Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Κρυπτογραφικοί Κώδικες Διόρθωσης Σφαλμάτων

Κωνσταντίνος Μιχαήλ Σεργίου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Κρυπτογραφικοί Κώδικες Διόρθωσης Σφαλμάτων

Κωνσταντίνος Μιχαήλ Σεργίου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2014

Περίληψη

Οι Κρυπτογραφικοί Κώδικες Διόρθωσης Σφαλμάτων έχουν σκοπό την ενοποίηση 2 κομματιών που χρησιμοποιούνται στην μετάδοση μηνυμάτων, την κρυπτογράφηση ενός μηνύματος και την κωδικοποίηση του μηνύματος.

Η ανάγκη για σωστή μετάδοση των μηνυμάτων κατά τα αρχικά στάδια της ανάπτυξης της μετάδοσης μηνυμάτων μας υποχρέωσε στην ανάπτυξη διαφόρων μεθόδων κωδικοποίησης καναλιού με σκοπό την μείωση της πιθανότητας να μεταδοθεί λανθασμένα ένα μήνυμα .

Μετά από την εδραίωση του δικτύου και της αποστολής μηνυμάτων εμφανίστηκε η ανάγκη για την κρυπτογραφία .Η κρυπτογράφηση του μηνύματος εξυπηρετεί την εμπιστευτικότητα του μηνύματος, την πιστοποίηση της ταυτότητας του αποστολέα αλλά και την ακεραιότητα του μηνύματος

Ο σύγχρονος τρόπος ζωής αύξησε την επιτακτικότητα της γρήγορης μετάδοσης και αυτοματοποίησης, για αυτούς τους λόγους κατά την διάρκεια των ετών παρατηρήθηκε η ανάπτυξη μεθόδων με σκοπό την κωδικοποίηση των μηνυμάτων. Οι κρυπτογραφικοί κώδικες Διόρθωσης Σφαλμάτων φαίνεται ότι μέχρι σήμερα επικράτησαν και γι' αυτό το λόγο στα πλαίσια της διατριβής θα αναλυθεί αυτή η πρακτική.

Η διατριβή χωρίζεται σε τρία κυρίως τμήματα: την παρουσίαση των τεχνικών κωδικοποίησης, την παρουσίαση των τεχνικών κρυπτογράφησης και την παρουσίαση των κρυπτογραφικών κωδίκων διόρθωσης σφαλμάτων .

Summary

The Cryptographic error correcting codes are trying to unite two pieces used to transmit messages, the encryption of a message and the encoding of the message.

The need for proper transmission of messages in the early stages of development of message transfer has forced us to develop different methods of channel coding in order to reduce the probability of incorrectly transmitting a message.

After the consolidation of the network and messaging appeared the need for cryptography. Encryption of the message serves the confidentiality of the message, the authentication of the sender but also the integrity of the message.

The modern lifestyle has increased the urgency of rapid transmission and automation, for these reasons during the years observed the development of methods to codify messages. The Cryptographic code debugging seems hitherto prevailed and for this reason during the thesis will analyze this practice.

The thesis is divided into three sections, the presentation of error correction technics, the presentation of encryption techniques and presentation of cryptographic codes for error correction.

Ευχαριστίες

Με την ολοκλήρωση της παρούσης διπλωματικής εργασίας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα αυτής, Καθηγητή, κ. Κωνσταντίνο Λιμιώτη, για την ενθάρρυνσή του να μελετήσω ένα τόσο ενδιαφέρον θέμα και την πολύτιμη καθοδήγησή του σε κάθε στάδιο της δημιουργίας της. Επιθυμώ να εκφράσω τη βαθιά ευγνωμοσύνη μου για την εμπιστοσύνη που επέδειξε στο πρόσωπό μου και την ουσιαστική συμβολή του.

θα ήθελα να ευχαριστήσω την οικογένειά μου, για την κατανόηση και την ψυχολογική συμπαράσταση .

Περιεχόμενα

Κεφάλαιο 1 6

Εισαγωγή 6

1.1 Αντικείμενο και δομή της Διατριβής 8

Κεφάλαιο 2 10

Κώδικες ανίχνευσης 10

σφαλμάτων 10

2.1 Τεχνικές ανίχνευσης και διόρθωσης σφαλμάτων 11

2.1.1 Ψηφίο Ισοτιμίας 11

2.1.2 Κώδικας Hamming 13

2.1.3 Γραμμικοί κώδικες τμήματος 14

2.1.4 Κυκλικοί κώδικες 18

2.1.5 Συνελικτικοί (Συγκεραστικοί) Κώδικες 20

Κεφάλαιο 2 26

Κρυπτογραφικοί αλγόριθμοι 26

3.1 Σύγχρονοι Αλγόριθμοι 28

3.1.1 Συμμετρικοί Αλγόριθμοι 28

3.1.1.1 Data Encryption Standard (DES) 29

3.1.2 Ασύμμετρα Κρυπτοσυστήματα (Αλγόριθμοι Δημοσίου Κλειδιού) 33

3.1.3 RSA 34

3.2 Κρυπτανάλυση 35

Κεφάλαιο 4 37

Κρυπτογράφηση στο φυσικο επιπεδο 37

4.1 Βασική ιδέα 37

4.2 Παράδειγμα κρυπτογράφησης στο φυσικό επίπεδο 40

Κεφάλαιο 5 43

ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ ΒΑΣΙΣΜΕΝΑ ΣΕ ΚΩΔΙΚΕΣ 43

4.1 Κρυπτοσύστημα McEliece 43

4.1.1 Κρυπτανάλυση στο κρυπτοσύστημα McEliece 48

4.2 Κρυπτοσύστημα Niederreiter 50

4.2.1 Κρυπτανάλυση στο κρυπτοσύστημα Niederreiter 51

4.3 Σύγκριση RSA , McEliece , Niederreiter 52

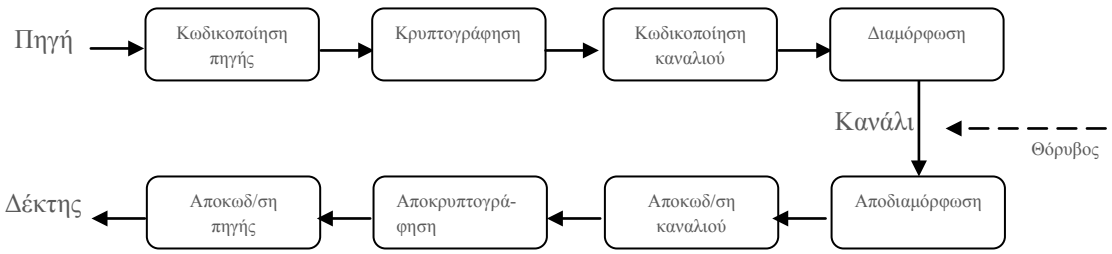
Επίλογος 54

Βιβλιογραφία 56

Κεφάλαιο 1
Εισαγωγή

Η εξέλιξη των τηλεπικοινωνιών υπήρξε ανέκαθεν ραγδαία, συμβαδίζοντας με την εξέλιξη της τεχνολογίας και της πληροφορικής. Ιδιαίτερα στις τελευταίες δεκαετίες, με την εμφάνιση καινοτόμων εφαρμογών, ο κλάδος των τηλεπικοινωνιών έχει γνωρίσει τεράστια άνθηση αξιοποιώντας κάθε υπάρχουσα τεχνολογική δυνατότητα. Τούτο με τη σειρά του επιτείνει την ανάγκη για περαιτέρω βελτίωση των υφιστάμενων τεχνικών που εφαρμόζονται, δεδομένων των μεγάλων απαιτήσεων που ανακύπτουν. Συγκεκριμένα, οι κύριοι στόχοι που πρέπει να επιτυγχάνονται σε ένα οποιουδήποτε τύπου τηλεπικοινωνιακό σύστημα είναι η αξιοπιστία, η απόδοση και η ασφάλεια – οι συγκεκριμένοι τομείς, παρά τις σημαντικές λύσεις που έχουν ήδη δοθεί, εξακολουθούν να αποτελούν τρέχον αντικείμενο έρευνας, ιδίως αν ληφθεί υπόψη ότι συχνά είναι αντικρουόμενοι.

Ανεξαρτήτως της εφαρμογής και του τύπου του τηλεπικοινωνιακού συστήματος, αυτό μπορεί να περιγραφεί από ένα διάγραμμα της ακόλουθης μορφής:



Σχήμα 1.1. Διάγραμμα ενός τυπικού τηλεπικοινωνιακού συστήματος

Η είσοδος από πηγή, σε ένα ψηφιακό τηλεπικοινωνιακό σύστημα, είναι μία ψηφιακή ακολουθία (ακολουθία από bit). Ο κωδικοποιητής πηγής (source encoder) αποσκοπεί στο να μετατρέψει την εισερχόμενη ακολουθία σε μία νέα, η οποία να έχει το μικρότερο δυνατό αριθμό bit (επιτυγχάνοντας έτσι μία συμπίεση της αρχικής ακολουθίας). Ακολούθως, η κρυπτογράφηση (encryption) αποσκοπεί στο να μετατρέψει την ακολουθία σε μία νέα, ακατάληπτη, έτσι ώστε να διασφαλίζεται η εμπιστευτικότητα της μετάδοσης. Εν συνεχεία, η κωδικοποίηση καναλιού (channel coding) εισάγει, με συστηματικό τρόπο, πλεονάζουσα πληροφορία (αυξάνοντας το συνολικό πλήθος bit της παραγόμενης ακολουθίας),, ώστε να αντιμετωπιστεί η επίδραση του θορύβου και των παρεμβολών που υπεισέρχονται στο κανάλι κατά τη μετάδοση του σήματος. Με άλλα λόγια, η κωδικοποίηση καναλιού αποσκοπεί στην ανίχνευση ή/και διόρθωση σφαλμάτων που λαμβάνουν χώρα κατά την μετάδοση του σήματος, οπότε και για αυτό το λόγο καλείται επίσης και κωδικοποίηση ανίχνευσης/διόρθωσης σφαλμάτων (error-detection ή error-correction coding). Τέλος, ο ψηφιακός διαμορφωτής μετατρέπει την ψηφιακή ακολουθία σε κυματομορφή κατάλληλη για τη μετάδοσή της στο φυσικό μέσο (καλώδιο, οπτική ίνα, ασύρματο μέσο μετάδοσης κτλ.).

Η κάθε μια από τις ανωτέρω δομικές βαθμίδες έχει το δικό της μαθηματικό υπόβαθρο και αποτελεί αυτόνομο αντικείμενο έρευνας. Υπάρχουν ήδη πολλές τεχνικές και αλγόριθμοι για την επίτευξη των ανωτέρω στόχων, σε κάθε μία από τις περιγραφόμενες βαθμίδες. Οι υπάρχουσες προσεγγίσεις, στην πλειοψηφία τους, αντιμετωπίζουν τα ανωτέρω ζητήματα μεμονωμένα και όχι σε συνδυασμό (για παράδειγμα, ο σχεδιαστής ενός κρυπτογραφικού αλγορίθμου δεν απασχολείται με ζητήματα κωδικοποίησης). Στη συγκεκριμένη εργασία θα εστιάσουμε στα θέματα της ασφάλειας (κρυπτογράφηση) και της αξιοπιστίας (κωδικοποίηση καναλιού). Ωστόσο, έμφαση θα δοθεί στο πεδίο έρευνας που εξετάζει συνδυαστικά και τα δύο αντικείμενα – δηλαδή θα εξεταστούν οι περιπτώσεις όπου η κρυπτογράφηση συνδυάζεται κατάλληλα με την κωδικοποίηση, για βελτίωση τόσο της ασφάλειας όσο και της συνολικής απόδοσης του συστήματος.

1.1 Αντικείμενο και δομή της Διατριβής

Το ζήτημα της ταυτόχρονης αξιοποίησης θεωρίας κρυπτογραφίας και κωδίκων ανίχνευσης σφαλμάτων, με σκοπό τη συνολική βελτίωση παραμέτρων ενός τηλεπικοινωνιακού συστήματος (π.χ. υλοποίηση μίας ενιαίας βαθμίδας, που επιτυγχάνει ταυτόχρονα κρυπτογράφηση και κωδικοποίηση), αποτελεί τις τελευταίες δεκαετίες μία σημαντική ερευνητική τάση. Σκοπός της εν λόγω εργασίας είναι η μελέτη όλων των σχετικών προσεγγίσεων που έχουν γίνει μέχρι σήμερα, καταγράφοντας τα ερευνητικά αποτελέσματα αλλά και τα ανοιχτά προβλήματα του συγκεκριμένου ερευνητικού πεδίου.

Η δομή της διατριβής έχει ως εξής:

Τα Κεφάλαια 2 και 3 παρέχουν το αναγκαίο υπόβαθρο που απαιτείται για την κατανόηση των υπολοίπων, ενώ παρατίθενται και οι ορισμοί των εννοιών που θα χρειαστούν μετέπειτα. Ειδικότερα, στο Κεφάλαιο 2 παραθέτονται οι βασικές έννοιας της θεωρίας κωδίκων, ενώ το Κεφάλαιο 3 εστιάζει στο αναγκαίο υπόβαθρο της κρυπτογραφίας, περιγράφοντας και τους πιο γνωστούς κρυπτογραφικούς αλγορίθμους.

Το Κεφάλαιο 4 εστιάζει στη βασική ιδέα υλοποίησης της κρυπτογραφικής λειτουργίας στο φυσικό επίπεδο. Παρουσιάζονται τα πλεονεκτήματα – αλλά και μειονεκτήματα - αυτής της τεχνικής: το βασικό της πλεονέκτημα είναι ότι ο επιτιθέμενος, που θέλει να πλήξει την εμπιστευτικότητα της μετάδοσης, καλείται να διαχειριστεί ένα κρυπτογραφημένο σήμα στο οποίο έχουν υπεισέλθει και σφάλματα κατά τη μετάδοση του καναλιού και τα οποία - προφανώς – δεν γνωρίζει: άρα, δεν έχει καν την πλήρη γνώση της κρυπτογραφημένης πληροφορίας. Στο ίδιο κεφάλαιο παρουσιάζεται μία πολύ πρόσφατη και υποσχόμενη τεχνική ταυτόχρονης υλοποίησης κρυπτογράφησης σε έναν κώδικα διόρθωσης σφαλμάτων. Με την τεχνική αυτή, χρησιμοποιώντας κατάλληλα έναν συγκεραστικό κώδικα μπορούμε, μέσω της τεχνικής «pruning» για την οποία οι παράμετροι παραμένουν μυστικές, να παράγουμε έναν άλλο κώδικα που θα χρησιμοποιηθεί για τη μετάδοση: η μυστικότητα των παραμέτρων διασφαλίζει και την ταυτόχρονη εμπιστευτικότητα της μεταδιδόμενης πληροφορίας.

Το Κεφάλαιο 5 μελετά αμιγώς κρυπτογραφικά συστήματα, τα οποία όμως για την κατασκευή τους υπεισέρχονται κώδικες ανίχνευσης σφαλμάτων. Η ασφάλεια των συστημάτων αυτών ανάγεται στην επίλυση προβλημάτων αποκωδικοποίησης τα οποία είναι γνωστά για τη δυσκολία τους. Με άλλα λόγια, τα συστήματα αυτά αξιοποιούν το υπόβαθρο από τη θεωρία κωδίκων προκειμένου να κατασκευαστούν ισχυροί κρυπτογραφικοί αλγόριθμοι.

Τέλος, σύνοψη της εργασίας και αποτύπωση ανοιχτών ερευνητικών προβλημάτων παρατίθενται στον Επίλογο αυτής.

