί αποτελεσματικός προϊόντος του χρόνου.

Στις 02 Ιανουαρίου 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. Το αξιοσημείωτο είναι ότι για πρώτη φορά στα χρονικά της σύγχρονης κρυπτογραφίας οι διαδικασίες αξιολογήσεως και επιλογής των υποψηφίων προτάσεων θα ήταν ανοικτές.

Στις 12 Σεπτεμβρίου του 1997 δημοσιοποιήθηκαν η τελική προκήρυξη, καθώς και οι προδιαγραφές που έπρεπε να πληρεί ο AES. Οι βασικότερες εξ' αυτών ήταν:

1. Ο αλγόριθμος έπρεπε να είναι συμμετρικός, τμήματος (block cipher).
2. Η επιλογή του κρυπτοσυστήματος θα είναι μια ανοικτή διαδικασία και ο επιλεγόμενος αλγόριθμος και οι λεπτομέρειες σχεδιασμού του θα έπρεπε να δημοσιοποιηθούν.
3. Ο αλγόριθμος θα έπρεπε να χρησιμοποιεί blocks μήκους 128 bits και 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.

Τα κριτήρια συγκριτικής αξιολόγησης των υποψηφίων αλγορίθμων εντάχθηκαν σε τρεις κατηγορίες:

- **Στην ασφάλεια των αλγορίθμων:** τα κριτήρια που εντάσσονται σε αυτήν την κατηγορία περιλάμβαναν τη ρωμαλεότητα των αλγορίθμων σε κρυπταναλυτικές επιθέσεις, την ορθότητα του μαθηματικού τους φορμαλισμού, τη σχετική συγκριτική ασφάλεια του αλγορίθμου σε σχέση με τους υπόλοιπους υποψήφιους αλγορίθμους και την τυχαιότητα της συμπεριφοράς της εξόδου. Σε γενικές γραμμές οι αλγόριθμοι έπρεπε να έχουν χαρακτηριστικά ασφάλειας τουλάχιστον ισοδύναμα με του αλγορίθμου TDES, αλλά να χαρακτηρίζονται ταυτόχρονα από σημαντικά βελτιωμένη αποδοτικότητα.
- **Στο κόστος:** τα κριτήρια που εντάσσονταν σε αυτή την κατηγορία αναφέρονταν στις απαιτήσεις μνήμης και υπολογιστικής ισχύος του αλγορίθμου, καθώς και στις απαιτήσεις περί προστασίας δικαιωμάτων πνευματικής ιδιοκτησίας και πατέντες ώστε το υπό ανάπτυξη πρότυπο να μπορεί να είναι αξιοποιήσιμο σε διεθνή κλίμακα.
- **Στην απλότητα:** τα κριτήρια που εντάσσονταν σε αυτήν την κατηγορία περιλάμβαναν την απλότητα, την ευελιξία - δηλαδή τη δυνατότητα του αλγορίθμου να χειρίζεται μεγέθη μυστικών κλειδιών και τμημάτων μη κρυπτογραφημένου κειμένου μεγαλύτερα από τα ελάχιστα τεθέντα - τη δυνατότητα υλοποίησης σε διάφορα περιβάλλοντα όπως λογισμικό, υλικό, υλικολογισμικό (firmware), καθώς και την παροχή συμπληρωματικών κρυπτογραφικών λειτουργιών.

Κατετέθησαν 15 συνολικώς προτάσεις οι οποίες θα υπεβάλονταν σε δύο γύρους αξιολογήσεων. Στον πρώτο γύρο πραγματοποιήθηκαν δύο δημόσια συνέδρια, τον Αύγουστο του 1998 και τον Μάρτιο του 1999 και τον Αύγουστο του ίδιου έτους δημοσιεύτηκε η λίστα των 5 υποψήφιων κρυπτοσυστημάτων που προκρίθηκαν στο δεύτερο γύρο. Οι αλγόριθμοι αυτοί ήταν οι MARS, RC6, Rijndael, Serpent, Twofish, με ψήφους πρόκρισης που φαίνονται παρακάτω:

- **Rijndael:** 86 υπέρ, 10 κατά
- **Serpent:** 59 υπέρ, 7 κατά
- **Twofish:** 31 υπέρ, 21 κατά
- **RC6:** 23 υπέρ, 37 κατά
- **MARS:** 13 υπέρ, 84 κατά

Τον Απρίλιο του 2000 έγινε το καθοριστικό συνέδριο και τα αποτελέσματα από αυτό ανακοινώθηκαν επίσημα στις 2 Οκτωβρίου 2000 και σύμφωνα με τα οποία επελέγη ως AES ο αλγόριθμος Rijndael, ο οποίος είχε υποβληθεί από τους Βέλγους κρυπτογράφους Joan Daemen και Vincent Rijmen και έλαβε την οριστική του σχεδιαστική μορφή στο τέλος του καλοκαιριού του 2001. Οι τελικοί βαθμοί των πέντε επικρατέστερων κρυπτοσυστημάτων ήταν:

	MARS	RC6	Rijndael	Serpent	Twofish
General Security	3	2	2	3	3
Implementation of Security	1	1	3	3	2
Software Performance	2	2	3	1	1
Smart Card Performance	1	1	3	3	2
Hardware Performance	1	2	3	3	2
Design Features	2	1	2	1	3

Τέλος αξίζει να σημειωθεί ότι το Rijndael, στις 26 Νοεμβρίου του 2001 έγινε και πρότυπο FIPS (Federal Information Processing Standard) Standard (FIPS 197) που σημαίνει ότι το Rijndael είναι ένας αποδεκτός κρυπταλγόριθμος συμμετρικής κρυπτογραφίας ο οποίος μπορεί να χρησιμοποιηθεί από κυβερνητικούς οργανισμούς των Η.Π.Α. για να προστατεύει ευαίσθητες πληροφορίες.

Αναλυτικώς οι 15 προτάσεις για το πρότυπο AES παρουσιάζονται στον ακόλουθο πίνακα (με έντονα γράμματα οι 5 επικρατέστερες, που προέκυψαν μετά τον δεύτερο γύρο):

ΑΛΓΟΡΙΘΜΟΣ	ΔΗΜΙΟΥΡΓΟΣ	ΧΩΡΑ
CAST-256	Entrust	Καναδάς
Crypton	Future Systems	N. Κορέα
DEAL	Outerbridge, Knudsen *	ΗΠΑ, Δανία
DFC	ENS-CNRS *	Γαλλία
E2	NTT	Ιαπωνία
Frog	TecApro	Κροατία
HPC	Schroeppel *	ΗΠΑ
LOKI97	Brown et al. *	Αυστραλία
Magenta	Deutsche Telekom	Γερμανία
MARS	**IBM**	**ΗΠΑ**
RC6	**RSA Laboratories**	**ΗΠΑ**
Rijndael	**Daemen, Rijmen ***	**Βέλγιο**
SAFER+	Cylink	ΗΠΑ
Serpent	**Anderson, Biham, Knudsen ***	**Αγγλία, Ισραήλ, Δανία**
Twofish	**Counterpane**	**ΗΠΑ**

* Οι συγκεκριμένοι συμμετασχόντες στον διαγωνισμό δεν ήταν εταιρείες, αλλά ανεξάρτητοι ερευνητές.

Το πρότυπο AES περιγράφει μια συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε μπλοκ δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε μπλοκ

δεδομένων γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα plaintext μπλοκ και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το μπλοκ που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο μπλοκ (ciphertext). Το μπλοκ αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plaintext μπλοκ.

3.2 Μαθηματικό Υπόβαθρο

Όπως ήδη αναφέρθηκε, ο AES τροφοδοτείται με ακολουθίες από bits των 128 bits (μπλοκ) καθώς και από κλειδιά, που μπορεί να έχουν μέγεθος 128, 192 ή 256 bits. Τα κλειδιά αυτά ονομάζονται κλειδιά κρυπτογράφησης (cipher keys) για να διαχωριστούν από τα κλειδιά που παράγονται κατά την λειτουργία του αλγορίθμου.

Η βασική μονάδα επεξεργασίας στον AES είναι το byte. Έτσι τα bits ενός μπλοκ ή ενός κλειδιού χωρίζονται σε ομάδες των 8 για να σχηματιστούν τα bytes. Κάθε byte στον AES αντιστοιχεί σε ένα πολυώνυμο (αριθμητική πεπερασμένων σωμάτων - finite field arithmetic). Αν υποθέσουμε ότι τα bits που αποτελούν ένα byte είναι τα $\{b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0\}$, τότε το byte αυτό αναπαριστά το πολυώνυμο :

$$b_7x^7+ b_6x^6+ b_5x^5+ b_4x^4+ b_3x^3+ b_2x^2+ b_1x^1+ b_0=\sum_{i=0}^{7} b_ix^i.$$

Έτσι για παράδειγμα το byte {11001101} αντιστοιχεί στο πολυώνυμο $x^7+x^6+x^3+x^2+1$.

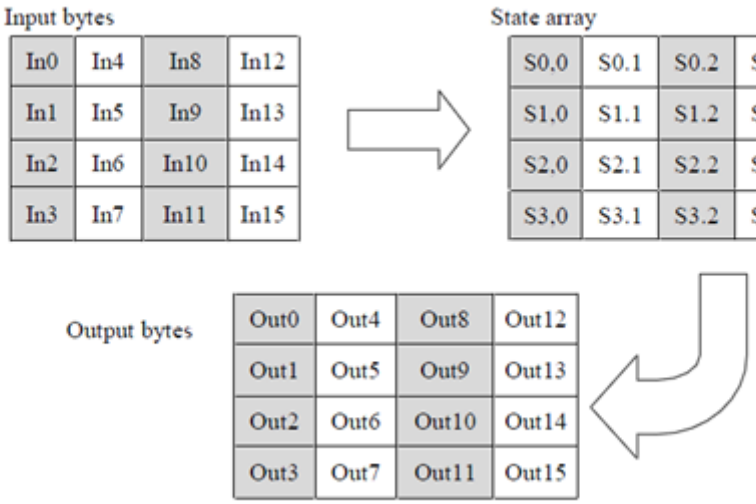
Κλείνοντας την αναφορά στις μονάδες των δεδομένων που διαχειρίζεται ο AES, πρέπει να αναφερθεί το πώς γίνεται η δεικτοδότηση των bits και των bytes στα μπλοκ και στα κλειδιά. Το Σχήμα 3.1 δείχνει την αντιστοιχία:

Input bit sequence	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	.....
Byte number	0								1								.....
Bit numbers in byte	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	.....

Σχήμα 3.1 Δεικτοδότηση των bits και bytes

Όλη η επεξεργασία που εκτελεί ο αλγόριθμος γίνετε πάνω σε ένα δισδιάστατο πίνακα που αποκαλείται Κατάσταση (State). Ο πίνακας αυτός περιλαμβάνει τέσσερις γραμμές από bytes, με κάθε μία γραμμή να αποτελείται από Nb bytes. Εφόσον στον AES υποστηρίζονται μπλοκ μεγέθους μόνο 128 bits, το Nb θα έχει τιμή 4. Το μπλοκ εισόδου περιλαμβάνει 16 bytes, τα οποία δεικτοδοτούνται in_0 έως in_{15}. Το κρυπτογραφημένο μπλοκ εξόδου περιλαμβάνει επίσης 16 bytes που δεικτοδοτούνται ως out_0 έως out_{15}. Η State

χρησιμοποιεί την μεταβλητή s με δύο δείκτες που δηλώνουν την θέση κάθε byte στον πίνακα. Η πρώτη λοιπόν και τελευταία λειτουργία που μπορεί να υποτεθεί ότι γίνεται στον AES είναι να αντιστοιχηθούν τα bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο. Το Σχήμα 3.2 δείχνει πώς γίνεται αυτό:



Σχήμα 3.2 Αντιστοίχηση των bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο

Η αντιστοίχηση που περιγράφηκε παραπάνω μπορεί να περιγραφεί μαθηματικά. Η αντιστοίχηση εισόδου στην State περιγράφεται από την σχέση:

$$s[r,c]=in[r+4c] \text{ για } 0\leq r<4 \text{ και } 0\leq c<Nb$$

ενώ η αντιγραφή της State στην έξοδο από την σχέση:

$$out[r+4c]=s[r,c] \text{ για } 0\leq r<4 \text{ και } 0\leq c<Nb$$

Ένας άλλος τρόπος να δει κάποιος τα περιεχόμενα της State είναι σαν 32-bit λέξεις (words) αντί για byte. Μια 32-bit word περιλαμβάνει τα 4 bytes μιας στήλης, οπότε τα 4 words που αποτελούν την State είναι τα ακόλουθα :

$$w_0=s_{0,0}s_{1,0}s_{2,0}s_{3,0}$$
$$w_1=s_{0,1}s_{1,1}s_{2,1}s_{3,1}$$
$$w_2=s_{0,2}s_{1,2}s_{2,2}s_{3,2}$$
$$w_3=s_{0,3}s_{1,3}s_{2,3}s_{3,3}$$

3.3 Ανάλυση Αλγορίθμου

Το πρότυπο AES είναι ένας επαναληπτικός αλγόριθμος και ένα από τα κυριότερα χαρακτηριστικά του είναι η απλότητα, που επιτυγχάνεται συνδυάζοντας με επαναλαμβανόμενο τρόπο αντικαταστάσεις (substitutions) και αναδιατάξεις (permutations) σε διαφορετικούς γύρους. 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. Το πραγματικό μέγεθος του κλειδιού εξαρτάται από το επιθυμητό επίπεδο ασφαλείας (security level). Ο αλγόριθμος AES-128 είναι ο επικρατέστερος και υποστηρίζεται από τις περισσότερες hardware υλοποιήσεις. 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.

