5 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

5.1. Εισαγωγή

Η συμμετρική κρυπτογραφία είναι κατά πολύ αρχαιότερη από την ασύμμετρη κρυπτογραφία. Η συμμετρική κρυπτογραφία χρονολογείται από την Αρχαία Αίγυπτο, ενώ η ασύμμετρη κρυπτογραφία εμφανίσθηκε τη δεκαετία του ’70. Η τόσο μεγάλη καθυστέρηση οφείλεται αφενός μεν στο γεγονός ότι δεν υπήρξε μέχρι πριν τριάντα χρόνια η ανάγκη για ασύμμετρα κρυπτοσυστήματα, αφετέρου δε στον τρόπο αντιμετώπισης της κρυπτογραφίας όπου εθεωρείτο περισσότερο τέχνη παρά επιστήμη. Σήμερα η κρυπτογραφία αποτελεί αναπόσπαστο κομμάτι της ασφάλειας των σύγχρονων ψηφιακών συστημάτων και η επιστημονική τεκμηρίωση απαιτείται για να προσδώσει την απαραίτητη διαβεβαίωση σε μια επένδυση του πληροφοριακού συστήματος.

5.2. Κρυπταλγόριθμοι τμήματος

Η πλειοψηφία των συμμετρικών κρυπταλγόριθμων στις σύγχρονες εφαρμογές αποδίδεται σε κρυπταλγόριθμους τμήματος. Η σχετικά μεγαλύτερη ασφάλεια που παρέχουν οι κρυπταλγόριθμοι τμήματος έναντι των κρυπταλγόριθμων ροής καθιστούν τους κρυπταλγόριθμους τμήματος ως πρώτη επιλογή. Ωστόσο, σε εφαρμογές όπου η ταχύτητα έχει μεγαλύτερη προτεραιότητα από την ασφάλεια, προτιμούνται οι κρυπταλγόριθμοι ροής.

Ένας κρυπταλγόριθμος τμήματος είναι συνήθως μια επαναληπτική εφαρμογή μιας κρυπτογραφικής πράξης η οποία αποτελείται από μία ή περισσότερες κρυπτογραφικές συναρτήσεις, σε διάταξη τέτοια ώστε να επιτρέπεται η διαδοχική σύνδεση της πράξης αυτής με τον εαυτό της ή με διαφορετικές πράξεις. Το αποτέλεσμα της σύνδεσης αυτής αποτελεί το κρυπτογραφικό γινόμενο, το οποίο υπό κατάλληλες συνθήκες μπορεί να καταστήσει ένα κρυπτοσύστημα ασφαλές. Το κάθε συστατικό του κρυπτογραφικού γινομένου αποτελεί το γύρο του κρυπταλγόριθμου. Σε κάθε γύρο τροφοδοτείται το αποτέλεσμα του προηγούμενου γύρου και το αντίστοιχο κλειδί του γύρου. Η ακολουθία των κλειδιών όλων των γύρων αποτελεί το πρόγραμμα κλειδιού και προκύπτει από κάποιο αρχικό κλειδί. Στον πρώτο

γύρο τροφοδοτείται το απλό κείμενο, ενώ το αποτέλεσμα του τελευταίου γύρου αποτελεί το κρυπτοκείμενο.

Ο αριθμός των γύρων εξαρτάται από την κρυπτογραφική δύναμη του κάθε γύρου. Γενικά το κρυπτογραφικό γινόμενο δύο σχετικά αδύναμων κρυπτογραφικών πράξεων ισοδυναμεί σε μια κρυπτογραφική πράξη η οποία είναι κατά πολύ κρυπτογραφικά δυνατότερη από τις επιμέρους πράξεις. Σύμφωνα με τον Shannon, αυτό ονομάζεται ***φαινόμενο της χιονοστιβάδας*** (avalanche effect), όπου οι επιμέρους πράξεις μπορεί να παρουσιάζουν χαμηλή σύγχυση και διάχυση, αλλά το αποτέλεσμα του κρυπτογραφικού γινομένου ενισχύει σημαντικά τις ποσότητες των δύο αυτών χαρακτηριστικών.

5.2.1. Τρόποι λειτουργίας

Οι τρόποι λειτουργίας (modes of operation) είναι τρόποι διασύνδεσης κρυπταλγόριθμων τμήματος, με στόχο την περαιτέρω αύξηση της κρυπτογραφικής δύναμης και την αποτελεσματικότερη απόκρυψη πιθανών υπολειμμάτων πληροφορίας του απλού κειμένου που μπορεί να υπάρχει στο κρυπτοκείμενο. Υπάρχουν τέσσερις τυποποιημένοι τρόποι λειτουργίας σύμφωνα με το πρότυπο FIPS 81, και αρκετοί μη τυποποιημένοι τρόποι λειτουργίας. Οι τέσσερις τυποποιημένοι τρόποι λειτουργίας είναι:

- ηλεκτρονικό κωδικοβιβλίο (electronic codebook, ECB)
- κρυπταλγόριθμος αλυσιδωτού τμήματος (cipher block chaining, CBC)
- ανάδραση κρυπταλγόριθμου (cipher feedback, CFB)
- ανάδραση εξόδου (output feeback, OFB)

Ηλεκτρονικό κωδικοβιβλίο, ECB

Ο τρόπος λειτουργίας ECB αποτελεί την ευθεία συνδεσμολογία όπου το απλό κείμενο τροφοδοτείται στον κρυπταλγόριθμο και το κρυπτοκείμενο προκύπτει από την έξοδο, όπως φαίνεται στο Σχήμα 5.1. Η ονομασία του τρόπου αυτού προέρχεται από την αναπαράσταση του κρυπτοσυστήματος ως ένα μεγάλο βιβλίο το οποίο περιέχει όλα τα ζεύγη απλού κειμένου και κρυπτοκειμένου για κάθε κλειδί. Έτσι για έναν κρυπταλγόριθμο τμήματος με μέγεθος απλού κειμένου και κρυπτοκειμένου n bits και μέγεθος κλειδιού k bits, μπορούμε να φανταστούμε ότι το βιβλίο περιέχει 2^k κεφάλαια, ένα για το κάθε κλειδί, και το περιεχόμενο του κάθε κεφαλαίου θα αποτελούνταν από 2×2^k καταχωρήσεις, οι μισές ταξινομημένες ως προς το απλό κείμενο, και οι υπόλοιπες ταξινομημένες ως προς το κρυπτοκείμενο.

Σχήμα 5.1 Τρόπος λειτουργίας ECB

Το απλό κείμενο χωρίζεται σε τμήματα $P = [p_1 p_2 ... p_l]$, όπου το κάθε τμήμα μεγέθους n bits τροφοδοτείται στον αλγόριθμο κρυπτογράφησης:

$$c_i = e_k(p_i).$$

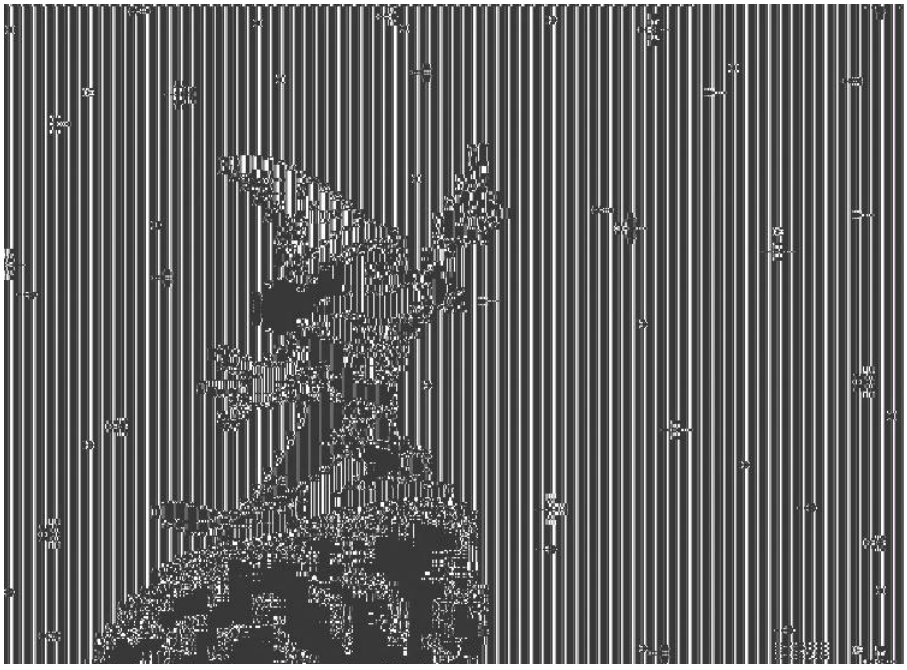
Η αναγκαία κατάτμηση του απλού κειμένου είναι και το μειονέκτημα της ECB λειτουργίας. Για όμοια τμήματα του απλού κειμένου, τα αντίστοιχα κρυπτοκείμενα που προκύπτουν είναι επίσης όμοια. Αυτό καθιστά την ECB ακατάλληλη για τις εφαρμογές στις οποίες υπάρχουν επαναλαμβανόμενα μοτίβα δεδομένων. Για παράδειγμα, στα δίκτυα ηλεκτρονικών υπολογιστών, τα δεδομένα που ανταλλάσσονται μεταξύ των υπολογιστών βασίζονται σε πρωτόκολλα επικοινωνίας τα οποία χρησιμοποιούν τυποποιημένα μηνύματα. Έτσι ο αντίπαλος είναι σε θέση να αναγνωρίζει τα επαναλαμβανόμενα τμήματα του απλού κειμένου, καθώς και τις στιγμές κατά τις οποίες γίνεται η αλλαγή του κλειδιού κρυπτογράφησης. Αυτή η διαρροή της πληροφορίας για τις περισσότερες εφαρμογές δεν είναι επιτρεπτή.

Χαρακτηριστική περίπτωση της ακαταλληλότητας της χρήσης της ECB λειτουργίας είναι η κρυπτογράφηση των εικόνων, όπου τα μοτίβα είναι βασικά δομικά στοιχεία της δισδιάστατης απεικόνισης. Στο Σχήμα 5.2 φαίνεται μια εικόνα ως απλό κείμενο, και στο Σχήμα 5.3 η εικόνα υπέστη κρυπτογράφηση[1] με τον κρυπταλγόριθμο τμήματος DES. Αν και τα ακριβή χαρακτηριστικά δεν είναι φανερά,

Σχήμα 5.2 Απλό κείμενο σε μορφή εικόνας.

[1] http://cui.unige.ch/tcs/cours/crypto/crypto5/

ο αντίπαλος είναι σε θέση να διακρίνει τα αντικείμενα τα οποία απαρτίζουν την εικόνα. Επιπλέον, αν ο αντίπαλος είχε συναντήσει στο παρελθόν την εικόνα αυτή (μη κρυπτογραφημένη), θα είναι σε θέση να συσχετίσει την «κρυπτοεικόνα» με την «απλή εικόνα». Επομένως, η κρυπτογραφική δύναμη του κρυπταλγόριθμου τμήματος δεν είναι σε θέση να επηρεάσει το αποτέλεσμα της συνολικής ασφάλειας του συστήματος, εφόσον υπάρχει μεγάλη ποσότητα επαναλαμβανόμενων μοτίβων στο απλό κείμενο.



Σχήμα 5.3 Κρυπτογραφημένη εικόνα με ECB.

Συμπεραίνουμε λοιπόν ότι, η αναγκαία κατάτμηση σε συνδυασμό με το γεγονός ότι το κάθε τμήμα κρυπτογραφείται ανεξάρτητα από τα υπόλοιπα τμήματα του απλού κειμένου δίνει το πλεονέκτημα στον αντίπαλο να αναγνωρίσει με αφαιρετικό τρόπο το περιεχόμενο του απλού κειμένου. Οι τρόποι λειτουργίας που ακολουθούν έχουν στόχο να επιδιορθώσουν αυτό το μειονέκτημα.

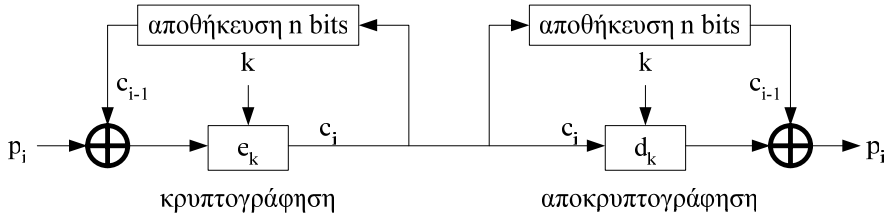
Κρυπταλγόριθμος αλυσιδωτού τμήματος, CBC

Η λειτουργία CBC παριστάνεται στο Σχήμα 5.4. Η κρυπτογράφηση ενός τμήματος του απλού κειμένου p_i εξαρτάται και από το προηγούμενο τμήμα $p_{i\text{-}1}$ με την ακόλουθη σχέση κρυπτογράφησης:

$$c_i = e_k(c_{i\text{-}1} \oplus p_i),$$

ενώ η αποκρυπτογράφηση ορίζεται από την:

$p_i = d_k(c_i) \oplus c_{i-1}$.



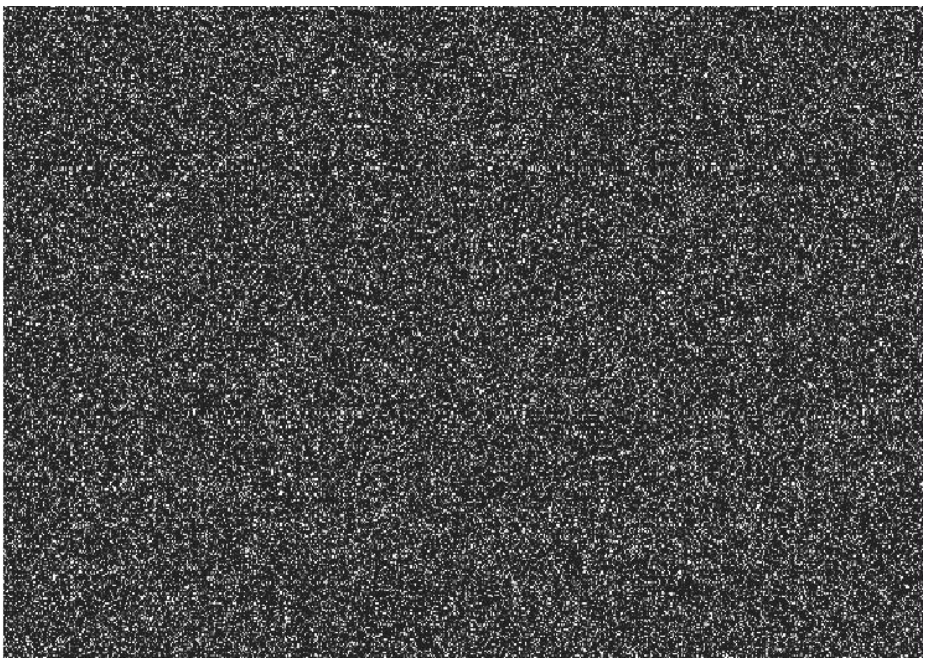
Σχήμα 5.4 Τρόπος λειτουργίας CBC

Η ορθότητα της σχέσης κρυπτογράφησης / αποκρυπτογράφησης είναι φανερή από:

$$p_i = d_k(c_i) \oplus c_{i-1} = c_{i-1} \oplus p_i \oplus c_{i-1} = (c_{i-1} \oplus c_{i-1}) \oplus p_i = p_i .$$

Μπορούμε να παρατηρήσουμε ότι η ποσότητα του κρυπτοκειμένου που εφαρμόζεται στην αποκλειστική διάζευξη είναι η ίδια τόσο στην πλευρά της κρυπτογράφησης, όσο και στην πλευρά της αποκρυπτογράφησης, και είναι αυτή που προκύπτει από την προηγούμενη κρυπτογράφηση.

Στο Σχήμα 5.5 παρουσιάζεται η εικόνα του Σχήματος 5.2 κρυπτογραφημένη με τον ίδιο κρυπταλγόριθμο DES, αλλά σε λειτουργία CBC. Τα επαναλαμβανόμενα μοτίβα που υπάρχουν στο απλό κείμενο δεν είναι πλέον φανερά στο κρυπτοκείμενο.



Σχήμα 5.5 Κρυπτογραφημένη εικόνα με CBC.

Το αρχικό και το τελικό τμήμα

Για να καθορισθεί πλήρως η κρυπτογράφηση της λειτουργίας CBC, θα πρέπει να ορισθούν η αρχική τιμή c_0, καθώς και το τελικό τμήμα του απλού κειμένου, στην περίπτωση που το μέγεθος του απλού κειμένου δεν είναι πολλαπλάσιο του n. Στην περίπτωση της κρυπτογράφησης του πρώτου τμήματος p_1 είναι:

$$c_1 = e_k(c_0 \oplus p_1),$$

που σημαίνει ότι απαιτείται η ποσότητα c_0. Αυτή η ποσότητα είναι το διάνυσμα αρχικοποίησης το οποίο θα πρέπει να είναι γνωστό τόσο κατά τη διαδικασία της κρυπτογράφησης, όσο και κατά τη διαδικασία της αποκρυπτογράφησης. Αν και η εμπιστευτικότητά του δεν είναι υποχρεωτική, αποτελεί κοινή πρακτική να στέλνεται στον αποδέκτη κρυπτογραφημένο με ECB.

Ένας δεύτερος λόγος που προτιμάται η κρυπτογραφημένη αποστολή του διανύσματος αρχικοποίησης, είναι η προστασία της ακεραιότητάς του, η οποία είναι σημαντικότερη από την εμπιστευτικότητα του διανύσματος. Η προστασία της ακεραιότητας πραγματοποιείται με τη χρήση συνάρτησης ακεραιότητας σε συνδυασμό με την κρυπτογράφηση ECB. Το διάνυσμα αρχικοποίησης διαιρείται σε δύο τμήματα, το πρώτο μήκους n-a bits και το δεύτερο μήκους a bits. Στο πρώτο τμήμα εφαρμόζεται κάποια μονόδρομη συνάρτηση hash, και τα πρώτα a bits του αποτελέσματος απαρτίζουν το δεύτερο τμήμα του διανύσματος. Με αυτόν τον τρόπο το δεύτερο τμήμα του διανύσματος αποτελεί τη σύνοψη του πρώτου τμήματος. Στη συνέχεια το διάνυσμα κρυπτογραφείται και αποστέλλεται στον αποδέκτη. Ο αποδέκτης με τη σειρά του το αποκρυπτογραφεί και ελέγχει αν το δεύτερο τμήμα του διανύσματος είναι η σύνοψη του πρώτου. Στην περίπτωση που ο αντίπαλος προσβάλλει την ακεραιότητα του διανύσματος, αυτό θα γίνει αντιληπτό από τον αποδέκτη.

Όσον αφορά το τελευταίο τμήμα του απλού κειμένου, υπάρχει το ενδεχόμενο το τμήμα αυτό να είναι μικρότερο του n. Αυτό συμβαίνει όταν το μέγεθος του κρυπτοκειμένου δεν είναι πολλαπλάσιο του n. Στην περίπτωση αυτή προστίθενται μηδενικά στο τέλος, έως ότου το τμήμα έχει μέγεθος ίσο με n bits. Στις εφαρμογές στις οποίες τα δεδομένα ακολουθούν αυστηρή τυποποίηση και δεν είναι επιτρεπτό να συμπεριλαμβάνονται τα επιπλέον μηδενικά, τα τελευταία bits του τμήματος χρησιμοποιούνται για την καταγραφή του πλήθους των επιπρόσθετων μηδενικών. Για z μηδενικά, απαιτούνται $\log_2(z)$ δυαδικές θέσεις.

ΠΑΡΑΔΕΙΓΜΑ 5.1 – Καθορισμός τυποποίησης επιπρόσθετων μηδενικών και περιγραφής του τελευταίου τμήματος. Έστω ο κρυπταλγόριθμος τμήματος που δέχεται απλό κείμενο των 64 bits. Θεωρούμε ότι πάντοτε το τελευταίο τμήμα θα περιέχει επιπρόσθετα μηδενικά, προκειμένου να υπάρχει μια τυποποιημένη διαδικασία καθορισμού του μήκους του απλού κειμένου. Ζητείται να βρεθεί το ελάχιστο απαιτούμενο πλήθος δυαδικών ψηφίων που απαιτείται για την αποθήκευση του πλήθους των επιπρόσθετων μηδενικών.

Στην περίπτωση όπου το τελευταίο τμήμα περιέχει μόνον ένα bit απλού κειμένου, θα έχουμε 63 δυαδικές θέσεις για μηδενικά, όπου συμπεριλαμβάνονται και οι θέσεις της αποθήκευσης του πλήθους των μηδενικών. Έτσι αρχικά θα είναι:

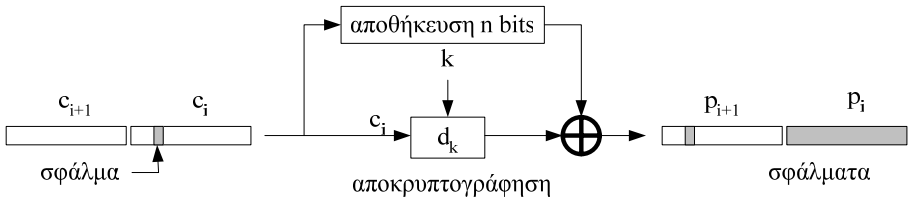
$$\lceil \log_2(63) \rceil = 6$$

Αν λοιπόν τα τελευταία 6 bits του τελευταίου τμήματος χρησιμοποιούνται πάντοτε για την αποθήκευση των επιπρόσθετων μηδενικών, το μέγιστο πλήθος δυαδικών ψηφίων απλού κειμένου για το τελευταίο τμήμα θα είναι 57 bits (η περίπτωση όπου το πλήθος των επιπρόσθετων μηδενικών είναι 0). Στην περίπτωση που τα bits του απλού κειμένου είναι 58, τότε απαιτείται ένα επιπλέον τμήμα με επιπρόσθετα μηδενικά. Δηλαδή το μέγιστο πλήθος των μηδενικών και σε αυτήν την περίπτωση θα είναι 5(*προτελευταίο τμήμα*) + 58(*τελευταίο τμήμα*) = 63 bits, το οποίο μπορεί να περιγραφεί από τα τελευταία 6 bits του τελευταίου τμήματος.