Κεφάλαιο 2
Κώδικες Ανίχνευσης Σφαλμάτων

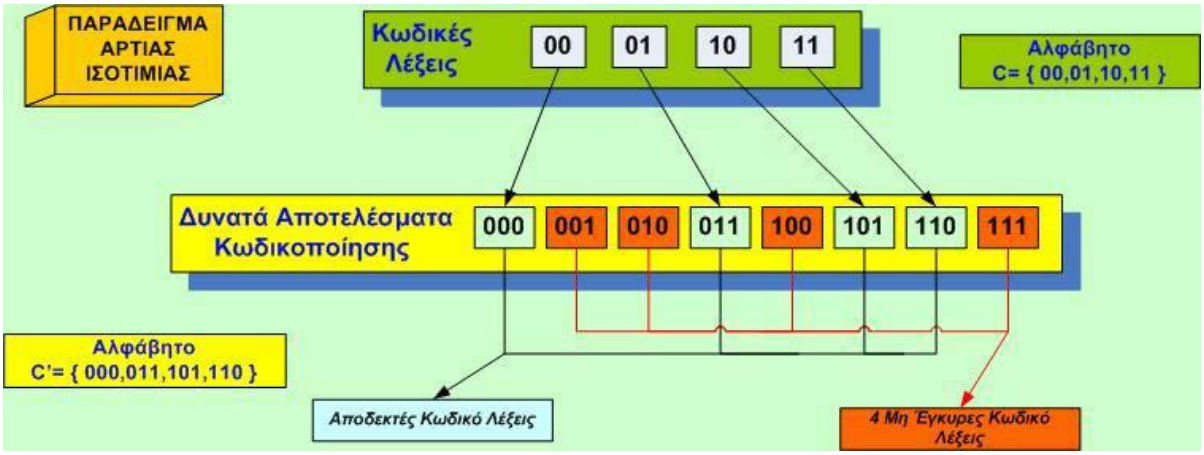
Η κωδικοποίηση του μηνύματος έχει σκοπό τη σωστή μετάδοση του μηνύματος, είτε με τεχνικές ανίχνευσης σφαλμάτων, είτε με τεχνικές που – πέραν από την ανίχνευση - επιτυγχάνουν και διόρθωση σφαλμάτων. Κώδικες αυτής της κατηγορίας ονομάζονται κώδικες ανίχνευσης σφαλμάτων (ή και διόρθωσης, για τη δεύτερη περίπτωση), ενώ επίσης η συγκεκριμένη κωδικοποίηση ονομάζεται κωδικοποίηση καναλιού (channel coding), υπό την έννοια ότι, μέσω αυτών, το μήνυμα προστατεύεται από σφάλματα που εισάγει το κανάλι μετάδοσης. Υπάρχουν τεχνικές που έχουν την ικανότητα απλά να ανιχνεύουν το σφάλμα και, ακολούθως, να ζητούν επανάληψη της αποστολής του μηνύματος , ενώ άλλες μπορούν όχι μόνο να ανιχνεύσουν τα λάθη αλλά και να τα διορθώσουν, χωρίς την ανάγκη επανάληψης αποστολής του μηνύματος. Υπάρχουν αρκετά πρωτόκολλα που χρησιμοποιούν κάποιο από τα μοντέλα (ή παραλλαγή αυτών) που θα περιγράψουμε πιο κάτω.

Η κωδικοποίηση είναι αναγκαία για την επιβεβαίωση της ορθής αποστολής ενός μηνύματος από τον αποστολέα στον δέκτη. Ως εκ τούτου, χρησιμοποιείται στην πλειοψηφία των τηλεπικοινωνιακών εφαρμογής (ασύρματα ή μη δίκτυα, κινητές επικοινωνίες, Διαδίκτυο κτλ.). Πρέπει να σημειωθεί ωστόσο ότι υπάρχουν και περιπτώσεις όπου η ταχύτητα μετάδοσης έχει πιο πολλή σημασία από την ορθή μετάδοση, με αποτέλεσμα να μην χρησιμοποιείται η κωδικοποίηση (ή οποία, όπως θα δούμε, επιδρά αρνητικά στην ταχύτητα) - για παράδειγμα, στην μετάδοση βίντεο, όπου είναι προτιμότερο να υπάρξει μία λανθασμένη λήψη εικόνας (frame) του βίντεο παρά να καθυστερεί/σταματά η μετάδοσή του .

2.1 Τεχνικές ανίχνευσης και διόρθωσης σφαλμάτων

2.1.1 Ψηφίο Ισοτιμίας

Η πιο απλή τεχνική ανίχνευσης σφαλμάτων είναι η χρήση του ψηφίου ισοτιμίας (parity bit). Ο σκοπός του είναι η προσθήκη ενός επιπλέον ψηφίου για τον έλεγχο της μετάδοσης. Το ψηφίο αυτό προκύπτει από την πρόσθεση (πράξη XOR) του συνόλου των ψηφίων του μηνύματος (ή τμήματος αυτού) με σκοπό το συνολικό πλήθος ψηφίων με τιμή «1» στην κωδική λέξη[1] να είναι πάντα άρτιο. Έτσι, παρέχει την δυνατότητα ανίχνευσης μονού πλήθους σφαλμάτων (γιατί αν υπάρχει άρτιο πλήθος σφαλμάτων, τότε ανά δύο αντισταθμίζονται). Δεν έχει την δυνατότητα να ανιχνεύσει όλα τα λάθη αλλά ούτε την δυνατότητα να διορθώσει τα λάθη. Σε περίπτωση ανίχνευσης κάποιου λάθους, τότε το μήνυμα ή κομμάτι του μηνύματος χρειάζεται να σταλεί εκ νέου.



Σχήμα 2.1: Παράδειγμα κωδικοποίησης με ψηφίο ισοτιμίας

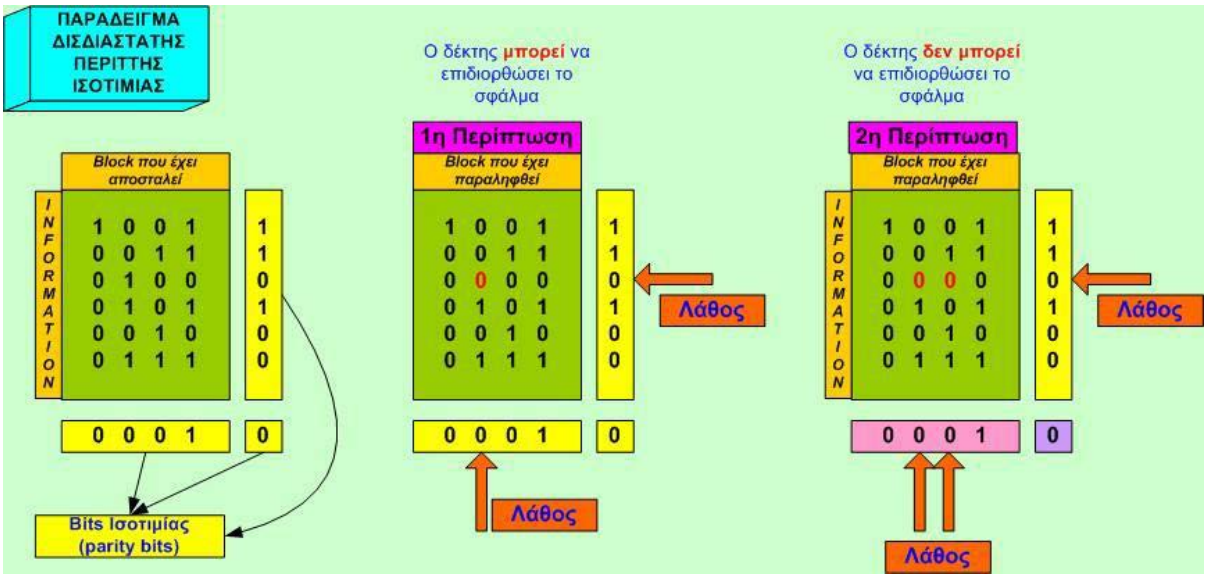
Στο Σχήμα 2.1 [1] έχουμε τα πιθανά μηνύματα (αλφάβητο) 00,01,10,11 όπου σε κάθε ένα από αυτά προσθέτεται το ψηφίο ισοτιμίας και προκύπτουν οι κωδικές λέξεις 000,011,101,110. Στη περίπτωση που στο δέκτη ληφθεί μία από τις λέξεις που σημειώνονται με κόκκινο χρώμα, τότε αυτή δεν γίνεται αποδεκτή γιατί δεν αντιστοιχεί σε καμία κωδική λέξη και συνεπώς δεν μπορεί να υπάρξει (με άλλα λόγια, ανιχνεύουμε σφάλμα κατά τη μετάδοση).

[1] Το πλήθος αυτό ονομάζεται βάρος Hamming, όπως θα δούμε στη συνέχεια

Μεταξύ δύο λέξεων χρειάζεται ένας αριθμός λαθών προκειμένου να μετατραπεί η μια λέξη στην άλλη και να μην ανιχνευτεί το λάθος. Η αριθμητική απόσταση μεταξύ των δύο ονομάζεται **απόσταση Hamming (Hamming distance)**.

Μια μετεξέλιξη του ψηφίου ισοτιμίας είναι η προσθήκη ψηφίου ισοτιμίας και σε κατακόρυφη μορφή, γνωστή και ως δισδιάστατη ισοτιμία. Στην δισδιάστατη ισοτιμία εκτός από το οριζόντιο ψηφίο ελέγχου έχουμε και το κάθετο, κάτι που μας επιτρέπει να εντοπίσουμε λάθη αλλά και σε κάποιες περιπτώσεις να τα διορθώσουμε. Ένα παράδειγμα δισδιάστατης ισοτιμίας βλέπουμε στο πιο κάτω σχήμα 2.2

Σχήμα 2.2



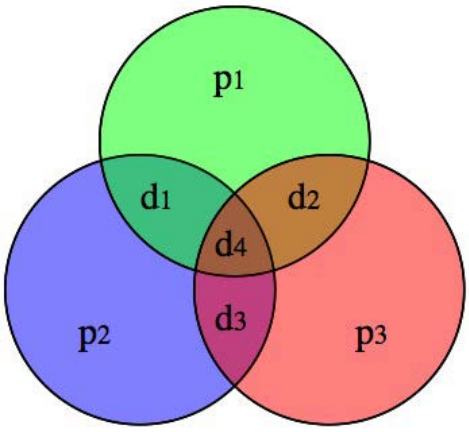
Με την βοήθεια του κάθετου ψηφίου ισοτιμίας μπορούμε να διορθώσουμε το λάθος γιατί με τον συμψηφισμό των κάθετων και οριζόντιων ελέγχων μπορούμε να προσδιορίσουμε την θέση του λάθους σε κάποιες περιπτώσεις. Η μέθοδος αυτή δεν μπορεί να ανιχνεύει και να διορθώνει όλα τα λάθη αλλά σε περίπτωση που ανιχνευτεί το λάθος και δεν μπορεί να διορθωθεί, τότε ξαναστέλνεται το μήνυμα.

2.1.2 Κώδικας Hamming

Ο κώδικας Hamming είναι μια εξέλιξη του ψηφίου ισοτιμίας, που έχει την δυνατότητα όχι μόνο να ελέγξει αν το μήνυμα είναι ορθό αλλά και να το διορθώσει . Ο κώδικας Hamming χρησιμοποιεί περισσότερα από ένα ψηφία ισοτιμίας ή ελέγχου ανά ομάδα (τμήμα) k bits.. Τα επιπλέον bits είναι ανάλογα από το μέγεθος του κομματιού.

Ένας κώδικας Hamming συμβολίζεται ως (n,k), όπου n το μέγεθος της κωδικής λέξης και k το μέγεθος του προς κωδικοποίηση μηνύματος: με άλλα λόγια, τα ψηφία ισοτιμίας που προστίθενται είναι πάντα n-k. Ο κώδικας Hamming είναι μία ειδική περίπτωση ενός γραμμικού κώδικα τμήματος (linear block code), οι οποίοι αναλύονται στη συνέχεια.

Ας δούμε, με ένα παράδειγμα, τον κώδικας Hamming(7,4), όπου σε κάθε 4 bits μηνύματος προστίθενται 3 bits ελέγχου . Στο πιο κάτω σχήμα, με d συμβολίζουμε τα bit του μηνύματος και ,με p τα bit ισοτιμίας: η κωδική λέξη είναι η **p1 p2d1 p3 D2 D3 D4** για σκοπούς ευκολίας



Σχήμα 2.4 τρόπος δημιουργίας bits ελέγχου

Στο σχήμα 2.4 βλέπουμε πώς προκύπτουν τα bit ελέγχου, με πράξεις XOR με κάποια από τα bits του μηνύματος. Σε περίπτωση που κάποιο bit μεταδοθεί λανθασμένα τότε τα ψηφία ελέγχου

είναι σε θέση να καθορίσουν ποιο από όλα είναι με την βοήθεια εύκολων μαθηματικών πράξεων. [2]

Ας σταθούμε λίγο περισσότερο στον (7,4) κώδικα Hamming. Κάθε κωδική λέξη των 7 bit αποτελείται από 4 bits δεδομένων . Όλα τα πιθανά μηνύματα μεγέθους 4 bits είναι 16. Έτσι, από τα 128 διαφορετικά τμήματα μεγέθους 7 bits, μόνο 16 από αυτά αντιστοιχούν σε κωδικές λέξεις: αυτό μας επιτρέπει να απορρίψουμε αυτόματα κάποια μηνύματα ως λανθασμένα και να υποθέσουμε πως το μήνυμα είναι το ποιο κοντινό σωστό μήνυμα . Μαθηματικώς αποδεικνύεται ότι η ελάχιστη απόσταση Hamming μεταξύ δύο οποιωνδήποτε κωδικών λέξεων ενός σχήματος H(7,4) είναι ίση με 3. Ο κώδικας (7,4) έχει την δυνατότητα να εντοπίσει και να διορθώσει ένα σφάλμα κατά την μετάδοση, γιατί η ληφθείσα λέξη θα απέχει απόσταση Hamming1 από την πλησιέστερη κωδική λέξη. .Σε περίπτωση όμως όπου συμβεί διπλό σφάλμα σε ένα πακέτο τότε ο κώδικας HAMMING, αν και είναι σε θέση να το εντοπίσει λόγω του ότι η ληφθείσα λέξη δεν θα είναι κωδική λέξη (θα απέχει απόσταση Hamming 2 από την πραγματική λέξη, ενώ δεν θα ταυτίζεται με καμία άλλη κωδική λέξη), εν τούτοις δεν θα μπορεί να το διορθώσει γιατί η ληφθείσα λέξη θα είναι πλησιέστερη (απόσταση Hamming 1) me κάποια άλλη πιθανή κωδική λέξη. Το πρόβλημα αυτό διορθώνεται στους κώδικες SECDED.

2.1.3 Γραμμικοί κώδικες τμήματος

Ο κώδικας σαν μια ιδέα είναι μια γλώσσα η γλώσσα μας είναι ένας κώδικας το ψηφίο ισοτιμίας είναι ένας κώδικας αν βάλουμε μια αντιστοίχιση του αλφαβήτου με αριθμούς για παράδειγμα A -00,B =01 κ.τ.λ. έχουμε τον κώδικα (00,01,……,24).Στους διαδίκους κώδικες που μας ενδιαφέρουν έχουμε την έννοια γραμμικός κώδικας. Ένας κώδικας ονομάζεται γραμμικός κώδικας αν το αποτέλεσμα της προσθήκης 2 λέξεων του συνόλου των λέξεων του κώδικα μας κάνει μια λέξη που υπάρχει στο σύνολο των λέξεων του κώδικα.