	Μήκος κλειδιού (Nk)	Μηκός λέξεων (Nb)	Αριθμός γύρων (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Σχήμα 3.3 Αντιστοίχηση Nk-Nb-Nr για AES-128, AES-192 και AES-256

Να σημειωθεί ότι οι παραπάνω συνδυασμοί μήκους λέξεων, μήκους κλειδιού και γύρων επεξεργασίας είναι αυτοί που ορίζονται αυστηρά στο πρότυπο AES.

Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Οι κυκλικές συναρτήσεις του Rijndael αποτελούνται από τέσσερις τύπους μετασχηματισμών :

- Ένας μετασχηματισμός αντικατάστασης bytes χρησιμοποιώντας κάποιον σχετικό πίνακα Αντικατάστασης (SubByte).
- Ένας μηχανισμός ολίσθησης των bytes της State κατά διαφορετικά offsets (ShiftRow).
- Μια διαδικασία ανάμειξης των bytes της State (MixColumns).
- Μια πρόσθεση ενός κλειδιού στην State (AddRoundKey).

3.3.1 Αλγόριθμος Κρυπτογράφησης

Στην αρχή της διαδικασίας κρυπτογράφησης ένα μπλοκ εισόδου (plaintext) αντιγράφεται στην State. Μετά από έναν αρχικό γύρο πρόσθεσης κλειδιού, ακολουθούν 10, 12 ή 14 γύροι επεξεργασίας, με τον τελευταίο γύρο να διαφέρει από τους υπόλοιπους. Η τελική State αντιγράφεται στην έξοδο και η επεξεργασία για το συγκεκριμένο block ολοκληρώνεται (παραγωγή του ciphertext μπλοκ).

Το μυστικό κλειδί κρυπτογράφησης που χρησιμοποιείται σαν είσοδος στον αλγόριθμο είναι το κλειδί που προστίθεται στο μπλοκ εισόδου πριν αρχίσει η επεξεργασία. Σε καθέναν από τους γύρους επεξεργασίας, όπως αναφέρθηκε παραπάνω, υπάρχει μια φάση κατά την οποία προστίθεται στο μπλοκ και ένα κλειδί. Το κλειδί που προστίθεται στις περιπτώσεις αυτές, δεν είναι το αρχικό μυστικό κλειδί αλλά κάποιο που έχει προκύψει με μια συγκεκριμένη διαδικασία από το μυστικό κλειδί και είναι διαφορετικό για κάθε γύρο. Για τον λόγο αυτό, τα κλειδιά αυτά ονομάζονται round keys. Η διαδικασία με την οποία προκύπτουν τα round κλειδιά ονομάζεται Επέκταση Κλειδιού και θα αναλυθεί στη συνέχεια.

Αυτό που πρέπει να διευκρινιστεί είναι η έννοια της πρόσθεσης στον AES αλγόριθμο. Σε προηγούμενη ενότητα έχει αναφερθεί ότι 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 ενθυμηθεί ότι η XOR πράξη μεταξύ δύο bits (συμβολίζεται με $\oplus$) έχει τον εξής πίνακα αληθείας :

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0.$$

Αν κάθε βασικός μετασχηματισμός του AES αναπαρασταθεί από μια συνάρτηση που επενεργεί στην State, τότε ο αλγόριθμος κρυπτογράφησης μπορεί να περιγραφεί από τον παρακάτω ψευδοκώδικα:

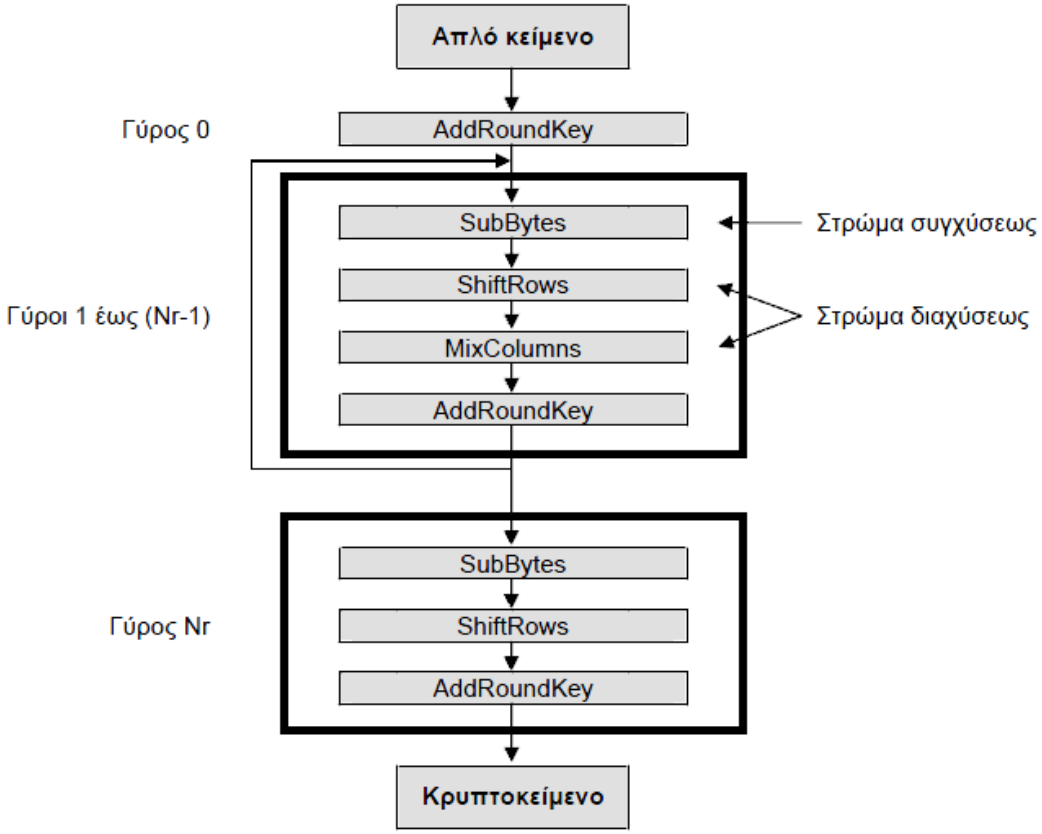
```
Cipher (byte in [4*Nb], byte out [4*Nb], byte key [4*Nb]
         word w [Nb*(Nr+1)])
begin
        byte state [4, Nb]
        state=in
        keyExpansion(key,w);
        AddRoundKey (state, w [0, Nb-1])
        for round=1 step 1 to Nr-1
                SubBytes (state)
                ShiftRows (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
```

Οι συναρτήσεις αυτές αναφέρονται ως SubBytes(), ShiftRows(), MixColumns() και AddRoundKey() και αντιστοιχούν (με αυτήν την σειρά) στους μετασχηματισμούς 1 έως 4 όπως αναφέρθηκαν παραπάνω. Να σημειωθεί ότι το array w χρησιμοποιείται για να δηλώσει την συλλογή των round keys που παράγονται από την διαδικασία επέκτασης κλειδιού.

Εξήγηση του ψευδοκώδικα για την διαδικασία κρυπτογράφησης. Όπως βλέπουμε παίρνει σαν είσοδο (in) το plaintext βγάζει σαν έξοδο (out) το cipher text και παίρνουμε και τον πινάκα W ο οποίος έχει δημιουργηθεί κατά την λειτουργία της συνάρτησης key expansion όπου εκεί έχει ανακατευτεί το κλειδί που έχουμε δώσει. Έτσι, στον γύρο 0 στο state όρισμα αντιγράφουμε το plaintext και στη συνέχεια καλούμε τη συνάρτηση AddRoundKey.

Μετά από το γύρο 1 έως τον Nr-1 (ανάλογα το bits αλγορίθμου που έχουμε επιλέξει για να δουλέψουμε 128,196,256) καλούμε με τη σειρά τις συναρτήσεις SubBytes, Shiftrows, MixColumns και AddRoundKey όπου εκεί θα ανακατευτεί διαδοχικά το state.

Στον τελευταίο γύρο το state θα ανακατευτεί με τις συναρτήσεις SubBytes, Shiftrows και AddRoundKey (δηλαδή όπως και στους προηγούμενους γύρους χωρίς όμως την MixColumns) όπου το τελικό αποτέλεσμα θα είναι το cipher text.



Σχήμα 3.4 Αλγόριθμος κρυπτογράφησης

3.3.1.1 Μετασχηματισμός SubBytes

Ο SubBytes μετασχηματισμός είναι ο μόνος μη γραμμικός μετασχηματισμός που εφαρμόζεται ανεξάρτητα σε κάθε byte του State χρησιμοποιώντας ένα look-up-table (LUT), το οποίο είναι ένας αντιστρέψιμος πίνακας 16x16 από bytes, και ονομάζεται S-box. Οι τιμές του πίνακα αυτού (που είναι αντιστρέψιμος) υπολογίζονται με την σύνθεση των δύο ακόλουθων μετασχηματισμών παίρνοντας τον πολλαπλασιαστικό αντίστροφο στο πεπερασμένο σώμα GF(2^8) με το στοιχείο {00} να αντιστοιχίζεται στον εαυτό του εφαρμόζοντας τον ακόλουθο μετασχηματισμό (στο GF(2)):

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

για $0 \le i < 8$, όπου b_i είναι το i-οστό bit του byte, και c_i είναι το i-οστό bit του byte c με την τιμή {63}, δηλαδή {01100011}. Ο πίνακας S-Box τυπικά δεν υπολογίζεται κατά την διαδικασία της κρυπτογράφησης, αλλά οι τιμές του έχουν προϋπολογιστεί. Στο Σχήμα 3.5 που ακολουθεί παρατίθενται οι τιμές του πίνακα S-Box όπως τις παρουσιάζει το NIST στο επίσημο έγγραφο για τον AES. Να σημειωθεί ότι ένας αριθμός στο δεκαεξαδικό σύστημα χρειάζεται 4 bits για να αναπαρασταθεί. Κατά συνέπεια, ένα byte αναπαρίσταται από 2 δεκαεξαδικά ψηφία χωρίζοντας το σε 2 ομάδες των 4 bits. Έτσι η γραμμή x του πίνακα αναφέρεται στα πρώτα 4 bits του byte και η στήλη y στα επόμενα 4.