Διάδοση σφαλμάτων στη λειτουργία CBC

Ένα από τα κριτήρια του Shannon σχετικά με την ποιότητα ενός κρυπτοσυστήματος είναι και η αξιοπιστία του όσον αφορά τη διάδοση των σφαλμάτων (μέτρο (5), §1.1.3). Έστω ότι κατά τη μετάδοση του τμήματος c_i του κρυπτοκειμένου, υπάρχει σφάλμα σε κάποιο bit αυτού, είτε λόγω μετάδοσης, είτε λόγω παρεμβολής του αντιπάλου. Από τον ορισμό της αποκρυπτογράφησης της λειτουργίας CBC προκύπτει ότι το c_i θα επηρεάσει τόσο την αποκρυπτογράφηση του εαυτού του, όσο και την αποκρυπτογράφηση του επομένου τμήματος c_{i+1}, όπως φαίνεται στο Σχήμα 5.6. Υποθέτουμε ότι ο κρυπταλγόριθμος είναι κρυπτογραφικά δυνατός με υψηλή σύγχυση και διάχυση. Επομένως η παραμικρή μεταβολή στο κρυπτοκείμενο θα επηρεάσει όλο το απλό κείμενο. Στη συνέχεια, κατά την αποκρυπτογράφηση του c_{i+1}, το σφάλμα που υπάρχει στο c_i θα επηρεάσει μόνον το bit του απλού κειμένου στην αντίστοιχη θέση. Επομένως, συνολικά ένα σφάλμα στο κρυπτοκείμενο επηρεάζει πλήρως το αντίστοιχο αποκρυπτογραφημένο τμήμα και μερικώς το ακόλουθο τμήμα. Στη συνέχεια τα τμήματα που θα καταφθάνουν θα αποκρυπτογραφούνται ορθά.

Η ιδιότητα που περιγράφθηκε στις παραπάνω γραμμές είναι η ιδιότητα της αυτοεπούλωσης (self healing) του συστήματος CBC. Ωστόσο, αν το σφάλμα έχει ως αποτέλεσμα την αύξηση του μεγέθους του κρυπτοκειμένου, τότε προκύπτει σφάλμα συγχρονισμού, από το οποίο το σύστημα δεν μπορεί να αναρρώσει.



Σχήμα 5.6 Διάδοση σφάλματος κατά τη λειτουργία CBC.

Στην περίπτωση που υπάρξει σφάλμα στο απλό κείμενο πριν από την κρυπτογράφηση, τότε όλα τα επόμενα κρυπτοκείμενα θα είναι εσφαλμένα. Αυτό από τη μια είναι ένα σημαντικό μειονέκτημα, αλλά από την άλλη, μπορεί να χρησιμοποιηθεί για την ανίχνευση της αυθεντικότητας και της ακεραιότητας ενός μηνύματος. Η λειτουργία CBC μπορεί να χρησιμοποιηθεί ως MAC με τον εξής τρόπο. Η Αλίκη κρυπτογραφεί το μήνυμα με CBC και επισυνάπτει το τελευταίο τμήμα του κρυπτοκειμένου στο απλό κείμενο. Επειδή το κρυπτοκείμενο προκύπτει με ανάδραση, θα εξαρτάται από όλα τα προηγούμενα κρυπτοκείμενα και κατά συνέπεια από το συνολικό απλό κείμενο που αποτελεί το μήνυμα. Στη συνέχεια η Αλίκη στέλνει το απλό κείμενο μαζί με την επισύναψη στον Βύρωνα. Ο Βύρων με τη σειρά του κρυπτογραφεί το μήνυμα με την ίδια λειτουργία CBC και ελέγχει αν το τελευταίο τμήμα του κρυπτοκειμένου συμπίπτει με αυτό που έλαβε από την Αλίκη.

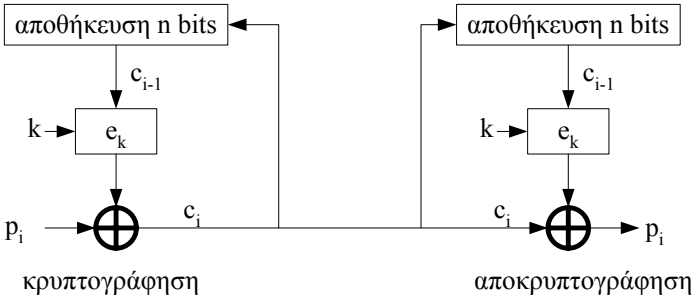
Ανάδραση κρυπταλγόριθμου, CFB

Ένα κρυπτοσύστημα σε λειτουργία CFB παρουσιάζεται στο Σχήμα 5.7. Το κρυπτοκείμενο προκύπτει από την επανακρυπτογράφηση του προηγούμενου κρυπτοκειμένου, συνδυασμένο με αποκλειστική διάζευξη με το απλό κείμενο. Έτσι η κρυπτογράφηση ορίζεται ως:

$$c_i = e_k(c_{i-1}) \oplus p_i$$

ενώ κατά την αποκρυπτογράφηση ισχύει:

$$p_i = e_k(c_{i-1}) \oplus c_i$$



Σχήμα 5.7 Τρόπος λειτουργίας CFB

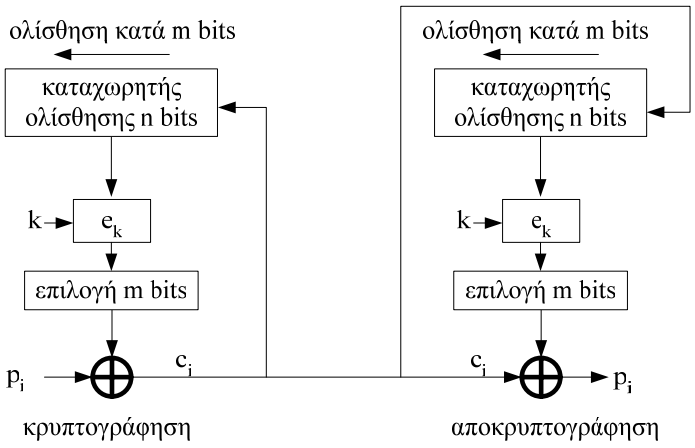
Η λειτουργία CFB μπορεί να θεωρηθεί ως κρυπταλγόριθμος ροής, όπου τα σύμβολα του απλού κειμένου είναι οι δυαδικές λέξεις μεγέθους *n* bits, που σημαίνει ότι το αλφάβητο του απλού κειμένου και του κρυπτοκειμένου αποτελείται από 2^n σύμβολα. Ο κρυπταλγόριθμος τμήματος λειτουργεί ως γεννήτρια κλειδοροής. Επίσης σε έναν κρυπταλγόριθμο ροής, οι γεννήτριες της κλειδοροής του αποστολέα και του αποδέκτη θα πρέπει να παράγουν την ίδια ακολουθία. Αυτό φαίνεται

και από την πράξη αποκρυπτογράφησης, όπου ο κρυπταλγόριθμος τμήματος εφαρμόζεται σε λειτουργία κρυπτογράφησης και όχι αποκρυπτογράφησης.

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

Παραλλαγές της CFB

Με βάση τη λειτουργία CFB ορίζεται μια οικογένεια τρόπων λειτουργίας, όπου τα σύμβολα της κλειδοροής και του απλού κειμένου μπορούν να ορίζονται από το αλφάβητο $\{0, 1\}^m$, όπου, $0 < m \leq n$. Η παραλλαγμένη CFB παριστάνεται στο Σχήμα 5.8 και περιλαμβάνει δύο νέα συστατικά, έναν καταχωρητή ολίσθησης και έναν επιλογέα των m bits.



Σχήμα 5.8 Λειτουργία m-bit CFB.

Ο καταχωρητής ολίσθησης χρησιμοποιείται για την αποθήκευση των n bits που απαιτούνται στην είσοδο του κρυπταλγόριθμου τμήματος. Κατά την κρυπτογράφηση του p_i, επιλέγονται τα m πρώτα bits από το σύνολο των n bits του κρυπτοκειμένου που παρέχει ο κρυπταλγόριθμος τμήματος. Το κρυπτοκείμενο c_i που προκύπτει αποθηκεύεται στον καταχωρητή ολίσθησης, ο οποίος δημιουργεί χώρο για το c_i, ολισθαίνοντας το περιεχόμενό του κατά m bits. Έτσι, σε κάθε κρυπτογράφηση αποβάλλονται τα αριστερότερα m bits.

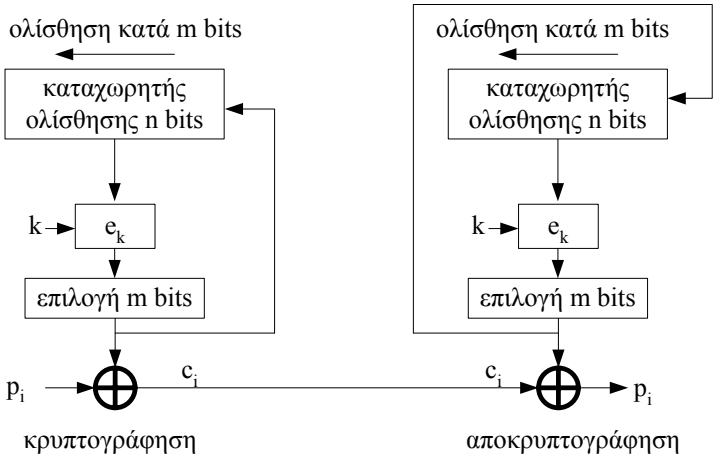
Στην περίπτωση όπου $m = 1$, το κάθε δυαδικό ψηφίο του απλού κειμένου κρυπτογραφείται χωριστά, ενώ στην περίπτωση όπου $m = n$, κρυπτογραφείται το τμήμα με το μέγιστο δυνατό μήκος.

Διάδοση σφαλμάτων στη λειτουργία CFB

Θα εξετάσουμε την περίπτωση της παραλλαγής της λειτουργίας CFB, όπου τα τμήματα του απλού κειμένου έχουν μέγεθος m bits. Έστω ότι υπάρχει σφάλμα κατά τη μετάδοση του τμήματος του κρυπτοκειμένου c_i. Τότε, το τμήμα αυτό θα έχει τη δυνατότητα να επηρεάσει τόσο την αποκρυπτογράφηση του εαυτού του, όσο και τα επόμενα τμήματα κρυπτοκειμένου, έως ότου αποβληθεί από τον καταχωρητή ολίσθησης του αποδέκτη. Για την ακρίβεια, το κρυπτοκείμενο c_i θα υπάρχει στον καταχωρητή ολίσθησης για $\lceil n/m \rceil$ το πολύ κρυπτοκείμενα. Αν το σφάλμα βρίσκεται στην αρχή του c_i (δηλαδή προς τα αριστερά), τότε το $\lceil n/m \rceil$-στο κρυπτοκείμενο θα αποκρυπτογραφηθεί σωστά. Στην περίπτωση που το σφάλμα βρίσκεται στο τέλος του c_i, τότε η αποκρυπτογράφηση θα διορθωθεί μετά από $\lceil n/m \rceil+1$ αποκρυπτογραφήσεις.

Ανάδραση εξόδου, OFB

Η λειτουργία OFB που παρουσιάζεται στο Σχήμα 5.9, είναι μια προσέγγιση του κρυπταλγόριθμου Vernam και ισοδυναμεί με κρυπταλγόριθμο ροής. Η κρυπτογράφηση πραγματοποιείται με την αποκλειστική διάζευξη του απλού κειμένου με την ακολουθία της κλειδοροής. Αντίστοιχα, η αποκρυπτογράφηση πετυχαίνεται με την αποκλειστική διάζευξη του κρυπτοκειμένου με την ακολουθία της κλειδοροής. Η διαδικασία δημιουργίας της κλειδοροής είναι ανεξάρτητη από το απλό κείμενο και το κρυπτοκείμενο.



Σχήμα 5.9 Λειτουργία m-bit OFB.

Θα μπορούσαμε να υποστηρίξουμε ότι η ασφάλεια της OFB είναι μικρότερη από την ασφάλεια των υπολοίπων τριών τρόπων λειτουργίας και αυτό γιατί ο μόνος τρόπος διασύνδεσης του απλού κειμένου και του κρυπτοκειμένου είναι η πράξη της αποκλειστικής διάζευξης. Εφόσον η γεννήτρια της κλειδοροής είναι μηχανή πεπερασμένων καταστάσεων, η κλειδοροή που παράγει θα είναι περιοδική. Επο-

μένως υπάρχει κάποια χρονική στιγμή όπου η κλειδοροή εμφανίζει τα ίδια κλειδιά. Αν ο αντίπαλος εντοπίσει την αρχή της περιόδου, τότε μπορεί να απομακρύνει την πληροφορία της κλειδοροής από το κρυπτοκείμενο με τον ακόλουθο τρόπο.

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

$$c_i \oplus c_j = (p_i \oplus k_i) \oplus (p_j \oplus k_i) = p_i \oplus p_j ,$$

δηλαδή η κλειδοροή έχει εξαλειφθεί. Αν το απλό κείμενο είναι κάποια φυσική γλώσσα με υψηλή περίσσεια, τότε ο αντίπαλος μπορεί να εντοπίσει την περίοδο με στατιστικές μεθόδους. Στη συνέχεια, μπορεί να συνδυάζει με αποκλειστική διάζευξη απλά κείμενα της γλώσσας στο παραπάνω άθροισμα για να ξεχωρίσει τα p_i και p_j.

Επομένως στην περίπτωση της λειτουργίας OFB δεν υπάρχει η ίδια ελευθερία επιλογής κρυπταλγόριθμου τμήματος που υπάρχει στους υπόλοιπους τρόπους λειτουργίας. Ο κρυπταλγόριθμος τμήματος θα πρέπει από τη μια να έχει μεγάλη περίοδο, ενώ από την άλλη θα πρέπει να αλλάζει το κλειδί προτού ξεπεραστεί αυτή η περίοδος. Η αλλαγή του κλειδιού του κρυπταλγόριθμου τμήματος θα έχει ως αποτέλεσμα η γεννήτρια κλειδοροής να μεταπίπτει σε άλλη ακολουθία κλειδοροής.

Διάδοση σφαλμάτων στη λειτουργία OFB

Η διαδικασία παραγωγής της ακολουθίας της κλειδοροής δε συνδέεται με το απλό κείμενο ή το κρυπτοκείμενο, με αποτέλεσμα να έχουμε την ελάχιστη δυνατή διάδοση των σφαλμάτων. Ένα σφάλμα στο κρυπτοκείμενο θα επηρεάσει μόνον το αντίστοιχο απλό κείμενο. Αυτό καθιστά τη λειτουργία OFB κατάλληλη για κρυπτογράφηση δορυφορικών ζεύξεων, κατά τη μετάδοση εικόνας και φωνής. Ένα κανάλι δορυφορικής επικοινωνίας χαρακτηρίζεται από τον μεγάλο αριθμό σφαλμάτων λόγω του υψηλού βαθμού θορύβου. Η περίπτωση αλλοίωσης του κρυπτογραφημένου σήματος προκαλεί το ίδιο αποτέλεσμα με την αλλοίωση του απλού σήματος. Έτσι, ο αποδέκτης μπορεί να παρατηρήσει παράσιτα μικρής έκτασης στην εικόνα, ή να έχει στιγμιαία παραμόρφωση ή έλλειψη του ήχου, αλλά τις περισσότερες φορές αυτό είναι ανεκτό. Η κρυπτογράφηση με OFB δεν μεταβάλλει το αποτέλεσμα, ενώ στην περίπτωση των υπολοίπων τριών τρόπων λειτουργίας, ένα σφάλμα μπορεί να ενισχυθεί.

Επιπλέον, μπορεί να διατεθεί κάποιο εύρος του καναλιού μετάδοσης για να μεταδοθεί επιπλέον περίσσεια πληροφορίας, η οποία μπορεί χρησιμοποιηθεί στη διόρθωση των σφαλμάτων.

Μη τυποποιημένοι τρόποι λειτουργίας

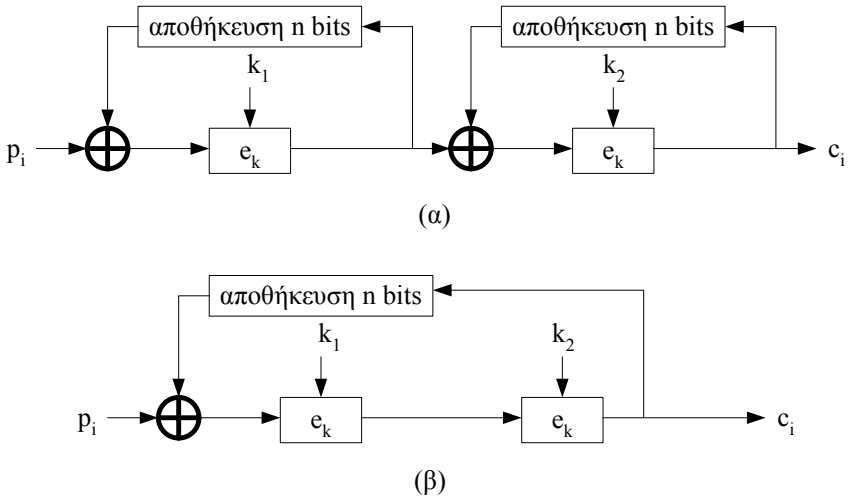
Εκτός από του τέσσερις τυποποιημένους τρόπους λειτουργίας που περιγράψαμε, μπορούμε να καθορίσουμε και μη τυποποιημένους τρόπους συνδυάζοντας έναν ή και περισσότερους κρυπταλγόριθμους τμήματος. Αν και στη βιβλιογραφία αναφέ-

ρονται αρκετοί εναλλακτικοί τρόποι λειτουργίας, ελάχιστοι από αυτούς έχουν διερευνηθεί σε βάθος. Επίσης, μια ελάχιστη μετατροπή στη διασύνδεση ενός τρόπου λειτουργίας μπορεί να καταλήξει σε ένα ασθενές κρυπτοσύστημα ή και αντίστροφα. Επομένως, σε περιπτώσεις όπου το ρίσκο δεν επιτρέπει «πειραματισμούς» με μη τυποποιημένους τρόπους λειτουργίας, συνιστάται η χρήση των τυποποιημένων τρόπων λειτουργίας.

Παρόλα αυτά θα περιγράψουμε ορισμένες αρχές οι οποίες μπορούν να καταλήξουν σε ασφαλή κρυπτοσυστήματα.

Τοποθέτηση της ανάδρασης

Όπως είδαμε στους παραπάνω τρόπους λειτουργίας, η ανάδραση είναι ένα δυνατό εργαλείο απόκρυψης των επαναλαμβανόμενων μοτίβων του απλού κειμένου. Όταν χρησιμοποιούμε περισσότερους από έναν κρυπταλγόριθμους τμήματος σε σειρά, προτιμάται η ανάδραση να περικλείει όλους τους κρυπταλγόριθμους, παρά να παρεμβάλλεται μεταξύ αυτών, όπως φαίνεται στο Σχήμα 5.10. Στην περίπτωση που υπάρχει ανάδραση ενδιάμεσα, δημιουργούνται μονοπάτια τα οποία ουσιαστικά «κόβουν δρόμο» με αποτέλεσμα ο αντίπαλος υπό κατάλληλες συνθήκες να μπορεί να τα διατρέξει. Έτσι το κρυπτοσύστημα (β) θεωρείται πιο δυνατό από το κρυπτοσύστημα (α).



Σχήμα 5.10 Τοποθέτηση της ανάδρασης

Στον παραπάνω σχεδιασμό δεν είναι υποχρεωτική η εφαρμογή του ίδιου κρυπταλγόριθμου τμήματος με διαφορετικά κλειδιά. Θα μπορούσαν να χρησιμοποιηθούν διαφορετικοί κρυπταλγόριθμοι. Έτσι, στην περίπτωση που η ανάδραση εφαρμόζεται συνολικά στην κατασκευή (περίπτωση (β)), ο πιο ασθενής κρυπταλγόριθμος προστατεύεται από τον πιο ισχυρό. Αντίθετα, στην περίπτωση που εφαρμόζονται οι αναδράσεις χωριστά, ο αντίπαλος θα έχει τη δυνατότητα να επιτεθεί

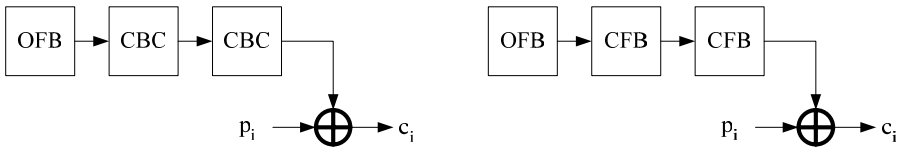
χωριστά στον πιο αδύναμο κρυπταλγόριθμο. Έτσι, αν τα κλειδιά προκύπτουν από κάποιον αλγόριθμο προγράμματος κλειδιών, ο αντίπαλος θα μπορέσει να ανακαλύψει το κλειδί του ασθενούς κρυπταλγόριθμου και στη συνέχεια θα χρησιμοποιήσει την πληροφορία αυτή για να επιτεθεί στο πρόγραμμα κλειδιών προκειμένου να ανακαλύψει το κλειδί του πιο ισχυρού κρυπταλγόριθμου.

