ΚΕΦΑΛΑΙΟ 4

Βασικές έννοιες της κρυπτογραφίας

Στο κεφάλαιο αυτό εισάγονται οι βασικές έννοιες της κρυπτογραφίας, όπως τα είδη των αλγορίθμων ανάλογα με το κλειδί, τα είδη αλγορίθμων ανάλογα με το πως συμπεριφέρονται στο αρχικό κείμενο κ.ά.

4.1 Εισαγωγή

Αρχικά, η Κρυπτογραφία αποτέλεσε την τεχνική της απόκρυψης του περιεχομένου ενός μηνύματος, από μη εξουσιοδοτημένες οντότητες. Στις μέρες μας η Κρυπτογραφία έχει αναχθεί σε επιστήμη, με τις εφαρμογές τις διαρκώς να πληθαίνουν. Προτού δούμε πως καταφέρνει να πετύχει τους στόχους της, οφείλουμε να δούμε κάποιους βασικούς ορισμούς τους οποίους θα χρησιμοποιούμε συνεχώς στο υπόλοιπο σύγγραμα

Ορισμός 65. Αρχικό κείμενο (plaintext), ονομάζεται το αρχικό μήνυμα που θέλουμε να κρυπτογραφήσουμε. Πολύ συχνά το ονομάζουμε και απλό ή καθαρό.

Ορισμός 66. Κρυπτογραφημένο κείμενο ή κρυπτογράφημα (ciphertext), ονομάζεται η μυστική-κρυπτογραφημένη μορφή του κειμένου.

Ορισμός 67. Αλγόριθμος κρυπτογράφησης (encyption algorithm) ή μέθοδος κρυπτογράφησης (ciphering), ονομάζεται η μέθοδος που ακολουθείται για τη μετατροπή του αρχικού κειμένου σε μυστική μορφή.

Ορισμός 68. Κρυπτογράφηση (encryption), ονομάζεται η διαδικασίας μετατροπής του αρχικού κειμένου σε κρυπτογράφημα.

Ορισμός 69. Αποκρυπτογράφηση (decryption, deciphering) ονομάζεται η αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή η μετατροπή του κρυπτογραφήματος σε αρχικό κείμενο.

Ορισμός 70. Κλειδί (key) κρυπτογράφησης, ονομάζεται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης. Το κλειδί για παράδειγμα μπορεί να είναι η αντιστοιχία γραμμάτων του αρχικού κειμένου και του κρυπτογραφήματος.

Ορισμός 71. Κάλυμμα ενός μηνύματος (padding), ονομάζουμε το επιπρόσθετο κείμενο το οποίο πρέπει να προσθέσουμε στο κείμενο προκειμένου το αρχικό κείμενο να αποκτήσει ένα συγκεκριμένο αρχικό μήκος που απαιτεί κάποιος αλγόριθμος κρυπτογράφησης.

Συνήθως το κείμενο που προστίθεται είναι το μήκος του αρχικού κειμένου ακολουθούμενο από μηδενικό ή αντίστροφα, προφανώς το κάλυμμα αφαιρείται κατά την αποκρυπτογράφηση.

Η υλοποίηση ενός κρυπτογραφικού αλγόριθμου ονομάζεται κρυπτογραφικό σύστημα ή κρυπτοσύστημα, ενώ πρωτόκολλα που κάνουν χρήση κρυπτογραφικών αλγορίθμων ονομάζονται κρυπτογραφικά.

Η κρυπτογραφία μαζί με την κρυπτανάλυση, που στοχεύει στην εύρεση αδυναμιών σ' ένα κρυπτογραφικό σύστημα, συνιστούν σήμερα το μεγαλύτερο μέρος της επιστήμης της κρυπτολογίας.

Γενικά στην σύγχρονη κρυπτογραφία, ακολουθείται ο κανόνας του Kerckhoffs. Ο Kerckhoffs το 1883 έθεσε ένα πολύ βασικό και απλό κανόνα για τους αλγόριθμους κρυπτογράφησης, η ασφάλειά τους θα πρέπει να βασίζεται μόνο στο κλειδί τους [93]. Θεωρητικά κάποιος ο οποίος θέλει να επιτεθεί στον αλγόριθμο, μπορεί να τον γνωρίζει. Έτσι αν η δομή του αλγορίθμου δεν είναι ασφαλής και ελεγμένη, η απόκρυψή της δεν την κάνει περισσότερο ασφαλή, μάλιστα η μυστικότητα, μπορεί να δώσει την ψευδή αίσθηση της ασφάλειας, κάτι το οποίο θα το δούμε και στη συνέχεια. Στη σύγχρονη κρυπτογραφία, όλο και περισσότερο οι αλγόριθμοι παρουσιάζονται δημόσια, προκειμένου η επιστημονική κοινότητα να εκτιμήσει την προσφερόμενη ασφάλεια, αφήνοντας την ασφάλεια να βασίζεται μόνο στην απόκρυψη των κλειδιών αποκρυπτογράφησης.

Από τον ορισμό που δώσαμε για τον αλγόριθμο κρυπτογράφησης, απουσιάζει η έννοια της ασφάλειας. Το γεγονός αυτό έγινε σκόπιμα, προκειμένου να δούμε αναλυτικά τις προϋποθέσεις τις οποίες πρέπει να πληροί ένας αλγόριθμος κρυπτογράφησης προκειμένου να θεωρείται ασφαλής και γιατί κάποιες συχνές υποθέσεις δεν οδηγούν σε πραγματικά ασφαλείς αλγόριθμους κρυπτογράφησης.

Έστω ότι έχουμε ένα αλγόριθμο για τον οποίο κανείς άλλος, εκτός των εξουσιοδοτημένων, δεν μπορεί να βρει σε πιο αρχικό κείμενο αντιστοιχεί κάποιο κρυπτογραφημένο κείμενο. Αν και ένας τέτοιος αλγόριθμος κρυπτογράφησης φαίνεται να είναι ασφαλής, δεν είναι. Κανείς δεν μπορεί να εγγυηθεί στον αλγόριθμο αυτό ότι ένας κρυπταναλυτής μπορεί να μην αποσύρει ολόκληρο το αρχικό κείμενο, αλλά μέρος του. Σε πολλές περιπτώσεις είναι προφανές πως αρκούν λίγες πληροφορίες για να βγάλουμε συμπεράσματα. Ας φανταστούμε ότι με ένα τέτοιο αλγόριθμο κρυπτογράφησης έχουμε κρυπτογραφήσει ένα βιβλίο, προφανώς αν ο κρυπταναλυτής καταφέρει να ανακτήσει ακόμα και μερικές σελίδες, μπορεί να κα-

ταλάβει πιο βιβλίο είναι.

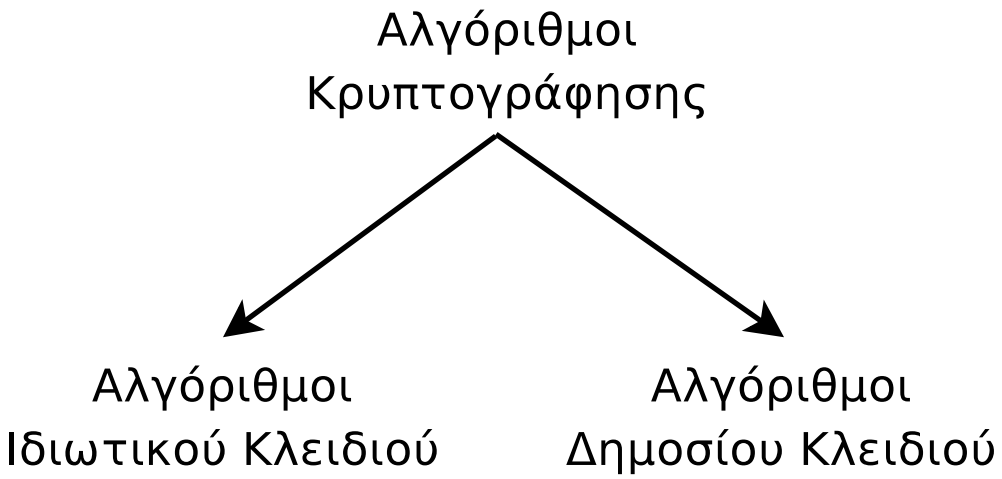
Ας υποθέσουμε τώρα ότι έχουμε ένα αλγόριθμο κρυπτογράφησης για τον οποίο κανείς άλλος, εκτός των εξουσιοδοτημένων, δεν μπορεί να ανακτήσει κανένα χαρακτήρα του αρχικού κειμένου από το κρυπτογραφημένο. Παρόλα αυτά, ίσως κάποιος να μπορεί να εξάγει πράγματα από το κρυπτογραφημένο. Αν για παράδειγμα είχαμε τις κρυπτογραφημένες βαθμολογίες μαθητών, να μπορούσε να καταλάβει κανείς ποιοι έχουν τον ίδιο βαθμό ή ποίοι έχουν μεγαλύτερο ή μικρότερο βαθμό. Η πληροφορία αυτή σε πολλές περιπτώσεις μπορεί να είναι ιδιαίτερα χρήσιμη.