X/Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	fb	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	fd	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	fd	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Σχήμα 3.5 Ο πίνακας αντικατάστασης S-Box

Εφόσον αναφέρθηκε ο θεωρητικός τρόπος με τον οποίο προκύπτει ο πίνακας S-Box, καλό θα ήταν να διευκρινιστεί τι σημαίνει πολλαπλασιασμός στο GF(2^8). Είναι ο πολλαπλασιασμός μεταξύ πολυωνύμων modulo ένα ανάγωγο πολυώνυμο βαθμού 8. Ανάγωγο (irreducible) ονομάζεται ένα πολυώνυμο αν

διαιρείται μονάχα από τον εαυτό του και την μονάδα. Το πολυώνυμο που έχει επιλεχθεί για το AES είναι το :

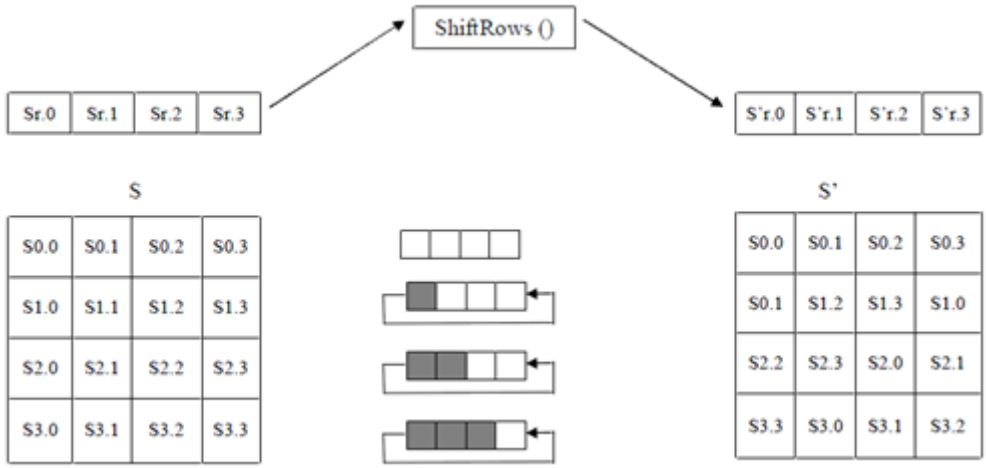
$$m(x)=x^8+ x^4+ x^3+ x+1$$

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 ●.

3.3.1.2 Μετασχηματισμός ShiftRows

Στον ShiftRows μετασχηματισμό, τα bytes στις τελευταίες τρείς γραμμές του State ολισθαίνουν κυκλικά για διαφορετικές τιμές bytes. Η πρώτη γραμμή δεν ολισθαίνει. Η δεύτερη γραμμή ολισθαίνει κυκλικά και αριστερόστροφα (left shifted) κατά ένα byte. Στην τρίτη γραμμή πραγματοποιείται ένα κυκλικό left shift κατά δύο bytes αυτή τη φορά. Τέλος, η τέταρτη γραμμή γίνεται κυκλικά left shifted κατά τρία byte.

Εφόσον οι μετασχηματισμοί MixColumns και AddRoundKey γίνονται στήλη παρά στήλη, ο ShiftRows διασφαλίζει ότι 4 bytes από μία στήλη διανέμονται σε τέσσερις διαφορετικές στήλες. Η επίδραση του ShiftRows μετασχηματισμού στον State array φαίνεται στο σχήμα 3.6:



Σχήμα 3.6 Ο μετασχηματισμός ShiftRows

3.3.1.3 Μετασχηματισμός MixColumns

Ο μετασχηματισμός αυτός εφαρμόζεται στις στήλες της State. Η κάθε στήλη θεωρείται σαν πολυώνυμο τρίτης τάξης με συντελεστές τις τιμές των bytes της στήλης:

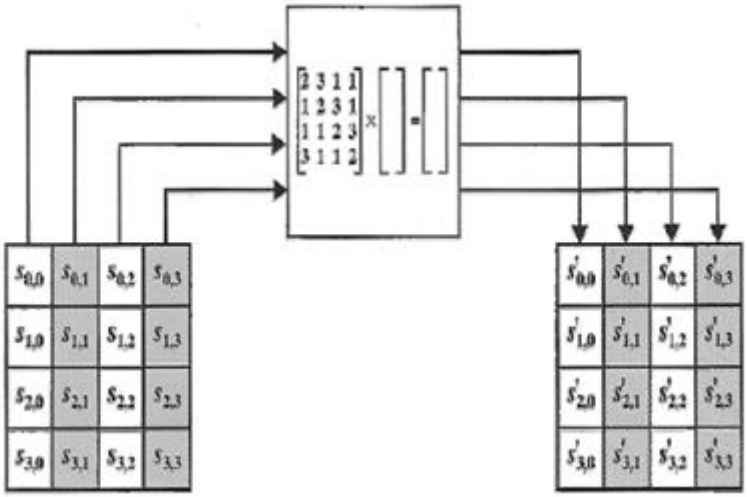
$$s(x)_i=s_{3,i}x^3+s_{2,i}x^2+s_{1,i}x+s_{0,i}$$

Τα πολυώνυμα πολλαπλασιάζονται modulo (x^4+1) με ένα καθορισμένο πολυώνυμο που δίνεται από την σχέση :

$$a(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$$

Η διαδικασία αυτή του υπολογισμού της αρχικής πράξης, $s'(x)=a(x)\otimes s(x)$, όπου με $\otimes$ συμβολίζεται ο modulo πολλαπλασιασμός, μετασχηματίζεται τελικά στις εξής σχέσεις :

$$s'_{0,c}=(\{02\}s_{0,c})\oplus(\{03\}s_{1,c})\oplus s_{2,c}\oplus s_{3,c}$$
$$s'_{1,c}=s_{0,c}\oplus(\{02\}s_{1,c})\oplus(\{03\}s_{2,c})\oplus s_{3,c}$$
$$s'_{2,c}=s_{0,c}\oplus s_{1,c}\oplus(\{02\}s_{2,c})\oplus(\{03\}s_{3,c})$$
$$s'_{3,c}=(\{03\}s_{0,c})\oplus s_{1,c}\oplus s_{2,c}\oplus(\{02\}s_{3,c}),$$
για $0\le c\le Nb$.



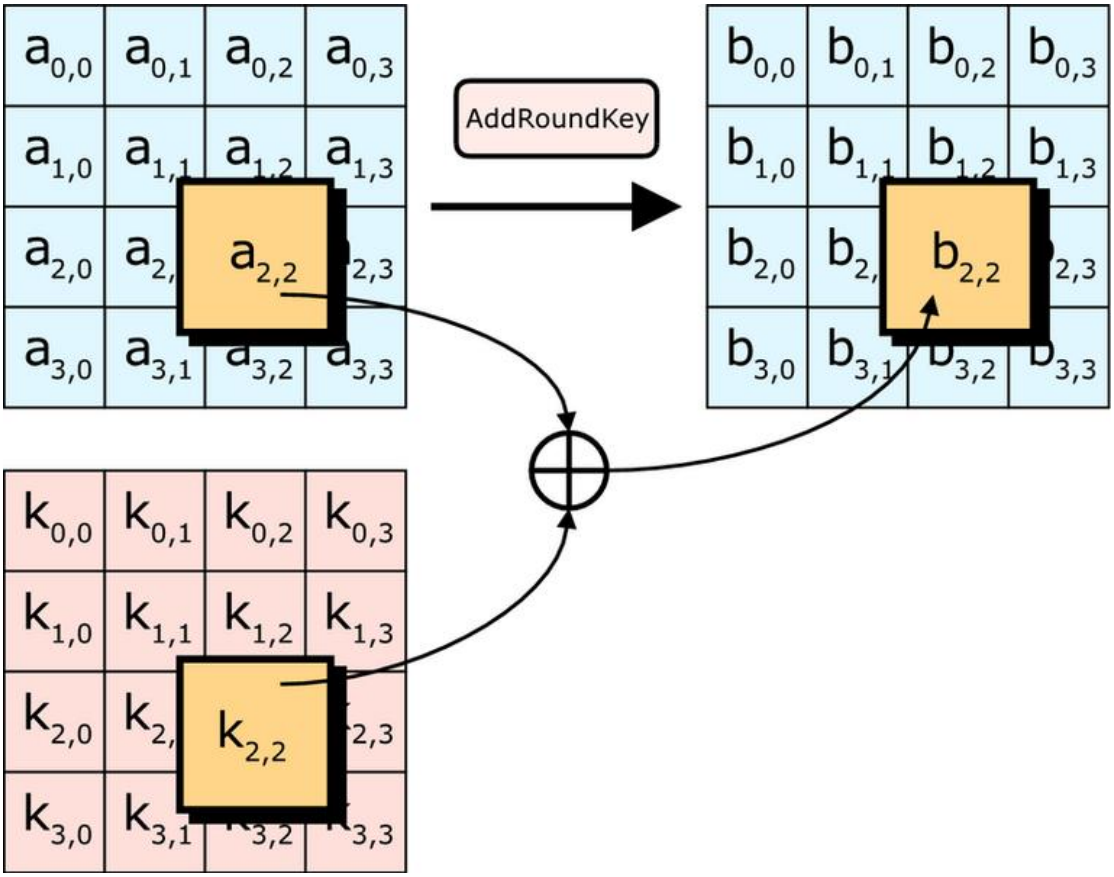
Σχήμα 3.7 Αριστερά παρατηρούμε την είσοδο της MixCollumn και δεξιά την έξοδο της

3.3.1.4 Μετασχηματισμός AddRoundKey

Ο AddRoundKey μετασχηματισμός είναι σχεδιασμένος σαν ένας stream cipher. Και τα 128 bits του State γίνονται XORed με τέσσερις 32-bit λέξεις του επεκταμένου κλειδιού. Η AddRoundKey είναι η μόνη λειτουργία που εμπλέκει τη χρήση του κλειδιού για να διασφαλίσει την προστασία των δεδομένων. Η πράξη θεωρείται σαν μία πράξη κατά στήλες (columnwise) μεταξύ των 4 byte μιας στήλης του State και μιας λέξης του round key.

Επειδή κάθε τιμή του round key 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:

$$[S'_{0,c}, S'_{1,c}, S'_{2,c}, S'_{3,c}]=[S_{0,c}, S_{1,c}, S_{2,c}, S_{3,c}]\oplus[W_{round*Nb+c}],$$
για $0\le c<Nb$.



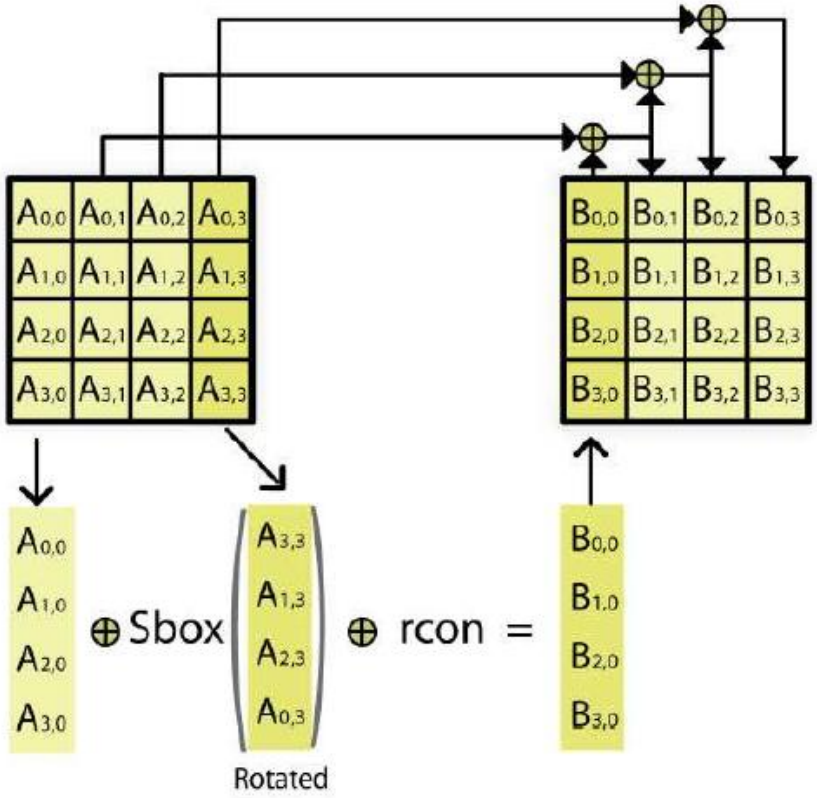
Σχήμα 3.8 Ο Μετασχηματισμός AddRoundKey

3.3.2. Ανάλυση επέκτασης Κλειδιού

Η διαδικασία επέκτασης του κλειδιού παίρνει το 128-bit κλειδί ως είσοδο και σε κάθε συνεδρία δίνει στην έξοδο ένα 44 32-bits word επεκταμένο κλειδί. Σε κάθε γύρο, ο AES cipher χρησιμοποιεί 4 από τις 44-word του επεκταμένου κλειδιού, στον AddRoundKey μετασχηματισμό.

Στο σχήμα 3.8 δείχνεται πώς γίνεται η επέκταση του κλειδιού. Οι 4 πρώτες words του πίνακα εξόδου, ο οποίος δείχνεται ως w, δεν είναι τίποτα άλλο από τα 16-byte (128 bits) εισόδου του κρυφού κλειδιού. Δηλαδή, το κλειδί αντιγράφεται στις τέσσερις πρώτες words του επεκταμένου κλειδιού.