Επιλογή των κλειδιών

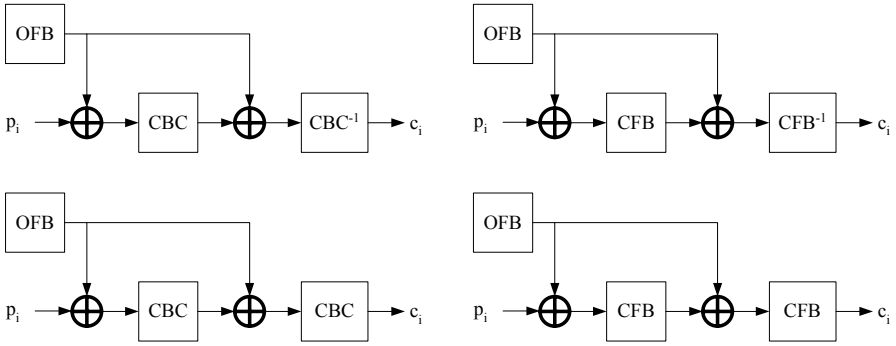
Όταν σε έναν τρόπο λειτουργίας υπάρχουν περισσότεροι από έναν κρυπταλγόριθμοι, απαιτούνται και περισσότερα από ένα κλειδιά. Πολλές φορές για λόγους ευκολίας χρησιμοποιείται το ίδιο κλειδί για όλους τους κρυπταλγόριθμους. Αυτό κρύβει και τον κίνδυνο που αναφέραμε στην προηγούμενη παράγραφο. Όταν χρησιμοποιείται το ίδιο κλειδί σε δύο ή περισσότερους κρυπταλγόριθμους, τότε ο αντίπαλος θα επιχειρήσει να εφαρμόσει κρυπτανάλυση στον πιο ασθενή από τους κρυπταλγόριθμους αυτούς. Παρόμοια, αν τα κλειδιά προκύπτουν από κάποιο αλγόριθμο δημιουργίας προγράμματος κλειδιών, ο αντίπαλος θα επιχειρήσει να ανακαλύψει το κλειδί που περιλαμβάνεται στο πιο ασθενές συστατικό του κρυπτοσυστήματος και στη συνέχεια θα επιτεθεί στον αλγόριθμο δημιουργίας του προγράμματος κλειδιών.

Πιθανές ασφαλείς κατασκευές

Ο Biham (1996) μελέτησε πολλούς συνδυασμούς των τυποποιημένων τρόπων λειτουργιών και κατέληξε σε ορισμένους οι οποίοι μπορούν να θεωρηθούν ασφαλείς με αρκετά μεγάλη πιθανότητα. Στο Σχήμα 5.11 παρατίθενται δύο τρόποι λειτουργίας οι οποίοι ισοδυναμούν με κρυπταλγόριθμο ροής. Στο Σχήμα 5.12 παριστάνονται τρόποι λειτουργίας για ισοδύναμο κρυπταλγόριθμο τμήματος. Με CBC^{-1} παριστάνεται ο τρόπος λειτουργίας CBC όπου ο αντίστοιχος κρυπταλγόριθμος τμήματος εκτελεί αποκρυπτογράφηση. Κάθε κρυπταλγόριθμος έχει διαφορετικό κλειδί.



Σχήμα 5.11 Ασφαλείς κατασκευές κρυπταλγόριθμου ροής



Σχήμα 5.12 Ασφαλείς κατασκευές κρυπταλγόριθμου τμήματος

Τριπλή κρυπτογράφηση

Η τριπλή κρυπτογράφηση αναλύεται ξεχωριστά, προκειμένου να επισημανθεί η μεγάλη διαφορά σε ασφάλεια από τη διπλή κρυπτογράφηση, η οποία είναι ευάλωτη στην επίθεση «συνάντησης στο ενδιάμεσο».

Έστω ένα κρυπτοσύστημα το οποίο αποτελείται από το κρυπτογραφικό γινόμενο:

$$e_{k_2}(e_{k_1}),$$

δηλαδή από την εφαρμογή ενός κρυπταλγόριθμου δύο φορές με δύο διαφορετικά κλειδιά. Έστω ότι το μέγεθος των κλειδιών είναι ίσο με k bits. Τότε, αν θεωρήσουμε ότι ο κρυπταλγόριθμος είναι πολύ ασφαλής και η μόνη γνωστή επίθεση είναι η εξαντλητική αναζήτηση, είναι λογικό να υποθέσουμε ότι αν χρησιμοποιήσουμε διπλή κρυπτογράφηση, το κρυπτοσύστημα που προκύπτει θα έχει κλειδοχώρο αναζήτησης ίσο με 2^{2k}, αφού τα επιτρεπτά κλειδιά θα είναι $2^k \times 2^k$. Ωστόσο, στην πραγματικότητα η αύξηση του κλειδοχώρου είναι ελάχιστη. Για την ακρίβεια, η εξαντλητική αναζήτηση αρκεί να εφαρμοστεί μόνον σε 2^{k+1} κλειδιά, χάριν της επίθεσης της ***συνάντησης στο ενδιάμεσο*** (meet in the middle attack).

Απαραίτητη προϋπόθεση για την επίθεση της συνάντησης στο ενδιάμεσο είναι ο αντίπαλος να έχει χώρο για να αποθηκεύει όλες τις κρυπτογραφήσεις που εκτελεί με τα διαφορετικά κλειδιά. Επίσης θεωρούμε ότι ο αντίπαλος έχει στην κατοχή του ένα ζευγάρι απλού κειμένου και του αντίστοιχου κρυπτοκειμένου (επίθεση με γνωστό απλό κείμενο).

Δεδομένου ότι η κρυπτογράφηση του απλού κειμένου είναι ισοδύναμη με την αποκρυπτογράφηση του κρυπτοκειμένου του, ο αντίπαλος αρχικά κρυπτογραφεί το απλό κείμενο εφαρμόζοντας μια μόνο φορά τον κρυπταλγόριθμο, με όλα τα δυνατά κλειδιά. Σε κάθε κρυπτογράφηση αποθηκεύει το αποτέλεσμα σε λίστα κρυπτοκειμένων με τέτοιον τρόπο, ώστε να γνωρίζει ποιο κλειδί χρησιμοποιήθηκε για την κρυπτογράφηση. Στη συνέχεια εκτελεί αποκρυπτογραφήσεις του αρχικού κρυπτοκειμένου με διαφορετικά κλειδιά. Για κάθε απλό κείμενο που προκύπτει,

ελέγχει αν αυτό βρίσκεται με τη μορφή κρυπτοκειμένου στη λίστα των κρυπτοκειμένων. Στην περίπτωση εύρεσης ισοδυναμίας, καταγράφονται τα δύο κλειδιά: το κλειδί της λίστας αντιστοιχεί στο κλειδί της πρώτης εφαρμογής του κρυπταλγόριθμου, ενώ το κλειδί της αποκρυπτογράφησης αντιστοιχεί στο κλειδί της δεύτερης εφαρμογής του κρυπταλγόριθμου. Αν βρεθούν παραπάνω από μια ισοδυναμίες, τότε απαιτείται και δεύτερο γνωστό απλό κείμενο.

Αν καταγράψουμε τον αριθμό των κρυπτογραφήσεων και αποκρυπτογραφήσεων στην παραπάνω διαδικασία, προκύπτει ότι εκτελούνται συνολικά 2×2^k κρυπτογραφήσεις και αποκρυπτογραφήσεις. Δηλαδή η χρησιμοποίηση διπλής κρυπτογράφησης δεν αυξάνει σημαντικά την ασφάλεια. Έτσι λέμε ότι ενώ το ***πραγματικό κλειδί*** έχει μήκος $2k$ bits, το ***ενεργό κλειδί*** έχει μήκος $k+1$ bits.

Επαγωγικά, κατά την τριπλή κρυπτογράφηση, αν χρησιμοποιηθούν τρία κλειδιά, το ενεργό κλειδί έχει μήκος $2k+1$ bits, λόγω της επίθεσης της συνάντησης στο ενδιάμεσο. Στην περίπτωση της τριπλής κρυπτογράφησης, ενδιάμεσο θεωρείται είτε το σημείο κατά την πρώτη κρυπτογράφηση, ή το σημείο κατά τη δεύτερη κρυπτογράφηση, οπότε και ο αντίπαλος θα πρέπει να κατασκευάσει τη λίστα των κρυπτοκειμένων και στη συνέχεια να εκτελέσει όλες τις αποκρυπτογραφήσεις, $d_{k_2}(d_{k_3})$, προκειμένου να βρει το απλό κείμενο που θα ισοδυναμεί με κάποιο από τα κρυπτοκείμενα της λίστας.

Επομένως, επειδή το ενεργό κλειδί κατά την τριπλή κρυπτογράφηση είναι περίπου ίσο με το μήκος δύο κλειδιών, η τριπλή κρυπτογράφηση ορίζεται ως:

$$p = e_{k_1}(d_{k_2}(e_{k_1}(c))),$$

δηλαδή το απλό κείμενο κρυπτογραφείται με το πρώτο κλειδί, στη συνέχεια αποκρυπτογραφείται με το δεύτερο κλειδί και τέλος κρυπτογραφείται με το πρώτο κλειδί. Η συγκεκριμένη τριπλή κρυπτογράφηση συμβολίζεται με EDE (Encrypt-Decrypt-Encrypt). Η δεύτερη πράξη στο κρυπτογραφικό γινόμενο έχει καθιερωθεί να είναι αποκρυπτογράφηση για λόγους συμβατότητας. Όταν τα δύο κλειδιά είναι ίσα, τότε το κρυπτοσύστημα ισοδυναμεί με απλή κρυπτογράφηση.

5.2.2. Αλγόριθμοι προγράμματος κλειδιών

Στους κρυπταλγόριθμους τμήματος που βασίζονται σε κρυπτογραφικό γινόμενο μιας ή περισσοτέρων κρυπτογραφικών πράξεων, απαιτείται το πρόγραμμα κλειδιών. Ο κάθε παράγοντας του κρυπτογραφικού γινομένου αποτελεί το γύρο του κρυπταλγόριθμου και απαιτεί κάποιο από τα κλειδιά του προγράμματος κλειδιών. Το πρόγραμμα κλειδιών είναι ένας αλγόριθμος που δέχεται ένα αρχικό κλειδί και με βάση αυτό δημιουργεί ένα σύνολο κλειδιών, ανάλογα με τις απαιτήσεις του κρυπταλγόριθμου γινομένου.

Όπως έχει τονιστεί επανειλημμένα σε διάφορα σημεία του βιβλίου, η ασφάλεια ενός κρυπτοσυστήματος εξαρτάται από το κλειδί. Επομένως η διαδικασία δημιουργίας του προγράμματος κλειδιών θα πρέπει να βασίζεται σε αρχές οι ο-

ποίες να εγγυώνται την ασφάλεια του κρυπτοσυστήματος, ή καλύτερα, να μην εισάγουν επιπλέον αδυναμίες στο κρυπτοσύστημα, λόγω κακού σχεδιασμού.

Ο Knudsen διέκρινε δύο κατηγορίες προγράμματος κλειδιών, τα ***ασθενή*** και τα ***δυνατά*** προγράμματα κλειδιών.

ΟΡΙΣΜΟΣ 5.1 – Ένα πρόγραμμα κλειδιών είναι ***ασθενές***, όταν υπάρχουν απλές σχέσεις f, g_1 και g_2 μεταξύ του κλειδιού, του απλού κειμένου και του κρυπτοκειμένου σε ένα κρυπτοσύστημα, έτσι ώστε:

$$e_k(p) = e_{f(k)}(g_1(p,k)) = g_2(c,k),$$

όπου e_k, ο αλγόριθμος κρυπτογράφησης γινομένου.

Από τον ορισμό προκύπτει ότι η δύναμη ενός προγράμματος κλειδιών εξαρτάται από τον κρυπταλγόριθμο. Ένα πρόγραμμα κλειδιών μπορεί να είναι ασθενές σε κάποιον κρυπταλγόριθμο αλλά ισχυρό σε κάποιον άλλον. Όταν συμβαίνει κάτι τέτοιο μπορούμε να συμπεράνουμε ότι το δεύτερο κρυπτοσύστημα είναι καλύτερα σχεδιασμένο από το πρώτο. Στο σχεδιασμό συμπεριλαμβάνεται και η επιλογή του προγράμματος κλειδιών.

Προκειμένου να ολοκληρώσουμε τον παραπάνω ορισμό, θα πρέπει να ορίσουμε και την έννοια της απλής σχέσης.

ΟΡΙΣΜΟΣ 5.2 – Οι σχέσεις f, g_1 και g_2 μεταξύ του κλειδιού, του απλού κειμένου και του κρυπτοκειμένου σε ένα κρυπτοσύστημα είναι ***απλές***, όταν η συνολική πολυπλοκότητα της εφαρμογής των τριών αυτών συναρτήσεων, είναι μικρότερη από την πολυπλοκότητα της εφαρμογής του αλγόριθμου κρυπτογράφησης e_k.

Η ύπαρξη των απλών σχέσεων επιταχύνει τη διαδικασία αναζήτησης του κλειδιού κατά την κρυπτανάλυση, αφού ο αντίπαλος μπορεί να εξετάζει τα κλειδιά μέσω των απλών σχέσεων όπου ο κύκλος τους πραγματοποιείται ταχύτερα από την κρυπτογράφηση. Επιπλέον, η ύπαρξη απλών σχέσεων μπορεί να μειώσει και τον κλειδοχώρο, με αποτέλεσμα η εξαντλητική αναζήτηση να καταστεί εφικτή για τον αντίπαλο.

Καθολικά δυνατά προγράμματα κλειδιών

Μια μέθοδος για τη δημιουργία δυνατών προγραμμάτων κλειδιών είναι η χρησιμοποίηση κρυπτογραφικών μονόδρομων hash συναρτήσεων. Η δυσκολία που αποδίδεται στη μονόδρομη hash όσον αφορά τον υπολογισμό της αντίστροφης σχέσης της συνάρτησης, μπορεί να χρησιμοποιηθεί με τέτοιον τρόπο ώστε η λίστα των κλειδιών ενός προγράμματος να είναι υπολογιστικώς ανεξάρτητα μεταξύ τους.

Ένα δυνατό πρόγραμμα κλειδιών μπορεί να κατασκευαστεί ως εξής. Έστω $k \in \{0,1\}^a$ το αρχικό κλειδί του κρυπτοσυστήματος. Έστω το πρόγραμμα κλειδιών $\{k_1,k_2,\ldots,k_r\}$ που αποτελείται από r κλειδιά, όπου το κάθε κλειδί ανήκει στο $\{0,1\}^b$. Έστω s: $\{0,1\}^* \rightarrow \{0,1\}^b$ μια κρυπτογραφική μονόδρομη hash. Τότε το κάθε κλειδί k_i του προγράμματος κλειδιών μπορεί να ορισθεί από την:

$$k_i = s(k \,||\, i)$$

ή από την

$$k_i = s(i \,||\, k),$$

για $1 \le i \le r$. Η πρώτη σχέση ορίζει διάταξη μυστικού προθέματος, ενώ η δεύτερη σχέση ορίζει διάταξη μυστικού προσφύματος, αφού το κλειδί είναι το μυστικό ενώ ο γύρος i είναι δημόσια πληροφορία. Λόγω των κρυπτογραφικών ιδιοτήτων της μονόδρομης hash, μπορούμε να υποθέσουμε ότι είναι αδύνατο να βρεθούν απλές σχέσεις, διότι αυτό θα κατέρριπτε την υπόθεση (ή απαίτηση) ότι η hash είναι ανθεκτική σε συγκρούσεις.

Το μειονέκτημα της χρήσης κρυπτογραφικών μονόδρομων hash ως αλγόριθμων προγράμματος κλειδιών, είναι οι σχετικά μεγάλες απαιτήσεις τόσο σε χώρο, όσο και σε όγκο υπολογισμών, σε σχέση με απλούστερους αλγόριθμους προγράμματος κλειδιών που μπορεί να αποτελούνται, για παράδειγμα, από μια σειρά κυκλικών ολισθήσεων του αρχικού κλειδιού. Ωστόσο, σε εφαρμογές όπου το ρίσκο είναι υψηλό, δεχόμαστε να θυσιάσουμε ταχύτητα για περισσότερη ασφάλεια.

5.2.3. Γραμμική και διαφορική κρυπτανάλυση

Η γραμμική και η διαφορική κρυπτανάλυση αποτελούν τις δύο βασικές κατηγορίες κρυπτανάλυσης που μπορούν να εφαρμοστούν στους κρυπταλγόριθμους τμήματος. Ο σχεδιασμός σύγχρονων κρυπταλγόριθμων τμήματος προβλέπει αντίσταση στη γραμμική και διαφορική κρυπτανάλυση. Αν και στο μέλλον είναι πιθανό να εμφανισθούν καινούργιες κατηγορίες επιθέσεων, είναι εξίσου πιθανό αυτές οι επιθέσεις να βασίζονται στις αρχές της γραμμικής και διαφορικής κρυπτανάλυσης.

Γραμμική κρυπτανάλυση

Η γραμμική κρυπτανάλυση αναπτύχθηκε από τον Matsui και είναι επίθεση που εφαρμόζεται σε κρυπταλγόριθμους γινομένου. Η βασική ιδέα της γραμμικής κρυπτανάλυσης είναι η έκφραση ορισμένων bits της εισόδου, ορισμένων bits της εξόδου και ορισμένων bits του κλειδιού με γραμμική προσέγγιση. Ο όρος προσέγγιση αναφέρεται στο γεγονός ότι η γραμμική σχέση των τριών συνόλων από bits ισχύει με κάποια πιθανότητα. Ένα κρυπτοσύστημα είναι ευάλωτο στη γραμμική κρυπτανάλυση, όταν βρεθεί γραμμική σχέση που ισχύει με πιθανότητα διαφορετική του 0.5. Μάλιστα, όσο πιο πολύ απέχει η πιθανότητα αυτή από το 0.5 τόσο πιο ευάλωτο είναι το κρυπτοσύστημα στη γραμμική κρυπτανάλυση. Αντίθετα, για γραμμικές σχέσεις όπου η πιθανότητα να ισχύουν ή να μην ισχύουν είναι «50-50», η γραμμική κρυπτανάλυση αδυνατεί να ολοκληρώσει με επιτυχία την επίθεση στο κρυπτοσύστημα.

Οι γραμμικές σχέσεις είναι της μορφής:

$$\boldsymbol{p}[i_1, i_2, ..., i_a] \oplus \boldsymbol{c}[j_1, j_2, ..., j_b] = \boldsymbol{k}[k_1, k_2, ..., k_c],$$

όπου $\boldsymbol{p}[i_1, i_2, \ldots, i_a]$ είναι τα bits στις θέσεις $i_1, i_2, \ldots, i_a$ του απλού κειμένου συνδυασμένα με αποκλειστική διάζευξη, ενώ $\boldsymbol{c}[j_1, j_2, \ldots, j_b]$ και $\boldsymbol{k}[k_1, k_2, \ldots, k_c]$ είναι τα επιλεγμένα bits του κρυπτοκειμένου και του κλειδιού αντίστοιχα.

Καθότι σε κάθε γύρο του κρυπταλγόριθμου υπάρχει το στάδιο στο οποίο εφαρμόζεται ένας μη γραμμικός μετασχηματισμός (όπως για παράδειγμα τα κουτιά αντικατάστασης που περιγράψαμε στο προηγούμενο κεφάλαιο), έπεται ότι η επιτυχία εύρεσης αποτελεσματικής γραμμικής σχέσης εξαρτάται από την επιτυχία περιγραφής του μη γραμμικού μετασχηματισμού του κάθε γύρου με γραμμική σχέση. Επίσης, η πιθανότητα εύρεσης αποτελεσματικής σχέσης είναι μεγαλύτερη για κλειδιά του τελευταίου γύρου του κρυπταλγόριθμου, από τα κλειδιά των προηγουμένων γύρων.

Έτσι η προσέγγιση της γραμμικής κρυπτανάλυσης είναι αρχικά η εξέταση των μη γραμμικών μετασχηματισμών του τελευταίου γύρου κρυπτογράφησης. Η μεθοδολογία εξαγωγής των γραμμικών σχέσεων εξαρτάται από το είδος των μη γραμμικών μετασχηματισμών. Η συντριπτική πλειοψηφία δημιουργίας μη γραμμικότητας στους συμμετρικούς κρυπταλγόριθμους τμήματος αποδίδεται στα κουτιά αντικατάστασης.

Στη συνέχεια, έχοντας αναπτύξει μια υποψήφια γραμμική προσέγγιση, κρυπτογραφούμε έναν μεγάλο αριθμό απλών κειμένων με το κρυπτοσύστημα του οποίου το κλειδί θεωρείται άγνωστο. Αυτή η υπόθεση επίθεσης είναι η κρυπτανάλυση με επιλεγμένο απλό κείμενο, όπου ο αντίπαλος έχει πρόσβαση στο κρυπτοσύστημα, αλλά δεν έχει γνώση του κλειδιού. Για κάθε ζευγάρι απλού κειμένου και κρυπτοκειμένου, επιλέγουμε τα bits που ορίζονται από τη γραμμική προσέγγιση και τα εφαρμόζουμε σε αυτήν. Το αποτέλεσμα του αριστερού τμήματος της γραμμικής προσέγγισης θα είναι ένα bit, **0** ή **1**. Για την τιμή αυτή, υπολογίζουμε όλα τα πιθανά υποψήφια bits των κλειδιών που ορίζονται στη δεξιά πλευρά της γραμμικής προσέγγισης. Όταν το υποσύνολο των bits του κλειδιού που ορίζονται στη γραμμική προσέγγιση υπάρχει και στο κλειδί κρυπτογράφησης, τότε θεωρούμε ότι έχουμε ένα «ορθό ζευγάρι» απλού κειμένου και κρυπτοκειμένου, ενώ στην αντίθετη περίπτωση, θεωρούμε ότι έχουμε ένα «λάθος ζευγάρι». Στο τέλος της διαδικασίας υπολογίζουμε τη συχνότητα εμφάνισης ορθών ζευγαριών, και ελπίζουμε να είναι διαφορετική και όσο το δυνατόν πιο μακριά από το 1/2. Δηλαδή, αν στις μισές περιπτώσεις είχαμε ορθά ζευγάρια, τότε η γραμμική προσέγγιση δεν μπορεί να μας βοηθήσει να εκτελέσουμε γραμμική κρυπτανάλυση. Ισοδύναμα, αυτό σημαίνει ότι η γραμμική προσέγγιση δεν είναι σε θέση να διαχωρίσει το κρυπτοσύστημα από μια πηγή τυχαίων αριθμών.