Το να υποθέσουμε ότι έχουμε ένα αλγόριθμο κρυπτογράφησης για τον οποίο κανείς άλλος, εκτός των εξουσιοδοτημένων, δεν μπορεί να ανακτήσει κάποια σημαντική πληροφορία από το κρυπτογραφημένο κείμενο για το αρχικό και πάλι δεν μπορεί να θεωρηθεί αρκετό, καθώς η έννοια της σημαντικότητας είναι καθαρά υποκειμενική. Συνεπώς, οδηγούμαστε σε ένα πιο ασαφή ορισμό, αυτόν των Katz και Lindell [70], ένας αλγόριθμος θεωρείται ασφαλής αν κανείς άλλος, εκτός των εξουσιοδοτημένων, δεν μπορεί να υπολογίσει οποιαδήποτε συνάρτηση του αρχικού κειμένου από οποιοδήποτε κρυπτογραφημένο κείμενο.

Ακόμα όμως και αυτός ο ορισμός δεν είναι αρκετός, καθώς όπως θα δούμε στην κρυπτανάλυση, υπάρχουν επιθέσεις στις οποίες κάποια ζεύγη αρχικού και κρυπτογραφημένου κειμένου είναι γνωστά στον κρυπταναλυτή και οδηγούν σε αποκάλυψη του κλειδιού κρυπτογράφησης. Οδηγούμαστε λοιπόν στον ακόλουθο ορισμό.

Ορισμός 72. Ένας αλγόριθμος θεωρείται ασφαλής αν κανείς άλλος, εκτός των εξουσιοδοτημένων, δεν μπορεί να υπολογίσει οποιαδήποτε συνάρτηση του αρχικού κειμένου, δεδομένων οποιοδήποτε άλλων ζευγών αρχικού και κρυπτογραφημένου κείμενο ή μόνο κρυπτογραφημένου κείμενου, σε γόνιμο για οποιοδήποτε εξουσιοδοτημένο χρήστη χρονικό διάστημα.

Στον ορισμό θέτουμε και τον χρονικό περιορισμό, καθώς αν κάποιος αντίπαλος μπορεί να ανακτήσει την απαραίτητη πληροφορία σε 400 χρόνια, όταν όλοι θα έχουν αποβιώσει, η πληροφορία πλέον θα είναι για αυτόν ανούσια. Επιπλέον με εξαντλητική αναζήτηση, είναι δεδομένο ότι κάποια στιγμή ο κρυπταναλυτής θα βρει το αρχικό κείμενο και ίσως να μπορεί να καταλάβει ότι αντιστοιχεί στο



Σχήμα 4.1: Αλγόριθμοι κρυπτογράφησης.

κρυπτογραφημένο κείμενο, το θέμα είναι να μπορούν οι εξουσιοδοτημένες οντότητες να ξέρουν ότι αν γίνει κάτι τέτοιο, η πληροφορία θα είναι πλέον άχρηστη.

Για να γίνει καλύτερα αντιληπτό ας πάρουμε για παράδειγμα την κρυπτογράφηση του αριθμού μίας πιστωτικής κάρτας. Αν αυτός μπορεί αποκαλυφθεί μετά από 100 χρόνια από ένα κρυπταναλυτή με όλους τους διαθέσιμους πόρους που μπορεί να έχει, τότε κατά πάσα πιθανότητα ο ιδιοκτήτης θα έχει πεθάνει, η κάρτα θα έχει ακυρωθεί και η πληροφορία δεν θα του είναι καθόλου χρήσιμη, έτσι λοιπόν ο αλγόριθμος θα πρέπει να θεωρείται ασφαλής.

4.2 Είδη αλγορίθμων κρυπτογράφησης

Οι αλγόριθμοι κρυπτογράφησης, ανάλογα με το είδος του κλειδιού χωρίζονται σε δύο βασικές κατηγορίες, τους αλγόριθμους ιδιωτικού κλειδιού και τους αλγόριθμους δημοσίου κλειδιού, σχήμα 4.1.

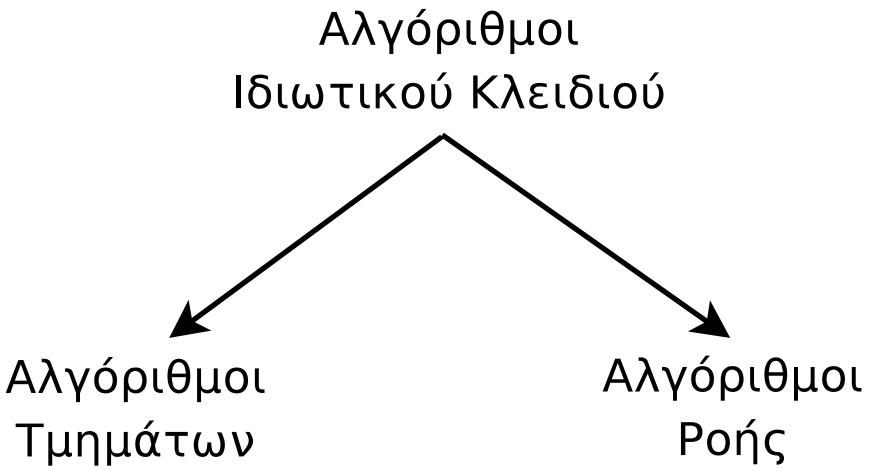
Οι αλγόριθμοι ιδιωτικού κλειδιού ονομάζονται αλλιώς μυστικού κλειδιού ή και συμμετρικοί, καθώς χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Από τη στιγμή που το κλειδί είναι κοινό, έπεται ότι πριν από οποιαδήποτε κρυπτογράφηση, θα πρέπει να έχει με-

ταβιβαστεί ένα μυστικό κλειδί μεταξύ των οντοτήτων που θέλουν να επικοινωνήσουν. Τίθεται λοιπόν το πρόβλημα της ύπαρξης ενός ασφαλούς δίαυλου επικοινωνίας μεταξύ των δύο οντοτήτων. Η απουσία ενός τέτοιου διαύλου μειώνει την δυνατότητα χρήσης τέτοιων αλγορίθμων. Αρκεί να φανταστεί κανείς ότι οι δύο οντότητες δεν έχουν τη δυνατότητα ίσως να έρθουν σε φυσική επαφή, σε γόνιμο χρονικό διάστημα, καθώς μπορούν να βρίσκονται σε αντιδιαμετρικά σημεία του πλανήτη, ή ακόμη και αν είναι κοντά, το χρονικό περιθώριο μπορεί να είναι τέτοιο που να μην είναι δυνατό να γίνει αυτή η ανταλλαγή κλειδιών. Στα χαρακτηριστικά αυτών των αλγορίθμων συγκαταλέγονται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης, το μικρό μήκος κλειδιού, καθώς και η ευκολία υλοποίησης σε επίπεδο υλικού και λογισμικού. Χαρακτηριστικοί αλγόριθμοι αυτής της κατηγορίας είναι οι DES, AES, RC5, RC6, Skipjack.