Για παράδειγμα αν έχουμε τον C1(000,111) κώδικα είναι γραμμικός γιατί το άθροισμα όλων των λέξεων σε όλους τους συνδυασμούς μας δίνει μια λέξη που έχουμε στο σύνολο των λέξεων του κώδικα C1

000 + 000 = 000

111 + 000 = 111
000 + 111 = 000
111 + 111 = 000

Ο C2 = (000; 001; 101) δεν είναι γιατί 001+101=100 και το 100 δεν υπάρχει στο σύνολο των λέξεων του κώδικα. Οποιοσδήποτε γραμμικός πίνακας περιέχει σαν λέξη του την μηδενική λέξη .

Η κάθε λέξη σε ‘ένα γραμμικό πίνακα έχει ένα βάρος που είναι το άθροισμα των θέσεων που είναι 1 για παράδειγμα η λέξη 01101 έχει βάρος 3 . κάθε γραμμικός κώδικας έχει ελάχιστο βάρος που αποδείχτηκε πώς είναι ή πιο μικρή απόσταση της μηδενικής λέξης και των υπολοίπων λέξεων . Για παράδειγμα αν έχουμε ένα κώδικα με την ελάχιστη απόσταση 2 τότε η πιο κοντινή λέξη θα έχει 2 μονάδες μέσα.

Ένα άλλο χαρακτηριστικό στους γραμμικούς κώδικες είναι οι γραμμικά ανεξάρτητοι πίνακες όπου μας βοηθούν να ομαδοποιούμε τους κώδικες. Δύο πίνακες λέγονται ανεξάρτητοι αν σε ένα σύνολο λέξεων πολλαπλασιάσουμε με ένα τυχαίο σύνολο αριθμό και το άθροισμα είναι 0 τότε ο πίνακας είναι γραμμικά ανεξάρτητος.

Δύο πίνακες λέγονται ισοδύναμοι αν ο ένας προέρχεται από τον άλλο εάν ακολουθηθεί μια ακολουθία στοιχειωδών πράξεων σε γραμμές. Οι στοιχειώδεις πράξεις σε γραμμές είναι η εναλλαγή και το άθροισμα της γραμμής με μια από τις άλλες γραμμές.

Κάθε πίνακας του οποίου οι γραμμές σχηματίζουν μια βάση του C, θα ονομάζεται γεννήτορας πίνακας του C και συμβολίζεται με G. Εάν ο C είναι (n, k, d) γραμμικός κώδικας ,ο G θα έχει διάσταση k*n.

Ένας πίνακας H καλείται parity check (πίνακας ελέγχου ισοτιμίας) για ένα γραμμικό κώδικα C αν οι στήλες του H αποτελούν μια βάση για τον δυϊκό κώδικα $C^{\perp}$. Εάν ο C είναι (n, k, d) γραμμικός κώδικας, ο $C^{\perp}$ θα έχει μήκος n και διάσταση n-k , οπότε κάθε parity check πίνακας για τον C πρέπει να έχει διάσταση: n*(n-k).

Για τον γεννήτορα και τον parity check πίνακα, αποδεικνύεται ένα σύνολο ιδιοτήτων. Χαρακτηριστικά αναφέρονται οι παρακάτω:

- H είναι ένας parity check πίνακας του C, αν και μόνο αν, είναι ένας γεννήτορας πίνακας για τον $C^{\perp}$.

- Αν G , H είναι γεννήτορες και parity check πίνακες αντίστοιχα, ενός γραμμικού κώδικα C τότε G * H = 0, όπου με 0 συμβολίζουμε τον μηδενικό πίνακα διάστασης k*(n-k).

κωδικοποίηση

Μία κωδική λέξη παράγεται πολλαπλασιάζοντας το μήνυμα με ένα πίνακα γεννήτορα G, διαστάσεων k x n, όπου οι k γραμμές του πίνακα είναι κωδικές λέξεις (γραμμικά ανεξάρτητες)

Για παράδειγμα αν έχουμε τον ποιο κάτω πίνακα G και θα στείλουμε το M = 0100

$$G = \begin{matrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{matrix}$$

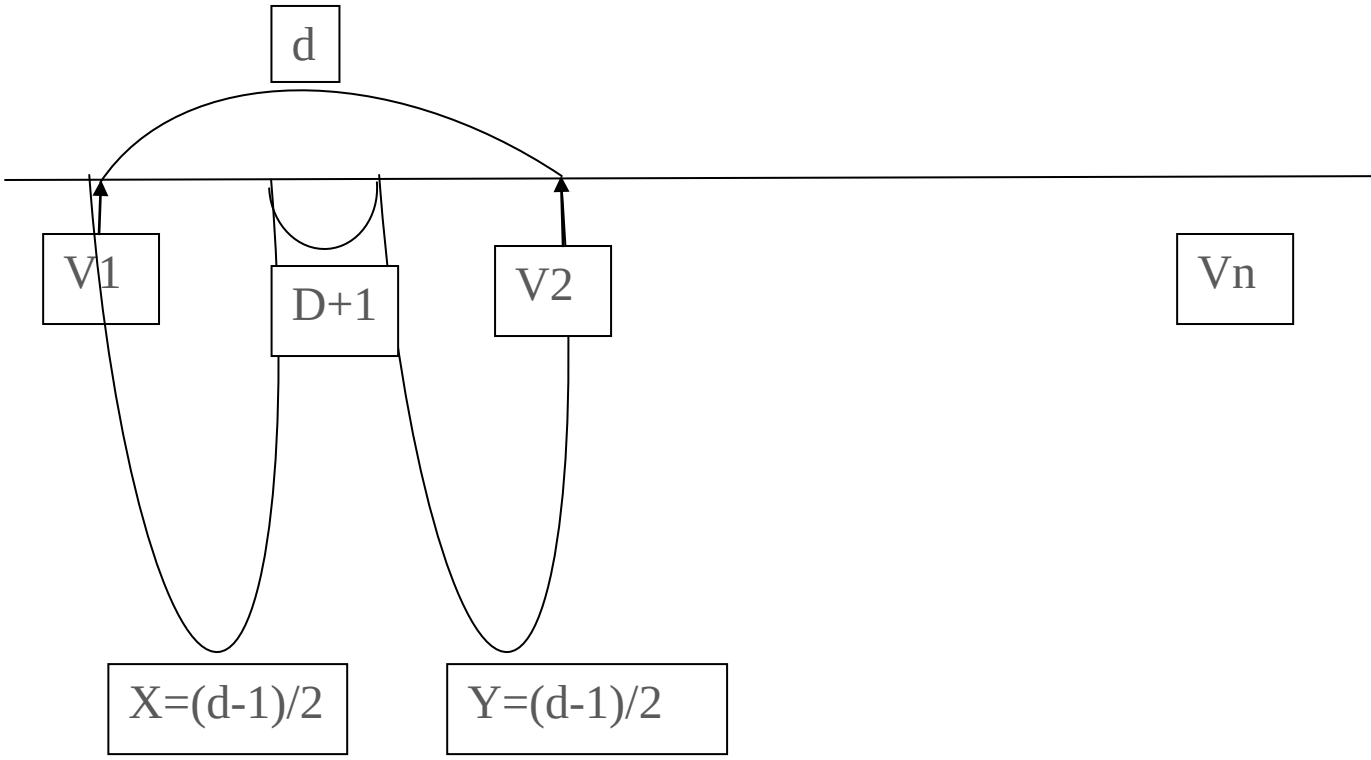
m*G= 0100101

το κωδικοποιημένο μήνυμα που θα στείλουμε είναι c=0100101

Αποκωδικοποίηση

κάθε πίνακας έχει πίνακα ισοτιμίας,. ο πίνακας ισοτιμίας έχει την ιδιότητα αν τον πολλαπλασιάσεις με οποιαδήποτε κωδική λέξη το αποτέλεσμα είναι 0. Αν πάρουμε την λέξη που λάβαμε και την πολλαπλασιάσουμε με τον πίνακα ισοτιμίας και το αποτέλεσμα είναι 0 τότε η λέξη που παραλάβαμε είναι ορθή και ανήκει στο σύνολο των λέξεων μας.

Κάθε γραμμικός κώδικας χαρακτηρίζεται από το d που είναι η ελάχιστη απόσταση μεταξύ των λέξεων. Ο κώδικας έχει την ικανότητα να ανιχνεύσει d-1 λάθη. Αν έχουμε d λάθη τότε η παραληφθείσα λέξη απέχειτην ίδια απόσταση από δύο πιθανές λέξεις. Αν ακολουθούμε την μέθοδο της πλήρης αποκωδικοποίησης μέγιστης πιθανότητας τότε αποκωδικοποιούμε σε μια από τις δύο. Αν ακολουθήσουμε την μέθοδο της ημιτελής αποκωδικοποίησης μέγιστης πιθανότητας τότε ζητούμε επανάληψη του μηνύματος.



Σχήμα 2,5 σχηματική αναπαράσταση της διορθωτικής ικανότητας γραμμικού κώδικα

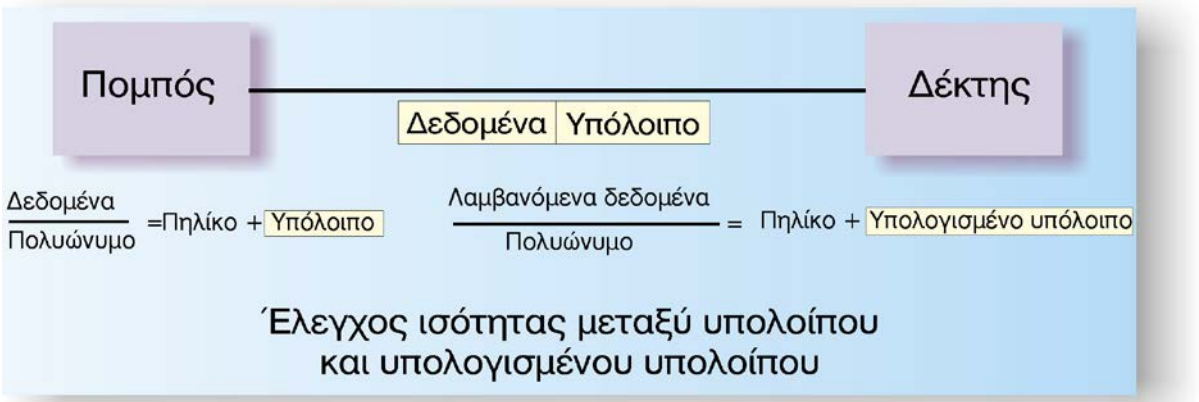
Στο σχήμα 2.5 βλέπουμε σχηματική αναπαράσταση της διορθωτικής ικανότητας κάποιου γραμμικού κώδικα. Αν έχουμε λάθος στο μέρος χ τότε επιλέγεται η λέξη v1 αν έχουμε λάθος στο μέρος ψ τότε επιλέγεται η λέξη v2. Αν έχουμε λάθος μεγέθους d+1 είναι η ενδιάμεση περίπτωση που είτε επιλέγουμε σταθερά ένα ανάμεσα στα v1 και v2 (ανάλογα με την τεχνική αποκωδικοποίησης) ή ζητούμε επανάληψη της αποστολής.

2.1.4 **Κυκλικοί κώδικες**

Οι κυκλικοί κώδικες είναι από τους πιο διαδεδομένους και πιο ικανούς κώδικες ανίχνευσης σφαλμάτων. [3] Στην ουσία, είναι γραμμικοί κώδικες τμήματος, με την πρόσθετη ιδιότητα ότι η κυκλική ολίσθηση μίας κωδικής λέξης παραμένει επίσης κωδική λέξη. Οι κώδικες αυτοί περιγράφονται με πολύ «κομψό» μαθηματικά τρόπο με πολλαπλασιασμό πολυωνύμων.

Για ένα κομμάτι μηνύματος μεγέθους k bit δημιουργείται μια ακολουθία πλαισίου (n-k), (Frame check sequence, FCS), όπου διαιρείται από κάποιο αριθμό ο οποίος είναι γνωστός και έχει προκαθοριστεί από τον αποστολέα και τον παραλήπτη του μηνύματος. Το υπόλοιπο της διαίρεσης αλλά και το μήνυμα αποστέλλονται στον παραλήπτη που επαναλαμβάνει την διαίρεση του μηνύματος και ελέγχει το δικό του υπόλοιπο με αυτό που έχει λάβει μαζί με το μήνυμα. Τα δύο υπόλοιπα όταν συμφωνούν τότε έχουμε σωστή μετάδοση του συγκεκριμένου κομματιού μηνύματος.

Οι κυκλικοί κώδικες έχουν την δυνατότητα σχεδόν να ανιχνεύσουν κάθε σφάλμα. Η πιθανότητα να μην ανιχνευθεί σφάλμα είναι της τάξης του 10^{-9}. [4]



Σχήμα 2.6 διαδικασία που ακλουθείτε και τα δεδομένα που αποστέλλονται .Το πολυώνυμο είναι ο προσυμφωνημένος διαιρέτης.

Η μέθοδος αυτή χρησιμοποιείται ευρέως για την μεγάλη δυνατότητα που έχει να εντοπίζει λάθη μετάδοσης. Ωστόσο χρειάζονται αρκετά επιπρόσθετα bits (σε σχέση με το ψηφίο ισοτιμίας) κατά την μετάδοση (overhead) που αυξάνουν το μέγεθος του τελικού μηνύματος. Η απλότητα του συστήματος επιτρέπει και την υλοποίηση του με εύκολα και φτηνά μηχανικά συστήματα με απλά κυκλώματα και πύλες XOR. [3]

Μετά τον έλεγχο του μηνύματος για ορθή μετάδοση έχουμε περιπτώσεις όπου το μήνυμα δεν στάλθηκε ορθά, σε τέτοια περίπτωση χρειάζεται με κάποιον τρόπο να διορθωθεί το σφάλμα. Υπάρχουν διάφοροι τρόποι και τεχνικές που χρησιμοποιούνται ανάλογα με το σύστημα και τις ανάγκες του,.

Η **αυτόματη αίτηση επανεκπομπής** (Automatic Repeat Request, ARQ) [5] είναι ένας από τους τρόπους διόρθωσης με τις λιγότερες απαιτήσεις κατά τον οποίο η διόρθωση μπορεί να γίνεται με επιβεβαίωση του κάθε κομματιού μηνύματος (**ARQ Stop and Wait)** . Άλλη περίπτωση είναι να γίνεται επαναποστολή πακέτων κατά παραγγελία (**ARQ Go-back-N**). Στην πρώτη περίπτωση της επιβεβαίωσης ο δέκτης μετά από κάθε πακέτο K bits το ελέγχει και αποστέλλει είτε θετικό αποτέλεσμα για να συνεχίσει στο επόμενο πακέτο ο αποστολέας ή αποστέλλει αρνητικό αποτέλεσμα για να ζητήσει επανεκπομπή του πακέτου. Στην δεύτερη περίπτωση ο αποστολέας στέλνει τα πακέτα των K bits μέχρι να γίνει κάποιο αίτημα για επανεκπομπή κάποιου πακέτου και τότε ξαναστέλνει τα πακέτα μετά από αυτό.

Ακόμη μια τεχνική είναι η **πρόσθια διόρθωση λαθών** όπου ο παραλήπτης μετά τον έλεγχο του μηνύματος σε περίπτωση που ανιχνεύει σφάλμα κάνει αυτόματη διόρθωση με βάση κανόνες κωδικοποίησης. Η διόρθωση γίνεται με βάση κανόνες και δεν είναι πάντα ορθοί . Η συγκεκριμένη τεχνική δεν απαιτεί αμφίδρομο κανάλι επικοινωνίας και χρησιμοποιείται σε περιπτώσεις όπου επιτρέπονται μικρά λάθη και χρειάζεται η αμεσότητα αποστολής του μηνύματος και το εύρος του καναλιού στοιχίζει περισσότερο από την πιθανότητα λάθους αποστολής κάπου πακέτου. Παράδειγμα χρήσης της πρόσθιας διόρθωσης λαθών είναι οι τηλεπικοινωνίες όπου δεν είναι πρόβλημα η διαστρέβλωση μιας λέξης αλλά προτεραιότητα έχει η αμεσότητα της μετάδοσης και το μέγεθος που χρειάζεται προκειμένου να μπορεί το κανάλι να εξυπηρετήσει περισσότερες επικοινωνίες.