Η διαδικασία εύρεσης γραμμικών σχέσεων μπορεί να απλοποιηθεί εφόσον κατέχουμε τις προδιαγραφές του κρυπτοσυστήματος. Η ευκαιρία απλοποίησης αποδίδεται στο λήμμα συσσωρεύσεως (piling-up lemma) που θα αναπτύξουμε στη συνέχεια.

ΟΡΙΣΜΟΣ 5.3 – Έστω μια τυχαία δυαδική μεταβλητή X, με πιθανότητες $\Pr\{X = 0\} = p$ και $\Pr\{X = 1\} = 1 - p$. Η ποσότητα:

$$\varepsilon = p - \frac{1}{2}$$

ονομάζεται ***πόλωση*** της μεταβλητής X.

Είναι φανερό ότι

$$\Pr\{X = 0\} = \frac{1}{2} + \varepsilon$$

και

$$\Pr\{X = 1\} = \frac{1}{2} - \varepsilon ,$$

ενώ οι τιμές της πόλωσης βρίσκονται στο διάστημα

$$-\frac{1}{2} \le \varepsilon \le \frac{1}{2} .$$

Στη γραμμική κρυπτανάλυση επιδιώκουμε να βρούμε γραμμικές σχέσεις με μεγάλη πόλωση. Το λήμμα συσσωρεύσεως που διατυπώνεται στη συνέχεια είναι η θεμελιώδης σχέση της γραμμικής κρυπτανάλυσης η οποία μας βοηθάει στην εύρεση γραμμικών σχέσεων με μεγάλη πόλωση.

Λημμα 5.1 – Έστω οι ανεξάρτητες τυχαίες μεταβλητές X_1, X_2, …, X_n με πολώσεις ε_1, ε_2,…, ε_n αντίστοιχα. Τότε η πόλωση της μεταβλητής $X_1 \oplus X_2 \oplus \ldots \oplus X_n$ θα είναι:

$$\varepsilon_{1,2,\ldots,n} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i .$$

Απόδειξη Η σχέση αποδεικνύεται με τη μέθοδο της επαγωγής. Αρχικά παρατηρούμε ότι για $n = 1$, η παραπάνω σχέση ισχύει (ταυτότητα). Έστω ότι ισχύει και για $n = k$. Θα αποδείξουμε ότι ισχύει για $n = k + 1$.

Αν η πιθανότητα για τη δυαδική μεταβλητή X_i είναι p_i, τέτοια ώστε $\Pr\{X_i = 0\} = p_i$ και $\Pr\{X_i = 1\} = 1 - p_i$, τότε για δύο οποιεσδήποτε δυαδικές μεταβλητές X_i και X_j οι οποίες είναι ανεξάρτητες μεταξύ τους ισχύουν:

$$\Pr\{X_i = 0, X_j = 0\} = p_i p_j ,$$
$$\Pr\{X_i = 1, X_j = 0\} = (1 - p_i) p_j ,$$
$$\Pr\{X_i = 0, X_j = 1\} = p_i (1 - p_j) ,$$
$$\Pr\{X_i = 1, X_j = 1\} = (1 - p_i)(1 - p_j) .$$

Συνεπώς για τη μεταβλητή $X_i \oplus X_j$ θα είναι:

$$\Pr\{X_i \oplus X_j = 0\} = p_i p_j + (1-p_i)(1-p_j)$$
$$= (\frac{1}{2}+\varepsilon_i)(\frac{1}{2}+\varepsilon_j) + (\frac{1}{2}-\varepsilon_i)(\frac{1}{2}-\varepsilon_j)$$

Επομένως για τη μεταβλητή $X_1 \oplus X_2 \oplus \ldots \oplus X_{k+1}$ θα ισχύει:

$$\Pr\{(X_1 \oplus X_2 \oplus \ldots \oplus X_k) \oplus X_{k+1} = 0\}$$
$$= \left(\frac{1}{2} + 2^{k-1}\prod_{i=1}^{k}\varepsilon_i\right)\left(\frac{1}{2}+\varepsilon_{k+1}\right) + \left(\frac{1}{2} - 2^{k-1}\prod_{i=1}^{k}\varepsilon_i\right)\left(\frac{1}{2}-\varepsilon_{k+1}\right)$$
$$= \frac{1}{2} + 2^k \prod_{i=1}^{k+1}\varepsilon_i$$

Από την τελευταία σχέση προκύπτει ότι

$$\varepsilon_{1,2,..,k+1} = 2^k \prod_{i=1}^{k+1}\varepsilon_i \ .$$

Από το παραπάνω λήμμα προκύπτει ότι όλες οι μεταβλητές οι οποίες συμμετέχουν στη γραμμική προσέγγιση θα πρέπει να έχουν πόλωση διάφορη του μηδενός, γιατί στην αντίθετη περίπτωση η γραμμική προσέγγιση θα έχει μηδενική πόλωση και δε θα μπορεί να χρησιμοποιηθεί σε γραμμική κρυπτανάλυση. Θα πρέπει επίσης να τονισθεί ότι η σχέση ισχύει στην περίπτωση όπου οι μεταβλητές είναι ανεξάρτητες.

Εφαρμογή σε κουτιά αντικατάστασης

Τα κουτιά αντικατάστασης χρησιμοποιούνται για να εισάγουν σε έναν κρυπταλγόριθμο μη γραμμικότητα. Επομένως η πρόκληση που καλείται ο αντίπαλος να αντιμετωπίσει, είναι να μπορέσει να περιγράψει με γραμμικές σχέσεις τα κουτιά αντικατάστασης. Ο Matsui περιέγραψε ένα συστηματικό τρόπο εύρεσης γραμμικών προσεγγίσεων με μέγιστη πόλωση στα κουτιά αντικατάστασης του κρυπταλγόριθμου DES, αλλά η μέθοδος αυτή μπορεί να εφαρμοσθεί σε οποιαδήποτε κουτιά αντικατάστασης.

Έστω το κουτί αντικατάστασης S: $\{0, 1\}^m \rightarrow \{0, 1\}^n$. Το κουτί δέχεται m bits εισόδου και παράγει στην έξοδο δυαδικές λέξεις των n bits. Αν το κάθε ένα από τα bits θεωρηθεί ως τυχαία μεταβλητή, θα έχουμε συνολικά $m + n$ τυχαίες μεταβλητές. Από αυτές, οι μεταβλητές που αντιστοιχούν στα bits της εισόδου θεωρούνται ανεξάρτητες μεταξύ τους και με πόλωση μηδενική (θεωρούμε ότι η είσοδος παίρνει όλες τις πιθανές λέξεις από το σύνολο $\{0, 1\}^m$). Αντίθετα, κατά την έξοδο, οι μεταβλητές που αντιστοιχούν στα bits της εισόδου εξαρτώνται τόσο από τα bits της εισόδου, όσο και από τα υπόλοιπα bits. Η εξάρτηση μπορεί να είναι ισχυρή ή ασθενής (ή μηδενική). Έστω ότι στα bits εισόδου αντιστοιχούν οι μεταβλητές P_1,

P_2, …, P_m και στα bits εξόδου αντιστοιχούν οι μεταβλητές C_1, C_2, …, C_n. Για τις μεταβλητές της εισόδου θα ισχύει:

$$\Pr\{P_1 = x_1, P_2 = x_2, ..., P_m = x_m\} = 2^{-m}$$

όπου $x_i \in \{0, 1\}$, για $1 \le i \le m$. Δηλαδή, οποιοσδήποτε συνδυασμός των bits της εισόδου έχει την ίδια πιθανότητα, ανάλογη του μεγέθους m.
Έστω ότι $x_i \in \{0, 1\}$, για $1 \le i \le m$ και $y_i \in \{0, 1\}$, για $1 \le i \le n$. Τότε:

$$\Pr\{P_1 = x_1, P_2 = x_2, ..., P_m = x_m, C_1 = y_1, C_2 = y_2, ..., C_n = y_n\} = 0,$$

στην περίπτωση που $S(x_1, x_2, ..., x_m) \neq (y_1, y_2, ..., y_n)$, και

$$\begin{aligned}
&\Pr\{P_1 = x_1, P_2 = x_2, ..., P_m = x_m, C_1 = y_1, C_2 = y_2, ..., C_n = y_n\} = \\
&\Pr\{P_1 = x_1, P_2 = x_2, ..., P_m = x_m\} \times \\
&\Pr\{C_1 = y_1, C_2 = y_2, ..., C_n = y_n \mid P_1 = x_1, P_2 = x_2, ..., P_m = x_m\} = \\
&2^{-m} \times 1 = 2^{-m}
\end{aligned}$$

στην περίπτωση που $S(x_1, x_2, \ldots, x_m) = (y_1, y_2, \ldots, y_n)$. Η σχέση προκύπτει από τον κανόνα του Bayes, της θεωρίας των πιθανοτήτων.

Έχοντας υπολογίσει τις παραπάνω ποσότητες, μπορούμε πλέον να υπολογίσουμε οποιονδήποτε γραμμικό συνδυασμό των bits εισόδου με τα bits της εξόδου. Ο συνολικός αριθμός γραμμικών σχέσεων είναι 2^{m+n}. Εκφράζοντας τις γραμμικές σχέσεις στη μορφή:

$$\left(\bigoplus_{i=1}^{m} a_i P_i\right) \oplus \left(\bigoplus_{i=1}^{n} b_i C_i\right),$$

όπου τα a_i και $b_i \in \{0,1\}$ καθορίζουν τον συνδυασμό των bits εισόδου και εξόδου που συμμετέχουν στη γραμμική σχέση, ο Matsui όρισε την ποσότητα $NS(m,n)$ ως εξής.

ΟΡΙΣΜΟΣ 5.4 – Για δεδομένο κουτί αντικατάστασης S:$\{0, 1\}^m \rightarrow \{0, 1\}^n$**,** και με δείκτες $a_i \in \{0, 1\}$, $1 \le i \le m$ και $b_i \in \{0, 1\}$, $1 \le i \le n$, ορίζεται η ποσότητα $NS(a,b)$ ως

$$\begin{aligned}
&N\,S(a,b) = \\
&= \left|\left\{\boldsymbol{p} : 0 \le (\boldsymbol{p})_{10} \le 2^m - 1, (P_1 P_2 ... P_m) = \boldsymbol{p}, (C_1 C_2 ... C_n) = S(\boldsymbol{p}), \bigoplus_{i=1}^{m} a_i P_i = \bigoplus_{i=1}^{n} b_i C_i\right\}\right|
\end{aligned}$$

όπου $(\boldsymbol{p})_{10}$ η έκφραση της ποσότητας $\boldsymbol{p}$ στο δεκαδικό σύστημα, και $a=(a_1 a_2 \ldots a_m)_{10}$, $b=(b_1 b_2 \ldots b_n)_{10}$.

Δηλαδή, για κάθε συνδυασμό bits εισόδου με bits εξόδου, η ποσότητα $NS(a,b)$ φανερώνει τη σχετική συχνότητα όπου η αποκλειστική διάζευξη των επιλεγμένων

bits της εισόδου είναι ίση με την αποκλειστική διάζευξη των επιλεγμένων bits της εξόδου. Η πόλωση προκύπτει άμεσα από την ποσότητα αυτή:

$$\varepsilon(a,b) = \frac{N\,S(a,b) - 2^{m-1}}{2^m}.$$

Η χρησιμότερη γραμμική προσέγγιση είναι εκείνη στην οποία η ποσότητα $|\,N\,S(a,b) - 2^{m-1}\,|$ είναι μέγιστη.

ΠΑΡΑΔΕΙΓΜΑ 5.2 – Εύρεση βέλτιστης γραμμικής προσέγγισης κουτιού αντικατάστασης. Έστω το κουτί S_4: $\{0, 1\}^4 \rightarrow \{0, 1\}^3$ που ορίζεται από τον Πίνακα 5.1. Θεωρούμε τον δείκτη a ο οποίος ορίζει τις δυαδικές μεταβλητές της εισόδου και τον δείκτη b ο οποίος ορίζει τις δυαδικές μεταβλητές της εξόδου. Ο δείκτης a παίρνει τιμές από 0 έως 15 ενώ ο b παίρνει τιμές από 0 έως 7. Η δυαδική απεικόνιση των δεικτών φανερώνει τα επιλεγμένα bits. Για παράδειγμα, αν $a = (5)_{10} = (0101)_2$ ο δείκτης αντιστοιχεί στο άθροισμα $P_1 \oplus P_3$. Με αυτήν την αναπαράσταση κατασκευάζουμε έναν δισδιάστατο πίνακα (Πίνακας 5.2), όπου οι γραμμές αντιστοιχούν στην είσοδο a, ενώ οι στήλες αντιστοιχούν στην έξοδο b.

P_1	P_2	P_3	P_4	C_1	C_2	C_3
0	0	0	0	1	0	1
0	0	0	1	1	1	0
0	0	1	0	0	0	0
0	0	1	1	1	1	0
0	1	0	0	0	1	1
0	1	0	1	1	1	0
0	1	1	0	1	1	0
0	1	1	1	1	1	1
1	0	0	0	0	0	0
1	0	0	1	0	1	1
1	0	1	0	1	0	1
1	0	1	1	0	1	0
1	1	0	0	1	1	0
1	1	0	1	1	0	1
1	1	1	0	0	1	1
1	1	1	1	1	0	1

Πίνακας 5.1 Πίνακας αληθείας του S_4

a \ b	0	1	2	3	4	5	6	7
0	16	8	8	8	8	8	8	8
1	8	6	6	12	10	6	8	8
2	8	10	10	8	10	10	8	8
3	8	6	10	8	8	8	6	10
4	8	8	8	8	8	6	8	10
5	8	8	8	4	6	8	6	8
6	8	8	8	8	6	8	10	8
7	8	4	8	8	8	10	4	6
8	8	10	10	8	8	8	10	10
9	8	10	10	4	6	10	8	8
10	8	6	14	8	6	14	8	8
11	8	10	6	8	8	8	10	6
12	8	8	8	8	8	10	8	6
13	8	8	8	4	2	8	10	8
14	8	8	8	8	10	8	6	8
15	8	4	8	8	8	6	4	10

Πίνακας 5.2 Τιμές της $N S_4(a,b)$

Όπως φαίνεται από τον παραπάνω πίνακα, υπάρχουν αρκετές γραμμικές προσεγγίσεις οι οποίες απέχουν από τη μέση τιμή 8. Πιο συγκεκριμένα, η μέγιστη απόσταση είναι ίση με 6, και συμβαίνει για τις τιμές (10,2), (10,5) και (13,4). Επομένως οι βέλτιστες γραμμικές σχέσεις που προκύπτουν είναι οι ακόλουθες:

$$P_2 \oplus P_4 = C_2,$$
$$P_2 \oplus P_4 = C_1 \oplus C_3 \text{ και}$$
$$P_1 \oplus P_3 \oplus P_4 = C_3,$$

με πιθανότητα 7/8 οι δύο πρώτες και 1/8 η τρίτη.

Διαφορική κρυπτανάλυση

Η διαφορική κρυπτανάλυση αναπτύχθηκε από τους Biham και Shamir το 1991. Η διαφορική κρυπτανάλυση εξετάζει τις διαφορές απλού κειμένου και τις διαφορές κρυπτοκειμένου, αντί τα καθαυτά απλά κείμενα και κρυπτοκείμενα. Η διαφορά δύο απλών κειμένων ορίζεται από την αποκλειστική διάζευξη των κειμένων αυτών, ενώ αντίστοιχα η διαφορά δύο κρυπτοκειμένων ορίζεται από την αποκλειστική διάζευξη των κρυπτοκειμένων.

Έστω x και x^* δύο δυαδικές λέξεις μεγέθους m bits. Η διαφορά τους συμβολίζεται με x' και ορίζεται από την

$$x' = x \oplus x^*,$$

η οποία είναι δυαδική λέξη μεγέθους m bits. Η διαφορική κρυπτανάλυση βασίζεται στο γεγονός ότι η κατανομή των διαφορών c' του κρυπτοκειμένου δεν είναι ομοιόμορφη, αλλά ορισμένες διαφορές εμφανίζονται περισσότερο από άλλες διαφορές και η κατανομή εξαρτάται από το κλειδί. Η επιτυχία της διαφορικής κρυπτανάλυσης μπορεί να μετρηθεί με την ποσότητα του διαφορικού χαρακτηριστικού (differential characteristic), που θα παρουσιάσουμε στη συνέχεια.

Έστω ένα κρυπτοσύστημα με r γύρους, όπου σε κάθε γύρο εφαρμόζεται ο μετασχηματισμός που ορίζεται από την πράξη:

$$c_i = e_{k_i}(c_{i-1}),$$

με $1 < i \leq r$, και $c_0 = p$. Θεωρούμε αρχικά ότι το κρυπτοσύστημα αποτελείται από έναν μόνο γύρο, με είσοδο x και έξοδο y, έτσι ώστε:

$y = e_k(x)$.

Έστω η διαφορά x'. Η διαφορά αυτή μπορεί να επιτευχθεί με 2^m ζευγάρια δυαδικών λέξεων μεγέθους m bits.

ΠΑΡΑΔΕΙΓΜΑ 5.3 – Έστω η διαφορά $x' = \{1101\}$. Τα ζευγάρια x και x^* που μπορούν να παράγουν τη διαφορά αυτή είναι τα ακόλουθα:

(0000,1101), (0001,1100) ,(0010,1111) ,(0011,1110)
(0100,1001), (0101,1000) ,(0110,1011) ,(0111,1010)
(1000,0101), (1001,0100) ,(1010,0111) ,(1011,0110)
(1100,0001), (1101,0000) ,(1110,0011) ,(1111,0010).

Όταν όμως η κάθε δυαδική λέξη του συνόλου των ζευγαριών εισόδου που αντιστοιχούν στη σταθερή διαφορά x' εισαχθεί στην κρυπτογραφική πράξη $e_k(x)$, το αποτέλεσμα δεν θα είναι μια εξίσου σταθερή διαφορά.

ΟΡΙΣΜΟΣ 5.5 – Έστω η διαφορά εισόδου x' στο κρυπτοσύστημα ενός γύρου, με κρυπτογραφική πράξη e_k. Η σχετική συχνότητα εμφάνισης της διαφοράς εξόδου $y' \in \{0, 1\}^m$, θα είναι ίση με $N_D e_k(x', y')$, η οποία ορίζεται από την:

$$N_D e_k(x', y') = |\{x, x^* : 0 \leq x \leq 2^m - 1,\ x^* = x \oplus x',\ e_k(x) \oplus e_k(x^*) = y'\}|$$

Από τον ορισμό της $N_D e_k(x', y')$ μπορούμε να υπολογίσουμε την πιθανότητα εμφάνισης κάποιας εξόδου διαφοράς y' δεδομένης εισόδου διαφοράς x':

$$\Pr\{y' \mid x'\} = \frac{N_D e_k(x', y')}{2^m},$$

δηλαδή, η πιθανότητα να εμφανισθεί στη έξοδο η διαφορά y' δεδομένου ότι η διαφορά στην είσοδο είναι ίση με x', είναι ίση με τον αριθμό εμφανίσεων $N_D e_k(x', y')$, προς τον αριθμό όλων των πιθανών επιτρεπτών διαφορών. Το ζευγάρι (x', y') ονο-

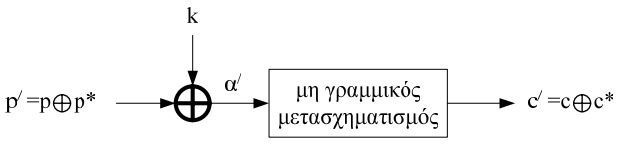
μάζεται ***διαφορικό χαρακτηριστικό*** και συμβολίζεται με $\boldsymbol{\Omega} = (\Omega_p, \Omega_C)$, ενώ η πιθανότητα του διαφορικού χαρακτηριστικού συμβολίζεται με $p^{\boldsymbol{\Omega}}$.

Η σημαντική ιδιότητα των διαφορικών χαρακτηριστικών φαίνεται στο κρυπτογραφικό γινόμενο δύο η περισσοτέρων κρυπτογραφικών πράξεων. Έστω το κρυπτοσύστημα το οποίο αποτελείται από δύο γύρους της e_k, όπου ο κάθε γύρος καθορίζεται από το διαφορετικό κλειδί, δηλαδή e_{k_1} και e_{k_2}. Τότε, αν το διαφορικό χαρακτηριστικό του πρώτου γύρου $\boldsymbol{\Omega}^1 = (\Omega_p, \Omega_\Lambda)$ έχει πιθανότητα $p^{\boldsymbol{\Omega}^1}$ και το διαφορικό χαρακτηριστικό του δευτέρου γύρου $\boldsymbol{\Omega}^2 = (\Omega_\Lambda, \Omega_C)$ έχει πιθανότητα $p^{\boldsymbol{\Omega}^2}$, το διαφορικό χαρακτηριστικό του συνολικού κρυπτοσυστήματος των δύο γύρων $\boldsymbol{\Omega} = (\Omega_p,\Omega_C)$ θα έχει πιθανότητα $p^{\boldsymbol{\Omega}} = p^{\boldsymbol{\Omega}^1} \times p^{\boldsymbol{\Omega}^2}$. Η σχέση ορίζεται επαγωγικά για περισσότερους από δύο όρους.