Οι αλγόριθμοι δημοσίου κλειδιού ή αλλιώς και ασύμμετροι, χρησιμοποιούν δύο κλειδιά, ένα δημόσιο για την κρυπτογράφηση και ένα μυστικό ή αλλιώς ιδιωτικό για την αποκρυπτογράφηση. Παρόλο που τα δύο κλειδιά σχετίζονται μεταξύ τους, η γνώση του δημοσίου κλειδιού δεν καθιστά εφικτό τον υπολογισμό του μυστικού κλειδιού από κανένα εκτός του δημιουργού τους. Στην περίπτωση αυτή το αρχικό μήνυμα κρυπτογραφείται με το δημόσιο κλειδί και μόνο ο κάτοχος του μυστικού κλειδιού (παραλήπτης) μπορεί να το αποκρυπτογραφήσει. Σε αυτήν την κατηγορία ανήκουν οι αλγόριθμοι RSA, ElGamal, NTRU και Paillier. Θα πρέπει να τονιστεί ότι οι αλγόριθμοι κρυπτογράφησης της συγκεκριμένης κατηγορίας, βασίζονται στην ύπαρξη συναρτήσεων καταπακτής, που αναλύθηκαν στο προηγούμενο κεφάλαιο. Χαρακτηριστικό αυτής της κατηγορίας αλγορίθμων αποτελεί το μεγάλο μήκος κλειδιού και η αργή τους ταχύτητα. Συγκριτικά με τους αλγορίθμους ιδιωτικού κλειδιού μπορεί και να είναι ακόμα και 1000 φορές πιο αργοί.

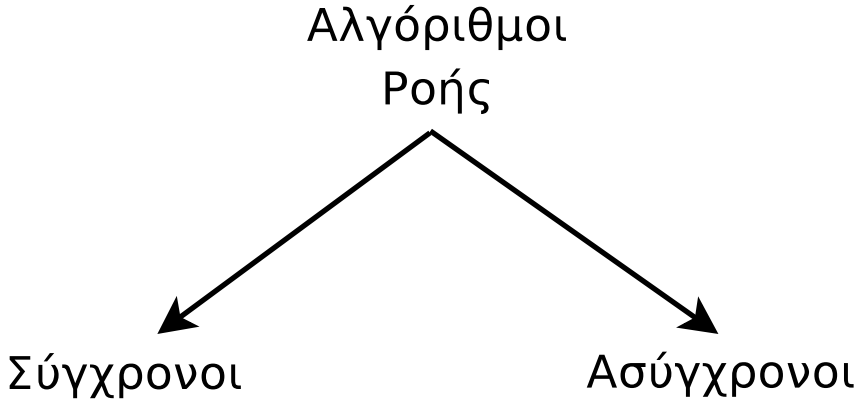
Κατηγοριοποίηση γίνεται και στους αλγόριθμους κρυπτογράφησης ιδιωτικού κλειδιού ανάλογα με τον τρόπο που ενεργούν στο αρχικό κείμενο. Έτσι έχουμε δύο κατηγορίες, τους αλγόριθμους τμημάτων (block ciphers) και τους αλγόριθμους ροής (stream ciphers), σχήμα 4.2.

Αλγόριθμοι τμημάτων n-bit (block cipher). Το αρχικό μήνυμα διαιρείται σε τμήματα των n-bits, και κάθε τμήμα κρυπτογραφείται



Σχήμα 4.2: Αλγόριθμοι ιδιωτικού κλειδιού.

ανεξάρτητα από τα υπόλοιπα. Οι αλγόριθμοι τμημάτων χωρίζουν το κείμενο σε τμήματα και κρυπτογραφούν ξεχωριστά καθένα από αυτά. Αυτό έχει ως αποτέλεσμα αν ένα τμήμα γίνει γνωστό, τότε κάθε φορά που εμφανίζεται, να μπορεί κάποιος να ξέρει τι σημαίνει. Ας υποθέσουμε ότι έχουμε ένα πίνακα με δύο στήλες, τη μία με τους αριθμούς μητρώων των φοιτητών και τη δεύτερη με τη βαθμολογία τους, κρυπτογραφημένη με ένα αλγόριθμο τμημάτων. Ας υποθέσουμε επιπλέον ότι ένας φοιτητής αποκτά πρόσβαση σε αυτόν τον πίνακα. Αν ξέρει τον βαθμό του μπορεί να μάθει πόσοι και ποίοι έχουν τον ίδιο βαθμό με αυτόν, απλά κοιτάζοντας πόσοι και ποιοι έχουν την ίδια κρυπτογραφημένη βαθμολογία με τον ίδιο. Επιπλέον μπορεί να αλλοιώσει τις βαθμολογίες χωρίς να το καταλάβει κανείς, αφού αν αντιγράψει τον κρυπτογραφημένο του βαθμό, ακόμα και αν δεν τον ξέρει, στη δεύτερη στήλη, όλοι θα έχουν την ίδια βαθμολογία με αυτόν. Η αλλοίωση αυτή δεν θα μπορεί να γίνει αντιληπτή από κανένα, εκτός και αν ήξερε τα δεδομένα από πριν. Αξίζει να προσέξουμε πως στην όλη διαδικασία που περιγράφηκε, το κλειδί κρυπτογράφησης και αποκρυπτογράφησης δεν χρησιμοποιήθηκε πουθενά. Για να αποφευχθούν τέτοια πρόβλημα οι αλγόριθμοι ροής έχουν διάφορες καταστάσεις λειτουργίας.

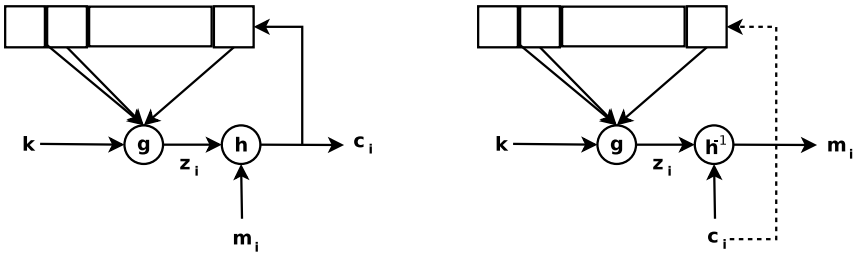


Σχήμα 4.3: Αλγόριθμοι ροής.

Αλγόριθμοι ροής (stream cipher). Σε αυτήν τη κατηγορία ανήκουν αλγόριθμοι των οποίων η κρυπτογράφηση αλλάζει με τη πάροδο του χρόνου εκτέλεσής τους, κρυπτογραφώντας έτσι διαφορετικά κάθε byte ή ακόμα και bit. Συνήθως βασίζονται σε γεννήτριες «ψευδο-τυχαίων» bit τα οποία γίνονται XOR με το απλό κείμενο. Επιστρέφοντας στο προηγούμενο παράδειγμα αν η κρυπτογράφηση είχε γίνει με αλγόριθμο ροής, αρχικά ο φοιτητής δεν θα μπορούσε να μάθε πόσοι έχουν τον ίδιο βαθμό με τον ίδιο, αφού και το ίδια να φαινόταν η κρυπτογραφημένη βαθμολογία τους, δε θα σήμαινε σε καμία περίπτωση ότι είχαν την ίδια βαθμολογία. Αν αποφασίσει να αλλοιώσει τις βαθμολογίες, αντιγράφοντας την κρυπτογραφημένη του βαθμολογία στη δεύτερη στήλη, τότε είναι πολύ πιθανό να γινόταν αντιληπτή η αλλοίωση, αφού η αποκρυπτογράφηση των δεδομένων πολύ πιθανό να μην οδηγούσε σε έγκυρες βαθμολογίες ή ακόμα να οδηγούσε και σε μη αριθμητικούς χαρακτήρες.

Οι αλγόριθμοι ροής χωρίζονται σε δύο κατηγορίες, στους σύγχρονους και τους ασύγχρονους, σχήμα 4.3, ανάλογα με το αν έχουν τη δυνατότητα να συνεχίσουν τη διαδικασία της κρυπτογράφησης-αποκρυπτογράφησης σε περίπτωση λανθασμένης μεταβίβασης δεδομένων.