Το υπόλοιπο επεκταμένο κλειδί γεμίζεται ανά τέσσερις λέξεις κάθε φορά. Η κάθε λέξη που προστίθεται w[i] εξαρτάται από την αμέσως προηγούμενη λέξη, w[i-1], και τη λέξη τέσσερις θέσεις πίσω, w[i-4]. Στις τρεις από τις τέσσερις περιπτώσεις, μια απλή XOR χρησιμοποιείται. Για μια λέξη της οποίας η θέση στο W array είναι πολλαπλάσιο του 4, μια πιο πολύπλοκη λειτουργία χρησιμοποιείται.



Σχήμα 3.9 Επέκταση κλειδιού

Στο σχήμα 3.9 απεικονίζεται η δημιουργία των πρώτων οκτώ λέξεων του επεκταμένου κλειδιού. Πιο συγκεκριμένα οι διεργασίες που εκτελούνται είναι οι ακόλουθες :

- **RotWord:** εκτελεί μία κυκλική αριστερόστροφη ολίσθηση κατά ένα byte σε μια λέξη. Αυτό σημαίνει ότι μια λέξη εισόδου [B_0, B_1, B_2, B_3] μετατρέπεται σε [B_1, B_2, B_3, B_0](εφαρμόζεται στην τελευταία στήλη του προηγούμενου round key).
- **SubWord:** εκτελεί μια αντικατάσταση (substitution) ενός byte, σε κάθε byte του μετατοπισμένου αποτελέσματος, κάνοντας χρήση των S-box. Μια λειτουργία παρόμοια με αυτήν που συναντήσαμε στον μετασχηματισμό SubBytes του AES cipher (εφαρμόζεται στην τελευταία στήλη του προηγούμενου round key).

Στο τελευταίο βήμα, το αποτέλεσμα των δύο παραπάνω ενεργειών, δηλαδή η αλλαγμένη word, γίνεται XORed με την σταθερά γύρου (round constant) RC[i] που είναι μια λέξη τις οποίας τα τρία δεξιότερα bytes είναι πάντα 0. Ο λόγος που χρησιμοποιούνται σταθερές γύρου είναι για να εξαλειφθούν οι συμμετρίες και ομοιότητες κατά την υλοποίηση του 4-word επεκταμένου κλειδιού κάθε γύρου. Έτσι, το αποτέλεσμα με XOR μιας λέξης με την RC είναι η πραγματοποίηση μίας λειτουργίας XOR για το αριστερό byte της λέξης. Οι σταθερές γύρου RC ορίζονται αναδρομικώς ως εξής:

$$RC(1)=x^0=01_{(16)}$$

$$RC(2)=x^{1}=02_{(16)}$$
Για i>2:
$$RC(i)=x^{i-1}=x\otimes RC(i-1)=02_{(16)}\otimes RC(i-1)$$

Λόγω του τρόπου χρήσεως των σταθερών γύρου στην επέκταση κλειδιού, είναι αδύνατον να χρειασθεί σταθερά RC(i) με i >10 . Οι δυνατές τιμές των σταθερών γύρου, επομένως, είναι οι:

i	$RC(i)$ [HEX]	$RC(i)$ [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

Πίνακας 3.10 Round Constant Bytes, RC σε δεκαεξαδική και δεκαδική μορφή

Στην επέκταση κλειδιού, οι σχέσεις μεταξύ των bytes k_i και W_i ορίζονται ευκολότερα, εάν θεωρήσουμε τα στοιχεία k(i, j) και W(i, j) που προκύπτουν από την διάταξη των αντιστοίχων bytes σε πίνακες 4×4 και 4×N_W. Ισχύουν τα εξής:

- Για $0\le j<N_k$ και $0\le i<4$
  $W(i, j)=k(i, j)$
- Για $N_k\le j<N_W$ με $j \bmod N_k=0$ και $i=0$
  $W(0, j)=W(0, j-N_k)\oplus S_{RD}(W(1, j-1))\oplus RC(j \text{ div } N_k)$
- Για $N_k\le j<N_W$ με $j \bmod N_k=0$ και $1\le i<4$
  $W(i, j)=W(i, j-N_k)\oplus S_{RD}(W((i+1) \bmod 4, j-1))$
- Για $N_k\le j<N_W$ και $0\le i<4$
  $W(i, j)=W(i, j-N_k)\oplus W(i, j-1)$

Στην περίπτωση που έχουμε $N_k=8$ ισχύει επιπλέον:

- Για $N_k\le j<N_W$ με $j \bmod N_k=4$ και $0\le i<4$
  $W(i, j)=W(i, j-N_k)\oplus S_{RD}(W(i, j-1))$

Σε κάποιες περιπτώσεις χρειάζεται τα κλειδιά γύρου να υπολογισθούν κατά φθίνουσα σειρά, αρχίζοντας από το κλειδί του τελικού γύρου. Η επέκταση κλειδιού στον AES έχει σχεδιασθεί κατά τέτοιον τρόπο, ώστε, με μία απλή τροποποίησή της, να είναι εφικτός ένας τέτοιος υπολογισμός. Η σχετική

διαδικασία ονομάζεται αντίστροφη επέκταση κλειδιού (inverse key expansion) και ορίζεται από τις ακόλουθες σχέσεις. Να σημειωθεί ότι με k(i, j) συμβολίζεται τώρα το κλειδί του τελικού γύρου.

- Για $0 \le j < N_k$ και $0 \le i < 4$
  $W(i, j) = k(i, j)$
- Για $N_k \le j < N_W$ με $j \bmod N_k = 0$ και $i = 0$
  $W(0, j) = W(0, j - N_k) \oplus S_{RD}(W(1, j-1) \oplus W(1, j-2)) \oplus RC((N_r + 1 - j) \text{div} N_k)$
- Για $N_k \le j < N_W$ με $j \bmod N_k = 0$ και $1 \le i < 4$
  $W(i, j) = W(i, j - N_k) \oplus S_{RD}(W((i+1) \bmod 4, j-1)) \oplus W((i+1) \bmod 4, j-2)$
- Για $N_k \le j < N_W$ και $0 \le i < 4$
  $W(i, j) = W(i, j - N_k) \oplus W(i, j - N_k - 1)$

Στην περίπτωση που έχουμε $N_k = 8$ ισχύει επιπλέον:

- Για $N_k \le j < N_W$ με $j \bmod N_k = 4$ και $0 \le i < 4$
  $W(i, j) = W(i, j - N_k) \oplus S_{RD}(W(i, j - N_k - 1))$

Παρακάτω παρατίθεται σε μορφή ψευδοκώδικα, η διαδικασία επέκτασης κλειδιού:

```
keyExpasion(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+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
```

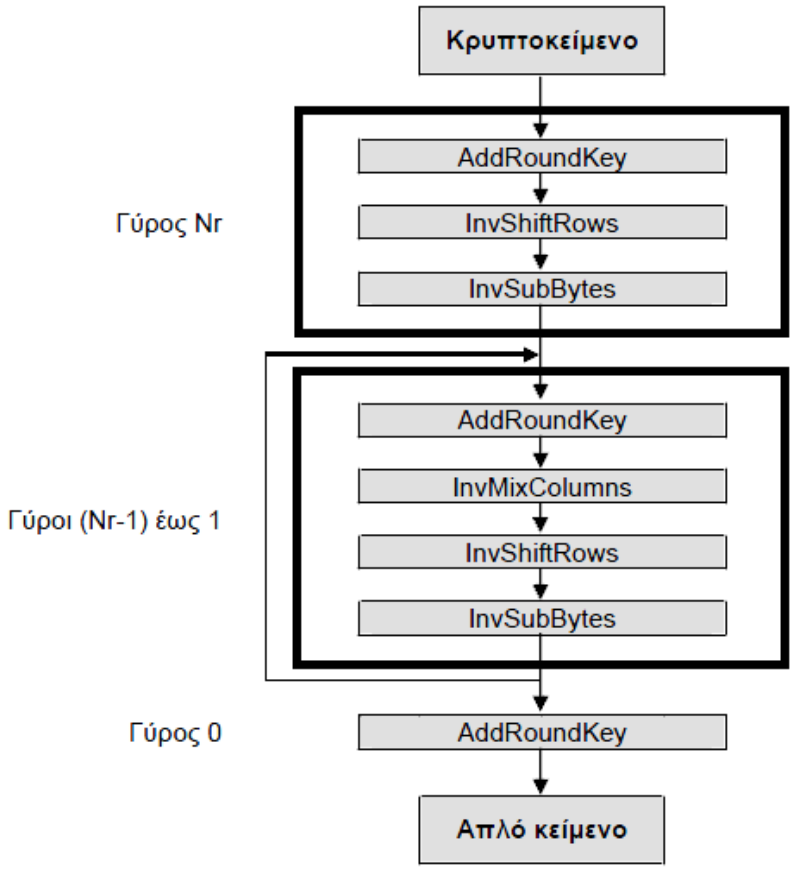
3.3.3 Αλγόριθμος Αποκρυπτογράφησης

Οι μετασχηματισμοί της διαδικασίας κρυπτογράφησης (όπως περιγράφηκαν στην προηγούμενη ενότητα) μπορούν να αντιστραφούν και να τοποθετηθούν σε αντίστροφη σειρά ώστε να παραχθεί μια διαδικασία που θα

αποκρυπτογραφεί ένα ciphertext του AES. Έτσι όπως και κατά την κρυπτογράφηση, υπάρχουν τέσσερις διακριτοί μετασχηματισμοί που επενεργούν πάνω στην State κατά την αποκρυπτογράφηση, οι InvShiftRows, InvSubBytes, InvMixColumns και AddRoundKey.

3.3.3.1 Αλγόριθμος ευθείας αποκρυπτογράφησης

Ο αλγόριθμος για την ευθεία αποκρυπτογράφηση (straightforward decryption) προκύπτει από την αναστροφή του αλγορίθμου κρυπτογραφήσεως και την αντικατάσταση των συναρτήσεών του από τις αντίστροφές τους. Η αρίθμηση των γύρων στην αποκρυπτογράφηση γίνεται αντιστρόφως (ακολουθώντας φθίνουσα πορεία), ώστε να ισχύει η αντιστοιχία με τα κλειδιά γύρου.

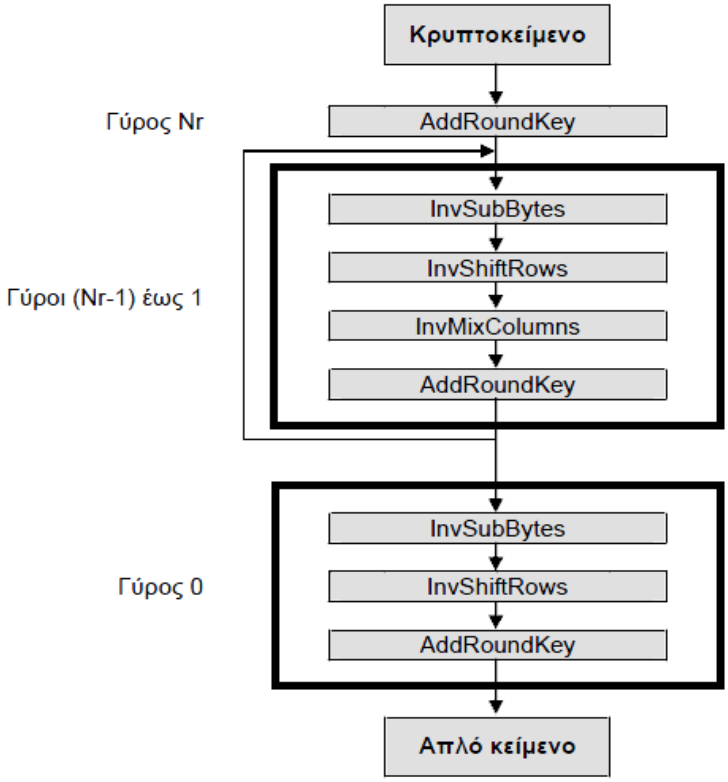


Σχήμα 3.11 Αλγόριθμος ευθείας αποκρυπτογράφησης

3.3.3.2 Αλγόριθμος ισοδύναμης αποκρυπτογράφησης

Η κατασκευή των συναρτήσεων του AES είναι τέτοια, που επιτρέπει τον ορισμό αλγορίθμου για ισοδύναμη αποκρυπτογράφηση (equivalent decryption). Αυτός ο αλγόριθμος έχει την δομή του αλγορίθμου κρυπτογραφήσεως. Διαφοροποιείται, ωστόσο στην χρήση των αντιστρόφων συναρτήσεων και στην αρίθμηση των γύρων, η οποία γίνεται αντιστρόφως, όπως και στην ευθεία αποκρυπτογράφηση. Διαφορετική είναι και η επέκταση

κλειδιού. Το επεκταμένο κλειδί στην περίπτωση αυτή προκύπτει από το κανονικό επεκταμένο κλειδί, αφού επενεργήσει στα κλειδιά των ενδιαμέσων γύρων (εκτός, δηλαδή, των γύρων 0 και N_r) η συνάρτηση InvMixColumns.