Η πρόκληση που καλείται να αντιμετωπίσει ο αντίπαλος σε κρυπτοσύστημα πολλών γύρων, είναι να επιδιώξει να εμφανίσει τις σωστές διαφορές στην είσοδο κάθε γύρου, με χειρισμό της διαφοράς της εισόδου του πρώτου γύρου. Για τα συμμετρικά κρυπτοσυστήματα τμήματος που βασίζονται σε δίκτυα Feistel, υπάρχει τρόπος να ελέγχονται αποτελεσματικά οι διαφορές στα διάφορα στάδια, για περιορισμένο αριθμό γύρων.

Η πλειοψηφία των συμμετρικών κρυπταλγόριθμων τμήματος χρησιμοποιεί κουτιά αντικατάστασης για να εισάγει μη γραμμικότητα στον κρυπταλγόριθμο. Μια δεύτερη κοινή πρακτική είναι η ανάμειξη των bits του κλειδιού με τα bits εισόδου του γύρου πριν από την εφαρμογή της μη γραμμικότητας. Αυτή η πρακτική έχει ως σκοπό την προστασία της μυστικότητας των κλειδιών. Στην περίπτωση όπου τα κλειδιά εφαρμόζονταν μετά από το μη γραμμικό βήμα, θα υπήρχε μεγαλύτερη έκθεση των κλειδιών του τελευταίου γύρου στην έξοδο του κρυπταλγόριθμου.

Στην περίπτωση που το κλειδί του γύρου συνδυάζεται με την είσοδο με αποκλειστική διάζευξη, η πιθανότητα των διαφορικών χαρακτηριστικών είναι ανεξάρτητη από τα bits του κλειδιού. Αυτό δίνει ένα πλεονέκτημα στον αντίπαλο ο οποίος μπορεί στην περίπτωση αυτή να εντοπίσει τα υποψήφια κλειδιά με μεγαλύτερη ευκολία, όπως φαίνεται στο Σχήμα 5.13. Ο αντίπαλος γνωρίζει τα p, p^*, p', a', c, c^* και c', και μπορεί να ξεχωρίσει τα πιθανά k από τα δυνατά a, a^* και γνωστό c'.



γνωστά	άγνωστα
p'	α
p	α*
p*	k
c'	
$\alpha'=p'$	

Σχήμα 5.13 Τυπική δομή γύρου κρυπτογράφησης

Όπως αναφέραμε, η διαφορά εισόδου a' του μη γραμμικού μετασχηματισμού είναι ανεξάρτητη του κλειδιού:

$$a' = p \oplus k \oplus p^* \oplus k = p \oplus p^* .$$

Για δεδομένη διαφορά εξόδου c', υπάρχουν συγκεκριμένες δυνατές διαφορές εισόδου a'. Έτσι η λίστα των δυνατών a, a^* σε συνδυασμό με τα γνωστά bits της εισόδου ορίζουν αντίστοιχα ορισμένα δυνατά bits κλειδιού.

ΠΑΡΑΔΕΙΓΜΑ 5.4 – Διαφορική κρυπτανάλυση κουτιού αντικατάστασης $S_1: \{0,1\}^6 \rightarrow \{0,1\}^4$ του DES. Θα παρουσιάσουμε το παράδειγμα των Biham και Shamir (J. of Cryptology, 1991) που χρησιμοποιήθηκε στην ανάπτυξη της μεθόδου της διαφορικής κρυπτανάλυσης και εφαρμόσθηκε στον κρυπταλγόριθμο DES. Το κουτί αντικατάστασης S_1 παρουσιάζεται στον Πίνακα 5.3. Για μια οποιαδήποτε είσοδο s_I των 6 bits, η έξοδος προκύπτει από τις συντεταγμένες x_I, y_I, όπου $x_I \in \{0,1\}^2$ και $y_I \in \{0,1\}^4$ ο αριθμός της γραμμής και ο αριθμός της στήλης αντίστοιχα. Οι συντεταγμένες προκύπτουν από την είσοδο ως εξής. Το πρώτο και τελευταίο bit της εισόδου αποτελεί την x_I, ενώ τα ενδιάμεσα bits αποτελούν την y_I.

Για παράδειγμα, αν s_I = (110101), τότε $x_I = (11)_2 = 3$ και $y_I = (1010)_2 = 10$. Η έξοδος του S_1 αντιστοιχεί στο στοιχείο που βρίσκεται στη γραμμή 3 και στη στήλη 10, δηλαδή $S_1(110101) = 3 = (0011)_2$.

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

Πίνακας 5.3 Το κουτί αντικατάστασης S_1

Θεωρούμε τη διαφορά εισόδου (110100) και τη διαφορά εξόδου (100). Χρησιμοποιώντας δεκαεξαδική βάση για κατάληψη μικρού χώρου στην αναπαράσταση των τιμών, θα είναι $(110100)_2 = 34_{16}$ και $(100)_2 = 4_{16}$. Η σχετική συχνότητα εμφάνισης για το ζευγάρι αυτό προκύπτει $N_D S_1(34_{16}, 4_{16}) = 2$. Στον Πίνακα 5.4 είναι συγκεντρωμένες όλες οι πιθανές διαφορές εισόδου, για όλες τις διαφορές εξόδου για το S_1. Οι δύο τιμές για τις οποίες η διαφορά εισόδου 34_{16} μπορεί να προκαλέσει τη διαφορά εξόδου 4_{16}, είναι η 13_{16} και η 27_{16}, ($13_{16} \oplus 27_{16} = 34_{16}$), με αντίστοιχες εξόδους 6_{16} και 2_{16}.

διαφορά εξόδου	πιθανές είσοδοι (σε δεκαεξαδική βάση) S_{1I}
1	03,0F,1E,1F,2A,2B,37,3B
2	04,05,0E,11,12,14,1A,1B,20,25,26,2E,2F,30,31,3A
3	01,02,15,21,35,36

4	13,27
7	00,08,0D,17,18,1D,23,29,2C,34,39,3C
8	09,0C,19,2D,38,3D
D	06,10,16,1C,22,24,28,32
F	07,0A,0B,33,3E,3F

Πίνακας 5.4 Πιθανές τιμές εισόδου της διαφοράς εισόδου 34_{16}, ως προς τη διαφορά εξόδου.

Έστω ότι για τη διαφορά εισόδου 34_{16}, η διαφορά εξόδου είναι D_{16}. Επίσης, έστω ότι η διαφορά αυτή δημιουργήθηκε από τις εισόδους 1_{16} και 35_{16}. Στην είσοδο του S_1 (μετά την εφαρμογή του κλειδιού), θα υπάρχει μια από τις 8 πιθανές τιμές που συγκεντρώνονται στον Πίνακα 5.4, για τη διαφορά εξόδου D_{16}. Επειδή όμως το κλειδί (S_{1K}), η είσοδος στο γύρο (S_{1E}), και η είσοδος στο S_1 (S_{1I}) συνδέονται με τη σχέση $S_{1I} = S_{1K} \oplus S_{1E}$, θα είναι ισοδύναμα και $S_{1K} = S_{1I} \oplus S_{1E}$. Η είσοδος στο γύρο είναι γνωστή, επομένως το σωστό κλειδί θα πρέπει να βρίσκεται σε κάποια από τις 8 σχέσεις που ορίζονται από τις 8 πιθανές εισόδους S_{1I}. Εφόσον γνωρίζουμε ότι η διαφορά εισόδου στο γύρο δημιουργήθηκε από τις εισόδους 1_{16} και 35_{16}, τότε το κλειδί θα περιέχεται στον Πίνακα 5.5. Αν χρησιμοποιηθεί και δεύτερο ζευγάρι εισόδου που αντιστοιχεί στην ίδια διαφορά εισόδου και παράγει διαφορά εξόδου διαφορετικής της D_{16}, τα πιθανά κλειδιά θα βρίσκονται στην τομή που ορίζεται από τον Πίνακα 5.5 των πιθανών κλειδιών και τον πίνακα που προκύπτει από το νέο ζευγάρι εισόδου.

πιθανές είσοδοι του S_1		Πιθανά κλειδιά	
06,	32	07,	33
10,	24	11,	25
16,	22	17,	23
1C,	28	1D,	29

Πίνακας 5.5 Πιθανά κλειδιά της διαφοράς εισόδου 34_{16}, που προκύπτει από τις εισόδους 1_{16} και 35_{16}.

5.2.4. Ο κρυπταλγόριθμος DES

Ο κρυπταλγόριθμος DES (Data Encryption Standard) είναι ένας κρυπταλγόριθμος τμήματος με $\boldsymbol{\mathcal{F}} = \boldsymbol{\mathcal{G}} = \{0, 1\}^{64}$ και $\boldsymbol{K} = \{0, 1\}^{56}$. Στην πραγματικότητα το αρχικό κλειδί έχει μέγεθος 64 bits, αλλά μόνον τα 56 από αυτά συμμετέχουν στην κρυπτογράφηση. Τα υπόλοιπα 8 bits του κλειδιού χρησιμοποιούνται για αρτιότητα (parity bits). Αποτελείται από 18 κρυπτογραφικές πράξεις, οι οποίες είναι μια αρχική μετάθεση του απλού κειμένου, ένα ισορροπημένο δίκτυο Feistel με 16 γύρους, και τέλος από μια μετάθεση του κειμένου του τελευταίου γύρου. Σε κάθε γύρο του κρυπτογραφικού γινομένου του δικτύου Feistel, συμμετέχουν 48 bits του κλειδιού, όπως καθορίζονται από το πρόγραμμα του κλειδιού.

Ο DES δημοσιεύθηκε το 1977 και είναι ο κρυπταλγόριθμος στον οποίο έχει γίνει η περισσότερη έρευνα σχετικά με την κρυπτογραφική του δύναμη. Οι απόπειρες κρυπτανάλυσης του DES είχαν σαν αποτέλεσμα την ανακάλυψη και καθιέρωση ποικίλλων αρχών σχεδίασης των κρυπταλγόριθμων τμήματος. Ο DES είναι βασισμένος στον κρυπταλγόριθμο Lucifer της IBM, του οποίου το τμήμα του απλού κειμένου, του κρυπτοκειμένου, καθώς και το μέγεθος του κλειδιού είναι 128 bits.

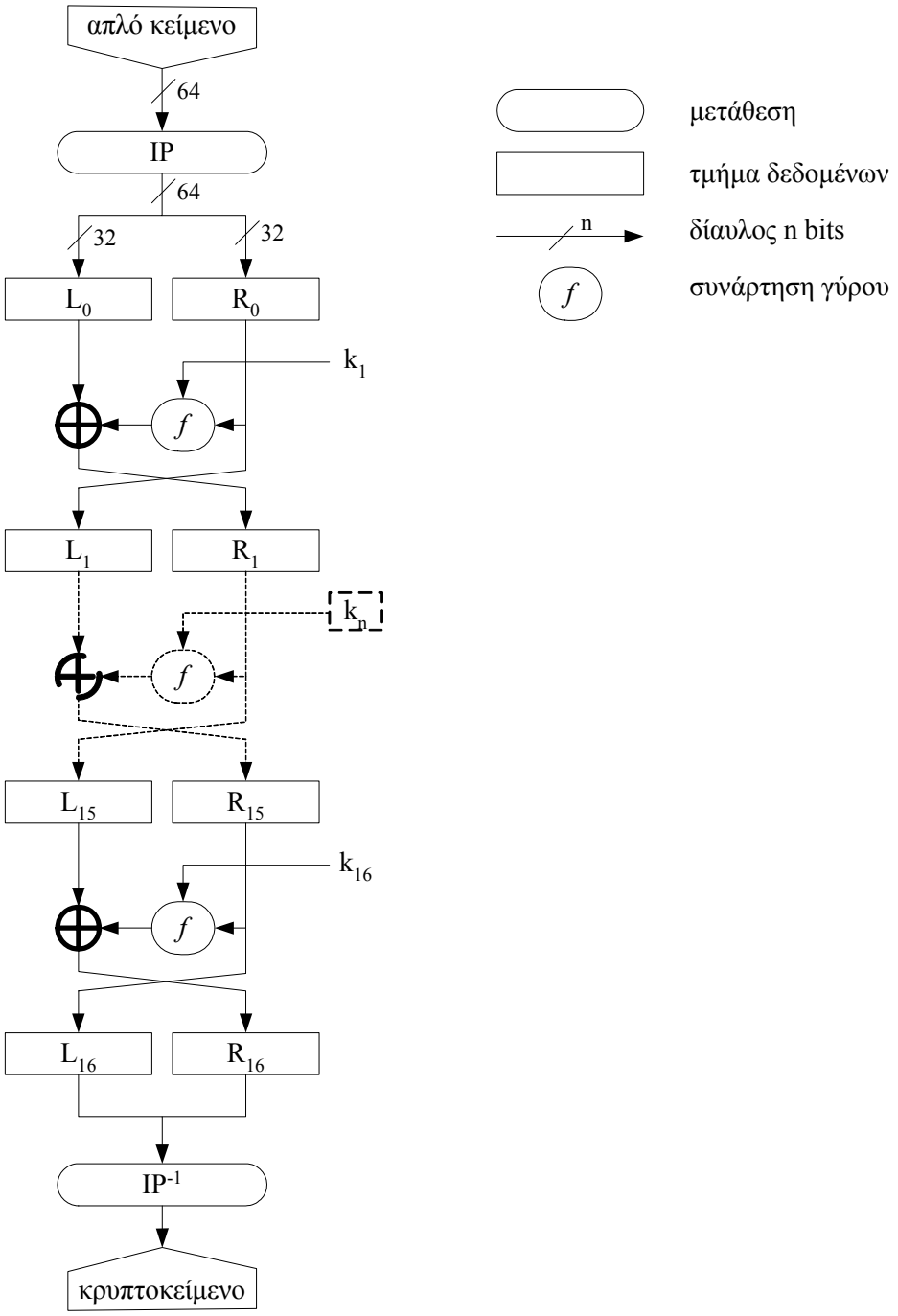
Ο DES σχεδιάσθηκε με βάση τα κριτήρια σχεδιασμού τα οποία διατυπώθηκαν το 1972 από το Υπουργείο Εμπορίου των ΗΠΑ, που επιζητούσε να βελτιωθεί η εθνική ασφάλεια με κρυπτογραφικές μεθόδους για την αποθήκευση, επεξεργασία, και διανομή της πληροφορίας. Τα κριτήρια ήταν τα ακόλουθα:

- υψηλό επίπεδο ασφάλειας,
- πλήρεις και διαφανείς προδιαγραφές,
- η ασφάλεια δε θα πρέπει να εξαρτάται από τη μυστικότητα του κρυπταλγόριθμου,
- διαθέσιμο σε, και προσβάσιμο από, όλους τους χρήστες,
- κατάλληλο για ποικιλία εφαρμογών,
- χαμηλό κόστος υλοποίησης,
- να είναι επιτρεπτή η εξαγωγή του,
- να είναι δυνατή η αξιολόγησή του.

Ωστόσο, στην πράξη συνέβησαν ορισμένα γεγονότα τα οποία ήρθαν σε αντίφαση με τα παραπάνω κριτήρια. Αρχικά, όσον αφορά το πρώτο κριτήριο της απαίτησης της υψηλής ασφάλειας, ο DES είχε πολύ μικρότερο κλειδί από αυτό του προκατόχου του, τον Lucifer. Στην περίπτωση του DES, ο κλειδοχώρος ορίζεται από $2^{56} \approx 72 \cdot 10^{15}$ κλειδιά, έναντι του κλειδοχώρου του Lucifer, ο οποίος περιέχει $2^{128} \approx 34 \cdot 10^{37}$ κλειδιά. Σε αυτό ευθύνεται η Υπηρεσία Εθνικής Ασφάλειας (National Security Agency, NSA) των ΗΠΑ, η οποία άσκησε πιέσεις για μικρό μήκος κλειδιού.

Όσον αφορά το κριτήριο της διαφάνειας των προδιαγραφών, τα κριτήρια σχεδιασμού των κουτιών αντικατάστασης που περιέχονται στη συνάρτηση γύρου του DES αποκαλύφθηκαν στα μέσα περίπου της δεκαετίας του ’90. Τα κριτήρια σχεδιασμού των κουτιών περιείχαν ενδείξεις ότι η τεχνική διαφορικής κρυπτανάλυσης που ανακαλύφθηκε επίσημα στις αρχές της δεκαετίας του ’90, ήταν γνωστή 15 χρόνια πριν. Επίσης η συγκεκριμένη επιλογή του αριθμού των γύρων του δικτύου Feistel του DES, έγινε ώστε ο DES να είναι ανθεκτικός σε διαφορική κρυπτανάλυση[2].

[2] Προσωπική επικοινωνία με τον Carl Meyer, που συμμετείχε στο σχεδιασμό του DES.



Σχήμα 5.14 Ο κρυπταλγόριθμος τμήματος DES.

Τεχνικά χαρακτηριστικά του DES

Ο κρυπταλγόριθμος DES παρουσιάζεται στο Σχήμα 5.14 , όπου διακρίνονται η είσοδος του απλού κειμένου, η αρχική μετάθεση IP, η ακολουθία των 16 γύρων τύπου Feistel, η τελική μετάθεση IP^{-1} και τέλος η έξοδος του κρυπτοκειμένου. Ο κρυπταλγόριθμος DES έχει το χαρακτηριστικό ότι η κρυπτογράφηση και η αποκρυπτογράφηση μπορούν να υλοποιηθούν με την ίδια διαδικασία, με τη μόνη διαφορά ότι το πρόγραμμα κλειδιού της αποκρυπτογράφησης παράγει την αντίστροφη ακολουθία που παράγει το πρόγραμμα κλειδιού της κρυπτογράφησης. Αν δηλαδή κατά την κρυπτογράφηση το πρόγραμμα κλειδιού είναι $\{k_1,k_2,...,k_{15}\}$, το πρόγραμμα κλειδιού κατά την αποκρυπτογράφηση θα είναι $\{k_{15},k_{14},...,k_1\}$.

Αρχική και τελική μετάθεση

Η αρχική μετάθεση είναι η αντιστροφή της τελικής μετάθεσης και αντίστροφα. Ο λόγος που επιλέχθηκε αυτή η εξάρτηση των δύο μεταθέσεων είναι για να μπορεί να χρησιμοποιηθεί η ίδια διαδικασία και στην κρυπτογράφηση και στην αποκρυπτογράφηση, με τη μόνη διαφορά του προγράμματος των κλειδιών, όπως αναφέρθηκε παραπάνω. Στις δύο αυτές μεταθέσεις δε συμμετέχει το κλειδί, και επομένως δεν προσθέτουν ουσιαστικά περαιτέρω ασφάλεια στην κατασκευή. Η ύπαρξη της αρχικής και τελικής μετάθεσης έγινε για λόγους πρακτικούς, για να υπάρχει κάποιος χώρος αποθήκευσης (μνήμη) του απλού κειμένου και του κρυπτοκειμένου, πριν και μετά την εφαρμογή του δικτύου Feistel. Η ύπαρξη αποθηκευτικών χώρων στην είσοδο και στα ηλεκτρονικά κυκλώματα είναι κοινή τακτική, και χρησιμοποιείται για να προσφέρει απομόνωση μεταξύ ενός ολοκληρωμένου κυκλώματος (microchip) και του υπολοίπου ηλεκτρονικού κυκλώματος.

Ένας δεύτερος λόγος της επιλογής της συγκεκριμένης μετάθεσης είναι ότι δημιουργούνται ομαδοποιήσεις. Τα bits που βρίσκονται σε θέση πολλαπλάσια του αριθμού 8 δημιουργούν δυαδικές λέξεις. Έτσι στην περίπτωση που το απλό κείμενο αποτελείται από χαρακτήρες ASCII, διαχωρίζεται η πληροφορία του χαρακτήρα από το όγδοο bit αρτιότητας. Ωστόσο, δεν υπάρχουν ενδείξεις αν ο διαχωρισμός αυτός μειώνει ή αυξάνει την κρυπτογραφική δύναμη του DES. Γενικότερα κατά την ανάλυση του DES δεν εξετάζονται η αρχική και η τελική μετάθεση, αλλά στην πράξη η συμμετοχή αυτών είναι υποχρεωτική λόγω της τυποποιημένης προδιαγραφής του κρυπταλγόριθμου.

Η αρχική μετάθεση παρουσιάζεται στον Πίνακα 5.6. Ο πίνακας αριθμείται από αριστερά προς δεξιά και από επάνω προς τα κάτω. Η αρίθμηση καθορίζει το bit εξόδου, ενώ το περιεχόμενο του πίνακα καθορίζει το bit εισόδου. Έτσι, στο πρώτο bit της εξόδου της μετάθεσης θα εμφανισθεί το πεντηκοστό όγδοο (58) bit του απλού κειμένου, στο δεύτερο bit της εξόδου, το πεντηκοστό (50) bit, κ.ο.κ.

IP=

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

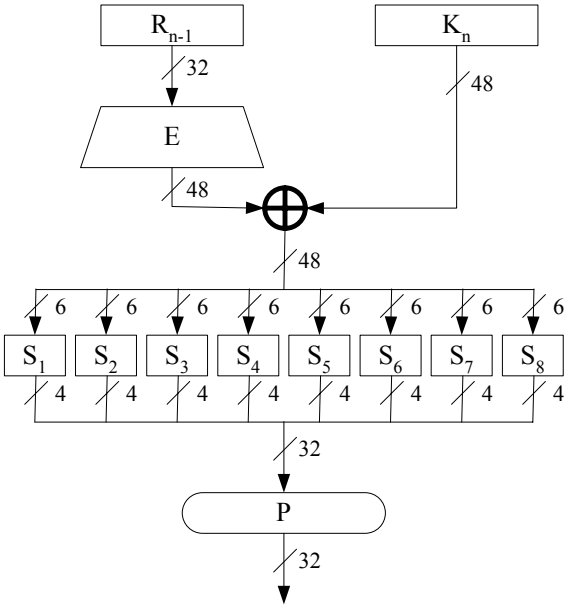
Πίνακας 5.6 Η αρχική αλληλομετάθεση IP.