Σύγχρονοι αλγόριθμοι ροής Σε αυτή τη περίπτωση, η επόμενη κατάσταση που θα βρίσκεται το σύστημα είναι ανεξάρτητη τόσο από

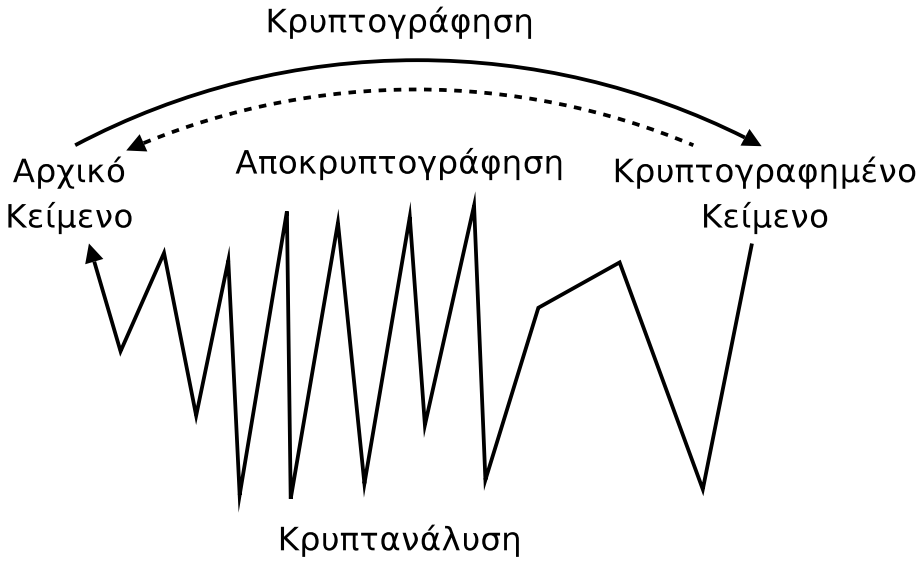


Σχήμα 4.4: Ασύγχρονοι αλγόριθμοι ροής

το κείμενο που κρυπτογραφείται, όσο και από και από το κρυπτογραφημένο κείμενο. Σε ένα τέτοιο αλγόριθμο, αν μεταβιβαστεί ένα bit λανθασμένα, τότε δεν θα επηρεαστεί η αποκρυπτογράφηση των επόμενων bits.

Ασύγχρονοι αλγόριθμοι ροής Αντίθετα με τους σύγχρονους αλγόριθμους στους ασύγχρονοι αλγόριθμους, η κατάσταση στην οποία βρίσκεται το σύστημα, είναι άμεσα εξαρτημένη από την το κείμενο που έχει προηγουμένως αποκρυπτογραφηθεί, σχήμα 4.4. Αυτό έχει σαν αποτέλεσμα αν μεταβιβαστεί ένα bit λανθασμένα, τα επόμενα bits να μη μπορούν να αποκρυπτογραφηθούν σωστά. Για αυτό το λόγο, οι αλγόριθμοι αυτοί ανά τακτά διαστήματα στέλνουν ειδικά μηνύματα επανασυγχρονισμού. Έτσι αν η τρέχουσα κατάσταση εξαρτάται από n προηγούμενες καταστάσεις, τότε σε n αποκρυπτογραφήσεις το πολύ, το λάθος θα γίνει αντιληπτό και θα γίνει επανασυγχρονισμός. Για το λόγο αυτό, οι αλγόριθμοι αυτοί ονομάζονται και αυτοσυγχρονιζόμενοι.

Η ιδιότητα των ασύγχρονων αλγορίθμων ροής να εξαρτώνται από n προηγούμενες καταστάσεις, μπορεί να θεωρηθεί ως μειονέκτημα, αφού κάποιος ο οποίος θέλει να κρυπταναλύσει τον αλγόριθμο χωρίς να γνωρίζει το κλειδί, ίσως να έχει αρκετά δεδομένα [65]. Παρόλα αυτά, υπάρχουν πολύ λίγες αναφορές τέτοιων αλγορίθμων [66, 67, 68].



Σχήμα 4.5: Κρυπτογράφηση και αποκρυπτογράφηση.

4.3 Δομικά στοιχεία ενός αλγορίθμου τμημάτων

Οι αλγόριθμοι τμημάτων όπως είπαμε επεξεργάζονται τμήματα σταθερού μήκους του αρχικού κειμένου. Συνήθως κατά την επεξεργασία αυτή, γίνονται όμοιες επαναλήψεις μίας διαδικασίας, τις επαναλήψεις αυτές τις ονομάζουμε γύρους. Στους γύρους χρησιμοποιούνται τις περισσότερες φορές μέρη των αρχικών κλειδιών, τα οποία ονομάζονται υποκλειδιά. Αν δύο κλειδιά δημιουργούν ίδια υποκλειδιά σε ένα αλγόριθμο, τα ονομάζουμε αδύνατα κλειδιά του αλγορίθμου.

Ένα άλλο βασικό χαρακτηριστικό που βρίσκεται σε πάρα πολλούς αλγορίθμους είναι τα κουτιά αντικατάστασης (s-boxes). Ένα s-box αντικαθιστά την είσοδο χρησιμοποιώντας τις τιμές ενός πίνακα που καθορίζεται από τον εκάστοτε αλγόριθμο.

Παράδειγμα 63. Έστω ένα s-box S το οποίο για είσοδο ένα αριθμό μήκους 4 bits χρησιμοποιεί τα πρώτα δύο bits για να βρει τη σειρά και τα επόμενα δύο για τη στήλη, το οποίο είναι της μορφής

	00	**01**	**10**	**11**
00	11	01	10	00
01	00	10	11	01
10	01	11	00	11
11	11	10	00	01

Τότε έχουμε ότι S(0001) = 01, S(1011) = 11 και S(1111) = 01.

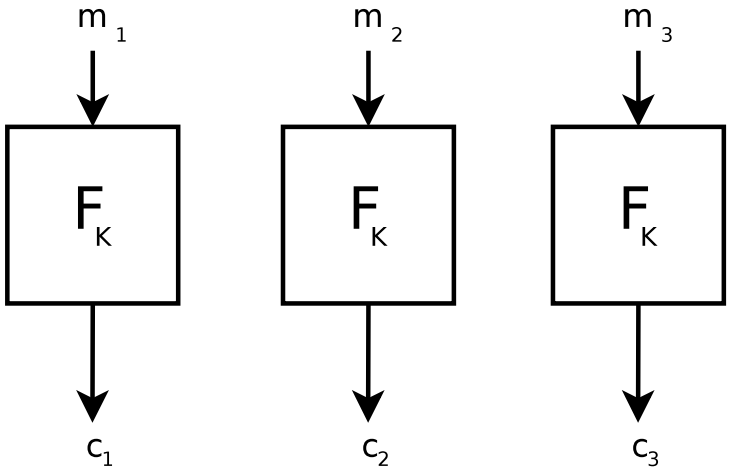
Θα πρέπει να προσέξουμε ότι ένα s-box δεν χρειάζεται να είναι ορίζει αντιστρέψιμη αντικατάσταση, ούτε το μήκος της εξόδου του να είναι όσο της εισόδου του.

4.4 Καταστάσεις λειτουργίας αλγορίθμων τμημάτων

Οι αλγόριθμοι τμημάτων ανάλογα με το πως διαχειρίζονται τα τμήματα κατά την κρυπτογράφηση, έχουν τις διάφορες καταστάσεις λειτουργίας. Ο βασικός λόγος είναι για να αποφευχθούν προβλήματα όπως αυτά που φαίνονται στο σχήμα 4.11, όπου είναι προφανές ότι η χρήση των αλγορίθμων τμημάτων μπορεί να αποτελέσει πρόβλημα. Στη εικόνα φαίνεται ότι κάθε pixel έχει 'χάσει' το χρώμα του, παρόλα αυτά, βλέποντας κανείς το κρυπτογραφημένο μήνυμα μπορεί να καταλάβει αρκετά για τη δομή του αρχικού. Έτσι λοιπόν έχουμε διάφορες καταστάσεις λειτουργίας, προκειμένου να έχουμε αποτελέσματα όπως αυτό στην εικόνα του σχήματος 4.12, αλλάζοντας την είσοδο του αλγορίθμου σε κάθε επανάληψή του.