Πλήθος σημαντικών εφαρμογών δεν θα μπορούσαν να υπάρξουν χωρίς τη χρήση κωδίκων διόρθωσης σφαλμάτων. Μία σημαντική κατηγορία κυκλικών κωδίκων γνωστής με το όνομα Reed-Muller χρησιμοποιήθηκαν για τη μετάδοση φωτογραφιών από τον πλανήτη Άρη στη δεκαετία του ’70, όπως αυτές ελήφθησαν από το σκάφος Mariner 9. Αργότερα, χρησιμοποιήθηκαν οι Reed-Solomon κώδικες, οι οποίοι είναι επίσης κυκλικοί. κώδικες Οι κώδικες αυτοί χρησιμοποιούνται ακόμη και σήμερα για τη διόρθωση σφαλμάτων σε δεδομένα που είναι αποθηκευμένα σε ψηφιακούς δίσκους (Compact Disks – CD) – και είναι ο λόγος που ακόμα και μια γρατσουνιά μπορεί τελικά να μην επηρεάσει την ανάγνωση του δίσκου.

2.1.5 Συνελικτικοί (Συγκεραστικοί) Κώδικες

Οι Συνελικτικοί (ή συγκεραστικοί) κώδικες (convolutional codes) αποτέλεσαν μια καινοτομία στην κωδικοποίηση του μηνύματος. Μέχρι τώρα είδαμε πώς με διάφορες τεχνικές προθέταμε σε ένα προκαθορισμένο τμήμα (block) μηνύματος κάποια bits ελέγχου, όπου είχαν την δυνατότητα να «ελέγξουν» το συγκεκριμένο τμήμα μηνύματος ως προς την ακεραιότητά του. Τα τμήματα λογίζονται ως αυτόνομα και ανεξάρτητα. [6] Οι συνελικτικοί κώδικες εισάγουν μια νέα ιδεολογία στην κωδικοποίηση του μηνύματος. Δεν «διασπούν» το μήνυμα σε τμήματα, αλλά το μήνυμα είναι μια ροή bits όπου διέρχεται από ένα κωδικοποιητή, είσοδος του οποίου είναι , εκτός από το μήνυμα, και κάποια bits όπου έχουν σταλεί προηγουμένως με την βοήθεια καταχωρητών

(μνήμης). Το αποτέλεσμα είναι να αποστέλλεται ένα μήνυμα βασισμένο στην ροή των bits και τον προηγούμενων κ bits ανάλογα με την μνήμη του . [3]

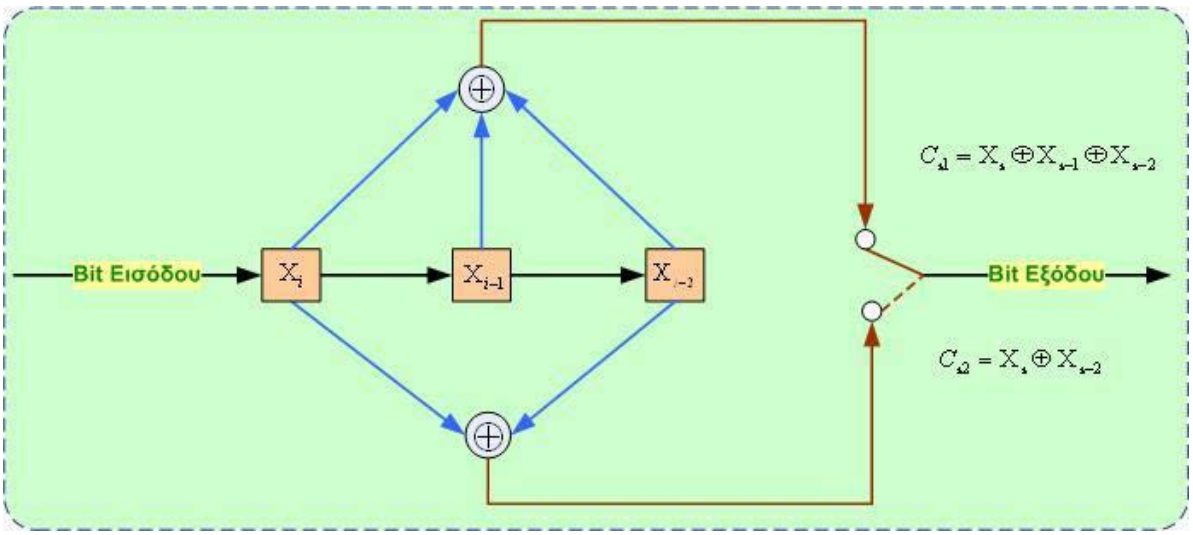
Οι συνελικτικοί κώδικες χωρίζονται σε συστηματικούς και μη συστηματικούς. Ένας κώδικας είναι συστηματικός όταν το μήνυμα της εισόδου εμφανίζεται αυτούσιο και στην έξοδο μαζί με τα πλεονάζοντα bits που παράγονται. Όταν δεν εμφανίζεται το μήνυμα αυτούσιο στην έξοδο τότε ο κώδικας αποκαλείται μη συστηματικός. Οι μη συστηματικοί κώδικες χωρίζονται στους αναδρομικούς και τους μη αναδρομικούς.

Ένας συνελικτικός κώδικας αποκαλείται καταστροφικός όταν κάποιο λάθος στη μετάδοση μεταδίδεται στο υπόλοιπο μήνυμα («προκαλεί» δηλαδή νέα λάθη στη λήψη του μηνύματος) και έτσι το μήνυμα χρειάζεται να ξανασταλθεί. Οι μη συστηματικοί κώδικες είναι καλύτεροι σε απόδοση συγκριτικά όμως προτιμούνται οι συστηματικοί κώδικες γιατί μπορούν να ελεχθούν για την ορθότητα τους ποιο εύκολα. Έχουν λιγότερες υπολογιστικές απαιτήσεις.

Ένας συνελικτικός κώδικας χαρακτηρίζεται από τρεις παραμέτρους .

- k είναι ο αριθμός των ψηφίων εισόδου
- n είναι ο αριθμός των ψηφίων εξόδου
- m είναι ο αριθμός των καταχωρητών

Παράδειγμα συστηματικού αναδρομικού κωδικοποιητή.



Σχήμα 2.7 παράδειγμα κωδικοποιητή

Στο σχήμα 2.7 βλέπουμε τον κωδικοποιητή με n=2, k=1, m=3. Τα κουτιά είναι οι καταχωρητές μνήμης και τα στρογγυλά + είναι XOR πύλες.

Στον ανωτέρω κωδικοποιητή θα εισάγουμε το μήνυμα 1011 προς κωδικοποίηση. Θα δούμε αναλυτικά πώς δρα ο κωδικοποιητής: θα χρησιμοποιηθεί μια στήλη για το χρόνο όπου θα εμφανίζονται και τα περιεχόμενα του καταχωρητή κάθε χρονική στιγμή και θα συνεχίσει μέχρι να αδειάσουν οι καταχωρητές και να ολοκληρωθεί το μήνυμα.

Χρόνος	**Είσοδος**	**Καταχωρητές**			**Έξοδος**	
T	**x**	**Register 1**	**Register 2**	**Register 3**	**C1**	**C2**
0	1	1	0	0	1	1
1	0	0	1	0	1	0
2	1	1	0	1	0	0
3	1	1	1	0	0	1
4	0	0	1	1	0	1
5	0	0	0	1	1	1

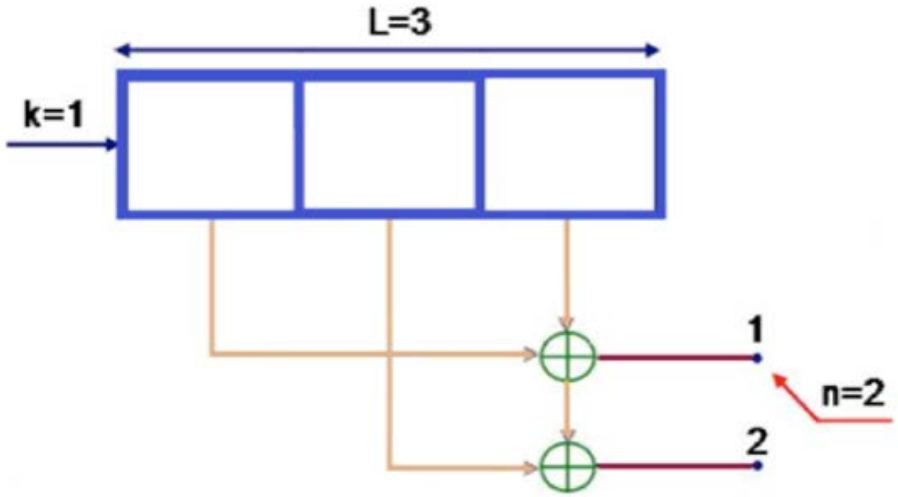
Το τελικό μήνυμα που θα σταλεί είναι το 111000010111.

Για την αποκωδικοποίηση υπάρχουν διάφορες τεχνικές, η ακολουθιακή αποκωδικοποίηση και η αποκωδικοποίηση μέγιστης πιθανοφάνειας. Γνωστός αλγόριθμος με την ακολουθιακή αποκωδικοποίηση είναι ο αλγόριθμος του Fano. Με την αποκωδικοποίηση μέγιστης πιθανοφάνειας γνωστός αλγόριθμος είναι ο αλγόριθμος του Viterbi.

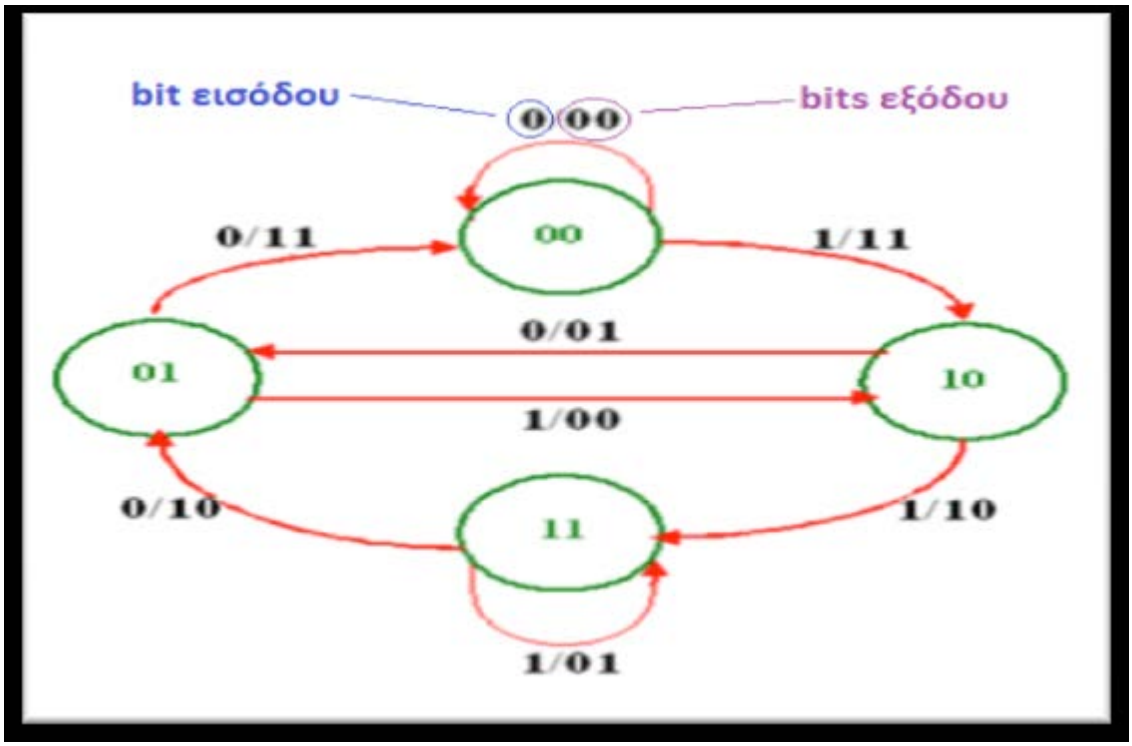
Ο Viterbi ακολουθεί την αποκωδικοποίηση μέγιστης πιθανοφάνειας με ευέλικτη απόφαση όπου κριτήριο πλέον δεν είναι η απόσταση Hamming αλλά η ευκλείδεια απόσταση Αν έχουμε ένα μήνυμα m και το κωδικοποιούμε και έχουμε το v κωδικοποιημένο μήνυμα και ο παραλήπτης λαμβάνει το μήνυμα r τότε ο αλγόριθμος υπολογίζει την πιθανότητα να πήρε το r δεδομένου ότι στάλθηκε το v για όλα τα πιθανά v . Το διάγραμμα trellis είναι μια σχηματική αναπαράσταση των πιθανών καταστάσεων με όλα τα πιθανά μονοπάτια και τις πιθανότητες τους.

Παράδειγμα

Θέλουμε να στείλουμε το μήνυμα m = 1111100 από τον πιο κάτω συνελικτικό κώδικα (n, k, L)=(2, 1, 3).

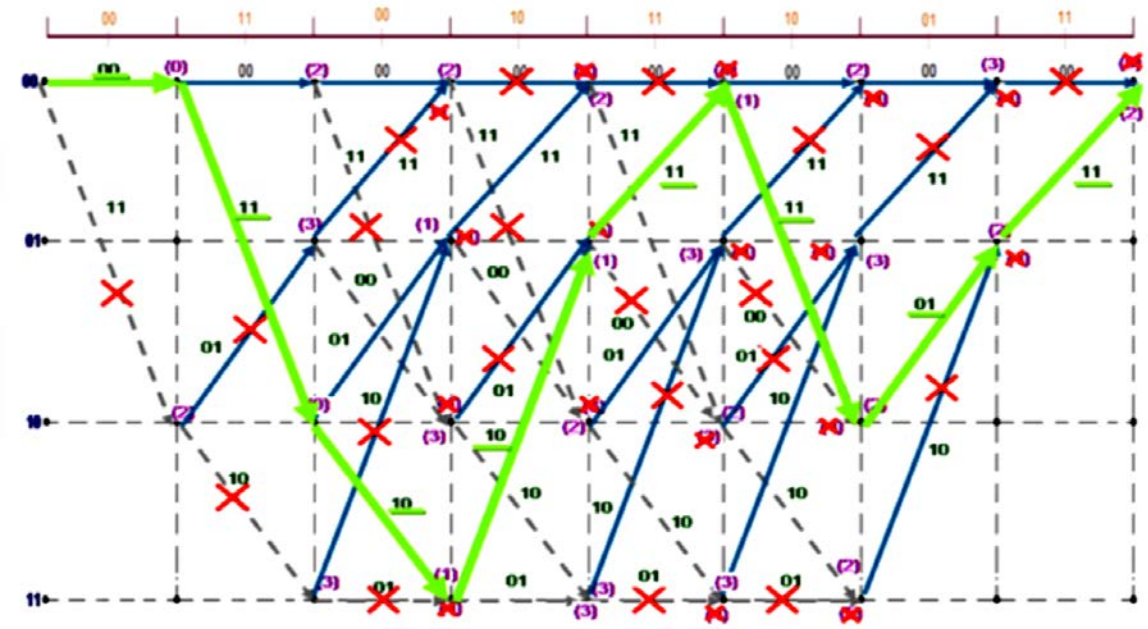


Σχήμα 2,8 κωδικοποιητής συνελικτικού κώδικα (2,1,3)



Σχήμα 2,9 διάγραμμα καταστάσεων

Στο διάγραμμα καταστάσεων βλέπουμε όλες τις πιθανές καταστάσεις και την πιθανότητα να πάμε από την μια στην άλλη με βάση τον κωδικοποίηση στο σχήμα 2,8. Θεωρούμε ότι πήραμε το μήνυμα r = 00 11 00 10 11 10 01 11 αντί για το μήνυμα V= 00 11 10 10 11 11 01 11 που παράχθηκε λόγω λαθών στην μετάδοση.