Η τελική μετάθεση προκύπτει από την αντιστροφή της IP. Για παράδειγμα, παρατηρούμε ότι το πρώτο bit της εισόδου στην IP εμφανίζεται στην 40-στη θέση, το δεύτερο bit στην όγδοη θέση, κ.ο.κ. Έτσι η τελική μετάθεση θα είναι:

IP^{-1}=| 40 8 48 … |

Η συνάρτηση γύρου, f

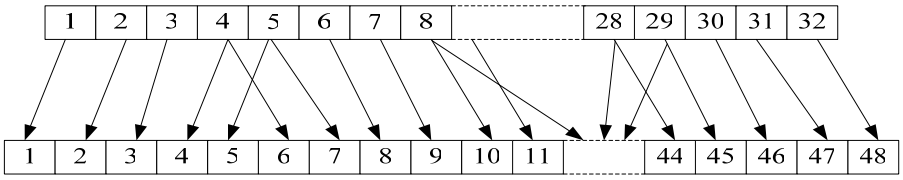
Η συνάρτηση γύρου αποτελείται από μια συνάρτηση επέκτασης $E:\{0,1\}^{32}\rightarrow\{0,1\}^{48}$, οκτώ κουτιά αντικατάστασης $S_i:\{0,1\}^{6}\rightarrow\{0,1\}^{4}$, και μια τελική συνάρτηση μετάθεσης P των 32 bits. Η συνάρτηση γύρου παριστάνεται στο Σχήμα 5.15.



Σχήμα 5.15 Η συνάρτηση γύρου του DES

Η συνάρτηση επέκτασης είναι μια μετάθεση στην οποία ορισμένα bits της ει-

σόδου εμφανίζονται σε περισσότερες από μια θέσεις στην έξοδο. Πιο συγκεκριμένα, τα bits εισόδου στις θέσεις 4, 5, 8, 9, 12, 13, …, 28, 29 εμφανίζονται διπλά, όπως φαίνεται στο Σχήμα 5.16. Είναι προφανές ότι υπάρχει γραμμική σχέση μεταξύ των bits της εισόδου και των bits της εξόδου της συνάρτησης επέκτασης.



Σχήμα 5.16 Η συνάρτηση επέκτασης Ε.

Η «καρδιά» του DES βρίσκεται στα οκτώ κουτιά αντικατάστασης. Τα κουτιά αυτά εισάγουν μη γραμμικότητα στην κατασκευή και η κρυπτογραφική δύναμη του κρυπταλγόριθμου εξαρτάται άμεσα από αυτά. Τα κριτήρια σχεδιασμού των κουτιών έγιναν γνωστά το 1994 σε δημοσίευση του Coppersmith και είναι τα εξής:

- Κάθε κουτί έχει είσοδο των 6 bits και έξοδο των 4 bits.
- Κανένα από τα bits της εξόδου δεν θα πρέπει να βρίσκεται σε γραμμική σχέση με οποιοδήποτε από το bits της εισόδου.
- Αν τα δύο πρώτα bits και τα δύο τελευταία bits της εισόδου είναι σταθερά ενώ τα ενδιάμεσα bits αλλάζουν, οι έξοδοι που προκύπτουν θα πρέπει να είναι μοναδικές.
- Αν η απόσταση Hamming δύο εισόδων είναι ίση με 1, τότε η απόσταση Hamming των αντίστοιχων εξόδων θα πρέπει να είναι το λιγότερο ίση με 2.
- Αν δύο είσοδοι διαφέρουν στα δύο μεσαία bits, τότε οι αντίστοιχες έξοδοι θα πρέπει να διαφέρουν το λιγότερο σε 2 bits.
- Αν δύο είσοδοι έχουν τα δύο πρώτα bits διαφορετικά ενώ τα δύο τελευταία bits είναι ίδια, τότε οι αντίστοιχες έξοδοι θα πρέπει να είναι διαφορετικές.
- Για οποιαδήποτε μη μηδενική διαφορά των 6 bits της εισόδου, θα πρέπει το πολύ 8 από τα 32 ζευγάρια να προκαλούν την ίδια διαφορά εξόδου.
- Όμοια με το παραπάνω κριτήριο, αλλά θα πρέπει να εφαρμόζεται συγχρόνως σε οποιαδήποτε 3 από τα 8 κουτιά αντικατάστασης.

Με βάση τα κριτήρια αυτά σχεδιάσθηκαν τα κουτιά S_1 έως S_8, όπως φαίνονται στον Πίνακα 5.3 και στους Πίνακες 5.7 έως 5.13.

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

Πίνακας 5.7 Το κουτί αντικατάστασης S_2

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

Πίνακας 5.8 Το κουτί αντικατάστασης S_3

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

Πίνακας 5.9 Το κουτί αντικατάστασης S_4

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

Πίνακας 5.10 Το κουτί αντικατάστασης S_5

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

Πίνακας 5.11 Το κουτί αντικατάστασης S_6

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

Πίνακας 5.12 Το κουτί αντικατάστασης S_7

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

Πίνακας 5.13 Το κουτί αντικατάστασης S_8

Τέλος, οι έξοδοι των οκτώ κουτιών εισέρχονται σε μια τελική μετάθεση P των 32 bits, που παρουσιάζεται στον Πίνακα 5.14.

P=

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

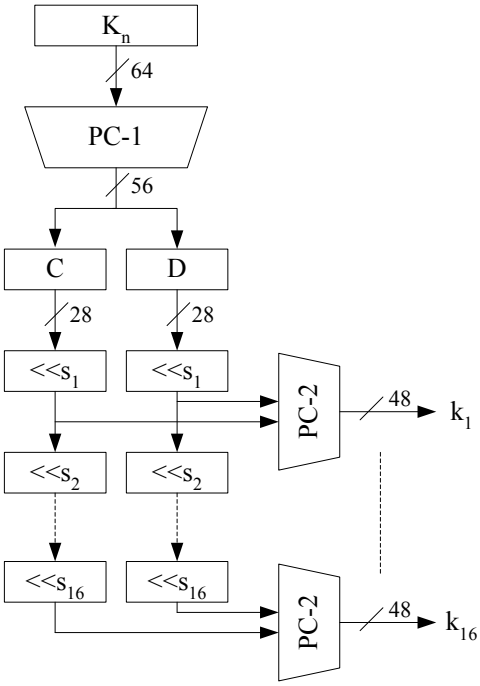
Πίνακας 5.14 Η μετάθεση P πριν από την έξοδο της συνάρτησης γύρου.

Το πρόγραμμα κλειδιού

Η είσοδος της συνάρτησης γύρου απαιτεί 32 bits δεδομένων και 48 bits του κλειδιού. Σε κάθε γύρο το κλειδί προκύπτει από το πρόγραμμα κλειδιού όπως φαίνεται στο Σχήμα 5.17. Το πρόγραμμα κλειδιού αποτελείται από δύο συναρτήσεις μετάθεσης επιλογής (permuted choice), PC-1:$\{0,1\}^{64}\rightarrow\{0,1\}^{56}$ και PC-2: $\{0,1\}^{56}\rightarrow\{0,1\}^{48}$, καθώς και από καταχωρητές ολίσθησης. Η μετάθεση επιλογής είναι μια μετάθεση κατά την οποία ορισμένα bits της εισόδου αγνοούνται και δεν εμφανίζονται στην έξοδο. Η PC-1 ξεχωρίζει όλα τα bits του αρχικού κλειδιού που θα συμμετάσχουν στο πρόγραμμα κλειδιού για τη δημιουργία των επιμέρους κλειδιών. Έτσι το κάθε όγδοο bit του αρχικού κλειδιού αγνοείται, με αποτέλεσμα να διατίθενται για την κρυπτογράφηση 64 – 8 = 56 bits.

Στη συνέχεια, τα 56 bits μοιράζονται σε δύο λέξεις των 28 bits και τροφοδοτούνται σε καταχωρητές ολίσθησης. Ανάλογα με τον γύρο, πραγματοποιείται μια ολίσθηση *n* προκαθορισμένων θέσεων όπως φαίνεται στον πίνακα του Σχήματος 5.17. Κατά την κρυπτογράφηση η ολίσθηση πραγματοποιείται προς την αριστερή φορά, ενώ κατά την αποκρυπτογράφηση η ολίσθηση εκτελείται προς τη δεξιά φορά. Ο αριθμός των ολισθήσεων έχει ως αποτέλεσμα το κλειδί να επανέλθει στην

αρχική του θέση. Έτσι κατά την αποκρυπτογράφηση εκτελούνται οι αντίστροφες (δεξιές) ολισθήσεις, με αρχική τη μηδενική ολίσθηση, δηλαδή: 0, 1, 2, 2, …, 1.



n	s_n
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Σχήμα 5.17 Το πρόγραμμα κλειδιού του DES

Κατά την ολοκλήρωση της κάθε ολίσθησης επιλέγονται 48 από τα 56 bits που βρίσκονται στον καταχωρητή ολίσθησης σύμφωνα με την μετάθεση επιλογής PC-2. Οι μεταθέσεις PC-1 και PC-2 παρουσιάζονται στον Πίνακα 5.15 και 5.16 αντίστοιχα.

PC-1=

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

Πίνακας 5.15 Μετάθεση επιλογής PC-1

PC-2=

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

Πίνακας 5.16 Μετάθεση επιλογής PC-2

Ασφάλεια του DES

Ο DES είναι ο κρυπταλγόριθμος που έχει μελετηθεί περισσότερο όσον αφορά το πλήθος των δημοσιευμένων μελετών και το χρονικό διάστημα. Πολλά πορίσματα που διατυπώθηκαν χάριν του DES μετατράπηκαν αργότερα σε αρχές σχεδιασμού συμμετρικών αλγόριθμων τμήματος τύπου DES.

Το πρώτο βήμα ανάλυσης του κρυπταλγόριθμου, είναι η εξέταση του μεγέθους του κλειδιού που ορίζει και το μέγεθος του κλειδοχώρου. Το DES επιτρέπει 2^{56} διαφορετικά κλειδιά. Αρχικά, το DES ήταν σχεδιασμένο για 2^{64} κλειδιά, αλλά το μέγεθος αυτό μειώθηκε για να συμπεριληφθεί η πληροφορία των bits αρτιότητας. Ο κλειδοχώρος του DES κατακρινόταν πάντοτε για το μικρό μέγεθος. Κατά τη δεκαετία του 80, ήταν οικονομικά επιτρεπτό σε μια κυβέρνηση να σπάσει το κρυπτοσύστημα με εξαντλητική αναζήτηση. Σήμερα, η κατανεμημένη υπολογιστική επιτρέπει τη συνεργασία μελών κοινότητας του Διαδικτύου, όπου το κάθε μέλος συνεισφέρει με την υπολογιστική ισχύ που διαθέτει για να επιτύχει η εξαντλητική αναζήτηση σε λογικό χρονικό διάστημα. Η κοινότητα γνωστή με το όνομα distributed.net πραγματοποίησε τον Ιανουάριο του 1999 εξαντλητική αναζήτηση στην πρόκληση "DES Challenge III" της εταιρείας RSA Laboratories, και το κλειδί βρέθηκε μετά από 22 ώρες και 15 λεπτά. Στην αναζήτηση συμμετείχαν 100.000 ηλεκτρονικοί υπολογιστές, με δυνατότητα αναζήτησης 245 δισεκατομμύρια κλειδιών ανά δευτερόλεπτο. Για να συνειδητοποιήσουμε πόσο ευάλωτος είναι ο DES όσον αφορά το μέγεθος του κλειδιού του, αρκεί να αναγάγουμε την υπολογιστική ισχύ του 1999 στα σημερινά δεδομένα (2003). Η αναζήτηση που επιτεύχθηκε το 1999 μπορεί σήμερα να πραγματοποιηθεί στον ίδιο χρόνο με 37.500 ηλεκτρονικούς υπολογιστές, ενώ στην περίπτωση που χρησιμοποιηθούν 100.000 σημερινοί ηλεκτρονικοί υπολογιστές, το κλειδί θα βρισκόταν σε 8 ώρες και 30 λεπτά.

Μια άλλη παράμετρος η οποία είναι εξίσου κατακριτέα είναι το μικρό μέγεθος των κουτιών αντικατάστασης. Η διαδικασία καθορισμού των κουτιών αντικατάστασης ήταν κρυφή για αρκετά χρόνια και η παρέμβαση της Υπηρεσίας Εθνικής Ασφάλειας στο σχεδιασμό, δημιούργησε υποψίες ύπαρξης «μυστικής πόρτας» (trapdoor), η οποία επιτρέπει την αποκρυπτογράφηση χωρίς τη γνώση του κλειδιού. Ωστόσο, η ανάλυση των κουτιών έδειξε ότι η επιλογή αυτών έγινε με ιδιαίτερη προσοχή, αφού στην περίπτωση χρησιμοποίησης τυχαίων κουτιών, η ασφά-

λεια του DES μειώνονταν σημαντικά. Βέβαια, κάτι τέτοιο δεν αποδεικνύει την ύπαρξη ή όχι κάποιας μυστικής πόρτας.

Ιδιότητα των συμπληρωματικών μεταβλητών

Μια ενδιαφέρουσα ιδιότητα είναι αυτή των συμπληρωματικών μεταβλητών. Μια δυαδική μεταβλητή Y ονομάζεται ***συμπληρωματική*** ως προς μια μεταβλητή X, όταν η Y είναι ίση με την αντιστροφή όλων των bits της X. Η συμπληρωματική μεταβλητή συμβολίζεται με $\overline{X}$. Για παράδειγμα, $\overline{1001} = 0110$.

Ο DES εμφανίζει τη συμπληρωματική ιδιότητα ως προς το απλό κείμενο, κλειδί και κρυπτοκείμενο. Αν η κρυπτογράφηση του DES ορίζεται από την:

$$c = e_k^{des}(p),$$

για οποιαδήποτε c, p και k, τότε ισχύει και

$$\overline{c} = e_{\overline{k}}^{des}(\overline{p}).$$

Αυτό οφείλεται στην αποκλειστική διάζευξη του τμήματος της εισόδου με το κλειδί, πριν εισαχθούν στα κουτιά αντικατάστασης. Η αντιστροφή μιας μεταβλητής ισοδυναμεί με την αποκλειστική διάζευξη αυτής με το μοναδιαίο διάνυσμα. Έτσι:

$$\overline{c} = 1^{64} \oplus c,$$
$$\overline{p} = 1^{64} \oplus p,$$
$$\overline{k} = 1^{64} \oplus k,$$

όπου $1^{64} = (11..1)$ (μήκους 64 bits). Συνεπώς, η αποκλειστική διάζευξη στην είσοδο της συνάρτησης γύρου, θα δώσει για το κλειδί $\overline{k}_n$ και τα δεδομένα $\overline{R}_{n-1}$:

$$\overline{R}_{n-1} \oplus \overline{k}_n = (1^{32} \oplus R_{n-1}) \oplus (1^{32} \oplus k_n) = R_{n-1} \oplus k_n,$$

δηλαδή η έξοδος της συνάρτησης γύρου δεν μεταβάλλεται με την αντιστροφή των c, p και k. Στη συνέχεια, η έξοδος της συνάρτησης γύρου προστίθεται με αποκλειστική διάζευξη στην $\overline{L}_{n-1}$ για να προκύψει η $\overline{R}_n$.

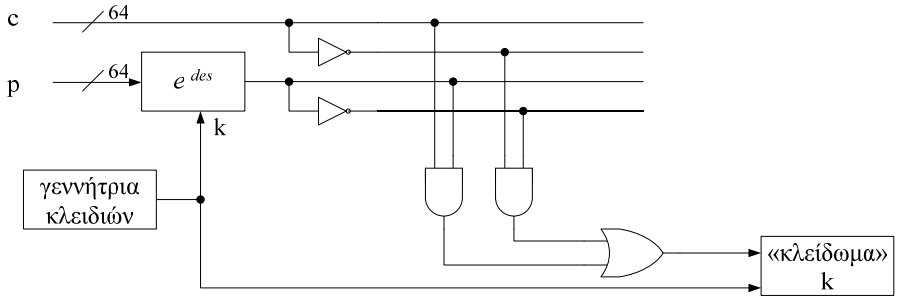
Επομένως η συμπληρωματική ιδιότητα του DES αποκαλύπτει την ύπαρξη απλών σχέσεων. Οι απλές σχέσεις είναι οι:

$$f(k) = \overline{k},$$
$$g_1(p,k) = \overline{p} \text{ και}$$
$$g_2(c,k) = \overline{c}$$

τέτοιες ώστε:

$$e_k^{des}(p) = e_{f(k)}^{des}(g_1(p,k)) = g_2(c,k).$$

Οι παραπάνω απλές σχέσεις μπορούν να χρησιμοποιηθούν για να μειωθεί ο χώρος αναζήτησης, από 2^{56} σε 2^{55}, αφού σε κάθε κρυπτογράφηση (ή αποκρυπτογράφηση) μπορούν να δοκιμασθούν 2 κλειδιά, όπως φαίνεται στο Σχήμα 5.18.



Σχήμα 5.18 Διάταξη για την εκμετάλλευση της συμπληρωματικής ιδιότητας του DES

Σχηματισμός ομάδας

Είναι γνωστό από την άλγεβρα ότι μια ομάδα ορίζεται από ένα σύνολο A και μια πράξη η οποία είναι εσωτερική στο σύνολο αυτό. Στην περίπτωση του DES, το σύνολο A αποτελείται από τις 2^{56} μεταθέσεις των δυαδικών λέξεων του $\{0,1\}^{64}$, οι οποίες καθορίζονται από το κλειδί. Θεωρούμε την πράξη ως το κρυπτογραφικό γινόμενο δύο στοιχείων του A. Τότε το κρυπτογραφικό γινόμενο ορίζει ομάδα με το A, αν για οποιαδήποτε δύο στοιχεία e_i και e_j του A, υπάρχει το στοιχείο e_k που επίσης ανήκει στο A, τέτοιο ώστε:

$$e_k(p) = e_j(e_i(p)), \quad \forall p \in \{0,1\}^{64},$$

για σταθερά i, j και k. Αν το κρυπτοσύστημα ορίζει ομάδα, τότε η πολλαπλή κρυπτογράφηση δε θα πρόσθετε παραπάνω ασφάλεια. Έχει αποδειχθεί ότι ο DES δεν σχηματίζει ομάδα, επομένως η τριπλή κρυπτογράφηση που ορίζεται σε προηγούμενη ενότητα μπορεί να υλοποιηθεί με τον κρυπταλγόριθμο αυτό.

Αδύναμα και ημιαδύναμα κλειδιά

Το πρόγραμμα κλειδιού του DES είναι αδύναμο, όχι μόνον επειδή από οποιοδήποτε κλειδί γύρου μπορεί να βρεθεί με σχετική ευκολία το αρχικό κλειδί, αλλά και επειδή υπάρχουν κλειδιά τα οποία παράγουν το ίδιο πρόγραμμα κλειδιού κατά την κρυπτογράφηση και την αποκρυπτογράφηση. Υπό κανονικές συνθήκες, το πρόγραμμα κλειδιού της αποκρυπτογράφησης έχει αντίστροφη σειρά του προγράμματος κλειδιού της κρυπτογράφησης. Στην περίπτωση όμως που το κλειδί είναι κάποιο από τα κλειδιά του Πίνακα 5.17, τότε το πρόγραμμα κλειδιών που προκύπτει

είναι το ίδιο τόσο στην κρυπτογράφηση, όσο και στην αποκρυπτογράφηση. Αυτό σημαίνει ότι στην περίπτωση που ένα σύστημα χρησιμοποιεί διπλή κρυπτογράφηση, το κρυπτοκείμενο που προκύπτει θα είναι ίδιο με το απλό κείμενο. Δηλαδή, η δεύτερη κρυπτογράφηση θα αναιρεί την πρώτη. Τα κλειδιά αυτά ονομάζονται ***αδύναμα κλειδιά***, και θα πρέπει να αποφεύγονται σε εφαρμογές που απαιτείται υψηλή ασφάλεια, όπως για παράδειγμα στη δημιουργία κλειδιών από ένα αρχικό κλειδί.

01	01	01	01	01	01	01	01
FE	FE	FE	FE	FE	FE	FE	FE
1F	1F	1F	1F	1F	1F	1F	1F
E0	E0	E0	E0	E0	E0	E0	E0

Πίνακας 5.17 Τα αδύναμα κλειδιά του DES (σε δεκαεξαδική αναπαράσταση)

Εκτός από τα αδύναμα κλειδιά, υπάρχουν και τα ***ημιαδύναμα κλειδιά*** (Πίνακας 5.18). Τα κλειδιά αυτά εμφανίζονται σε ζευγάρια, όπου το πρόγραμμα κλειδιού του ενός είναι ισοδύναμο με το πρόγραμμα κλειδιού του άλλου, με αντίστροφη σειρά. Έτσι, η κρυπτογράφηση του ενός κλειδιού ακολουθούμενη από την κρυπτογράφηση του δεύτερου κλειδιού που ορίζουν ζευγάρι, έχει ως αποτέλεσμα το κρυπτοκείμενο να είναι ίσο με το αρχικό απλό κείμενο. Η ύπαρξη τόσο των αδύναμων κλειδιών, όσο και των ζευγαριών των ημιαδύναμων κλειδιών, οφείλεται στην απλοϊκή κατασκευή του αλγόριθμου του προγράμματος κλειδιών.