Electronic Codebook (ECB). Σε αυτήν τη κατάσταση λειτουργίας, ο αλγόριθμος κρυπτογραφεί κάθε τμήμα ξεχωριστά με αποτέλεσμα το ίδιο τμήμα να έχει πάντα την ίδια κρυπτογράφηση. Έτσι λοιπόν η κρυπτογράφηση ενός τμήματος μηνύματος εξαρτάται αποκλειστικά από το κλειδί και από το τμήμα του μηνύματος, σχήμα 4.6.

Cipher Block Chaining (CBC). Σε αυτήν τη κατάσταση λειτουργίας, ξεκινάμε με μία τυχαία τιμή $s_0 = IV$ την οποία κάνουμε αποκλειστική διάζευξη με το πρώτο αρχικό κείμενο, στη συνέχεια ο



Σχήμα 4.6: Κατάσταση λειτουργίας ECB.

αλγόριθμος κρυπτογραφεί το κάθε τμήμα και κάνει αποκλειστική διάζευξη της εξόδου με το επόμενο τμήμα που έχει να κρυπτογραφηθεί. Με αυτόν τον τρόπο αν και ο αλγόριθμος είναι τμημάτων, είναι σχεδόν αδύνατο το ίδιο τμήμα να έχει πάντα την ίδια κρυπτογράφηση. Αντίθετα μπορούμε να έχουμε δύο διαφορετικά τμήματα με την ίδια κρυπτογράφηση, σχήμα 4.7. Έχουμε δηλαδή ότι

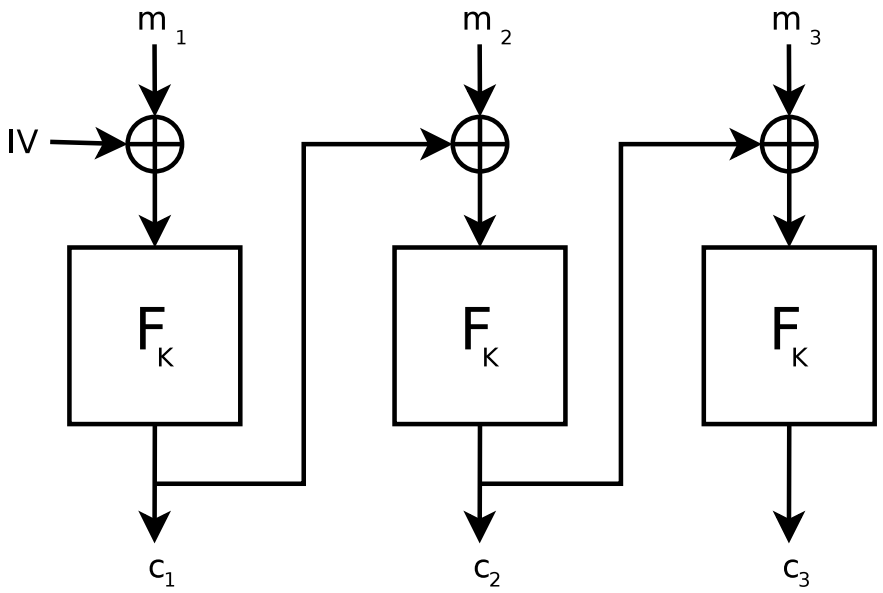
$$c_i = F_K(m_i \oplus c_{i-1})$$

όπου F_K η συνάρτηση κρυπτογράφησης με κλειδί K.

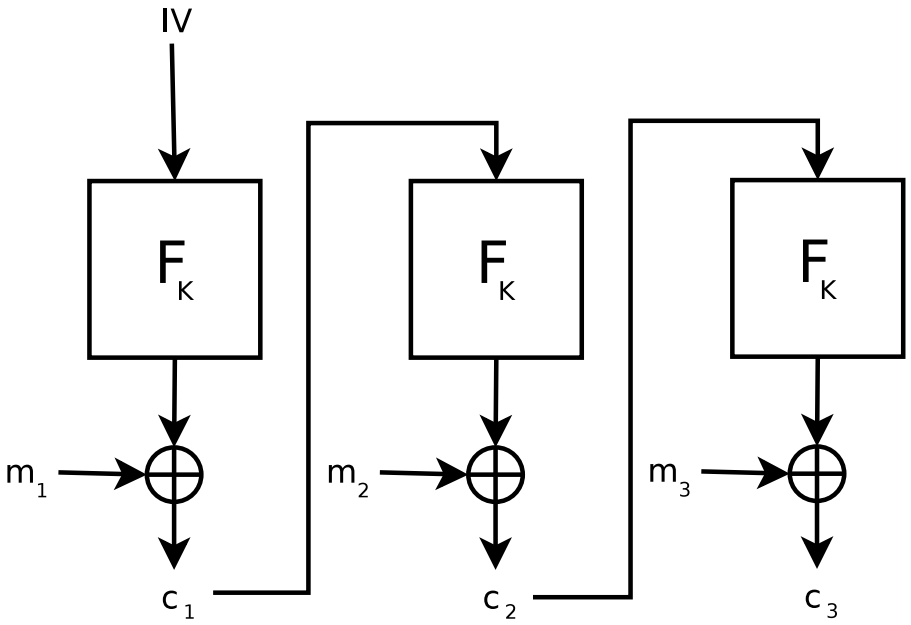
Cipher Feedback (CFB). Σε αυτήν την κατάσταση λειτουργίας, ξεκινάμε με μία τυχαία τιμή $s_0 = IV$, την οποία κρυπτογραφούμε και κάνουμε αποκλειστική διάζευξη με το πρώτο μέρος του κειμένου παράγοντας το c_1. Στην συνέχεια κρυπτογραφούμε το κάθε c_i και το κάνουμε αποκλειστική διάζευξη με το τμήμα του κειμένου που πρέπει να κρυπτογραφηθεί, σχήμα 4.8. Έχουμε δηλαδή ότι

$$c_i = m_i \oplus F_K(c_{i-1})$$

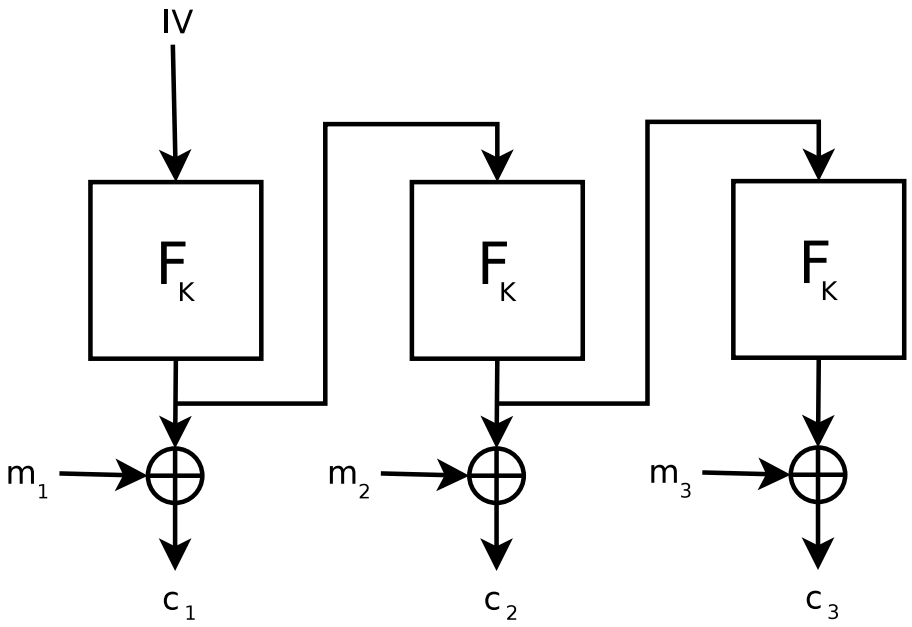
όπου F_K η συνάρτηση κρυπτογράφησης με κλειδί K.