Σχήμα 3.12 Αλγόριθμος ισοδύναμης αποκρυπτογράφησης

Παρακάτω παρουσιάζεται ο ψευδοκώδικας που περιγράφει την διαδικασία ισοδύναμης αποκρυπτογράφησης. Να σημειωθεί ότι το array w που εμφανίζεται είναι το ίδιο ακριβώς array με τα κλειδιά (cipher και round) που χρησιμοποιήθηκε και κατά την κρυπτογράφηση. Η διαδικασία παραγωγής των κλειδιών είναι ταυτόσημη με αυτή που περιγράφηκε στην προηγούμενη ενότητα.

```
invCipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
        byte state[4,Nb]
        state=in
        AddRoundKey(state, w)
        for round=1 step 1 to Nr-1
                invSubBytes(state)
                invShiftRows(state)
                invMixColumns(state)
                AddRoundKey(state, w+round*Nb)
        end for
        invSubBytes(state)
        invShiftRows(state)
        invAddRoundKey(state, w+Nr*Nb)
end
```

3.3.3.3 Συναρτήσεις του Αλγορίθμου Αποκρυπτογράφησης

3.3.3.3.1 Μετασχηματισμός InvSubBytes

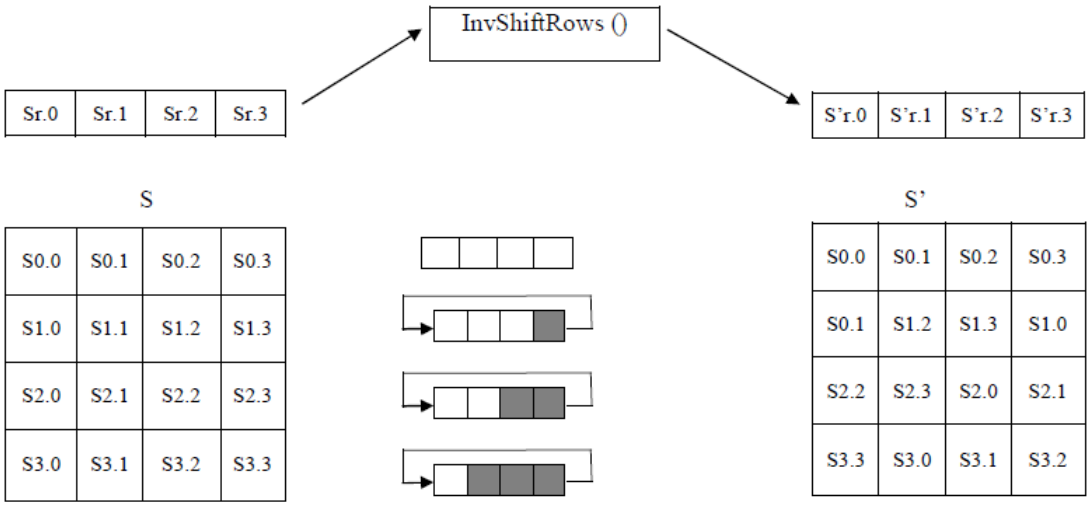
Ο μετασχηματισμός αυτός, όπως δηλώνει και το όνομα του, είναι ο αντίστροφος του μετασχηματισμού αντικατάστασης bytes της κρυπτογράφησης. Έτσι, στην περίπτωση αυτή, αντί για το S-Box πίνακα χρησιμοποιείται ο αντίστροφος του (inverse S-Box), ο οποίος και παρουσιάζεται στο Σχήμα 3.13:

X/Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	Ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	A0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Σχήμα 3.13 Ο πίνακας inverse S-Box

3.3.3.3.2 Μετασχηματισμός InvShiftRows

Ο μετασχηματισμός InvShiftRows είναι ο αντίστροφος του ShiftRows της διαδικασίας κρυπτογράφησης. Τα bytes στις τελευταίες τρεις γραμμές της State ολισθαίνουν κατά διαφορετικά offsets, με αντίθετη φορά από ότι στην ShiftRows διαδικασία. Στο Σχήμα 3.14 παρουσιάζεται ο ακριβής μηχανισμός:



Σχήμα 3.14 Ο μετασχηματισμός InvShiftRows

3.3.3.3.3 Μετασχηματισμός InvMixColumns

Είναι ο αντίστροφος του μετασχηματισμού MixColumns. Όπως και ο MixColumns εφαρμόζεται πάνω στις στήλες της State, θεωρώντας κάθε μία από αυτές ένα πολυώνυμο τεσσάρων όρων. Κάθε στήλη, θεωρείται πολυώνυμο του GF(2^8) και πολλαπλασιάζεται modulo x^4+1 με ένα καθορισμένο πολυώνυμο $a^{-1}(x)$:

$$a^{-1}(x)=\{0b\}+\{0d\}x^2+\{09\}x+\{0e\}.$$

Σαν αποτέλεσμα του παραπάνω πολλαπλασιασμού, τα 4 bytes σε μια στήλη αντικαθίστανται από τα ακόλουθα bytes :

$$s'_{0,c}=(\{0e\}s_{0,c})\oplus(\{0b\}s_{1,c})\oplus(\{0d\}s_{2,c})\oplus(\{09\}s_{3,c})$$
$$s'_{1,c}=(\{09\}s_{0,c})\oplus(\{0e\}s_{1,c})\oplus(\{0b\}s_{2,c})\oplus(\{0d\}s_{3,c})$$
$$s'_{2,c}=(\{0d\}s_{0,c})\oplus(\{09\}s_{1,c})\oplus(\{0e\}s_{2,c})\oplus(\{0b\}s_{3,c})$$
$$s'_{3,c}=(\{0b\}s_{0,c})\oplus(\{0d\}s_{1,c})\oplus(\{09\}s_{2,c})\oplus(\{0e\}s_{3,c})$$

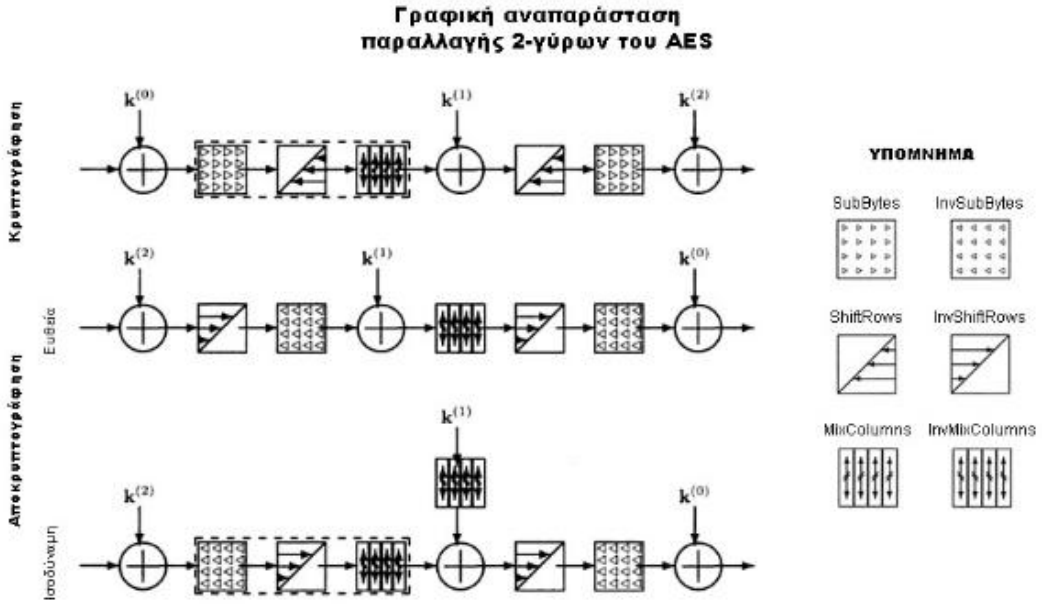
$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Σχήμα 3.15 Ο παραπάνω πίνακας απεικονίζει τον πολλαπλασιασμό τον bytes

3.3.3.3.4 Αντίστροφος Μετασχηματισμός AddRoundKey

Εφόσον ο μετασχηματισμός αυτός είναι μια απλή XOR πράξη, είναι από μόνος του αντιστρέψιμος και κατά συνέπεια είναι ταυτόσημος με τον μετασχηματισμό που περιγράφηκε στην ενότητα 3.3.1.4.

3.3.4 Συγκεντρωτικό διάγραμμα αλγορίθμων



3.4 Παρουσίαση διαδικασίας κρυπτογράφησης μέσω παραδείγματος

Με το πέρας της περιγραφής των συναρτήσεων του AES και των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης, κρίνεται σκόπιμο, για την εμπέδωση και καλύτερη κατανόηση των προηγουμένων, να γίνει αναλυτική παρουσίαση των δύο πρώτων γύρων της διαδικασίας κρυπτογράφησης (γύροι 0 και 1), βήμα προς βήμα, διά παραδείγματος (όλες οι τιμές του παραδείγματος είναι στο δεκαεξαδικό σύστημα αρίθμησης).

Έστω το απλό κείμενο

p = [32 43 F6 A8 88 5A 30 8D 31 31 98 A2 E0 37 07 34]

και το αρχικό κλειδί των 128 bits (N_k=4)

k = [2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C]

1. Μετατροπή των εισόδων (απλό κείμενο και αρχικό κλειδί) από διανύσματα σε πίνακες 4 γραμμών.

$$p=\begin{bmatrix} 32 & 88 & 31 & E0 \\ 43 & 5A & 31 & 37 \\ F6 & 30 & 98 & 07 \\ A8 & 8D & A2 & 34 \end{bmatrix} \qquad k=\begin{bmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{bmatrix}$$

2. Επέκταση κλειδιού

$$W = \left[\begin{array}{cccc|cccc|c} 2B & 28 & AB & 09 & A0 & 88 & 23 & 2A & \ldots \\ 7E & AE & F7 & CF & FA & 54 & A3 & 6C & \ldots \\ 15 & D2 & 15 & 4F & FE & 2C & 39 & 76 & \ldots \\ 16 & A6 & 88 & 3C & 17 & B1 & 39 & 05 & \ldots \end{array}\right]$$

Τα στοιχεία των πρώτων 4 στηλών του W είναι ίδια με αυτά των 4 πρώτων στηλών του k . Τα υπόλοιπα προκύπτουν αναδρομικώς, βάσει των σχέσεων της παραγράφου 3.3.2.