Σχήμα 2,10 διάγραμμα trellis για την μετάδοση

Με την βοήθεια των πιθανοτήτων στο σχήμα 2,9 και το διάγραμμα trellis στο σχήμα 2,10 επιλέγουμε την βέλτιστη διαδρομή που είναι 00 11 10 10 11 11 01 11 διορθώνοντας τα λάθη μετάδοσης

Το διάγραμμα trellis μεγαλώνει ανάλογα με το μέγεθος του μηνύματος και τις πιθανές καταστάσεις. Αν έχουμε πολλές πιθανότητες με μεγάλο μήνυμα τότε η απόδοση του αλγόριθμου μειώνεται. Σήμερα ο αλγόριθμος Viterbi χρησιμοποιείται σε πολλές από τις καθημερινές μας επικοινωνίες όπως τα ασύρματα δίκτυα τα τηλεφωνικά δίκτυα GSM αλλά και την τηλεόραση σε διάφορες μορφές μετάδοσης όπως το DVB (digital video broadcasting).

Κεφάλαιο 3
Κρυπτογραφικοί Αλγόριθμοι

Η κρυπτογραφία αναπτύχθηκε σε μεγάλο βαθμό λόγω της ανάγκης ασφαλούς επικοινωνίας κατά τον 1ο και 2ο παγκόσμιο πόλεμο. Η πιθανότητα να υποκλέψει ο εχθρός το μήνυμα μπορούσε να σημάνει μεγάλες απώλειες και αυτό ανάγκασε όλες τις χώρες κατά την διάρκεια του πολέμου να ασχοληθούν ουσιαστικά για τη εύρεση τρόπων ασφαλούς επικοινωνίας. Πολύ γνωστή είναι η μηχανή κωδικοποίησης Enigma.

Η κρυπτογραφία είναι μια ανάγκη που εμφανίστηκε με σκοπό να μεταφέρεται το μήνυμα μυστικά χωρίς να είναι προσβάσιμο από άλλα άτομα εκτός από τον αποστολέα και τον δέκτη. Ο πιο απλός τρόπος κρυπτογράφησης είναι η αντικατάσταση συμβόλων, με πλέον κλασικό τον αλγόριθμο του Καίσαρα όπου το κάθε γράμμα στο αρχικό κείμενο αντικαθίσταται από το γράμμα που ήταν 3 θέσεις δεξιά στο αλφάβητο. Ο παραλήπτης έκανε το αντίστροφο, δηλαδή κάθε γράμμα του λαμβανομένου κρυπτοκειμένου το αντικαθιστούσε με εκείνο που βρίσκεται 3 θέσεις αριστερά στο αλφάβητο, και μπορούσε να ανακτήσει το κείμενο. Σχετικό παράδειγμα αντιπαραβάλλεται στο σχήμα 3,1

Μήνυμα	Κρυπτοκείμενο
A	D
B	E
C	F
D	G
E	H
F	I
G	J
H	K
I	L

J	M
K	N
L	O
M	P
N	Q
O	R
P	S
Q	T
R	U
S	V
T	W
U	X
V	Y
W	Z
X	A
Y	B
Z	C

Σχήμα 3,1

Παράδειγμα

Μήνυμα: MEET ME AFTER THE PARTY

Κρυπτοκείμενο: PHHW PH DIWHU WKH SDUWB

Παρόμοιος - αν και πολύ πιο ασφαλής - τρόπος κρυπτογραφίας είναι η πολυαλφαβητική αντικατάσταση – για παράδειγμα, ο αλγόριθμος Virgene. Στον συγκεκριμένο αλγόριθμο ο παραλήπτης και ο αποστολέας μοιράζονται ένα κλειδί K και η κρυπτογράφηση γίνεται όπως στο παράδειγμα

m=μήνυμα

c = κρυτποκείμενο

K = κλειδί

Ο αποστολέας δημιουργεί το κρυπτοκείμενο με την πράξη C=m+k mod26

Ο παραλήπτης μετατρέπει το κρυπτοκείμενο στο αρχικό μήνυμα m= c-k mod 26

Παράλληλα αναπτύχθηκε ακόμη ένας τύπος αλγορίθμου, αυτός της αντιμετάθεσης, όπου τα γράμματα του μηνύματος άλλαζαν θέσεις με βάση μια μαθηματική πράξη.

Οι αλγόριθμοι αυτοί στήριζαν την ασφάλεια τους όμως στην μυστικότητα του κλειδιού και όχι στην δυσκολία του αλγορίθμου. Αν κάποιος είχε το κλειδί μπορούσε να πάρει και το μήνυμα με μεγάλη ευκολία. Μετά από προσπάθειες με επιθέσεις γνωστού κειμένου ή γνωστού κρυπτοκειμένου αποδείχτηκε ότι μπορούσαν εύκολα να σπάσουν τόσο ο αλγόριθμος Virgene αλλά και ο αλγόριθμος της αντιμετάθεσης. Παρόλα αυτά, οι τεχνικές αντικατάστασης και αντιμετάθεσης αποτελούν τη βάση πολλών σύγχρονων αλγορίθμων.

3.1 Σύγχρονοι Αλγόριθμοι

Οι σύγχρονοι αλγόριθμοι χωρίζονται σε 2 κατηγορίες, τους συμμετρικούς αλγόριθμους και τα ασύμμετρα κρυπτοσυστήματα. Η κρυπτογραφία στα δίκτυα σήμερα εξυπηρετεί εκτός από την ιδιωτικότητα του μηνύματος, την αυθεντικοποίηση του μηνύματος αλλά και την αυθεντικοποίηση του αποστολέα.

- **Ιδιωτικότητα του μηνύματος** είναι η διατήρηση της πληροφορίας κρυφής από όλους, πλην εκείνων που είναι εξουσιοδοτημένοι να τη δουν.

- **Αυθεντικοποίηση του μηνύματος** είναι διασφάλιση του ότι η πληροφορία δεν έχει κακόβουλα παραποιηθεί.

- **Αυθεντικοποίηση του αποστολέα** είναι η δυνατότητα εξακρίβωσης από την πλευρά του παραλήπτη ενός μηνύματος ότι ο αποστολέας αυτού είναι πράγματι αυτός που ισχυρίζεται.

3.1.1 Συμμετρικοί Αλγόριθμοι

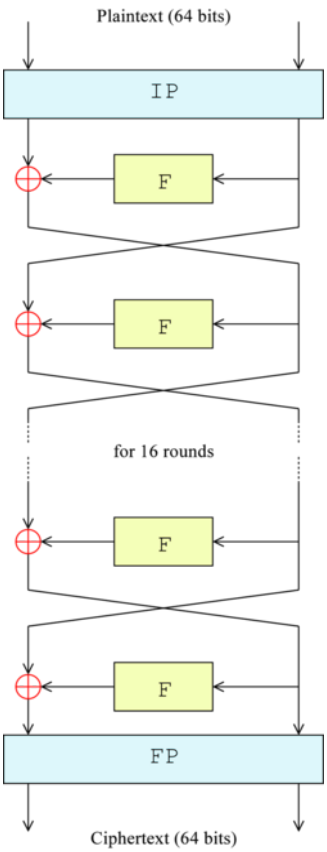
Η συμμετρική κρυπτογραφία εμφανίστηκε κατά την δεκαετία του 1970. Οι συμμετρικοί αλγόριθμοι χωρίζονται σε 2 υποκατηγορίες ,τους αλγόριθμους ροής (stream ciphers) και τους αλγόριθμους τμήματος (block ciphers). Το κοινό χαρακτηριστικό είναι η γνώση μόνο από τον αποστολέα και τον παραλήπτη του κοινού κλειδιού κρυπτογράφησης που χρησιμοποιείται τόσο κατά την κρυπτογράφηση αλλά και κατά την αποκρυπτογράφηση του μηνύματος. Στους αλγόριθμους ροής έχουμε γνωστούς αλγόριθμους όπως τον One Time Pad ή τον Rc4. Στους

αλγόριθμους τμήματος υπήρξε για περίπου δύο δεκαετίες πρότυπο κρυπτογράφησης ο DES, ο οποίος στη συνέχεια αντικαταστάθηκε από τον αλγόριθμο AES . Στην πλειοψηφία όμως έχουμε χρήση των αλγόριθμων τμήματος γιατί προσφέρουν μεγαλύτερη ασφάλεια σε σχέση με τους αλγόριθμους ροής. Οι κρυπταλγόριθμοι ροής χρησιμοποιούνται σε περιπτώσεις κυρίως όπου η ταχύτητα είναι προτεραιότητα από την ασφάλεια .

3.1.1.1 Data Encryption Standard (DES)

Ο αλγόριθμος DES είναι ο αλγόριθμος που χρησιμοποιήθηκε από την δεκαετία του 1970 μέχρι και το 1997 σαν πρότυπο κρυπτογράφησης (το 2005 επήλθε η επίσημη «απόσυρσή» του). Η δομή του θεωρείται ακόμα αρκετά ισχυρή – το μόνο του ουσιαστικό μειονέκτημα ήταν το μέγεθος του κλειδιού (56 bit), Περί τα 1997, λόγω της αύξησης των δυνατοτήτων των ηλεκτρονικών υπολογιστών, κατέστη δυνατόν να σπάσει ο κώδικας μετά από 22,5 ώρες επίθεσης εξαντλητικής αναζήτησης ("Brute Force Attack").

Ο αλγόριθμος DES βασίζεται στην επαναληπτική εφαρμογή μιας κρυπτογραφικής πράξης η οποία έχει σαν είσοδο της το μήνυμα και το κλειδί. Σε κάθε γύρο η είσοδος είναι η έξοδος της προηγούμενης κρυπτογραφικής πράξης και στη τελευταία έξοδο έχουμε το κρυπτογραφημένο μήνυμα. Ο αριθμός των γύρων είναι ανάλογος με το κλειδί και τον βαθμό δυσκολίας του κάθε γύρου κρυπτογράφησης, για παράδειγμα ο Des έχει 16 γύρους. Για την αποκρυπτογράφηση του μηνύματος έχουμε ακριβός τον ίδιο αριθμό κρυπτογραφικών πράξεων όπου εισάγουμε το κρυπτογραφημένο μήνυμα και το ίδιο κλειδί και παίρνουμε το αρχικό μήνυμα.



Σχήμα 3.2

Η κρυπτογραφική δύναμη βασίζεται όχι μόνο στις επαναλήψεις της κρυπτογράφησης αλλά και στην κρυπτογραφική δύναμη κάθε γύρου. Στον αλγόριθμο DES υπάρχουν 4 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)

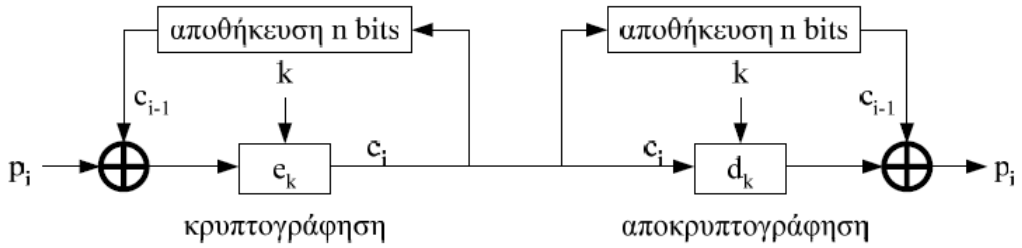
Ηλεκτρονικό κωδικοβιβλίο, ECB

Ο τρόπος λειτουργίας ECB είναι ο πιο απλός και γίνεται απλά η κωδικοποίηση με το κλειδί και το κομμάτι του μηνύματος που θα κρυπτογραφηθεί. Στο Σχήμα 3.3 βλέπουμε ένα γύρο της κωδικοποίησης και ένα γύρο της αποκωδικοποίησης.

Σχήμα 3.3 DES με τρόπο λειτουργίας ECB

Κρυπταλγόριθμος αλυσιδωτού τμήματος, CBC

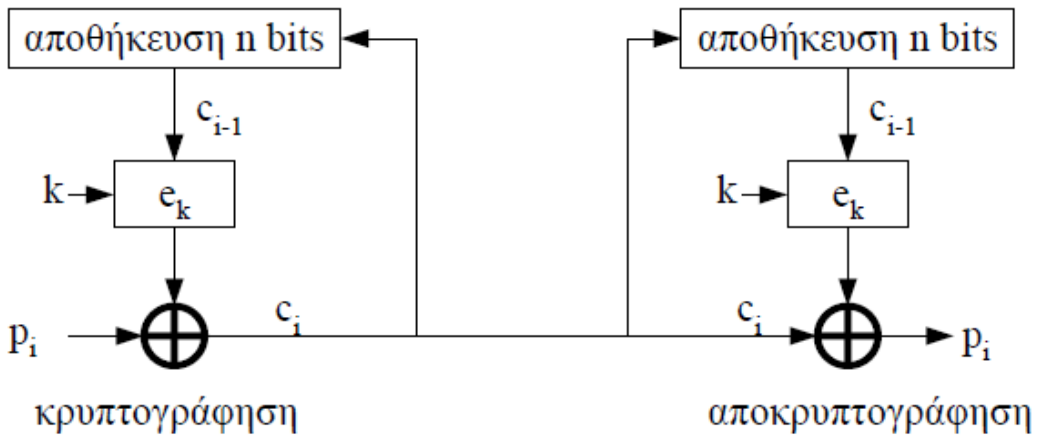
Ο τρόπος λειτουργίας CBC εισάγει ένα βαθμό πολυπλοκότητας εισάγοντας στην κωδικοποίηση το κλειδί , το κομμάτι του μηνύματος, αλλά και το προηγούμενο κομμάτι του μηνύματος που έχει σταλεί. Παράδειγμα ενός γύρου κωδικοποίησης και ενός γύρου αποκωδικοποίησης φαίνεται και στο Σχήμα 3.4



Σχήμα 3.4 DES με τρόπο λειτουργίας CBC

Ανάδραση ρυπταλγόριθμου, CFB

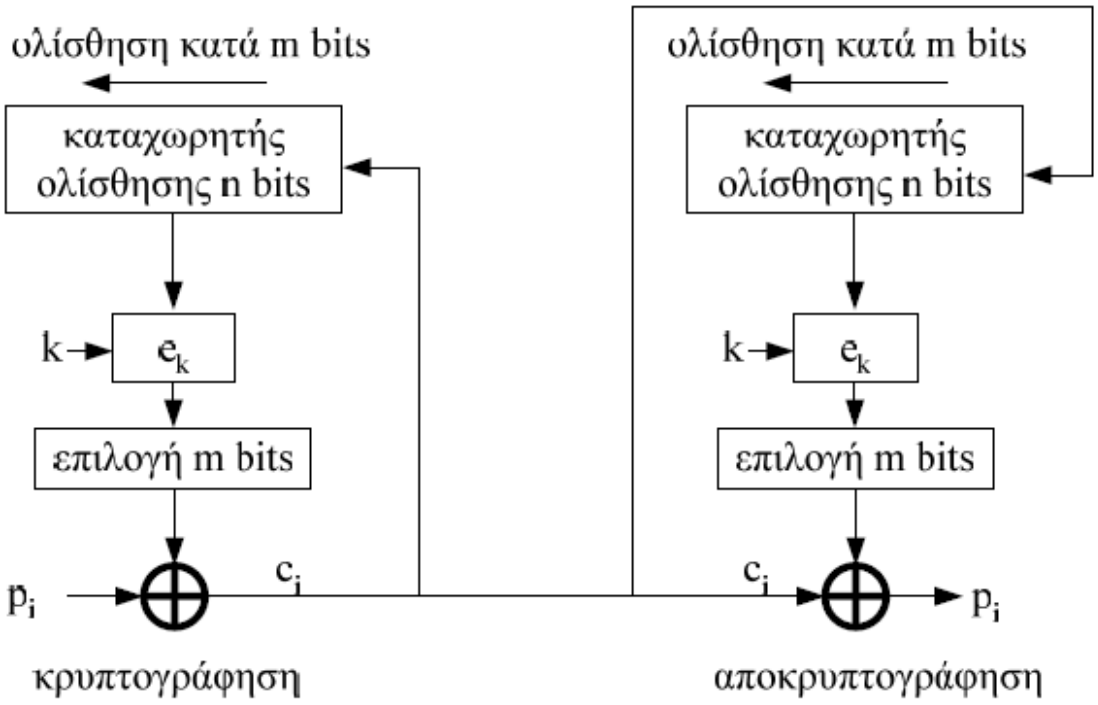
Ο τρόπος λειτουργίας CFB κρυπτογραφεί ξανά το προηγούμενο κομμάτι του μηνύματος με το κλειδί και μετά το συνδυάζει με το κομμάτι του μηνύματος που θα κρυπτογραφηθεί.