Σχήμα 4.7: Κατάσταση λειτουργίας CBC.



Σχήμα 4.8: Κατάσταση λειτουργίας CFB.



Σχήμα 4.9: Κατάσταση λειτουργίας OFB.

Output Feedback (OFB). Σε αυτήν την κατάσταση λειτουργίας, ξεκινάμε με μία τυχαία τιμή $s_0 = IV$, την οποία διαρκώς κρυπτογραφούμε παράγοντας τα επόμενα s_i. Το κάθε s_i το κάνουμε αποκλειστική διάζευξη με το τμήμα του κειμένου που πρέπει να κρυπτογραφηθεί, σχήμα 4.9. Έχουμε δηλαδή ότι

$$c_i = m_i \oplus s_i$$

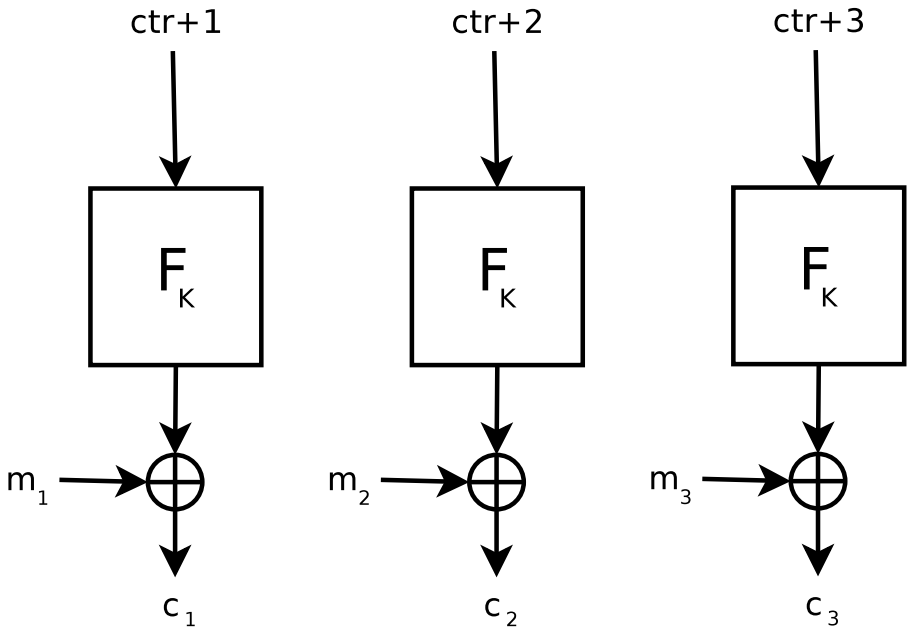
όπου

$$s_i = F_K(s_{i-1})$$

και F_K η συνάρτηση κρυπτογράφησης με κλειδί K.

Counter (CTR) Αν και υπάρχουν διάφορες εκδοχές αυτής της κατάστασης λειτουργίας, εδώ θα περιγράψουμε την λεγόμενη 'τυχαιοποιημένη' μορφή της. Έστω λοιπόν ότι έχουμε μια τυχαία τιμή την ctr και έστω ότι συμβολίζουμε την συνάρτηση κρυπτογράφηση ενός τμήματος m_i με τον αλγόριθμο τμημάτων F_K, όπου K το κλειδί. Τότε η κρυπτογράφηση του i τμήματος θα είναι

$$c_i = m_i \oplus F_K(ctr + i)$$



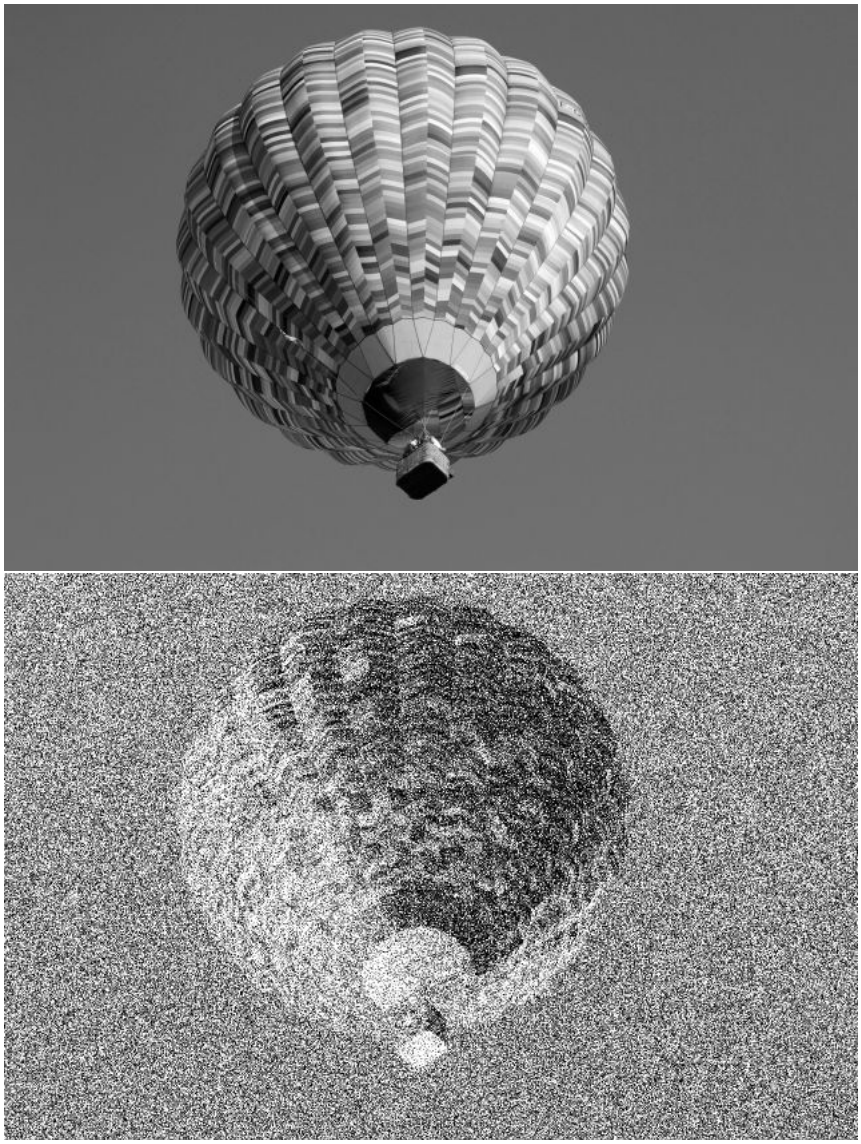
Σχήμα 4.10: Κατάσταση λειτουργίας Counter.

Διαγραμματικά, η κατάσταση λειτουργίας αυτή φαίνεται στο σχήμα 4.10.

Χρησιμοποιώντας κάποιον άλλο τρόπο λειτουργίας από τον ECB η έξοδος που έχει ένας αλγόριθμος τμημάτων μπορεί να γίνει έξοδος αλγορίθμου ροής. Θα μπορούσαμε λοιπόν να πούμε πως οι αλγόριθμοι ροής μπορούν να θεωρηθούν ως πολύ απλοί αλγόριθμοι τμημάτων όπου το μήκος του τμήματος είναι ίσο με 1 bit.