Ενδεικτικώς:

$W(0,4)=W(0,4-4)\oplus S_{RD}(W(1,4-1))\oplus RC(4div4)=$

$=W(0,0)\oplus S_{RD}(W(1,3))\oplus RC(1)=$

$=2B\oplus S_{RD}(CF)\oplus 01=$

$=2B\oplus 8A\oplus 01=$

$=A0$

$W(2,4)=W(2,4-4)\oplus S_{RD}(W((2+1)mod4,4-1))=$

$=W(2,0)\oplus S_{RD}(W(3,3))=$

$=15\oplus S_{RD}(3C)=$

$=15\oplus EB=$

$=FE$

$W(1,6)=W(1,6-4)\oplus W(1,6-1) =$

$=W(1,2)\oplus W(1,5) =$

$=F7\oplus 54 =$

$=A3$

3. Γύρος 0: Η Κατάσταση s προκύπτει από XOR μεταξύ του αρχικού κλειδιού και του απλού κειμένου:

$$s=\begin{bmatrix}32 & 88 & 31 & E0\\ 43 & 5A & 31 & 37\\ F6 & 30 & 98 & 07\\ A8 & 8D & A2 & 34\end{bmatrix}\oplus\begin{bmatrix}2B & 28 & AB & 09\\ 7E & AE & F7 & CF\\ 15 & D2 & 15 & 4F\\ 16 & A6 & 88 & 3C\end{bmatrix}=\begin{bmatrix}19 & A0 & 9A & E9\\ 3D & F4 & C6 & F8\\ E3 & E2 & 8D & 48\\ BE & 2B & 2A & 08\end{bmatrix}.$$

4. Η νέα Κατάσταση προκύπτει από εφαρμογή της συναρτήσεως SubBytes στην προηγούμενη Κατάσταση:

$$s=\begin{bmatrix}S_{RD}(19) & S_{RD}(A0) & S_{RD}(9A) & S_{RD}(E9)\\ S_{RD}(3D) & S_{RD}(F4) & S_{RD}(C6) & S_{RD}(F8)\\ S_{RD}(E3) & S_{RD}(E2) & S_{RD}(8D) & S_{RD}(48)\\ S_{RD}(BE) & S_{RD}(2B) & S_{RD}(2A) & S_{RD}(08)\end{bmatrix}=\begin{bmatrix}D4 & E0 & B8 & 1E\\ 27 & BF & B4 & 41\\ 11 & 98 & 5D & 52\\ AE & F1 & E5 & 30\end{bmatrix}.$$

5. Η νέα Κατάσταση προκύπτει από εφαρμογή της συναρτήσεως ShiftRows στην προηγούμενη Κατάσταση:

$$s=\begin{bmatrix}D4 & E0 & B8 & 1E\\ BF & B4 & 41 & 27\\ 5D & 52 & 11 & 98\\ 30 & AE & F1 & E5\end{bmatrix}.$$

6. Η νέα Κατάσταση προκύπτει από εφαρμογή της συναρτήσεως MixColumns στην προηγούμενη Κατάσταση:

$$s=\begin{bmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{bmatrix}\otimes\begin{bmatrix}D4 & E0 & B8 & 1E\\ BF & B4 & 41 & 27\\ 5D & 52 & 11 & 98\\ 30 & AE & F1 & E5\end{bmatrix}=\begin{bmatrix}04 & E0 & 48 & 28\\ 66 & CB & F8 & 06\\ 81 & 19 & D3 & 26\\ E5 & 9A & 7A & AC\end{bmatrix}$$

Ενδεικτικώς:

$$s(3,2)= 03\otimes B8\oplus 01\otimes 41\oplus 01\otimes 11\oplus 02\otimes F1=$$
$$=03\otimes B8\oplus 41\oplus 11\oplus 02\otimes F1.$$

Ο υπολογισμός της πράξεως ⊗ μεταξύ δύο bytes πραγματοποιείται κατά την μέθοδο που περιγράφεται στο Παράρτημα Α. Κατά συνέπεια, τα αποτελέσματα 03⊗B8 και 02⊗F1 προκύπτουν ως εξής:

$$03\otimes B8=03\exp[(\log_{03}03+ \log_{03}B8)\text{mod}FF]=$$

$$=03\exp[(01+3B)\text{mod}FF]=$$

$$=03\exp(3C\text{mod}FF)=03\exp 3C=D3$$

$$02\otimes F1=03\exp[(\log_{03}02+ \log_{03}F1)\text{mod}FF]=$$

=03exp[(19+4A)modFF]=

=03exp(63modFF)=03exp63=F9.

Τελικώς: s(3,2)=D3⊕41⊕11⊕F9=7A.

7. Η νέα Κατάσταση προκύπτει από XOR μεταξύ της προηγουμένης Καταστάσεως και του κλειδιού γύρου:

$$S=\begin{bmatrix} 04 & E0 & 48 & 28 \\ 66 & CB & F8 & 06 \\ 81 & 19 & D3 & 26 \\ E5 & 9A & 7A & AC \end{bmatrix} \oplus \begin{bmatrix} A0 & 88 & 23 & 2A \\ FA & 54 & A3 & 6C \\ FE & 2C & 39 & 76 \\ 17 & B1 & 39 & 05 \end{bmatrix} = \begin{bmatrix} A4 & 68 & 6B & 02 \\ 9C & 9F & 5B & 6A \\ 7F & 35 & EA & 50 \\ F2 & 2B & 43 & 49 \end{bmatrix}.$$

Τα βήματα 4 έως 7 απαρτίζουν την δομή όλων των ενδιαμέσων γύρων και στο συγκεκριμένο παράδειγμα επαναλαμβάνονται άλλες 8 φορές. Ο $10^{ος}$ και τελικός γύρος του παραδείγματος περιλαμβάνει τα βήματα 4,5 και 7. Μετά το πέρας του τελικού γύρου η Κατάσταση μετατρέπεται από πίνακα 4x4 σε διάνυσμα 16 bytes και αποτελεί, πλέον, το κρυπτοκείμενο.

3.5 Ζητήματα ασφαλείας και κρυπτανάλυσης

3.5.1 Κριτήρια ασφαλείας

Θεωρούμε την είσοδο, μήκους l_b bits, σε έναν κρυπταλγόριθμο τμήματος που χρησιμοποιεί κλειδί μήκους l_k bits. Για δεδομένα l_b και l_k ορίζεται το σύνολο C, που περιέχει όλους τους δυνατούς κρυπταλγορίθμους. Η είσοδος του κρυπταλγορίθμου έχει 2^{l_b} πιθανές τιμές. Στο σύνολο των 2^{l_b} πιθανών εισόδων ορίζονται $M_b=(2^{l_b})!$ μεταθέσεις. Το κλειδί, με την σειρά του, ορίζει $M_k=(2^{l_k})$ πιθανές μεταθέσεις. Συνδυάζοντας τα προηγούμενα, καταλήγουμε ότι το πλήθος N των στοιχείων του συνόλου C είναι:

$$N=M_b^{M_k}.$$

Οι N διαφορετικοί κρυπταλγόριθμοι διαχωρίζονται, βάσει του παρεχομένου επιπέδου ασφαλείας, στα εξής δύο υποσύνολα:

1. Το υποσύνολο C_S των θεωρουμένων ασφαλών κρυπταλγορίθμων, με πλήθος N_S στοιχεία.

2. Το υποσύνολο C_W των κρυπταλγορίθμων με εκμεταλλεύσιμες αδυναμίες (ή άλλως "τρύπες" ασφαλείας), με πλήθος N_W στοιχεία.

Για τιμές των l_b και l_k που χρησιμοποιούνται στην πράξη (π.χ. μεγαλύτερες του 40), ισχύει $N_W << N_S$.

Για την διακρίβωση του επιπέδου ασφαλείας που προσφέρει ένας κρυπταλγόριθμος τμήματος, υπάρχουν δύο βασικά κριτήρια ελέγχου: η K-ασφάλεια (K-security) και η έννοια του ερμητικού (hermetic) κρυπταλγορίθμου.

Ένας κρυπταλγόριθμος τμήματος είναι K-ασφαλής (K-secure), εάν όλες οι πιθανές τακτικές κρυπταναλυτικών επιθέσεων για αυτόν έχουν τον ίδιο παράγοντα επιτυχίας και τις ίδιες απαιτήσεις αποθηκευτικού χώρου και για τους κρυπταλγορίθμους ιδίων διαστάσεων του υποσυνόλου C_S.

Το κριτήριο της K-ασφαλείας είναι μία πολύ ισχυρή αντίληψη για την ασφάλεια. Παύει να υφίσταται εάν σε έναν κρυπταλγόριθμο ισχύει μία τουλάχιστον εκ των κατωτέρω προϋποθέσεων:

- Ύπαρξη μεθόδων κρυπτανάλυσης ταχυτέρων από την εξαντλητική αναζήτηση (shortcut attacks).
- Ύπαρξη συμμετρίας στην απεικόνιση του απλού κειμένου σε κρυπτοκείμενο.
- Ύπαρξη μη αμελητέας ποσότητος αδυνάμων κλειδιών (αδύναμα κλειδιά υπάρχουν στους κρυπταλγορίθμους DES και IDEA).
- Ο κρυπταλγόριθμος είναι ευάλωτος σε επίθεση σχετιζομένων κλειδιών (related key attack). Τα σχετιζόμενα κλειδιά είναι κλειδιά που διατηρούν σημαντικό μέρος τους αμετάβλητο.

Η K-ασφάλεια είναι σχετική έννοια. Επί παραδείγματι, ένας κρυπταλγόριθμος τμήματος των 8 bits με μήκος κλειδιού 8 bits, επίσης, είναι δυνατόν να πληροί το κριτήριο της K-ασφαλείας, αλλά παραμένει ευάλωτος εξ αιτίας του μικρού μήκους κλειδιού.

Παρά ταύτα, είναι πιθανόν υπό ορισμένες προϋποθέσεις και για μεγαλύτερα μήκη τμήματος κειμένου και κλειδιού να υπάρξουν ευάλωτοι K-ασφαλείς κρυπταλγόριθμοι. Για τον λόγο αυτό έχει εισαχθεί η έννοια του ερμητικού κρυπταλγορίθμου, που συμπληρώνει την έννοια της K-ασφαλείας.

Ένας κρυπταλγόριθμος τμήματος είναι ερμητικός (hermetic) εάν δεν έχει αδυναμίες που δεν εμφανίζονται στο υποσύνολο C_S, για τις ίδιες διαστάσεις.

Σχεδιαστικός στόχος του AES είναι να είναι K-ασφαλής και ερμητικός για κάθε τιμή του μήκους κλειδιού, εξ αυτών που υποστηρίζει. Εάν κάποια μελλοντική κρυπταναλυτική επίθεση δεν καταρρίψει αυτόν τον στόχο, τότε ο AES θα θεωρείται πως είναι όσο ασφαλής μπορεί να είναι ένας κρυπταλγόριθμος με τις ίδιες διαστάσεις, έναντι οποιασδήποτε επίθεσης.

3.5.2 Αντοχή του AES σε γραμμική και διαφορική κρυπτανάλυση

Δύο μέθοδοι που χρησιμοποιούνται ευρέως για κρυπταναλυτικές επιθέσεις σε κρυπταλγορίθμους τμήματος είναι η διαφορική και η γραμμική κρυπτανάλυση. Και οι δύο αυτές μέθοδοι ανήκουν στην κατηγορία των επιθέσεων με επιλεγμένο απλό κείμενο.

Η μέθοδος γραμμικής κρυπτανάλυσης υπήρξε επινόηση του Mitsuru Matsui και επεδείχθη για πρώτη φορά το 1992. Βρίσκει εφαρμογή κυρίως σε κρυπταλγορίθμους γινομένου. Προσπάθεια της μεθόδου αυτής είναι να ανακαλύψει γραμμικές προσεγγίσεις της σχέσεως μεταξύ μέρους (ή του συνόλου) των bits του απλού κειμένου, του κλειδιού και του κρυπτοκειμένου. Οι γραμμικές σχέσεις που προκύπτουν ισχύουν με κάποια πιθανότητα Pε[0,1]. Ορίζεται, ακόμη, ως πόλωση, η ποσότητα

$$\varepsilon=P-\frac{1}{2}.$$

Εάν $\varepsilon=0\Leftrightarrow P=\frac{1}{2}$, τότε η γραμμική κρυπτανάλυση είναι ατελέσφορη. Αντιθέτως, για να είναι ένα κρυπτοσύστημα ευάλωτο στην γραμμική κρυπτανάλυση, πρέπει να υπάρχουν για αυτό γραμμικές προσεγγίσεις με $\varepsilon\neq0$. Όσο περισσότερες τέτοιες προσεγγίσεις προκύψουν και όσο μεγαλύτερη είναι σε αυτές η ποσότητα $|\varepsilon|$, τόσο πιο ευάλωτο θεωρείται το κρυπτοσύστημα.

Επειδή ο μόνος μη γραμμικός μετασχηματισμός στην συμμετρική κρυπτογραφία είναι τα S-κουτιά, η γραμμική κρυπτανάλυση στοχεύει στην όσο γίνεται ακριβέστερη "γραμμικοποίησή" τους. Επομένως, η αντοχή ενός κρυπταλγορίθμου σε επιθέσεις γραμμικής κρυπτανάλυσης εξαρτάται από την δομή των S-κουτιών του.

Αξίζει να αναφερθεί, επίσης, πως μεγαλύτερη πιθανότητα ευρέσεως αποτελεσματικών γραμμικών σχέσεων υπάρχει για τα κλειδιά των τελευταίων γύρων (κυρίως του τελευταίου).