Σχήμα 3.5 DES με τρόπο λειτουργίας CFB

Ανάδραση εξόδου, OFB

Ο τρόπος λειτουργίας OFB εισάγει ένα βαθμό πολυπλοκότητας εισάγοντας στην κωδικοποίηση το κλειδί , το κομμάτι του μηνύματος, αλλά και ένας καταχωρητής ολίσθησης .



Σχήμα 3.6 DES με τρόπο λειτουργίας OFB

Η βασική λειτουργία σε κάθε γύρο κρυπτογράφησης είναι μια πράξη αντικατάστασης,: συγκεκριμένα, κατά τη διαδικασία της κρυπτογράφησης, υπάρχουν ειδικές μονάδες αντικατάστασης (S-box) οι οποίες επενεργούν σε τμήματα από bit μεγέθους **6** και τα αντικαθιστούν από άλλα τμήματα μεγέθους 4 bit**.**

3.1.2 Ασύμμετρα Κρυπτοσυστήματα (Αλγόριθμοι Δημοσίου Κλειδιού)

Οι αλγόριθμοι δημοσίου κλειδιού ή ασύμμετρα κρυπτοσυστήματα βασίζονται στην ιδέα της χρήσης διαφορετικών κλειδιών από τον αποστολέα και τον παραλήπτη. Η ασύμμετρη

κρυπτογραφία χρησιμοποίει δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Δεν χρειάζεται πλέον ο αποστολέας και ο παραλήπτης του μηνύματος να μοιράζονται το ίδιο κλειδί. Το μόνο που χρειάζεται είναι να ξέρει ο κάθε χρήστης το δημόσιο κλειδί του χρήστη που θα στείλει το μήνυμα. Ο κάθε χρήστης έχει το δημόσιο κλειδί που είναι γνωστό και ένα αντίστοιχο ιδιωτικό κλειδί που μόνο ο ιδιοκτήτης του κλειδιού το ξέρει. Τα ασύμμετρα κρυπτοσυστήματα εκτός από την κρυπτογράφηση του μηνύματος και την ασφαλή επικοινωνία έχουν και την δυνατότητα για αυθεντικοποίηση του μηνύματος και αυθεντικοποίηση του αποστολέα.

3.1.3 RSA

Ο RSA είναι ο πιο γνωστός αλγόριθμος δημοσίου κλειδιού. Παρουσιάστηκε στα τέλη της δεκαετίας του 1970. Ο αλγόριθμος RSA βασίζει την ασφάλεια του στην μαθηματική δυσκολία εύρεσης των πρώτων παραγόντων μεγάλων αριθμών (πρόβλημα της παραγοντοποίησης – factorization problem).

Ο RSA έχει 2 κλειδιά για τον κάθε χρήστη, το ιδιωτικό κλειδί όπου είναι μόνο για τον ίδιο και το αντίστοιχο δημόσιο που μπορεί να έχει πρόσβαση όποιος θέλει να στείλει κάτι στον κάτοχό τους Τα 2 κλειδιά στον RSA δεν είναι τυχαία αλλά υπάρχει συγκεκριμένος τρόπος για την δημιουργία τους. Ο χρήστης επιλέγει 2 μεγάλους αριθμούς της τάξης των 200 bits τους p και q. Στη συνέχεια υπολογίζει το γινόμενο τους $n=p\times q$. Μετά επιλέγει τυχαία ένα αριθμό e που να ικανοποιεί τη σχέση ΜΚΔ $(e,(p-1)*(q-1))=1$,. Το ιδιωτικό κλειδί d είναι ο αντίστροφος τους e mod **(p-1)(q-1),** δηλαδή $d=e^{-1}(\mathrm{mod}(p-1)(q-1))$ και, το αντίστοιχο δημόσιο κλειδί είναι το ζεύγος των αριθμών (n,e)

Όταν θέλει να στείλει κάποιος ένα μήνυμα m στον χρήστη θα κάνει την πράξη $c=m^e(\mathrm{mod}(n))$.

Ο χρήστης θα παραλάβει το κρυπτογραφημένο μήνυμα c και θα ανακτήσει το αρχικό κείμενο με την πράξη $m=c^d(\mathrm{mod}(n))$. Εφόσον κανείς άλλος δεν ξέρει το d μόνο ο αληθινός χρήστης μπορεί να πάρει το σωστό μήνυμα .

Το αδύνατο σημείο του RSA όπως και κάθε αλγορίθμου δημοσίου κλειδιού, είναι η ορθότητα του δημοσίου κλειδιού κάποιου χρήστη. Εάν ένας χρήστης δεν ανακτήσει το σωστό δημόσιο κλειδί του συνομιλητή του (δηλαδή του παραλήπτη των μηνυμάτων του) αλλά κάποιου άλλου τρίτου κακόβουλου χρήστη, τότε προφανώς κάθε μήνυμα που κρυπτογραφεί θα μπορεί να αποκρυπτογραφείται από τον κακόβουλο αυτό χρήστη. Έτσι, στην περίπτωση όπου κάποιος επιτιθέμενος θέλει να υποκλέψει κάτι, μπορεί να βάλει το δικό του κλειδί στην θέση του χρήστη που θέλει να πάρει το μήνυμα και έτσι ό,τι στέλλεται θα είναι κωδικοποιημένο με το κλειδί του υποκλοπέα. Στη συνέχεια αυτός με την σειρά του θα ξαναστέλνει το μήνυμα στον σωστό παραλήπτη και με την ανάποδη διαδικασία θα παίρνει την απάντηση. Ο τρόπος υποκλοπής αυτού του είδους ονομάζεται Man-In-The-Middle. Για την αντιμετώπιση αυτών των επιθέσεων χρησιμοποιούνται τα λεγόμενα ψηφιακά πιστοποιητικά, τα οποία δημιουργούνται από έγκυρες και αναγνωρισμένες οντότητες για να πιστοποιούν τη γνησιότητα των δημόσιων κλειδιών.

3.2 Κρυπτανάλυση

Η κρυπτανάλυση είναι η μελέτη των αρχών και των μεθόδων που αποσκοπούν στην αποκρυπτογράφηση του μηνύματος χωρίς να είναι γνωστό το κλειδί. Με απλά λόγια να αποκτήσουμε πρόσβαση στο κρυπτογραφημένο μήνυμα χωρίς να έχουμε στην πραγματικότητα άδεια για πρόσβαση. Κατά καιρούς έχουν παρουσιαστεί διάφορες μεθόδοι κρυπτανάλησης ανάλογες με την μέθοδο κρυπτογράφησης. Κάποιες γνωστές μέθοδοι είναι:

- Known-plaintext attack (γνωστού μηνύματος): Στις επιθέσεις αυτές, ο επιτιθέμενος γνωρίζει, εκτός από το κρυπτοκείμενο, και ένα τμήμα του μηνύματος. Με αυτήν την πληροφορία, καλείται να ανακαλύψει είτε ολόκληρο το μήνυμα είτε το μυστικό κλειδί.

- Chosen - plaintext attack (επιλεγμένου μηνύματος) :Στις επιθέσεις αυτές, ο επιτιθέμενος είναι σε θέση να επιλέξει ο ίδιος συγκεκριμένα τμήματα του αρχικού μηνύματος που θα γνωρίζει, και να παρατηρεί τα αντίστοιχα κρυπτογραφήματα που προκύπτουν.

- Chosen - cipher text attack (επιλεγμένου κρυπτοκειμένου):Είναι αντίστροφης λογικής με την ανωτέρω: εδώ, ο επιτιθέμενος είναι σε θέση να επιλέξει συγκεκριμένα τμήματα του κρυπτοκειμένου και στη συνέχεια να μάθει πώς αυτά θα αποκρυπτογραφούνταν (δηλ. σε ποια αρχικά μηνύματα) αν χρησιμοποιηθεί το μυστικό κλειδί αποκρυπτογράφησης.

- Επιθέσεις βάσει λεξικού: σε αυτή την περίπτωση ο επιτιθέμενος παίρνει μια βάση με πιθανές λέξεις και τις κρυπτογραφεί με τον ίδιο τρόπο με το κείμενο και μετά συγκρίνει τα δύο κρυπτογραφήματα και αν ταιριάζουν η λέξη είναι το μήνυμα.

- Man in the middle (Άνθρωπος στη μέση) : αυτή είναι μια μέθοδος όπου ο επιτιθέμενος μπορεί να μπει ανάμεσα στον αποστολέα και τον παραλήπτη και να παίρνει τα μηνύματα προσποιούμενος τον ανάλογο ρόλο και μετά ξαναστέλνοντας τα μηνύματα στον πραγματικό παραλήπτη να μην είναι αντιληπτός.

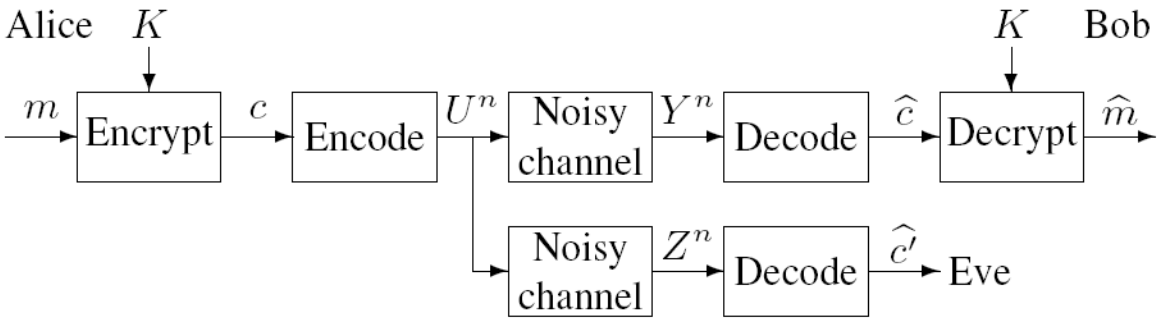
Κεφάλαιο 4
Κρυπτογράφηση Στο Φυσικό Επίπεδο

Στο Κεφάλαιο αυτό θα εστιάσουμε σε κάποιες βασικές προσεγγίσεις που έχουν προταθεί αναφορικά με την κρυπτογράφηση στο φυσικό επίπεδο. Με αυτόν τον τρόπο, οι λειτουργίες της κρυπτογράφησης και της κωδικοποίησης «συμπλέκονται» κατάλληλα, γεγονός που πολλές φορές είναι εξαιρετικά χρήσιμο σε επίπεδο υλοποίησης – ενώ επίσης, όπως θα δούμε, υπάρχουν πολλοί ισχυρισμοί και ως προς το κομμάτι της ενίσχυσης της ασφάλειας που παρέχεται με αυτόν τον τρόπο.

4.1 Βασική ιδέα

Έχουμε δει σε μεγάλο βαθμό τόσο την κωδικοποίηση καναλιού αλλά και την κρυπτογράφηση σαν δύο σημαντικές λειτουργίες σε ένα δίκτυο. Κατά κανόνα αποτελούν δύο διαφορετικές διαδικασίες: η μεν κωδικοποίηση καναλιού αποσκοπεί στην ανίχνευση και διόρθωση σφαλμάτων κατά τη μετάδοση, ενώ η κρυπτογράφηση στοχεύει κυρίως στην εμπιστευτικότητα αλλά, με κατάλληλα σχήματα, και αυθεντικοποίηση του μηνύματος, καθώς και στην αυθεντικοποίηση του αποστολέα .

Αν θεωρήσουμε τη διαστρωμάτωση των δικτύων επικοινωνιών με βάση το μοντέλο OSI, η κωδικοποίηση του καναλιού πραγματοποιείται στο φυσικό επίπεδο (physical layer), στο τελευταίο στάδιο πριν από την μετάδοση. Η κρυπτογράφηση εκτελείται σε κάποιο από τα υψηλότερα επίπεδα, αναλόγως του τρόπου που επιλέγεται:. Για παράδειγμα, μπορούμε να έχουμε κρυπτογράφηση πάνω από το επίπεδο εφαρμογής, όπως στην περίπτωση της εφαρμογής PGP (Pretty Good Privacy), αλλά και στο επίπεδο μεταφοράς δεδομένων όπως το SSL (Secure Socket Layer). Σε κάθε περίπτωση, ένα τυποποιημένο τηλεπικοινωνιακό μοντέλο είναι το εξής:



Σχήμα 4.1 κλασικός τρόπος επικοινωνίας

M =μήνυμα

c = κρυπτογραφημένο μήνυμα

U = κωδικοποιημένο μήνυμα

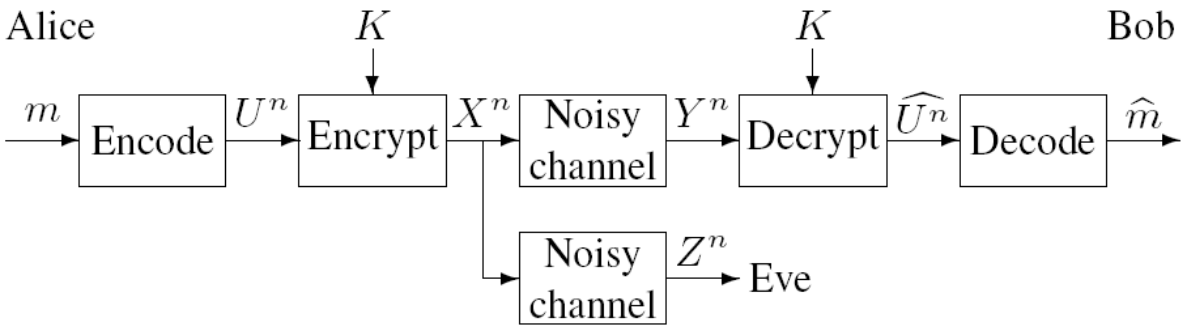
Y= το μήνυμα που λαμβάνει ο δέκτης (U, με θόρυβο μετάδοσης προς παραλήπτη)

Z= το μήνυμα που παρατηρεί ο επίδοξος υποκλοπέας (U με θόρυβο μετάδοσης προς υποκλοπέα)

Στο σχήμα 4.1 βλέπουμε τον κλασικό τρόπο επικοινωνίας με την χρήση κρυπτογράφησης ακολουθούμενη από κωδικοποίηση: κατά τη λήψη γίνεται το αντίστροφο, δηλαδή πρώτα διόρθωση των λαθών μετάδοσης και μετά αποκρυπτογράφηση. Με αυτό τον τρόπο η κωδικοποίηση δεν εμπλέκεται στην κρυπτογράφηση και όποιος θέλει να υποκλέψει το μήνυμα έχει άμεση πρόσβαση στο κρυπτοκείμενο. Η ασφάλεια του μηνύματος βασίζεται μόνο στην κρυπτογραφία και τον τρόπο που γίνεται, αφού θεωρούμε ότι ο επίδοξος υποκλοπέας ξέρει τον τρόπο κωδικοποίησης του καναλιού και μπορεί να διορθώσει το μήνυμα από τα λάθη μετάδοσης. Η ασφάλεια του μηνύματος παρέχεται αποκλειστικά από τον αλγόριθμο κρυπτογράφησης και βασίζεται ουσιαστικά στη δυσκολία ανεύρεσης του κλειδιού.