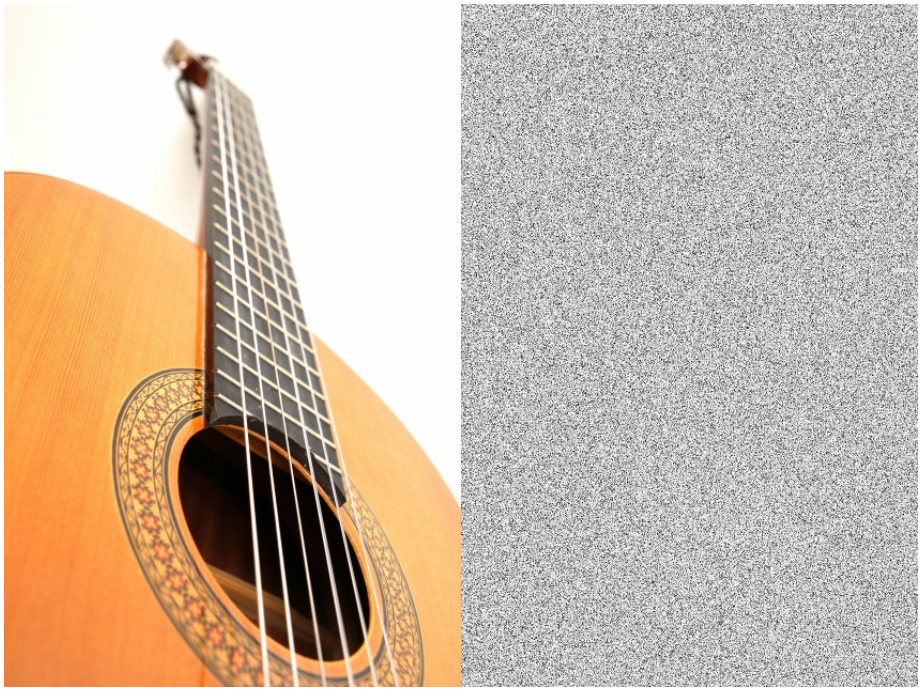
4.5 Δίκτυα αντικατάστασης και μετάθεσης

Τα δίκτυα αντικατάστασης και μετάθεσης (Substitution-Permutation Networks) προσπαθούν να ακολουθήσουν πιστά τις αρχές του Claude Shannon, ο οποίος θέτει ως βασικές αρχές για την δημιουργία ενός ασφαλούς αλγόριθμου κρυπτογράφησης, την σύγχυση (confusion) και την διάχυση (difussion) της πληροφορίας [73]. Έτσι σε κάθε γύρο ενός αλγορίθμου τμημάτων, υπάρχει ένα κουτί αντικατάστασης



Σχήμα 4.11: Η κρυπτογράφηση μίας φωτογραφίας με τη χρήση της μεθόδου ECB.

Η κρυπτογραφημένη εικόνα μας δίνει στοιχεία για την αρχική.

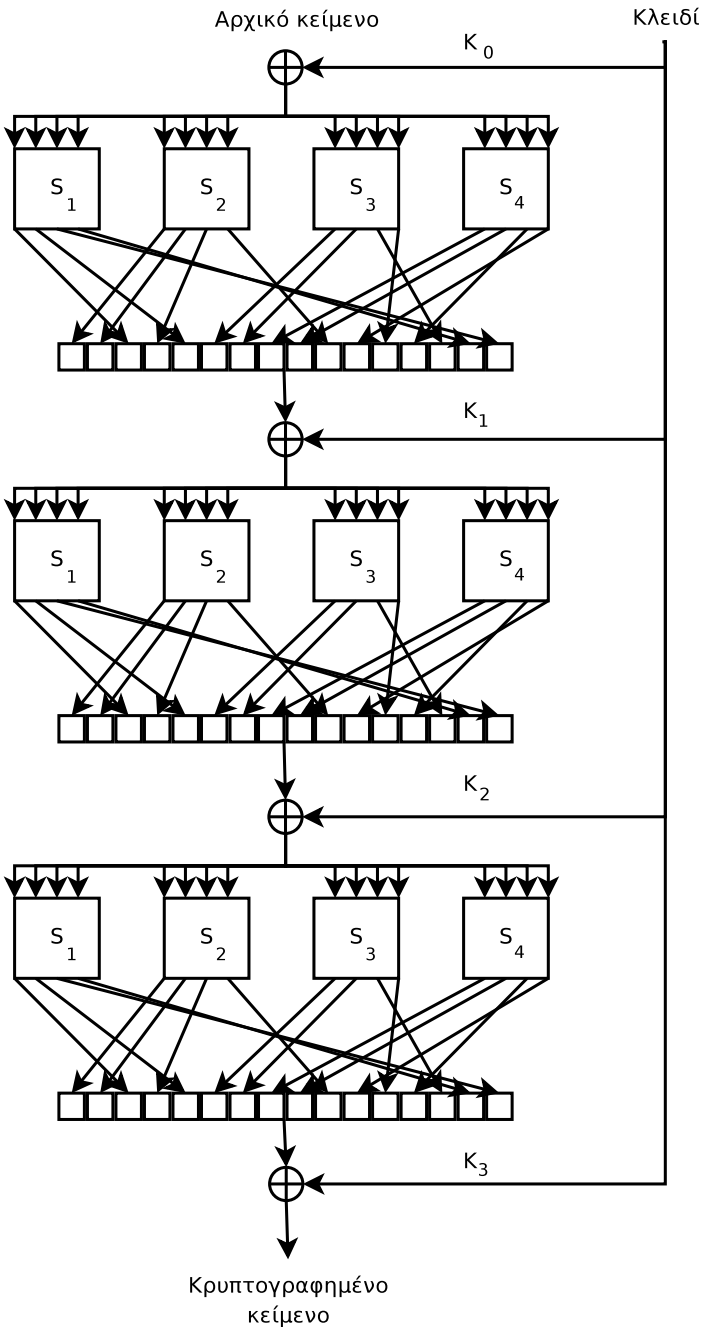


Σχήμα 4.12: Η κρυπτογράφηση μίας φωτογραφίας με τη χρήση της μεθόδου CBC.

Η κρυπτογραφημένη εικόνα δεν μας δίνει στοιχεία για την αρχική.

(s-box) για να προκαλέσει τη σύγχυση της πληροφορίας και μετάθεση των bits, για να επιτευχθεί η διάχυση της πληροφορίας. Στο τέλος κάθε γύρου, γίνεται αποκλειστική διάζευξη με το κλειδί του κάθε γύρου, που πηγάζει από το αρχικό κλειδί. Γραφική αναπαράσταση των δικτύων αντικατάστασης και μετάθεσης δίνεται στο σχήμα 4.13.

Αυτός ο σχεδιασμός αλγορίθμων τμημάτων ακολουθείται από πάρα πολλούς σύγχρονους αλγόριθμους κρυπτογράφησης, όπως θα δούμε και στη συνέχεια. Χαρακτηριστικό αυτών των αλγορίθμων είναι πως τόσο τα s-boxes όσο και οι μεταθέσεις, πρέπει να αντιστρέφονται προκειμένου, εφαρμόζοντας τα βήματα του αλγορίθμου με αντίθετη σειρά, να οδηγούμαστε από το κρυπτογραφημένο κείμενο, στο αρχικό.



Σχήμα 4.13: Δίκτυα αντικατάστασης και μετάθεσης

4.6 Δομές Feistel

Οι δομές Feistel αποτελούν βασικές δομές που χρησιμοποιούνται από αλγορίθμους τμημάτων. Η ιδέα που είχε ο Feistel ήταν αρκετά απλή και είχε ως βασικό άξονα την απόδειξη της ασφάλειας ενός αλγορίθμου μέσω μη αντιστρέψιμων συναρτήσεων. Προσπάθησε να θέσει την ιδέα ότι τα μοντέλα των κρυπτογραφικών αλγορίθμων τμημάτων θα πρέπει να είναι όσο γίνεται πιο απλά. Το να προσθέτει κανείς μέρη τα οποία είναι ασφαλή, το καθένα ανεξάρτητα από το άλλο, δεν συνεπάγεται ότι το σύνολο είναι ασφαλές.

Ακόμα και το γεγονός ότι πολλές φορές επιλέγουμε κομμάτια να είναι αντιστρέψιμα, όπως τα s-boxes, τα οποία θα δούμε αργότερα, εισάγει μία δομή μέσα στον αλγόριθμο η οποία μπορεί να είναι προς όφελος του κρυπταναλυτή και όχι της ασφάλειας ή της ταχύτητας αποκρυπτογράφησης.