Η μέθοδος διαφορικής κρυπτανάλυσης υπήρξε δημιούργημα των Eli Biham και Adi Shamir, στα τέλη της δεκαετίας του 1980. Είναι παρόμοια με την γραμμική κρυπτανάλυση. Αντί, όμως, να προσπαθεί να δημιουργήσει γραμμικές σχέσεις, εξετάζει την συχνότητα εμφανίσεως διαφοράς δύο κρυπτοκειμένων για δεδομένη διαφορά δύο απλών κειμένων. Η διαφορά Δx δύο κρυπτοκειμένων ή δύο απλών κειμένων x και x′ ορίζεται από μία συνάρτηση διαφοράς h(x, x′), η οποία είναι σχεδόν πάντοτε η πράξη XOR. Συνήθως, δηλαδή, $\Delta x=x\oplus x'$.

Ένα κρυπτοσύστημα με μήκος τμήματος l_b θα έχει 2^{l_b} πιθανές τιμές κρυπτοκειμένου, άρα και ισάριθμες πιθανές τιμές διαφορών κρυπτοκειμένου (έξοδος). Εάν η πιθανότητα εμφανίσεως μίας εξόδου είναι 2^{-l_b}, για κάθε έξοδο (ομοιόμορφη κατανομή), τότε η διαφορική κρυπτανάλυση δεν μπορεί να έχει

αποτέλεσμα στο συγκεκριμένο κρυπτοσύστημα. Ένα κρυπτοσύστημα θα είναι ευάλωτο στην διαφορική κρυπτανάλυση εάν οι διαφορές του κρυπτοκειμένου δεν ακολουθούν ομοιόμορφη κατανομή, αλλά υπάρχουν κάποιες τιμές με μηδενική πιθανότητα εμφανίσεως και κάποιες με πιθανότητα πολλαπλάσια του 2^{-l_b}. Όσο πιο πολύ πλησιάζει η κατανομή των διαφορών την ομοιόμορφη, τόσο ασφαλέστερο είναι το κρυπτοσύστημα σε αυτό το είδος επίθεσης.

Όσον αφορά στον AES, έχει θεωρητικώς αποδειχθεί ότι ακόμη και μία παραλλαγή του AES με 4 μόλις γύρους είναι ασφαλής έναντι επιθέσεων γραμμικής ή διαφορικής κρυπτανάλυσης. Αυτό σημαίνει ότι η δομή του AES δεν έχει τρωτά σημεία που να μπορούν να εκμεταλλευθούν οι δύο αυτές μέθοδοι.

3.5.3 Αντοχή του AES σε άλλα είδη επιθέσεων

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.

Ωστόσο, έγιναν δοκιμές της αντοχής του AES και σε άλλα είδη επιθέσεων, που ήταν είτε πιο σύγχρονες, είτε προσανατολισμένες στον κρυπταλγόριθμο αυτό. Συγκεκριμένα, πραγματοποιήθηκαν δοκιμές ασφαλείας του AES έναντι των εξής επιθέσεων:

- Επίθεση κόλουρων διαφορικών (Truncated differentials attack).
- Επιθέσεις κορεσμού (Saturation attacks).
- Επίθεση Gilbert-Minier.
- Επιθέσεις παρεμβολής (Interpolation attacks).
- Αναζήτηση αδυνάμων κλειδιών (weak keys) σαν αυτά των κρυπταλγορίθμων DES και IDEA.
- Επιθέσεις σχετιζομένων κλειδιών (Related key attacks).

Σε όλα τα προηγούμενα είδη επιθέσεων ο AES απεδείχθη είτε απολύτως ασφαλής, είτε ασφαλής λόγω του αριθμού των γύρων του (υπήρξαν δηλαδή κάποιες επιτυχείς επιθέσεις σε παραλλαγές του AES με μικρότερο αριθμό γύρων).

Η μοναδική, έως τώρα, προοπτική ευρέσεως τρωτού σημείου του AES είναι η κρυπταναλυτική μέθοδος XSL (eXtended Sparse Linearization) συνδυασμένη με το μοντέλο BES για την περιγραφή του AES. Η μέθοδος XSL, των Nicolas Courtois και Josef Pieprzyk, που παρουσιάσθηκε το 2002, παρά τις καλές θεωρητικές προοπτικές της, δεν απεδείχθη πρακτικώς εφαρμόσιμη. Ωστόσο, οι Sean Murphy και Matthew Robshaw παρουσίασαν το 2003 μία διαφορετική μαθηματική προσέγγιση του AES (τον ισοδύναμο κρυπταλγόριθμο που προέκυψε τον ονόμασαν BES), η οποία επιτρέπει την απλοποίηση της μαθηματικής περιγραφής του AES. Εικάζεται ότι η μέθοδος XSL μπορεί να έχει

ικανοποιητικά αποτελέσματα, εάν εφαρμοσθεί στον BES, πάντως δεν έχει αποδειχθεί κάτι σχετικό έως σήμερα.

3.5.4 Εξαντλητική αναζήτηση κλειδιού του AES

Εφόσον, όπως έγινε σαφές στις δύο προηγηθείσες παραγράφους, ο AES είναι ασφαλής έναντι οιασδήποτε γνωστής επιθέσεως, μπορούμε να τον θεωρήσουμε K-ασφαλή. Τότε, κατά τον ορισμό της K-ασφαλείας, όλες οι επιθέσεις στον AES θα είναι ισοδύναμες, ως προς τους απαιτούμενους πόρους (επεξεργαστική ισχύς, μνήμη, κόστος κλπ) και την αποτελεσματικότητα, με την επίθεση εξαντλητικής αναζητήσεως κλειδιού.

Η εξαντλητική αναζήτηση κλειδιού εξετάζει, ένα προς ένα, όλα τα πιθανά κλειδιά ενός κρυπτοσυστήματος. Θεωρώντας το μήκος του κλειδιού l_k bits, τα δυνατά κλειδιά είναι 2^{l_k}. Στατιστικώς, η εύρεση του σωστού κλειδιού αναμένεται μετά τον έλεγχο των μισών, περίπου, κλειδιών. Υποθέτουμε λοιπόν ότι απαιτούνται, έως το "σπάσιμο" του κρυπτοσυστήματος, περίπου $\frac{1}{2}2^{l_k}=2^{l_k-1}$ εφαρμογές του κρυπταλγορίθμου. Τα αριθμητικά δεδομένα που προκύπτουν για τον AES είναι:

Μήκος κλειδιού [bits]	Αναμενόμενος αριθμός επαναλήψεων του AES έως το «σπάσιμό» του
128	$2^{127} \cong 1{,}70 \cdot 10^{38}$
192	$2^{191} \cong 3{,}14 \cdot 10^{57}$
256	$2^{255} \cong 5{,}79 \cdot 10^{76}$

3.6 Συστήματα Τρίτης Γενιάς (UMTS)

3.6.1 Εισαγωγή

Το 1992 η Ευρωπαϊκή Ένωση συμφώνησε στην ανάπτυξη του συστήματος τρίτης γενιάς (3G) με το όνομα UMTS (Universal Mobile Telecommunications Systems) ως Ευρωπαϊκή (και Ιαπωνική) πρόταση στη Διεθνή Ένωση Τηλεπικοινωνιών ITU (International Telecommunication Union) για το IMT-2000. Τα συστήματα 3G αναπτύσσονται και προτυποποιούνται από δύο μη κερδοσκοπικούς οργανισμούς γνωστούς ως 3rd Generation Partnership Project (3GPP) και 3GPP2.

Ανάμεσα στα πλεονεκτήματα των UMTS δικτύων ξεχωρίζουμε τους αυξημένους όγκους μετάδοσης των δεδομένων και την ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής. Πιο συγκεκριμένα, το

UMTS δίκτυο στην αρχική του φάση, θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbit/sec σε περιπτώσεις που παρατηρείται αυξημένη κινητικότητα του χρήστη (vehicular). Αντίθετα, όταν ο χρήστης είναι πεζός ή καλύτερα παραμένει ακίνητος, οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ πλησιάζοντας την θεωρητική τιμή των 2 Mbits/sec (1920 kbits/sec).

Από πλευράς ασφάλειας, είναι γνωστό ότι τα συστήματα ασύρματων κινητών επικοινωνιών αντιμετωπίζουν περισσότερες απειλές σε σχέση με τα ενσύρματα. Έτσι, η ασφάλεια των εκπεμπόμενων δεδομένων (data) αλλά και της σηματοδοσίας (signaling) αποτελεί ουσιώδες κεφάλαιο σε ένα σύστημα κινητών επικοινωνιών. Σε ένα ασύρματο δίκτυο η πρόσβαση δεν μπορεί να περιοριστεί σε φυσικά περιορισμένο χώρο. Επιπλέον, τα εκπεμπόμενα δεδομένα των χρηστών αλλά και της σηματοδοσίας μεταξύ δικτύου και των τερματικών κινητών σταθμών μπορούν να ληφθούν από οποιονδήποτε διαθέτει έναν κατάλληλο δέκτη.

Κατά συνέπεια, είναι απαραίτητο να χρησιμοποιηθούν κατάλληλοι μηχανισμοί προστασίας, όπως κρυπτογραφικές τεχνικές, προκειμένου να προστατέψουν κατάλληλα τα δεδομένα, τη σηματοδοσία αλλά και τους πόρους του δικτύου. Τα θέματα που κρίνεται απαραίτητο να αντιμετωπιστούν είναι η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity) και η διαθεσιμότητα (availability) των δεδομένων και των υπηρεσιών του δικτύου καθώς και η ιδιωτικότητα (privacy) των χρηστών. Πολύ σημαντικό είναι επίσης το ζήτημα της αναγνώρισης (identification) και πιστοποίησης της ταυτότητας των χρηστών, του δικτύου και των δεδομένων (authentication).

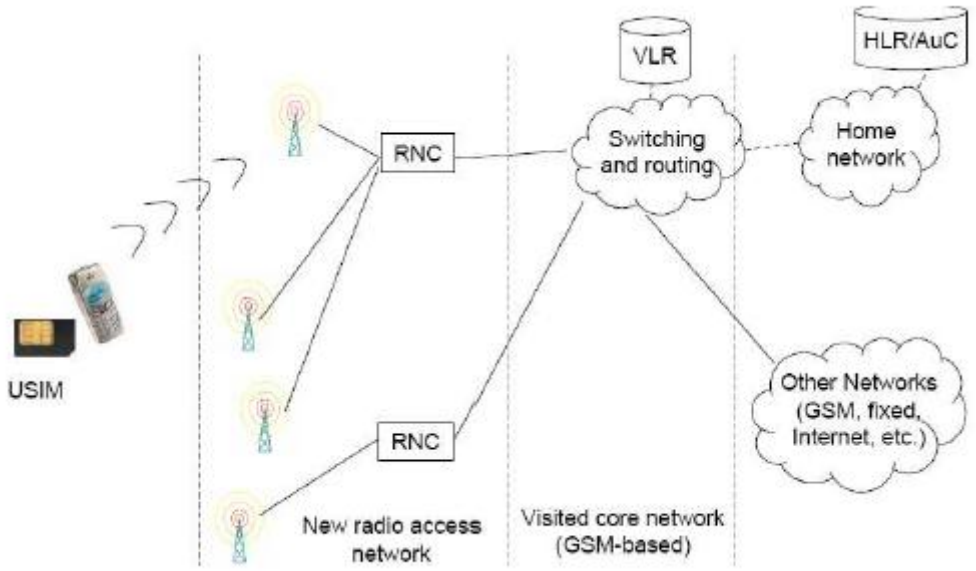
Για τους σκοπούς της εργασίας αυτής θα επικεντρωθούμε στο ζήτημα της πιστοποίησης των δεδομένων (authentication) και πιο συγκεκριμένα θα παρουσιάσουμε και θα αναλύσουμε το πρωτόκολλο αυθεντικοποίησης (UMTS Authentication) που χρησιμοποιείται στα UMTS δίκτυα.