01	FE	01	FE	01	FE	01	FE	1F	E0	1F	E0	0E	F1	0E	F1
FE	01	FE	01	FE	01	FE	01	E0	1F	E0	1F	F1	0E	F1	0E
01	E0	01	E0	01	F1	01	F1	1F	FE	1F	FE	0E	FE	0E	FE
E0	01	E0	01	F1	01	F1	01	FE	1F	FE	1F	FE	0E	FE	0E
01	1F	01	1F	01	0E	01	0E	E0	FE	E0	FE	F1	FE	F1	FE
1F	01	1F	01	0E	01	0E	01	FE	E0	FE	E0	FE	F1	FE	F1

Πίνακας 5.18 Τα ημιαδύναμα κλειδιά του DES

Διαφορική και γραμμική κρυπτανάλυση του DES

Από τις δύο αυτές επιθέσεις, η γραμμική κρυπτανάλυση είναι συγκριτικά η οικονομικότερη επίθεση, απαιτώντας 2^{43} ζευγάρια γνωστών απλών κειμένων και κρυπτοκειμένων, κρυπτογραφημένα με το άγνωστο κλειδί. Στην περίπτωση της διαφορικής κρυπτανάλυσης απαιτούνται 2^{47} ζευγάρια επιλεγμένου κρυπτοκειμένου, ενώ στην περίπτωση κρυπτανάλυσης γνωστού κρυπτοκειμένου ο αριθμός των ζευγαριών είναι 2^{55}.

5.2.5. Ο κρυπταλγόριθμος AES

Ο κρυπταλγόριθμος AES (Advanced Encryption Standard) προέκυψε από μια προσπάθεια αντικατάστασης του DES. Η προσπάθεια δημοσιοποιήθηκε τον Σεπτέμβριο του 1997 με την προκήρυξη του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST), για μια παγκόσμια συμμετοχή στη δημιουργία του AES. Από τους 21 υποβληθέντες κρυπταλγόριθμους, 15 βρέθηκαν να πληρούν τα απαραίτητα κριτήρια. Σύμφωνα με τη διαδικασία επιλογής, από τους 15 κρυπταλγόριθμους επιλέχθηκαν αρχικά 5 και τελικά στις 2 Οκτωβρίου του 2000 κατοχυρώθηκε ο Rijndael ως ο AES.

Σε αντίθεση με τη μυστικότητα του DES, η διαδικασία δημιουργίας του AES πληρούσε το κριτήριο του Kerchoff σχετικά με την εξάρτηση της ασφάλειας και δημοσιοποίησης. Τόσο η προκήρυξη του AES, όσο και η πρόσκληση εξέτασης της ασφάλειας των προτεινόμενων κρυπταλγόριθμων ήταν ανοικτές.

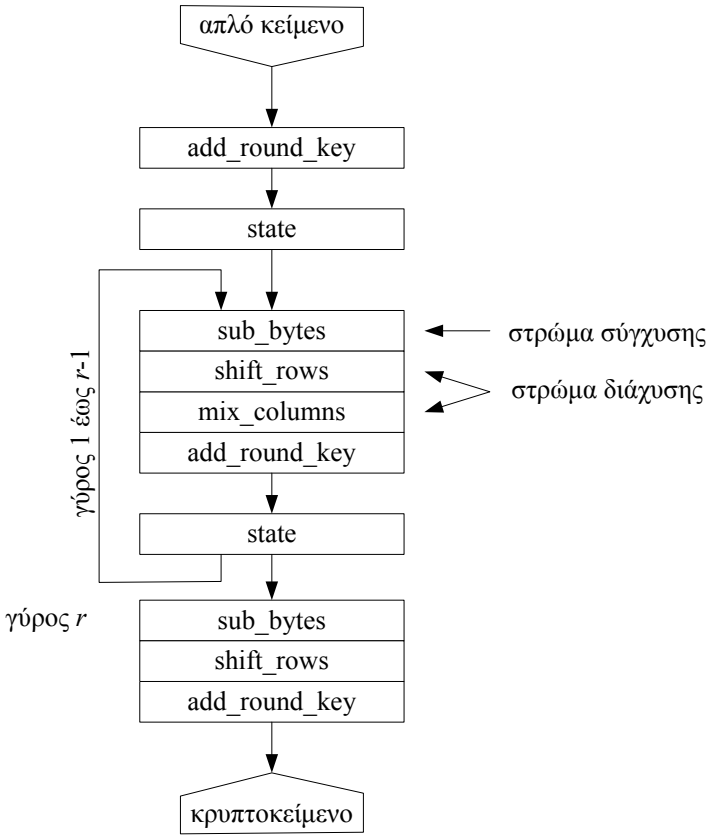
Τα κριτήρια αξιολόγησης του AES ήταν τα εξής:

- ασφάλεια. Αυτό ήταν και το κριτήριο με το μεγαλύτερο βάρος. Αν υπήρχαν οποιεσδήποτε ενδείξεις ότι ο προτεινόμενος κρυπταλγόριθμος δεν ήταν ασφαλής, θα απορρίπτονταν.
- κόστος. Το κριτήριο του κόστους αναφέρεται τόσο στην υπολογιστική πολυπλοκότητα που θα απαιτούσε ο κρυπταλγόριθμος προκειμένου να εκτελέσει κρυπτογράφηση και αποκρυπτογράφηση, όσο και στις απαιτήσεις μνήμης. Κρυπταλγόριθμοι με χαμηλή σχετικά απαίτηση σε αριθμό πράξεων και μνήμης ήταν προτιμότεροι διότι οι υλοποιήσεις συμπεριέλαβαν έξυπνες κάρτες.
- χαρακτηριστικά υλοποίησης του κρυπταλγόριθμου, τα οποία περιελάμβαναν απλότητα των αλγορίθμων, ευκαμψία (flexibility), και φυσικά καθορισμό των μεγεθών του απλού κειμένου, του κρυπτοκειμένου και του κλειδιού.

Τεχνικά χαρακτηριστικά του AES

Ο AES είναι ένας κρυπταλγόριθμος τμήματος με $\mathcal{F} = \mathcal{G} = \{0, 1\}^{128}$, ενώ το κλειδί έχει μεταβλητό μέγεθος και μπορεί να είναι ίσο με 128, 192 ή 256 bits. Ο εξαιρετικά μεγάλος κλειδοχώρος καθιστά την εξαντλητική αναζήτηση πρακτικώς αδύνατη. Ο AES είναι επαναληπτικός κρυπταλγόριθμος και βασίζεται σε κρυπτογράφηση γινομένου. Ο αριθμός των γύρων r εξαρτάται από το μέγεθος του κλειδιού. Έτσι ο αριθμός των γύρων είναι ίσος με $r_{128} = 10$, $r_{192} = 12$ ή $r_{256} = 14$ για μεγέθη κλειδιών 128, 192 και 256 bits αντίστοιχα.

Σε αντίθεση με τον DES, η δομή του AES δεν είναι δίκτυο Feistel. Ένα δίκτυο Feistel κρυπτογραφεί ένα μέρος της εισόδου του σε κάθε γύρο (στην περίπτωση του DES, τα μισά bits της εισόδου). Στην περίπτωση του AES, σε κάθε γύρο κρυπτογραφείται όλη η είσοδος. Αυτό έχει σαν αποτέλεσμα να απαιτούνται λιγότεροι αριθμοί γύρων.



Σχήμα 5.19 Τα βασικά συστατικά του κρυπταλγόριθμου AES

Στο Σχήμα 5.19 παριστάνεται ο AES. Ο βασικός αποθηκευτικός χώρος συμβολίζεται με "state" και αρχικά περιέχει το απλό κείμενο, ενώ στο τέλος της διαδικασίας περιέχει το κρυπτοκείμενο. Ο AES περιγράφεται με τη μορφή στρωμάτων, όπου το κάθε στρώμα αντιστοιχεί σε ένα συγκεκριμένο μετασχηματισμό του state.

Το στρώμα σύγχυσης

Η διαδικασία sub_bytes αποτελεί το στρώμα που είναι υπεύθυνο για την αύξηση της σύγχυσης. Αντιστοιχεί με κουτί αντικατάστασης και αποτελεί τον μη γραμμικό μετασχηματισμό του AES. Η είσοδος χωρίζεται σε 16 δυαδικές λέξεις των 8 bits, και η μη γραμμικότητα εφαρμόζεται στην κάθε λέξη χωριστά.

Χρησιμοποιώντας πολυωνυμική αναπαράσταση, τα οκτώ bits μιας δυαδικής λέξης εισόδου $(a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7)$ εκφράζονται ισοδύναμα με το πολυώνυμο:

$$A(x) = \sum_{0}^{7} a_i x^i \ .$$

Έτσι, η είσοδος αντιστοιχεί σε στοιχείο του πεπερασμένου σώματος $GF(2^8)$ στο οποίο εκτελούνται οι πράξεις. Από τη θεωρία των αλγεβρικών δομών, το σώμα αυτό μπορεί να αναπαραχθεί από ανάγωγο πολυώνυμο με βαθμό ίσο του 8. Το πολυώνυμο που ορίζεται στον AES είναι το:

$$P(x) = x^8 + x^4 + x^3 + x + 1.$$

Κατά τη διαδικασία sub_bytes εκτελούνται τα ακόλουθα βήματα. Αρχικά υπολογίζεται το $B(x)$, τέτοιο ώστε:

$$A(x)B(x) \equiv 1 \pmod{P(x)}.$$

Στη συνέχεια, εφαρμόζεται ο ακόλουθος γραμμικός μετασχηματισμός:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

με $C(x)$ το αποτέλεσμα της διαδικασίας sub_bytes. Η παραπάνω διαδικασία είναι η ίδια και για τις 16 δυαδικές λέξεις της εισόδου. Οι παραπάνω μετασχηματισμοί μπορούν να υλοποιηθούν με κουτί αντικατάστασης, το οποίο όμως ορίζεται αλγεβρικά και συνεπώς μπορεί να καταλαμβάνει μικρό χώρο. Έτσι μια άλλη διαφορά με τον DES είναι ότι στην περίπτωση του AES, όλες οι λέξεις της εισόδου τροφοδοτούνται στο ίδιο κουτί αντικατάστασης.

Το στρώμα διάχυσης

Το στρώμα διάχυσης αποτελείται από δύο υποστρώματα, τη διαδικασία shift_rows και τη διαδικασία mix_columns.

Κατά τη διαδικασία shift_rows, η είσοδος απεικονίζεται με τις 16 δυαδικές λέξεις ($s_0 s_1 \ldots s_{15}$), όπου η κάθε λέξη έχει μέγεθος 8 bits, οι οποίες διατάσσονται κάθετα σε πίνακα 4x4 ως εξής:

s_0	s_4	s_8	s_{12}
s_1	s_5	s_9	s_{13}
s_2	s_6	s_{10}	s_{14}
s_3	s_7	s_{11}	s_{15}

Στη συνέχεια, πραγματοποιείται ολίσθηση των λέξεων ως προς τις γραμμές:

s_0	s_4	s_8	s_{12}	καμία ολίσθηση
s_5	s_9	s_{13}	s_1	αριστερή ολίσθηση μιας θέσης
s_{10}	s_{14}	s_2	s_6	αριστερή ολίσθηση δύο θέσεων
s_{15}	s_3	s_7	s_{11}	αριστερή ολίσθηση τριών θέσεων

και το αποτέλεσμα είναι η έξοδος της διαδικασίας shift_rows:

$$(s_0 s_5 s_{10} s_{15} s_4 s_9 s_{14} s_3 s_8 s_{13} s_2 s_7 s_{12} s_1 s_6 s_{11}) .$$

Τέλος, η διαδικασία mix_columns δέχεται τις λέξεις ανά τετράδες και εφαρμόζει τον ακόλουθο μετασχηματισμό:

$$\begin{pmatrix} c_i \\ c_j \\ c_k \\ c_l \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_i \\ s_j \\ s_k \\ s_l \end{pmatrix},$$

όπου $(i, j, k, l) \in \{(0, 5, 10, 15), (4, 9, 14, 3), (8, 13, 2, 7), (12, 1, 6, 11)\}$ και οι πράξεις εκτελούνται στο σώμα $GF(2^8)$. Η έξοδος της διαδικασίας απαρτίζεται από την:

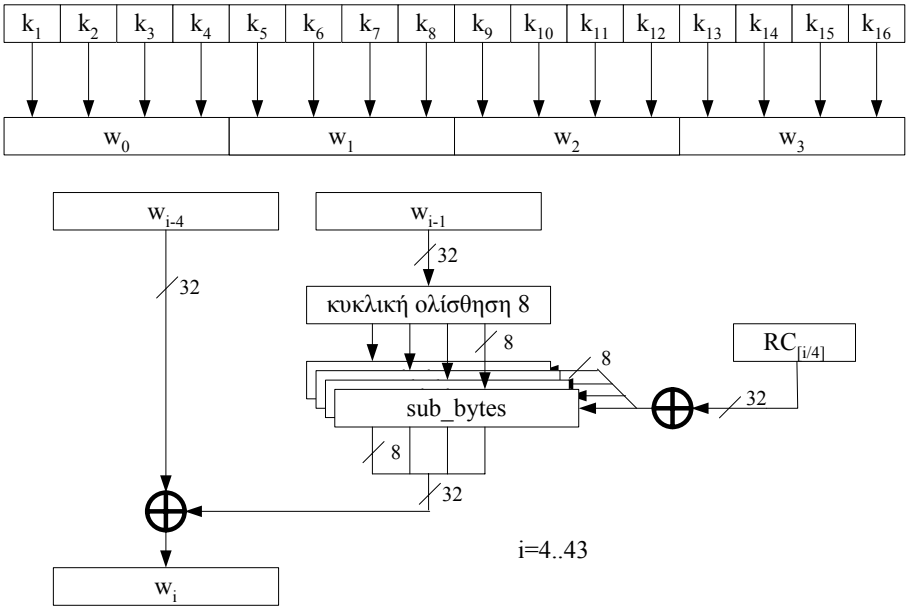
$$(c_0 c_5 c_{10} c_{15} c_4 c_9 c_{14} c_3 c_8 c_{13} c_2 c_7 c_{12} c_1 c_6 c_{11}) .$$

Το πρόγραμμα κλειδιού

Το πρόγραμμα κλειδιού παρουσιάζεται στο Σχήμα 5.20. Στον αλγόριθμο του προγράμματος κλειδιού οι πράξεις εκτελούνται σε λέξεις των 32 bit (w_i). Ο στόχος του προγράμματος είναι να δημιουργηθεί μια ακολουθία εκτεταμένου κλειδιού (expanded key) μεγέθους 44×32 = 1408 bits.

Αρχικά οι τέσσερις πρώτες λέξεις φορτώνονται με τα 128 bits του κλειδιού. Στη συνέχεια ακολουθεί η διαδικασία που επαναλαμβάνεται 40 φορές για να καθορισθούν οι λέξεις w_4 έως w_{43}. Η κυκλική ολίσθηση εκτελεί τη μετατόπιση της λέξης εισόδου για 8 θέσεις προς τα αριστερά. Για παράδειγμα, στην περίπτωση της w_3 η κυκλική ολίσθηση θα δώσει:

$$(k_{14} k_{15} k_{16} k_{13}) .$$



Σχήμα 5.20 Το πρόγραμμα κλειδιού του AES

Στη συνέχεια ο αλγόριθμος εκμεταλλεύεται τη διαδικασία sub_bytes του κυρίως κρυπταλγόριθμου, προκειμένου να εισάγει μη γραμμικότητα στο πρόγραμμα κλειδιού. Οι ποσότητες $RC_{\lfloor i/4 \rfloor}$, όπου με $\lfloor i/4 \rfloor$ συμβολίζεται το ακέραιο μέρος του πηλίκου $i/4$, είναι οι εξής (σε δεκαεξαδική μορφή):

$RC_1 = 01000000$ $\quad$ $RC_6 = 20000000$

$RC_2 = 02000000$ $\quad$ $RC_7 = 40000000$

$RC_3 = 04000000$ $\quad$ $RC_8 = 80000000$

$RC_4 = 08000000$ $\quad$ $RC_9 = 1B000000$

$RC_5 = 10000000$ $\quad$ $RC_{10} = 36000000$

Η διαδικασία του προγράμματος κλειδιού παράγει 44 λέξεις, όπου χρησιμοποιούνται ανά τέσσερις από τη διαδικασία add_round_key, η οποία είναι η αποκλειστική διάζευξη των δεδομένων με το κλειδί.

Ασφάλεια του AES

Όπως είναι αναμενόμενο, ο AES μπορεί να αντισταθεί αποτελεσματικά σε όλες τις γνωστές κρυπταναλυτικές μεθόδους. Η αλγεβρική κατασκευή των κουτιών αντικατάστασης βασίζεται σε τεχνικές με τις οποίες η κατανομή των συχνοτήτων εμφάνισης των διαφορών εξόδου είναι ομοιόμορφη, με αποτέλεσμα να μην υπάρχουν ισχυρά διαφορικά χαρακτηριστικά, ούτε γραμμικές σχέσεις με αυξημένη πόλωση.

Αξίζει να σημειώσουμε ότι στο πρόσφατο συνέδριο CRYPTO 2002, οι Murphy και Robshaw παρουσίασαν μια διαφορετική προσέγγιση στην περιγραφή του AES, η οποία επιτρέπει την ανάλυση του AES σε ένα απλοποιημένο μαθηματικό υπόβαθρο. Η προσέγγιση αυτή έχει ανοίξει νέα παράθυρα στη κρυπταναλυτική έρευνα, η οποία εάν ολοκληρωθεί με επιτυχία, το ενεργό κλειδί του AES θα είναι πολύ μικρότερο από το πραγματικό κλειδί του.

5.3. Κρυπταλγόριθμοι ροής

Οι τακτικές σχεδιασμού κρυπταλγόριθμων ροής μοιάζουν με αυτές των κρυπταλγόριθμων τμήματος. Αρχικά τίθενται τα κρυπτογραφικά κριτήρια που πρέπει να πληροί ο υποψήφιος κρυπταλγόριθμος ροής και στη συνέχει ακολουθεί ο σχεδιασμός και η ανάλυσή του.

Σύμφωνα με τον Kumar, τα κριτήρια που θα πρέπει να πληροί ένας κρυπταλγόριθμος τμήματος αναφέρονται στη γεννήτρια της ψευδοτυχαίας ακολουθίας που είναι υπεύθυνη για την κατασκευή της κλειδοροής και είναι τα εξής:

- Η περίοδος της κλειδοροής θα πρέπει να είναι όσο το δυνατόν μεγαλύτερη. Λόγω του περιορισμού της απαίτησης να αναπαράγεται αξιόπιστα η κλειδοροή, οι μηχανισμοί παραγωγής της είναι τέτοιοι ώστε η ακολουθία να έχει πεπερασμένο μέγεθος (δηλαδή περίοδο) και σε κάποια χρονική στιγμή επαναλαμβάνεται. Το πλεονέκτημα του αντιπάλου συσχετίζεται αντίστροφα με το μέγεθος της περιόδου. Το ανάλογο σε κρυπταλγόριθμο τμήματος είναι το κρυπτοσύστημα Vigenère.
- Τα bits της ακολουθίας της κλειδοροής θα πρέπει να περνάν με επιτυχία όλους τους γνωστούς ελέγχους περί τυχαιότητας. Στην περίπτωση αυτή, η ακολουθία της κλειδοροής θα μοιάζει με μια τυχαία ακολουθία bits. Η μίξη της κλειδοροής με το απλό κείμενο θα έχει σαν αποτέλεσμα τη δημιουργία μιας ψευδοτυχαίας ακολουθίας, της οποίας η κρυπτανάλυση θα είναι δύσκολη.
- Το κλειδί του κρυπταλγόριθμου ροής καθορίζει την αρχική κατάσταση της γεννήτριας της κλειδοροής, που αντιστοιχεί στον προσδιορισμό της αρχικής θέσης στην περιοδική ακολουθία της κλειδοροής. Επομένως, το κλειδί θα πρέπει να είναι αρκετά μεγάλο ώστε να μην είναι πρακτικά δυνατή η εξαντλητική αναζήτηση αυτού.

5.3.1. Κλειδοροές βασισμένες σε καταχωρητές ολίσθησης με γραμμική ανάδραση

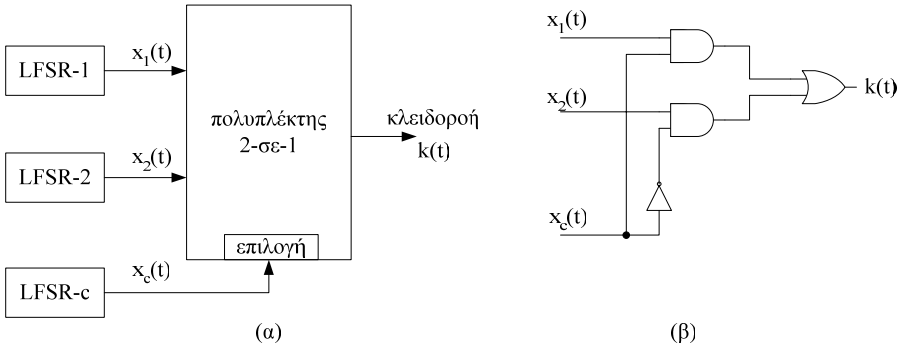
Μια από τις πιο δημοφιλείς συναρτήσεις που χρησιμοποιούνται στους κρυπταλγόριθμους ροής είναι η γραμμική ανάδραση των στοιχείων που περιέχονται σε καταχωρητές ολίσθησης, LFSR (Linear Feedback Shift Register). Οι γεννήτριες LFSR προτιμούνται για τις μαθηματικά αναγνωρισμένες ιδιότητές τους, οι οποίες συμβάλλουν στη δημιουργία κλειδοροής με μέγιστη περίοδο.