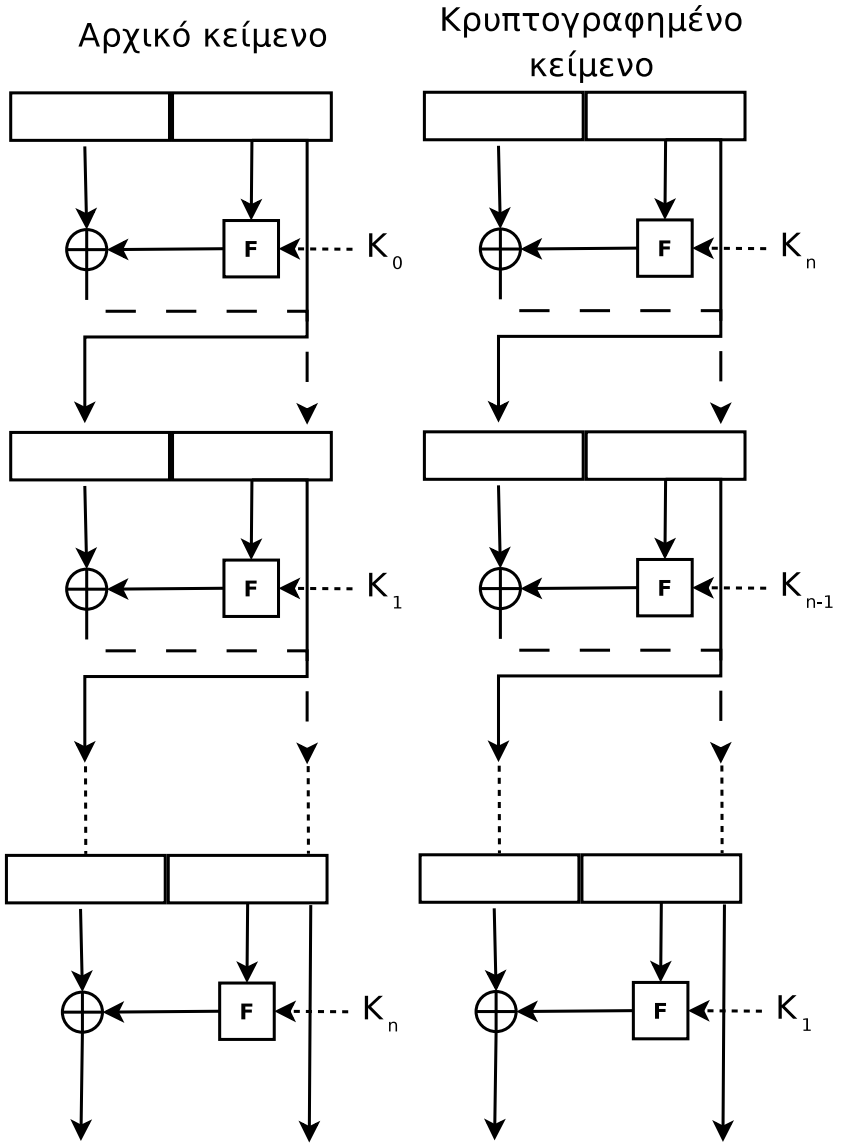
Ο Feistel [71] λοιπόν εισήγαγε τις δικές του δομές, οι οποίες ακολουθούνται από πάρα πολλούς σύγχρονους αλγόριθμους. Αρχικά μέσω μία συνάρτησης g παράγουμε τα κλειδιά του κάθε γύρου K_i από το αρχικό κλειδί K. Σε κάθε γύρο ενός αλγορίθμου τμημάτων, η είσοδός του χωρίζεται στη μέση, έχουμε έτσι το αριστερό και το δεξιό μέρος, αν λοιπόν είμαστε στον i γύρο, έχουμε τα L_{i-1} και R_{i-1} αντίστοιχα τα οποία έχουν n bits το κάθε ένα. Υπάρχει μία συνάρτηση f_i, η συνάρτηση γύρου, η οποία δε χρειάζεται να είναι αντιστρέψιμη με είσοδο, με είσοδο το κλειδί του γύρου και το R_{i-1} και έχει ως έξοδο n bits. Τότε ορίζουμε

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

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

Από τη δομή αυτή αν αντιστρέψουμε τα βήματα και γνωρίζουμε το κλειδί, είναι προφανές ότι μπορούμε να βρούμε το αρχικό κείμενο από το κρυπτογραφημένο. Γραφική αναπαράσταση των δομών Feistel δίνεται στο σχήμα 4.14.

Συνεπώς όλη η ασφάλεια του αλγόριθμου έγκειται στο να βρεθούν ασφαλείς συναρτήσεις γύρου f_i. Αποδεικνύοντας ότι αυτές είναι ασφαλείς, αποδεικνύεται ότι και ο αλγόριθμος είναι ασφαλής. Οι δομές Feistel γενικεύτηκαν αργότερα από τους B. Schneier και J. Kelsey με τις μη ισορροπημένες δομές Feistel [72], ώστε να κα-



Σχήμα 4.14: Δομές Feistel

λύπτουν περιπτώσεις όπου η είσοδος σε κάθε γύρο δεν χωρίζεται στη μέση.

Για να είναι μία συνάρτηση ασφαλής, είναι προφανές ότι δεν θα πρέπει να είναι γραμμική, άρα μία βασική παραδοχή την οποία θα κάνουμε είναι ότι οι μη γραμμικές συναρτήσεις είναι σίγουρα πιο ασφαλείς. Σε αυτό λοιπόν το πλαίσιο οι Meier και Staelbach, όρισαν τις τέλειες μη γραμμικές συναρτήσεις [78].

Ορισμός 73. Έστω

$$N_f(a,b) = |\{x \in \mathbb{F}_q : f(x+a) - f(x) = b\}|$$

Αν $N_f(a,b) = 1, \forall a,b \in \mathbb{F}_q^*$, τότε η συνάρτηση f θα ονομάζεται τέλεια μη γραμμική συνάρτηση.

Από τον ορισμό έπεται ότι οι τέλειες μη γραμμικές συναρτήσεις έχουν το πολύ μία τιμή για την οποία ισχύει η γραμμικότητα ή για να το δούμε στην περίπτωσή που έχουμε συναρτήσεις Boole, αν κανείς αλλάξει κάποια bits τις εισόδου τότε κατά 50% αλλάζει και το αποτέλεσμα, θα λέγαμε λοιπόν ότι 'αντιδρούν' τυχαία στις αλλαγές που τους γίνονται.

Ανάλογος ορισμός υπάρχει και για τις συναρτήσεις Bent [80].

Ορισμός 74. Έστω μία συνάρτηση f, θα καλείται συνάρτηση Bent αν απέχει μέγιστα από όλες τις τις γραμμικές.

Από τον ορισμό και λόγο του ότι στην περίπτωση μας έχουμε να κάνουμε με bits, μία καλή συνάρτηση απόστασης είναι αυτή του Hamming, όπου μετρά σε πόσες θέσεις διαφέρουν τα bits δύο ακολουθιών bits του ίδιου μήκους.

Προφανώς τόσο οι τέλειες μη γραμμικές συναρτήσεις, όσο και οι συναρτήσεις Bent αποτελούν πολύ καλές υποψηφιότητες για να αποτελούν συναρτήσεις γύρου σε ένα αλγόριθμο τμημάτων.

4.7 Ασκήσεις

Άσκηση 22. Να εξεταστεί ποιά είναι η διαδικασία αποκρυπτογράφησης για κάθε κατάσταση λειτουργίας ενός αλγορίθμου τμημάτων.

Άσκηση 23. Να κατασκευαστεί s-box μεγέθους 4×4 μη αντιστρέψιμο.

Άσκηση 24. Να κατασκευαστεί αντιστρέψιμο s-box μεγέθους 4×4.

Άσκηση 25. Να αποδειχθεί ότι μία δομή Feistel είναι αντιστρέψιμη.

Άσκηση 26. Ορίζοντας μία συνάρτηση γύρου f_i, να κατασκευάσετε μία δομή Feistel τεσσάρων γύρων.