3.6.2 Αρχιτεκτονική του UMTS Δικτύου

Το μοντέλο του UMTS δικτύου αποτελείται από δύο κύρια μέρη:

- Από την πλευρά του χρήστη βρίσκεται το τερματικό του, το οποίο καλείται εξοπλισμός χρήστη (User Equipment, UE). Το τερματικό διαθέτει ασύρματη πρόσβαση στο ραδιοδίκτυο (Radio Acces Network, RAN) του παρόχου υπηρεσιών. Επιπλέον, αποτελείται από δύο διακριτά μέρη: Το φορητό εξοπλισμό (Mobile equipment) δηλαδή την κυρίως συσκευή και τη USIM.
- Το ράδιο-δίκτυο (RAN) συνδέεται με το δίκτυο κορμού (core) του παρόχου υπηρεσιών. Το δίκτυο κορμού είναι υπεύθυνο για τη δρομολόγηση των τηλεφωνημάτων καθώς και για τις συνδέσεις για μεταφορά δεδομένων με εξωτερικά δίκτυα. Τα δύο κυριότερα στοιχεία του είναι το υποσύστημα μεταγωγής κυκλωμάτων (MSC) και το Home

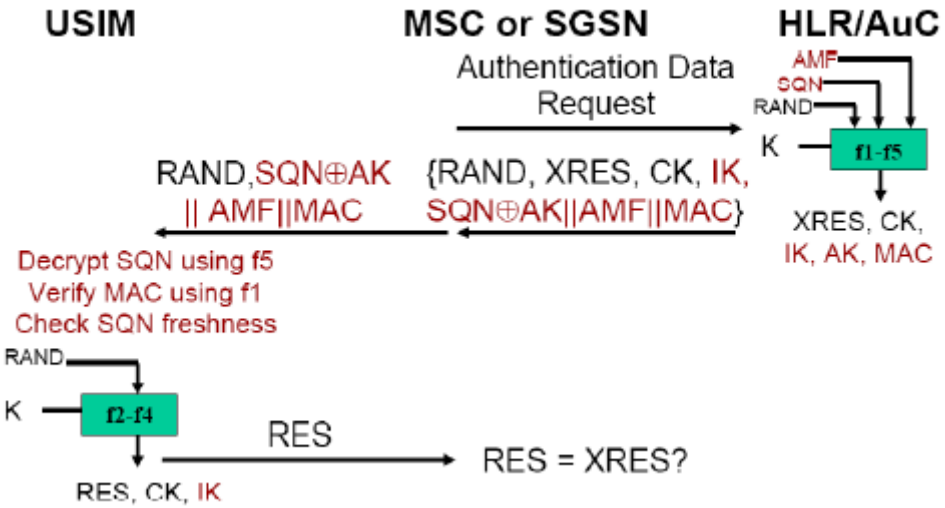
Location Register (HLR). Το υποσύστημα μεταγωγής κυκλωμάτων (MSC) συνήθως ενσωματώνει ένα Visitor Location Register (VLR). Το τελευταίο περιέχει μια βάση δεδομένων των χρηστών που κινούνται στη περιοχή που ελέγχεται από το τοπικό MSC. Το στοιχείο Home Location Register (HLR) αποθηκεύει στατικές πληροφορίες για όλους τους συνδρομητές που χρησιμοποιούν τις υπηρεσίες του συγκεκριμένου παρόχου. Εκτός των πληροφοριών αυτών δημιουργεί και άλλες, οι οποίες χρησιμοποιούνται για διάφορες υπηρεσίες όπως για παράδειγμα στην αυθεντικοποίηση χρηστών.



Σχήμα 3.16 Αρχιτεκτονική UMTS δικτύου

3.6.3 Μηχανισμός Αυθεντικοποίησης Χρηστών στα UMTS δίκτυα

Στο UMTS ο μηχανισμός αυθεντικοποίησης των χρηστών είναι γνωστός και ως Authentication and Key Agreement (AKA). Η διαδικασία αυθεντικοποίησης βασίζεται σε ένα συμμετρικό κλειδί K μήκους 128-bits το οποίο είναι αποθηκευμένο στη κάρτα USIM του συνδρομητή και στο αντίστοιχο HLR/AuC (Authentication Centre). Η διαδικασία αυθεντικοποίησης αποτελεί συνδυασμό του γνωστού πρωτοκόλλου πρόκλησης- απάντησης (challenge-response) και του γενικού μηχανισμού αυθεντικοποίησης που βασίζεται σε αριθμούς ακολουθίας (sequence numbers) όπως αυτός καθορίζεται από τον οργανισμό ISO.



Σχήμα 3.17 Διαδικασία Αυθεντικοποίησης σε UMTS δίκτυα

Ανάλυση του Πρωτοκόλλου

Τρείς δικτυακές οντότητες λαμβάνουν μέρος στη διαδικασία αυθεντικοποίησης ενός χρήστη. Αυτές είναι: Το τερματικό του χρήστη και συγκεκριμένα η κάρτα USIM, το MSC του οικείου δικτύου ή του δικτύου εξυπηρέτησης και το HLR/AuC του οικείου δικτύου του χρήστη. Το πρωτόκολλο πετυχαίνει αμφοτεροβαρή αυθεντικοποίηση (mutual authentication) αφού το δίκτυο και ο χρήστης αυθεντικοποιούνται αμοιβαία. Μετά από επιτυχή αυθεντικοποίηση, τα δύο μέρη δημιουργούν ή έχουν στη διάθεσή τους δύο ακόμα συμμετρικά κλειδιά (το CK=cipher key και το IK=integrity key) προκειμένου να υποστηρίξουν υπηρεσίες εμπιστευτικότητας και ακεραιότητας. Τα κλειδιά αυτά παράγονται από το κύριο κλειδί K και αλλάζουν κάθε φορά που ο χρήστης αυθεντικοποιείται εκ νέου. Η διαδικασία ξεκινάει στην περίπτωση που η ταυτότητα του χρήστη αναγνωριστεί από το MSC. Ακολούθως το MSC αποστέλλει μια αίτηση για δεδομένα αυθεντικοποίησης (Authentication Data Request) στο HLR/AuC που βρίσκεται στο οικείο δίκτυο του εν λόγω χρήστη. Δεδομένου ότι το HLR/AuC διαθέτει το κύριο κλειδί K για κάθε χρήστη και τις συναρτήσεις αυθεντικοποίησης f1, f1*, f2 και παραγωγής κλειδιού f3, f4, f5, f5*, είναι ικανό να δημιουργήσει τα αντίστοιχα διανύσματα αυθεντικοποίησης τα οποία τα στέλνει πίσω στο MSC ως authentication data response. Μόλις το υπεύθυνο MSC έχει στη διάθεσή του διάνυσμα για το χρήστη που απαιτείται πρόσβασης, αποστέλλει μια αίτηση αυθεντικοποίησης (User Authentication Request) σ' αυτόν. Στην αίτηση περιέχονται δύο παράμετροι, ο τυχαίος αριθμός RAND (Random Number) και ο AUTH=SQN⊕AK‖AMF‖MAC (Authentication Token) όπου SQN=sequence number (48-bits), $AK=f5_K(RAND)$=Anonymity Key (48-bits), AMF=Authentication Management Field (16-bits) και $MAC=f1_K(SQN‖RAND‖AMF)$=Message Authentication Code (64-bits). Έπειτα οι εν λόγω παράμετροι μεταφέρονται στο ασφαλές περιβάλλον της USIM. Επειδή η USIM διαθέτει το κλειδί K , μπορεί να το χρησιμοποιήσει μαζί με τις παραμέτρους RAND και AUTH σε υπολογισμούς αντίστοιχους με αυτούς που έλαβαν χώρα στο HLR/Auc. Το αποτέλεσμα αυτής

της επεξεργασίας δίνει τη δυνατότητα στη USIM να επιβεβαιώσει ότι πράγματι η παράμετρος AUTH δημιουργήθηκε από το HLR/AuC του οικείου δικτύου και επιπλέον ότι δεν έχει σταλεί ήδη προηγουμένως (replay). Σε περίπτωση που ο παραπάνω έλεγχος έχει θετικό αποτέλεσμα, η υπολογισθείσα παράμετρος RES αποστέλλεται πίσω στο MSC. Σε αυτό το σημείο, το MSC είναι σε θέση να συγκρίνει την παράμετρο RES με την XRES ,η οποία περιέχεται στο διάνυσμα αυθεντικοποίησης και ακολούθως να αποφανθεί θετικά ή αρνητικά.

Δεν υπάρχει κάποιο πρότυπο που να επιβάλλει τη χρήση συγκεκριμένων αλγορίθμων στις συναρτήσεις αυθεντικοποίησης f1, f1*, f2 και παραγωγής κλειδιού f3, f4, f5, f5* αλλά το πιο συνηθισμένο σύνολο από αλγορίθμους που ονομάζεται MILENAGE βασίζεται στο κρυπτοσύστημα Rijndael που αργότερα ονομάστηκε AES.

Κεφάλαιο 4
Ανακεφαλαίωση

4.1 Συνοπτική σύγκριση του DES με τον AES

Σκοπός της εργασίας αυτής είναι η γνωριμία με την κρυπτογραφία μέσα από τους αλγόριθμους DES και AES, συνεπώς μετά την ολοκλήρωση της αναλυτικής παρουσίασής τους, κρίνεται σκόπιμο να γίνει μία σύντομη συγκριτική αντιπαράθεση μεταξύ τους:

Σημείο σύγκρισης	**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 (έως τώρα)

4.2 Συμπεράσματα

Η κρυπτογραφία είναι μια επιστήμη που έχει τις ρίζες της στην αρχαιότητα και εφαρμόζεται σε πολλούς τομείς της σύγχρονης ζωής ανάμεσα στους οποίους και η επιστήμη υπολογιστών. Κρυπτογραφία είναι η μελέτη των μαθηματικών τεχνικών που σχετίζονται με τις πτυχές της ασφάλειας όπως είναι η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η αυθεντικότητα και η πιστοποίηση αυθεντικότητας. Η κρυπτογραφία δεν είναι μόνο το μέσο που προστατεύει την πληροφορία αλλά ένα σύνολο τεχνικών.

Απαραίτητοι για την εφαρμογή της κρυπτογραφίας είναι κάποιοι αλγόριθμοι, όπως οι DES, Triple DES, AES, RC4-RC5 και IDEA. Οι παραπάνω είναι κάποιοι από τους αλγόριθμους κρυπτογράφησης ιδιωτικού κλειδιού, καθένας από τους

οποίους είναι κατάλληλος για την υλοποίηση μιας ή περισσοτέρων από τις υπηρεσίες που προσφέρει η κρυπτογραφία.

Ο DES είναι ένας block cipher, δηλαδή, ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, που λαμβάνει μια σειρά από bits απλού κειμένου (plaintext) σταθερού μήκους και την μετατρέπει, μέσω μιας σειράς πολύπλοκων ενεργειών, σε μια άλλη σειρά bits, το κρυπτοκείμενο (ciphertext) με το ίδιο μήκος. Στην περίπτωση του DES το μέγεθος μπλοκ είναι 64 bits και το κλειδί που χρησιμοποιεί αποτελείται από 64 bits. Μετά από πολλές επιθέσεις, ο DES έπαψε να θεωρείται ασφαλής και κρίθηκε σκόπιμη η αντικατάστασή του.

Ο AES είναι το επόμενο πρότυπο μετά τον DES. Συγκεκριμένα είναι ο αλγόριθμος Rijndael που επικράτησε στον διαγωνισμό του NIST (National Institute of Standards and Technology) και λειτουργεί με ομάδες των 128bits (block cipher) χρησιμοποιώντας κλειδιά των 128, 192, και 256 bits. Μέχρι και σήμερα ο AES θεωρείται το ασφαλέστερο κρυπτοσύστημα, καθώς ακόμα δεν έχει βρεθεί τρόπος για να σπάσει.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Κρυπτογραφία
   Χ. Κουκουβίνος – Α. Παπαϊωάννου
   Εκδόσεις Εθνικού Μετσοβίου Πολυτεχνείου, Αθήνα 2007

2. Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία
   Ευστάθιος Ζάχος
   2007

3. Introduction to Cryptography with Coding Theory
   Wade Trappe **-** Lawrence C. Washington
   Εκδόσεις Pearson, 2002

4. Modern Cryptography: Theory and Practice
   Wenbo Mao
   Εκδόσεις Prentice Hall, 2003

5. Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)
   Douglas R. Stinson
   Εκδόσεις CRC Press, 1995

6. Cryptography: An Introduction
   Nigel P. Smart
   Εκδόσεις McGraw Hill, 2002

7. Handbook of Applied Cryptography
   Alfred J. Menezes – Paul C. van Oorschot – Scott A. Vanstone
   Εκδόσεις CRC Press, 1997

8. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης
   Β.Α. Κάτος – Γ.Χ. Στεφανίδης
   Εκδόσεις Ζυγός, Θεσσαλονίκη 2003

9. Cryptography and Network Security: Principles and Practice
   William Stallings
   Εκδόσεις Prentice Hall, 2006

10. The Design of Rijndael
    Joan Daemen - Vincent Rijmen
    Εκδόσεις Springer, Βερολίνο 2002

11. Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων
    Γ. Πάγκαλος - Ι. Μαυρίδης
    Εκδόσεις Ανικούλα, Θεσσαλονίκη 2002