Ωστόσο, η μεγάλη αδυναμία των LFSR είναι ότι αν αποκαλυφθεί μέρος του απλού κειμένου, τότε μπορούν να κρυπταναλυθούν με σχετικά μεγάλη ευκολία. Έτσι στην πράξη ένας LFSR δεν χρησιμοποιείται αυτούσιος, αλλά σε συνδυασμό με κάποια βαθμίδα απομόνωσης που παρεμβάλλεται μεταξύ της κλειδοροής του LFSR και των δεδομένων του απλού κειμένου (ή κρυπτοκειμένου στην περίπτωση της αποκρυπτογράφησης).

Στη συνέχεια θα παρουσιάσουμε αντιπροσωπευτικά παραδείγματα γεννητριών κλειδοροής που βασίζονται σε LFSR.

Γεννήτρια Geffe

Η γεννήτρια Geffe φαίνεται στο Σχήμα 5.21. Αποτελείται από τρεις LFSR, και έναν πολυπλέκτη 2-σε-1. Ο πολυπλέκτης είναι ένα λογικό κύκλωμα το οποίο έχει μια σειρά εισόδων, μια είσοδο ελέγχου και μια έξοδο. Η είσοδος ελέγχου «αποφασίζει» ποια από τις υπόλοιπες εισόδους θα εμφανισθεί στην έξοδο. Έτσι, όταν η έξοδος του LFSR-c είναι ίση με **1**, επιλέγεται η έξοδος του LFSR-1, ενώ όταν ο έλεγχος είναι **0**, επιλέγεται η έξοδος του LFSR-2. Το κλειδί της γεννήτριας αποτελείται από τα τρία επιμέρους κλειδιά των LFSR, τα οποία αντιστοιχούν στις αρχικές καταστάσεις αυτών, αλλά μπορεί να αποτελείται και από τα χαρακτηριστικά πολυώνυμα των γραμμικών συναρτήσεων ανάδρασης.



Σχήμα 5.21 (α) Η γεννήτρια Geffe, (β) το λογικό κύκλωμα του πολυπλέκτη

Αν οι LFSR έχουν μέγεθος n_1, n_2 και n_c, τότε η γραμμική πολυπλοκότητα της κατασκευής θα είναι ίση με:

$$(n_c + 1)n_1 + n_n n_2$$

ενώ η περίοδος της γεννήτριας θα είναι ίση με το ελάχιστο κοινό πολλαπλάσιο των περιόδων των τριών LFSR.

Η γεννήτρια Geffe είναι κρυπτογραφικά αδύναμη, διότι δεν παρέχει ουσιαστική απομόνωση μεταξύ της εξόδου της γεννήτριας και των LFSR-1 και LFSR-2. Από το λογικό κύκλωμα του πολυπλέκτη, μπορούμε να υπολογίσουμε την πιθανό-

τητα το bit της εξόδου να είναι ίσο με το bit της ακολουθίας που παράγεται από τον LFSR:

$$\Pr\{k(t) = x_1(t)\} = \Pr\{x_c(t) = 1\} + \Pr\{x_c(t) = 0\} \cdot \Pr\{x_2(t) = x_1(t)\}$$
$$= \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4},$$

δηλαδή για το 75% του χρόνου, η έξοδος συμπίπτει με την έξοδο του LFSR-1. Αυτή η άνιση κατανομή δίνει το πλεονέκτημα στον αντίπαλο για να αναπτύξει επίθεση αυτοσυσχέτισης στη γεννήτρια.

Γεννήτρια κατωφλίου

Η γεννήτρια κατωφλίου, από πλευράς ασφάλειας, είναι συγκρίσιμη με τη γεννήτρια Geffe. Θεωρητικά, η χρησιμοποίηση πολλών LFSR δημιουργεί ασφαλέστερη γεννήτρια, αλλά γενικά η κατασκευή είναι ευάλωτη στις ίδιες απειλές με αυτές της γεννήτριας Geffe.

Η γεννήτρια κατωφλίου αποτελείται από παράλληλα LFSR πλήθους n, όπου κατά προτίμηση το n περιττός αριθμός. Όταν περισσότεροι από $n/2$ LFSR παράγουν **1**, τότε η έξοδος της γεννήτριας είναι **1**, ενώ στην αντίθετη περίπτωση, η έξοδος της γεννήτριας είναι **0**. Αν το πλήθος των LFSR είναι περιττός αριθμός, τότε είναι αναμενόμενο η σχετική συχνότητα των **1** να είναι ίση με αυτήν των **0**. Προκειμένου να επιτευχθεί μέγιστη περίοδος, θα πρέπει τα μεγέθη των LFSR να μην έχουν κοινούς παράγοντες και τα χαρακτηριστικά πολυώνυμα των αναδράσεων να είναι πρωτεύοντα.

Η γραμμική πολυπλοκότητα της κατασκευής είναι ίση με το άθροισμα όλων των γινομένων μεγεθών των καταχωρητών ανά δύο. Για παράδειγμα, στην περίπτωση των τριών LFSR μεγέθους n_1, n_2 και n_3 αντίστοιχα, η γραμμική πολυπλοκότητα θα είναι ίση με:

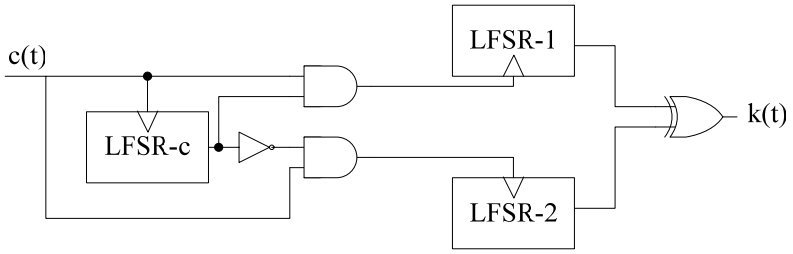
$$n_1 n_2 + n_1 n_3 + n_2 n_3 .$$

Γεννήτρια εναλλασσομένου βήματος

Στις γεννήτριες LFSR υπάρχει στην πράξη μια επιπλέον είσοδος που δεν έχουμε αναφέρει μέχρι το σημείο αυτό. Η επιπλέον είσοδος είναι η είσοδος του «ρολογιού», η οποία καθορίζει την ταχύτητα με την οποία ο LFSR θα παράγει την ακολουθία. Τυπικά η ακολουθία της εισόδου είναι μια σταθερή εναλλαγή σειράς **0** και **1**. Κάθε φορά που εμφανίζεται η εναλλαγή από **0** σε **1**, ο LFSR υπολογίζει το επόμενο bit εξόδου. Έτσι η ακολουθία ρολογιού **000111000111…** προκαλεί τη γεννήτρια LFSR να παράγει έξοδο με ρυθμό τρεις φορές μικρότερο από το ρολόι που παράγει την ακολουθία **0101010…**.

Η είσοδος του ρολογιού μπορεί να εκμεταλλευθεί στην επιλογή μεταξύ διαφορετικών LFSR. Η γεννήτρια εναλλασσομένου βήματος βασίζεται στην αρχή αυτή και παριστάνεται στο Σχήμα 5.22. Ο LFSR-c ελέγχει ποιο από τα LFSR-1 και

LFSR-2 θα υπολογίσουν το επόμενο bit. Σε οποιαδήποτε χρονική στιγμή κάποιος από τους δύο LFSR θα υπολογίσει αποκλειστικά το επόμενο bit, ενώ ο άλλος θα παραμείνει με σταθερή έξοδο.



Σχήμα 5.22 Γεννήτρια εναλλασσομένου βήματος

Η κλειδοροή που παράγεται από τη γεννήτρια εναλλασσομένου βήματος έχει τη μέγιστη περίοδο όταν τα μεγέθη των LFSR δεν έχουν κοινούς διαιρέτες μεγαλύτερους της μονάδας ανά δύο. Στην περίπτωση αυτή η περίοδος της ακολουθίας θα είναι ίση με:

$$2^{n_c}(2^{n_1}-1)(2^{n_2}-1),$$

ενώ η γραμμική πολυπλοκότητα βρέθηκε να είναι μεταξύ των ορίων:

$$(n_1+n_2)\cdot 2^{n_c-1} < LC(k(t)) \le (n_1+n_2)\cdot 2^{n_c}$$

Προς το παρόν δεν έχει καταγραφεί επιτυχής επίθεση στη γεννήτρια, επομένως για μεγάλες τιμές μεγεθών των καταχωρητών, η κατασκευή θεωρείται ασφαλής.

5.3.2. Κρυπταλγόριθμοι ροής βασισμένοι στη θεωρία πολυπλοκότητας

Η θεωρία πολυπλοκότητας χρησιμοποιείται από τη σύγχρονη κρυπτογραφία ως μέσο ανάδειξης «δύσκολων» προβλημάτων. Ο τρόπος σχεδιασμού ενός κρυπταλγόριθμου ροής με βάση τη θεωρία πολυπλοκότητας, έχει ομοιότητες με τα ασύμμετρα κρυπτοσυστήματα που εξετάζονται στο επόμενο κεφάλαιο. Σύμφωνα με τη θεωρία, το κρυπτοσύστημα σχεδιάζεται με βάση κάποιο από τα γνωστά «δύσκολα» προβλήματα, δηλαδή προβλήματα όπου ο καλύτερος διαθέσιμος αλγόριθμος που μας οδηγεί στη λύση τους, χρειάζεται εκθετικό χρόνο ως προς κάποια ελεγχόμενη παράμετρο.

Η γεννήτρια Blum, Blum και Shub (BBS)

Η ασφάλεια της γεννήτριας BBS βασίζεται στη δυσκολία παραγοντοποίησης κάποιου σύνθετου ακέραιου αριθμού *n*. Η παραγοντοποίηση είναι ένα από τα πιο γνωστά «δύσκολα» προβλήματα στα μαθηματικά, με πολλές εφαρμογές στην κρυπτογραφία.

Η γεννήτρια κατασκευάζεται ως εξής. Έστω p και q δύο πρώτοι αριθμοί για τους οποίους το υπόλοιπο της διαίρεσης με το 4 είναι 3. Το γινόμενο $n = pq$ ονομάζεται ***ακέραιος Blum***. Έστω x ένας αριθμός τέτοιος ώστε $\gcd(x, n) = 1$. Η αρχική τιμή x_0 της γεννήτριας υπολογίζεται από τη σχέση:

$$x_0 = x^2 \bmod n .$$

Το i-στό bit της ακολουθίας είναι το πρώτο από τα δεξιά bit του x_i (εκφρασμένο σε δυαδική μορφή), που ορίζεται από τη σχέση:

$$x_i = x_{i-1}^2 \bmod n .$$

Το κλειδί της γεννήτριας είναι ο αριθμός x. Οι παράγοντες p και q είναι μυστικοί, αλλά ο ακέραιος n επιτρέπεται να είναι δημόσια πληροφορία.

ΠΑΡΑΔΕΙΓΜΑ 5.5 – Δημιουργία κλειδοροής με τη γεννήτρια BBS. Δημιουργούμε τους δύο μεγάλους πρώτους p και q οι οποίοι διαιρούμενοι με 4 δίνουν υπόλοιπο 3:

p = 24672462467892469787 (= 6168115616973117446 · 4 + 3)
q = 396736894567834589803 (= 99184223641958647450 · 4 + 3)

Θέτουμε

$n = pq$ = 9788476140853110794168855217413715781961

και εκλέγουμε τυχαία έναν x τέτοιον ώστε $\gcd(x, n) = 1$. Ένας τέτοιος x είναι ο

x = 873245647888478349013

για τον οποίο πράγματι είναι

gcd(873245647888478349013,
9788476140853110794168855217413715781961) = 1.

Η αρχική τιμή x_0 είναι

$x_0 = x^2 \bmod n$ = 884529871047878009708991774601012286317 2.

Οι τιμές για τους $x_1, x_2, \ldots, x_{13}$ είναι

x_1 = 71188942811313295227459624554981238224 08
x_2 = 31451746088888931641513801520607045182 27
x_3 = 48980077823071562332722331855748994303 55
x_4 = 39354578189351129223470935461896723103 89
x_5 = 67509951151009704890176130319874024604 0
x_6 = 42899148287717401335461906582665151713 26
x_7 = 44310667114543782608903863855938175216 68
x_8 = 73368761241950463974142353336750053724 36
x_9 = 44507140707696264630629954950396580940 6

x_{10} = 297452148493377896922269953037509550661 0
x_{11} = 411584510969558468488918520236621988196 6
x_{12} = 246100424258716107455505690264137829302 6
x_{13} = 534148949234149580093205789114991579817 3.

Παίρνοντας το λιγότερο σημαντικό δυαδικό ψηφίο (bit) για κάθε έναν απ' αυτούς, που μπορεί εύκολα να γίνει ελέγχοντας απλά αν ο ακέραιος είναι περιττός ή άρτιος, παράγεται η ακολουθία, $b_1, b_2, \ldots, b_{13}$ = 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1.

Το μεγάλο πρακτικό πλεονέκτημα της γεννήτριας BBS είναι ότι στην περίπτωση που οι παράγοντες p και q του ακεραίου Blum είναι γνωστοί, είναι δυνατόν να υπολογισθεί απευθείας η τιμή x_i, χωρίς την επαναληπτική διαδικασία που απαιτεί η παραπάνω σχέση υπολογισμού. Πιο συγκεκριμένα, η x_i μπορεί να ορισθεί από την μη αναδρομική σχέση:

$$x_i = x_0^{2^i \bmod ((p-1)\cdot(q-1))}.$$

Η γεννήτρια BBS είναι ασφαλής όσο δεν είναι γνωστοί οι παράγοντες του ακεραίου Blum.

Η γεννήτρια Blum Micali (BM)

Η γεννήτρια BM βασίζεται στο πρόβλημα του διακριτού λογάριθμου. Γενικότερα, οι Blum και Micali ανέπτυξαν έναν τρόπο δημιουργίας γεννητριών με βάση την ακόλουθη θεωρία, στην οποία βασίζεται και η γεννήτρια BM.

Έστω μια συνάρτηση f η οποία ορίζει μεταθέσεις σε ένα σύνολο $\boldsymbol{F}$, δηλαδή f:$\boldsymbol{F}\rightarrow\boldsymbol{F}$, και μια συνάρτηση g:$\boldsymbol{F}\rightarrow\{0, 1\}$, τέτοια ώστε ο υπολογισμός της $g(x)$, για $x\in\boldsymbol{F}$ είναι δύσκολος, ενώ αν είναι γνωστή η ποσότητα $y = f^{-1}(x)$, τότε η $g(x)$ υπολογίζεται αποτελεσματικά. Τότε η ακολουθία

$$g(x_1)\,g(x_2)\,g(x_3)...$$

που ορίζεται από την:

$$x_i = f(x_{i-1})$$

είναι κρυπτογραφικά ασφαλής. Με βάση την παραπάνω θεωρητική κατασκευή, η γεννήτρια BM ορίζεται από το σύνολο $\boldsymbol{F} = \boldsymbol{Z}_p^*$, όπου p πρώτος και τις συναρτήσεις:

$$f(x) = a^x \bmod p \quad \text{και}$$

$$g(f(x)) = \begin{cases} 1 & \log_a(f(x)) \le \dfrac{p-1}{2} \\ 0 & \log_a(f(x)) > \dfrac{p-1}{2} \end{cases}$$

όπου το a είναι γεννήτορας $\boldsymbol{Z}_p^*$.

Το κλειδί της γεννήτριας είναι η αρχική τιμή x.

5.3.3. Ο κρυπταλγόριθμος RC4

Ο RC4 είναι από τους πιο διαδεδομένους κρυπταλγόριθμους ροής. Χρησιμοποιείται από πρωτόκολλα ασφαλείας όπως το SSL και για μεγάλο μήκος κλειδιού θεωρείται ασφαλής.

Ο RC4 είναι κρυπταλγόριθμος ροής όπου το αλφάβητο του απλού κειμένου αποτελείται από τα γράμματα του συνόλου $\{0, 1\}^8$. Οι αποθηκευτικοί χώροι απαρτίζονται από δύο πίνακες $S[0..255]$ και $T[0..255]$, όπου το κάθε στοιχείο του πίνακα αντιστοιχεί σε δυαδική λέξη των 8 bits.

Κατά την έναρξη της διαδικασίας, οι πίνακες αρχικοποιούνται:

$$S[i] = i \ , \ \text{για } 0 \le i \le 255,$$
$$T[i] = K[i \bmod k] \ , \ \text{για } 0 \le i \le 255,$$

όπου $K[j]$ η j-στη οκτάδα των bits του κλειδιού και k το μέγεθος του κλειδιού. Η έκφραση $i \bmod k$ προκαλεί ανακύκλωση των τιμών $1,2,\ldots,k$ μέχρις ότου γεμίσει ο πίνακας T από τα bits του κλειδιού.

Στη συνέχεια πραγματοποιείται μια αντιμετάθεση των στοιχείων του S, ελεγχόμενη από το κλειδί T:

$$\left.\begin{array}{l} j \leftarrow 0 : \ \text{αρχική τιμή} \\ j \leftarrow j + S[i] + T[i] \bmod 256 \\ \alpha ντιμετάθεση : S[i] \leftrightarrow S[j] \end{array}\right\} \ \text{για } 0 \le i \le 255.$$

Τέλος, εκτελείται η κυρίως διαδικασία που παράγει την ακολουθία της κλειδοροής:

$$\left.\begin{array}{l} i \leftarrow 0, j \leftarrow 0 : \ \text{αρχικές τιμές} \\ i \leftarrow i + 1 \bmod 256 \\ j \leftarrow j + S[i] \bmod 256 \\ \alpha ντιμετάθεση : S[i] \leftrightarrow S[j] \\ t \leftarrow S[i] + S[j] \bmod 256 \\ k = S[t] \end{array}\right\} n \ \text{φορές}$$

όπου n το μέγεθος του απλού κειμένου κατά την κρυπτογράφηση ή του κρυπτοκειμένου κατά την αποκρυπτογράφηση. Σε κάθε ολοκλήρωση του κύκλου υπολογισμών, η μεταβλητή k περιέχει το σύμβολο της κλειδοροής το οποίο συνδυάζεται με τα δεδομένα (απλό κείμενο ή κρυπτοκείμενο) με αποκλειστική διάζευξη.

Ασφάλεια του RC4

Παρόλο που ο RC4 είναι πολύ απλός στην κατασκευή, για μέγεθος κλειδιού ίσο με 128 bits και άνω, παραμένει ασφαλής. Οι σχετικά μικρές απαιτήσεις σε μνήμη και υπολογιστική ισχύ, καθιστούν τον RC4 μια από τις πρώτες επιλογές ως κρυπταλγόριθμο ροής. Ως λογικό επακόλουθο της απλής δομής και περιορισμένων πράξεων, ο RC4 είναι ένας από τους γρηγορότερους κρυπταλγόριθμους.

Όροι-κλειδιά του κεφαλαίου

- τρόποι λειτουργίας κρυπταλγόριθμων τμήματος
- τριπλή κρυπτογράφηση
- συνάντηση στο ενδιάμεσο
- φαινόμενο χιονοστιβάδας
- γραμμική κρυπτανάλυση
- διαφορική κρυπτανάλυση και διαφορικό χαρακτηριστικό
- αδύναμα και ημιαδύναμα κλειδιά
- συμπληρωματική ιδιότητα του DES

5.4. Ασκήσεις

1. Έστω ότι επιθυμούμε να κρυπτογραφήσουμε τα παρακάτω είδη δεδομένων:
   - εικόνα υπό μορφή bmp
   - εικόνα συμπιεσμένη υπό μορφή jpeg
   - επιστολές αρχείων txt
   - ροή δεδομένων τηλεοπτικής μετάδοσης (video-stream)

   Για καθένα από τα παραπάνω είδη, ποιόν τρόπο λειτουργίας επιλέγετε; Αιτιολογήστε την απάντησή σας.
2. Δίνεται το κουτί αντικατάστασης με τον παρακάτω πίνακα αληθείας:

P_1	P_2	P_3	C_1	C_2
0	0	0	1	1
0	0	1	0	0
0	1	0	0	1
0	1	1	0	0
1	0	0	1	0
1	0	1	1	0
1	1	0	0	1
1	1	1	1	0

   Βρείτε την καλύτερη γραμμική προσέγγιση.

3. Εξηγείστε γιατί η τελική μετάθεση επιλέχθηκε στον κρυπταλγόριθμο DES, να είναι η αντιστροφή της αρχικής.
4. Υπολογίστε την πόλωση της τυχαίας μεταβλητής
   $P_2 \oplus C_1 \oplus C_2 \oplus C_3$
   για κάθε ένα από τα κουτιά αντικατάστασης του DES.
5. Έστω ένας κρυπταλγόριθμος τμήματος με μέγεθος απλού κειμένου και κρυπτοκειμένου ίσο με 128 bits και μέγεθος κλειδιού ίσο με 128 bits. Μετά από κάποια στατιστική επίθεση, ανακαλύπτουμε τις ακόλουθες σχέσεις:
   - για οποιοδήποτε απλό κείμενο $[p_1p_2...p_{128}]$ και αντίστοιχο κρυπτοκείμενο $[c_1c_2...c_{128}]$, η αντιστροφή του p_1 έχει ως αποτέλεσμα την αντιστροφή των c_{127} και c_{128}.
   - για οποιοδήποτε απλό κείμενο $[p_1p_2...p_{128}]$ και αντίστοιχο κρυπτοκείμενο $[c_1c_2...c_{128}]$, η αντιστροφή του $p_1p_2...p_{64}$ έχει ως αποτέλεσμα την αντιστροφή του $c_{65}c_{66}\ldots c_{128}$.

   (α) Υπολογίστε τη μείωση του χώρου αναζήτησης του κλειδιού.
   (β) Ποιο είναι το ενεργό μέγεθος του κλειδιού;
   (γ) Σχεδιάστε το λογικό κύκλωμα που εκμεταλλεύεται τις παραπάνω σχέσεις, προκειμένου να πραγματοποιηθεί εξαντλητική αναζήτηση στον μειωμένο χώρο.