Ένας εναλλακτικός τρόπος επικοινωνίας είναι η χρήση της κωδικοποίησης πριν από την κρυπτογράφηση - κάτι που αλλάζει τον κλασικό τρόπο επικοινωνίας. Συγκεκριμένα, μπορούμε πρώτα να κάνουμε την κωδικοποίηση του μηνύματος και μετά να το κρυπτογραφήσουμε στο φυσικό επίπεδο: η κρυπτογράφηση μπορεί να είναι μία απλή πράξη XOR με μία κλειδοροή – δηλ. να χρησιμοποιηθεί κρυπταλγόριθμος ροής (stream cipher) ή ενας κρυπταλγόριθμος τμήματος (block cipher) σε τρόπο λειτουργίας π.χ. CFB (βλ. προηγούμενο κεφάλαιο). Ένας εύκολος τρόπος

παραγωγής της κωδικολέξης είναι η χρήση του κλειδιού που ξέρουν μόνο ο αποστολέας και ο παραλήπτης και μιας δεδομένης συνάρτησης .



Σχήμα 4.2 εναλλακτικός τρόπος επικοινωνίας

M =μήνυμα

U = κωδικοποιημένο M

X =κρυπτογραφημένο (U)

Y= x με θόρυβο μετάδοσης

Στο σχήμα 4.2 βλέπουμε μια απεικόνιση του εναλλακτικού αυτού τρόπου επικοινωνίας, που διαφέρει από τον κλασικό [7] Ο εναλλακτικός αυτός τρόπος προσθέτει και ένα νέο επίπεδο ασφάλειας γιατί ο επίδοξος υποκλοπέας λαμβάνει ένα μήνυμα που περιέχει το αποτέλεσμα της τελευταίας XOR πράξης (κρυπτογράφηση) αλλά και τα λάθη μετάδοσης που εισήγαγε το κανάλι και τα οποία και δεν μπορεί να διορθώσει. Ο τρόπος αυτός καθιστά την επίθεση γνωστού κειμένου σχεδόν αδύνατο να εφαρμοστεί: και αυτό διότι το κρυπτογραφημένο μήνυμα που παρατηρεί δεν αποτελεί κρυπτογράφηση του αρχικού μηνύματος αλλά περιέχει και τα σφάλματα που προκλήθηκαν κατά τη μετάδοση, τα οποία και δεν έχουν διορθωθεί. Συνεπώς, αυτός ο τρόπος μετάδοσης (κρυπτογράφηση στο φυσικό επίπεδο) φαίνεται ότι προσθέτει ακόμη ένα βήμα στην ασφάλεια του μηνύματος.

Αξίζει να σημειωθεί ότι ένα πραγματικό παράδειγμα αυτής της τεχνικής μετάδοσης είναι η τεχνολογία GSM (Global System for Mobile communications) της κλασικής κινητής τηλεφωνίας,

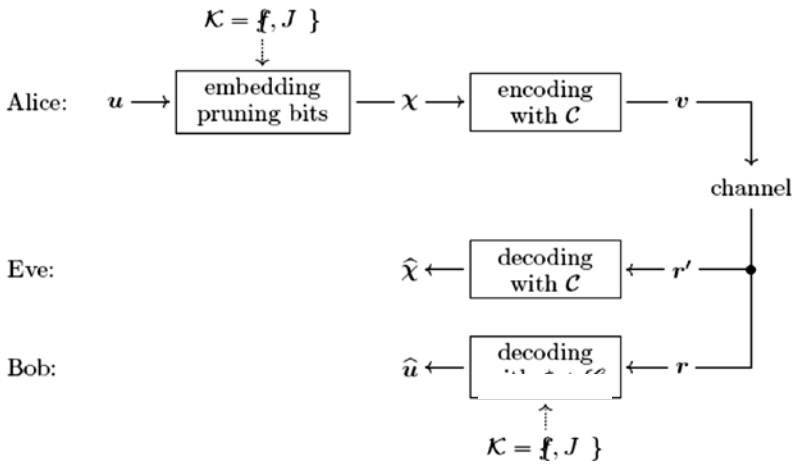
όπου η κρυπτογράφηση [7] με τον κρυπταλγόριθμο ροής A5/1 stream cipher γίνεται πάνω στα πακέτα που είδη έχουν προστεθεί bit κωδικοποίησης.

Από τα παραπάνω γίνεται σαφές ότι ο σωστός συνδυασμός κρυπτογράφησης και κωδικοποίησης μπορεί να αποφέρει πρόσθετα πλεονεκτήματα. Η παραπάνω τεχνική ωστόσο (κρυπτογράφηση σε φυσικό επίπεδο) δεν είναι και η πλέον συνήθης, και οι λόγοι για αυτό έχουν να κάνουν κυρίως με θέματα υλοποίησης. Ωστόσο, από την άλλη πλευρά, μπορεί κανείς να χρησιμοποιήσει κατάλληλα κάποιους κώδικες διόρθωσης σφαλμάτων προκειμένου να κατασκευάσει ισχυρά κρυπτογραφικά συστήματα. Αυτό είναι και το αντικείμενο του επόμενου κεφαλαίου.

4.2 Παράδειγμα κρυπτογράφησης στο φυσικό επίπεδο

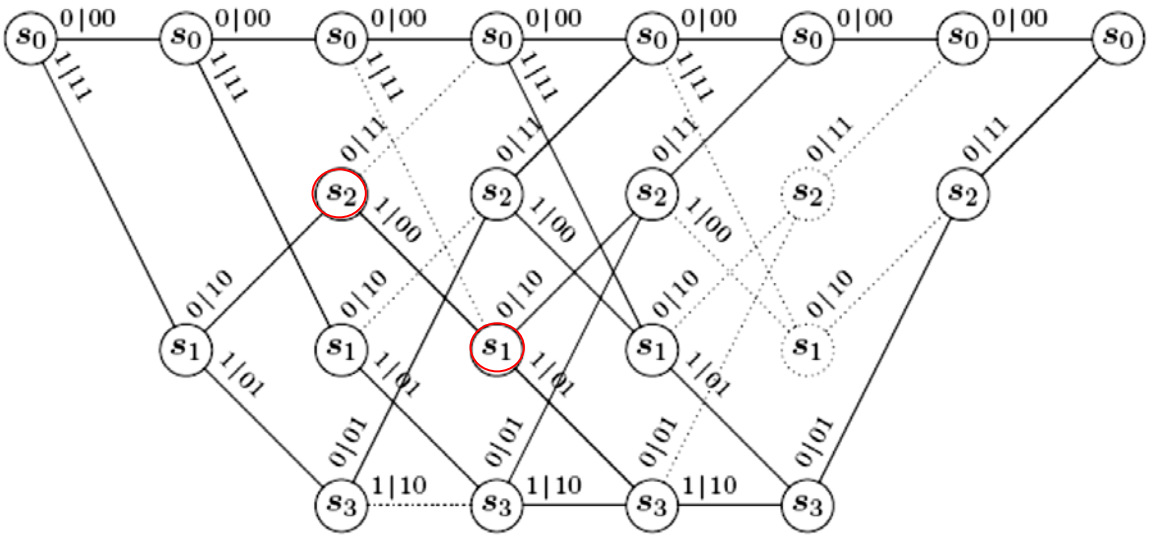
Μια καινούργια ιδέα ενσωμάτωσης κρυπτογραφικής λειτουργίας σε κωδικοποιητές διόρθωσης σφαλμάτων προτάθηκε πολύ πρόσφατα στο [8] και βασίζεται στους συνελικτικούς κώδικες που είδαμε στο κεφάλαιο της κωδικοποίησης. Σκοπός αυτής της νέας προσέγγισης δεν είναι να αντικατασταθούν οι υφιστάμενοι τρόποι κρυπτογράφησης, αλλά η προσθήκη ενός νέου εύκολου τρόπου κρυπτογράφησης που θα προσαυξήσει την ασφάλεια και που μπορεί να βοηθήσει ιδιαίτερα σε συστήματα με περιορισμένες υπολογιστικές δυνατότητες. Η ιδέα είναι να εφαρμόσουμε σε έναν συγκεραστικό κώδικα μία διαδικασία γνωστή ως απαλοιφή μονοπατιών του διαγράμματος trellis (pruning). Ουσιαστικά, κατά την κωδικοποίηση, εισάγουμε ενδιαμέσως των bits του μηνύματος κάποια πρόσθετα bits, που λέγονται pruning bits, πλήθους J και με βάση μία συνάρτηση F που καθορίζει τις τιμές τους αλλά και τις θέσεις τους. Το κλειδί μας στην περίπτωση αυτή είναι το ζεύγος (F, J). Η ασφάλεια της τεχνικής αυτής βασίζεται στο γεγονός της μη γνώσης του κλειδιού από τον υποκλοπέα, με αποτέλεσμα η αποκωδικοποίηση με βάση τον αλγόριθμο Viterbi να τον οδηγεί σε ένα μήνυμα που δεν έχει σχέση με το γνήσιο που έχει αποσταλεί. Ο παραλήπτης, που γνωρίζει τόσο τα pruning bits όσο και τις ακριβείς τους θέσεις, μπορεί κατά την αποκωδικοποίηση κατά Viterbi να απαλείφει τα μονοπάτια του trellis που δεν χρειάζονται, ανακτώντας με αυτόν τον τρόπο το αρχικό σωστό μήνυμα.

Ας δούμε τις λεπτομέρειες της εν λόγω τεχνικής: Η Alice θέλει να επικοινωνήσει με τον Bob. Για το σκοπό αυτό χρησιμοποιεί έναν (n,1) συγκεραστικό κώδικα *C* με m βαθμίδες,. Με την κλασική διαδικασία της κωδικοποίησης, η είσοδος στον κωδικοποιητή θα ήταν η ακολουθία u που αποτελεί το αρχικό μήνυμα. Με την προτεινόμενη τεχνική, η u μετατρέπεται σε μία άλλη ακολουθία χ, έχοντας παρεμβάλει J νέα bits σε διάφορες θέσεις, βάσει μίας συνάρτησης f.



Σχήμα 4.3 λογικό διάγραμμα της ιδέας κωδικοποίησης [8]

Τα ανωτέρω αποτυπώνονται στο Σχήμα 4.3. Το μυστικό κλειδί K=(f, J) διαφοροποιεί το μήνυμα που εισάγεται στον κωδικοποιητή από u σε χ. Ο κωδικοποιητής παράγει μία κωδική λέξη *υ* που προέρχεται από την κωδικοποίηση του «παραποιημένου» μηνύματος χ. Η λέξη αυτή αποστέλλεται και ο παραλήπτης λαμβάνει μία r' η οποία είναι μία παραποιημένη εκδοχή της κωδικής λέξης *υ* λόγω των σφαλμάτων που εισήγαγε το κανάλι μετάδοσης. Τόσο ο Bob, όσο και η Eve που είναι κακόβουλη και θέλει να υποκλέψει την επικοινωνία, γνωρίζουν το ληφθέν μήνυμα r'. Η Eve, το μόνο που μπορεί να κάνει, είναι να επιχειρήσει να αποκωδικοποιήσει το r' χρησιμοποιώντας τον κώδικα C – από όπου και θα ανακτήσει μία προσέγγιση του χ: όσο όμως πλησίον του χ και αν είναι η προσέγγιση αυτή (ιδανικά θα ταυτίζεται, αν ο κώδικας είναι σε θέση να διορθώσει όλα τα σφάλματα που εισήγαγε το κανάλι), η Eve δεν θα μπορεί να ανακτήσει το αρχικό μήνυμα u. Ο Bob από την άλλη θα αποκωδικοποιήσει έχοντας εις γνώσιν του τις θέσεις και τιμές των pruning bits, οπότε κατά την αποκρυπτογράφηση με τον αλγόριθμο Viterbi θα «αγνοεί» κάποια μονοπάτια, με αυτόν τον τρόπο μπορεί να αποκωδικοποιήσει στο αρχικό μήνυμα u (ουσιαστικά θα υπολογίσει μία προσέγγιση αυτού, όπου αν ο κώδικας μπορεί να διορθώσει όλα τα σφάλματα η ανάκτηση που θα επιτύχει θα είναι πλήρης για το αρχικό μήνυμα).



Σχήμα 4.4 Διάγραμμα trellis με την προσθήκη pruned bits

Ένα διάγραμμα trellis που αποτυπώνει την ανωτέρω περιγραφείσα διαδικασία αποκωδικοποίησης αποτυπώνεται στο Σχήμα 4.4. Οι διακεκομμένες γραμμές αντιστοιχούν στις θέσεις των pruning bits – δηλαδή τις γνωρίζει μόνο ο νόμιμος παραλήπτης και όχι ο επίδοξος υποκλοπέας και περιγράφουν τις μεταβάσεις καταστάσεων που δεν μπορούν να συμβούν ποτέ. Για παράδειγμα, στο διάγραμμα αυτό φαίνεται ότι το τρίτο bit της εισόδου του κωδικοποιητή είναι pruning bit. Ο παραλήπτης γνωρίζει αυτήν την πληροφορία και, συνεπώς, αν π.χ. γνωρίζει ότι βρίσκεται στην κατάσταση s2, ξέρει ότι η επόμενη κατάσταση είναι σίγουρα η s1 και όχι η s0, ανεξαρτήτως της κωδικής λέξης που έλαβε (βλ. τις γραμμοσκιασμένες με κόκκινο χρώμα καταστάσεις). Η Eve δεν το γνωρίζει αυτό και θα θεωρήσει και το μονοπάτι s1 - > s0 ως πιθανό, κατά τη διαδικασία της αποκωδικοποίησης.

Περαιτέρω έρευνα απαιτείται ακόμη προκειμένου να θεσπιστούν κανόνες για την επιλογή των σχεδιαστικών παραμέτρων ενός τέτοιου συστήματος, όπως είναι η επιλογή του αρχικού κώδικα, ιδιότητες και πλήθος των pruning bits, ενώ ακόμα η μαθηματική θεμελίωση της ασφάλειας είναι ένα ζήτημα που πρέπει να διερευνηθεί. Παρόλα αυτά, η εν λόγω τεχνική είναι εξαιρετικά υποσχόμενη, καταδεικνύοντας τα πλεονεκτήματα που μπορεί να αποκομίσει κανείς «εμφυτεύοντας» την κρυπτογράφηση στο φυσικό επίπεδο.

Κεφάλαιο 5

ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ ΒΑΣΙΣΜΕΝΑ ΣΕ ΚΩΔΙΚΕΣ

Στο συγκεκριμένο κεφάλαιο θα μελετήσουμε δύο αμιγώς κρυπτογραφικά σχήματα, των οποίων η κατασκευή βασίζεται σε κώδικες ανίχνευσης σφάλματος: αυτά είναι το κρυπτοσύστημα McEliece και το κρυπτοσύστημα Niederreiter.

5.1 Κρυπτοσύστημα McEliece

Ο κρυπταλγόριθμος McEliece [7] ανήκει στα ασύμμετρα συστήματα κρυπτογράφησης. Πέρα από την αρχική του έκδοση που προτάθηκε στο [7]., έχουν υπάρξει και παραλλαγές του – με σημαντικότερη αυτή στο [9]. Στην εργασία αυτή θα παρουσιάσουμε τον αλγόριθμο στην κλασική του μορφή.

Ο αλγόριθμος παρουσιάστηκε το 1978 από τον Robert McEliece. Συγκριτικά με τον RSA – που είναι επίσης ένας σημαντικός αλγόριθμος ασύμμετρης κρυπτογράφησης - είναι πιο γρήγορος στην λειτουργία του: όμως έχει πολύ μεγαλύτερο δημόσιο κλειδί – συγκεκριμένα, το δημόσιο κλειδί του McEliece είναι μεγέθους 512 kilobits .

Οι κώδικες που ο ίδιος ο McEliece πρότεινε για το κρυπτοσύστημά του είναι οι λεγόμενοι κώδικες Goppa, οι οποίοι συνιστούν μία σημαντική κατηγορία κυκλικών κωδίκων: ωστόσο, μπορούν να χρησιμοποιηθούν και άλλοι κώδικες (αν και σε άλλη περίπτωση - πλην των Goppa κωδίκων - χρήζει προσοχής η παρεχόμενη ασφάλεια).

Στο κρυπτοσύστημα McEliece, κάθε χρήστης έχει δύο κλειδιά: το ιδιωτικό κλειδί, όπου είναι γνωστό μόνο στον ιδιοκτήτη του, και το δημόσιο κλειδί. Για τη δημιουργία των δύο κλειδιών

χρησιμοποιείται ένας γραμμικός (n, k) κώδικας, ικανός να διορθώσει t λάθη (δηλαδή με διορθωτική ικανότητα t – αυτό σημαίνει ότι η ελάχιστη απόσταση του κώδικα είναι $d_{min}=2t + 1$). Κατασκευάζουμε έναν πίνακα-γεννήτορα G του κώδικα με διαστάσεις k x n, έναν τυχαίο δυαδικό τετραγωνικό πίνακα S διαστάσεων k x k ο οποίος είναι αντιστρέψιμος, καθώς και έναν τυχαίο δυαδικό τετραγωνικό πίνακα P διαστάσεων n x n, όπου κάθε γραμμή αλλά και κάθε στήλη του έχει ακριβώς ένα «1». Από τους ανωτέρω πίνακες υπολογίζουμε τον πίνακα G', διαστάσεων k x n, ως εξής:

$$G' = SGP$$

Η τριπλέτα (S,G,P) αποτελεί το ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί είναι το ζευγάρι (G', t).

Για να κρυπτογραφήσουμε το μήνυμα m χρησιμοποιούμε το δημόσιο κλειδί του παραλήπτη (G',t), ως εξής:

α) Επιλέγουμε ένα διάνυσμα e μήκους n με βάρος Hamming μικρότερο ή ίσο του t

β) Υπολογίζουμε το διάνυσμα c=m*G'+t (όπου η πρόσθεση είναι δυαδική).

Στην ουσία, η κρυπτογραφημένη λέξη c δεν είναι τίποτα άλλο παρά η κωδική λέξη για το μήνυμα m, εάν χρησιμοποιήσουμε ως κώδικα αυτόν που έχει πίνακα-γεννήτορα τον G', όπου όμως στην κωδική αυτή λέξη έχουμε εισάγει ένα πλήθος σφαλμάτων (σε εκείνες τις θέσεις που προσδιορίζονται από το διάνυσμα e). Με άλλα λόγια, το κρυπτοκείμενο αποτελεί μία αλλοιωμένη εκδοχή της κωδικής λέξης.

Ο παραλήπτης, έχοντας το ιδιωτικό του κλειδί (S,G,P), λαμβάνοντας το κρυπτοκείμενο c κάνει τις πιο κάτω ενέργειες:

α) Πολλαπλασιάζει (από δεξιά) το c με τον αντίστροφο πίνακα του P:

$$(mG'+e)P^{-1} = mG'P^{-1} + eP^{-1} = mSG + eP^{-1}$$

β) Το παραπάνω δεν είναι τίποτα άλλα παρά η κωδική λέξη του αυθεντικού (αρχικού) κώδικα (δηλ. του κώδικα με πίνακα-γεννήτορα G) για το μήνυμα mS, στην οποία όμως κωδική λέξη έχουν προστεθεί σφάλματα. Το πλήθος των σφαλμάτων είναι ίσο με το πλήθος των «1» στο διάνυσμα eP^{-1}, το οποίο με τη σειρά του είναι ίσο με το πλήθος των «1» στο διάνυσμα e (αφού το διάνυσμα eP^{-1}, λόγω της ιδιαίτερης μορφής του P, δεν είναι τίποτα άλλα παρά μία αντιμετάθεση των στοιχείων του e). Κατά συνέπεια, τα σφάλματα που έχουν εισαχθεί είναι εντός της διορθωτικής ικανότητας του κώδικα, οπότε και ο παραλήπτης μπορεί να αποκωδικοποιήσει την

κωδική λέξη (με κάποια από τις γνωστές τεχνικές κωδικοποίησης του κώδικα[2]). Με άλλα λόγια, ο παραλήπτης από το διάνυσμα $mSG + eP^{-1}$ μπορεί να υπολογίσει (αφού γνωρίζει το G) το διάνυσμα mS.

γ) Έχοντας το διάνυσμα mS, μπορεί να υπολογίζει το αρχικό μήνυμα m πολλαπλασιάζοντάς το, από δεξιά, με το S^{-1}.

Παράδειγμα κρυπτοσυστήματος McEliece

[10]Ας θεωρήσουμε τον (7,4) Hamming κώδικα που περιγράψαμε στο κεφάλαιο της κωδικοποίησης. Ο κώδικας έχει την ικανότητα να διορθώσει όλα τα απλά (μονά) λάθη, όπως εξηγήσαμε - άρα το t είναι 1.

Ο πίνακας γεννήτορας G του κώδικα είναι:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Για k=4 και n=7, παράγουμε τους ακόλουθους πίνακες S και P, οι οποίοι πληρούν τις επιθυμητές ιδιότητες:

$$S = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

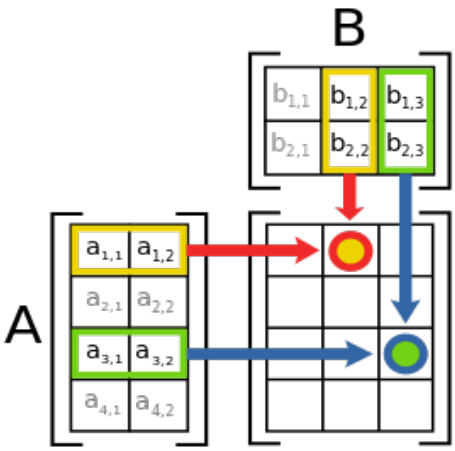
$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

[2] Οι τεχνικές αποκωδικοποίησης των κωδίκων Goppa είναι εκτός του αντικειμένου της παρούσας εργασίας

Η ανωτέρω τριπλέτα (G, S, P) αποτελεί το ιδιωτικό μας κλειδί, από όπου μπορούμε πλέον να υπολογίσουμε το G' (που αποτελεί τμήμα του δημόσιου κλειδιού), μέσω της πράξης G' =SGP. Το αποτέλεσμα από αυτόν τον πολλαπλασιασμό πινάκων είναι

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

όπου ο πολλαπλασιασμός πινάκων γίνεται κατά τα γνωστά (βλ. ενδεικτικά Σχήμα 5.1):



Σχήμα 5.1 παράδειγμα πολλαπλασιασμού πινάκων

Δημόσιο κλειδί του αλγορίθμου είναι ο πίνακας G', καθώς και η διορθωτική ικανότητα t του αρχικού κώδικα (που είναι μυστικός).

Γι α να κρυπτογραφήσει ένας χρήστης το μήνυμα m πρέπει να επιτελέσει την πράξη m*G'+e =c

Για να στείλει, παραδείγματος χάρη, το μήνυμα m = (1 1 0 1), έχουμε

$$\begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} x \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Στη συνέχεια, προσθέτουμε ένα διάνυσμα e που έχει βάρος t, δηλαδή 1: έστω λοιπόν το διάνυσμα e =(0000100), οπότε και

c=(0110010)+ (0000100) =(0110110)

Συνεπώς, το τελικό κρυπτοκείμενο που θα αποσταλεί είναι το c =(0110110).

Ο παραλήπτης υπολογίζει τους αντίστροφους των πινάκων S και P (που είναι και ο μόνος που τους γνωρίζει, αφού είναι τμήμα του ιδιωτικού του κλειδιού):

$$P^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$S^{-1} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Ακολούθως υπολογίζει το διάνυσμα $c' = c \times P^{-1}$ - όπου, εν προκειμένω, θα έχουμε c' = (1 0 0 0 1 1 1).

Το c' αποτελεί μία κωδική λέξη του αρχικού Hamming κώδικα, η οποία όμως περιέχει λάθη, το πλήθος των οποίων (εν προκειμένω, ένα) είναι εντός της διορθωτικής ικανότητας του κώδικα: συνεπώς, με την χρήση του ίδιου κώδικα που χρησιμοποιήθηκε κατά την δημιουργία του G μπορούμε να εντοπίσουμε τα λάθη μετάδοσης, οπότε και κατ' επέκταση το e αλλά και τη σωστή κωδική λέξη. Αποκωδικοποιώντας λοιπόν με βάση τον αρχικό (μυστικό) Hamming κώδικα, ανασκευάζουμε τη σωστή κωδική λέξη (1 0 0 0 1 1 0) – δηλαδή, είχε συμβεί ένα σφάλμα στο τελευταίο bit. Από αυτήν την κωδική λέξη βρίσκουμε ότι το αντίστοιχο μήνυμα είναι το χ = (1 0 0 0). Ως εκ τούτου, το αρχικό μήνυμα m προκύπτει αν πολλαπλασιάσουμε το χ με τον πίνακα S^{-1}, από όπου βρίσκουμε τελικά:

$$m = \chi S^{-1} = (1\ 1\ 0\ 1)$$

Ο αλγόριθμος McEliece όπως είδαμε έχει την ικανότητα ότι, εκτός από κρυπτογραφία, προσθέτει και υπηρεσίες κωδικοποίησης καναλιού χωρίς επιπλέον πράξεις. Το τελικό μήνυμα μετά την αποκρυπτογράφηση μπορεί να περιέχει λάθη μετάδοσης - όμως ακολούθως επιλέγεται η πλησιέστερη λέξη ανάλογα με τον αλγόριθμο που χρησιμοποιήσαμε και επιλέγουμε το αντίστοιχο μήνυμα αυτής ως αυτό που τελικά εστάλη (soft decision αποκωδικοποίηση) και με αυτό τον τρόπο διορθώνονται τα λάθη μετάδοσης. Σε περίπτωση που ο αλγόριθμος είναι σε

θέση να εντοπίσει λάθος μετάδοσης αλλά όχι σε θέση να το διορθώσει τότε μπορεί να γίνει επανάληψη της μετάδοσης .

Στο αρχικό σύστημα που πρότεινε ο McEliece, οι προτεινόμενες τιμές των (n,k,t) ήταν (1024, 524, 50) αντίστοιχα. Η ασφάλεια του αλγορίθμου McEliece βασίζεται στο ότι αποκωδικοποιώντας γενικά έναν τυχαίο γραμμικό κώδικα - όπως είναι ο κώδικας που παράγεται από το δημόσιο κλειδί G' - είναι ένα πρόβλημα δύσκολο [11], επίσης, ο αρχικός (μυστικός) κώδικας που παράγεται από το G (δηλαδή το ιδιωτικό κλειδί του χρήστη) δεν μπορεί να υπολογιστεί από κάποιον επιτιθέμενο, εάν επιλεγούν προσεχτικά οι διάφορες παράμετροι του συστήματος (G, P, S). Σε κάθε περίπτωση, ο επιτιθέμενος γνωρίζει ότι το κρυπτοκείμενο είναι μία «αλλοιωμένη» κωδική λέξη ενός μυστικού κώδικα και, γενικά, από αυτήν και μόνη την πληροφορία δεν μπορεί να αποκωδικοποιήσει – άρα, δεν μπορεί να αποκρυπτογραφήσει.

5.1.1 Κρυπτανάλυση στο κρυπτοσύστημα McEliece

Ο McEliece θεωρείται ανθεκτικός έναντι επιθέσεων κρυπτανάλυσης σαν αυτών που περιγράψαμε στο κεφάλαιο 3: αυτό έγκειται στη διαδικασία εισαγωγής του λάθους που μπορεί να διορθωθεί από τον παραλήπτη που τροποποιεί το μήνυμα με τέτοιο τρόπο που δεν μπορεί να γίνει κάποια επίθεση γνωστού κειμένου ή γνωστού κρυπτοκειμένου.

Παρόλα αυτά έχουν μελετηθεί επιθέσεις που σε ειδικές περιπτώσεις και κάτω από κάποιες συγκεκριμένες συνθήκες μπορούν να αποφέρουν αποτελέσματα. Ο McEliece όμως ακόμη παραμένει - με κατάλληλη επιλογή των σχεδιαστικών παραμέτρων - ασφαλής αλγόριθμος.

Επιθέσεις εύρεσης ιδιωτικού κλειδιού

Δεν υπάρχει γνωστός αλγόριθμος ο οποίος , δοθέντος του G', να υπολογίζει την τριπλέτα P, G, S (ένας τέτοιος αλγόριθμος θα επέτρεπε την εύρεση του ιδιωτικού κλειδιού από το δημόσιο). Μία τέτοια επίθεση, γνωστή με το όνομα **δομική επίθεση** (**structural attack)**, έχει προταθεί στο [12], η οποία μπορεί να είναι αποτελεσματική μόνο αν το δημόσιο κλειδί G' έχει μία συγκεκριμένη δομή που το καθιστά κρυπτογραφικά αδύναμο – κατά συνέπεια, με κατάλληλη επιλογή των κλειδιών, αυτές οι επιθέσεις μπορούν να αποφευχθούν.

Γενικότερα, επιθέσεις αυτής της μορφής βασίζονται στην εύρεση ισοδύναμων κωδίκων, δηλαδή από τον κώδικα με πίνακα γεννήτορα τον G' να βρούμε έναν ισοδύναμο κώδικα με πίνακα γεννήτορα G ο οποίος να είναι ισοδύναμος του αρχικού – δηλαδή αν αντιμεταθέσουμε τα bits

των κωδικών λέξεων από τον έναν κώδικα να προκύψει ο άλλος. Δεν υπάρχει όμως πρακτικά η δυνατότητα έλεγχου όλων των δυνατών ισοδύναμων κωδίκων, ακόμη και από τον πιο ισχυρό υπολογιστή. Αν οι αρχικές παράμετροι είναι, n = 1024 και t = 50, η επίθεση αυτή θα χρειαστεί να ελέγξει περίπου 2^{466} κώδικες .

Επίθεση εύρεσης κωδικής λέξης χαμηλού βάρους

Υπάρχουν τεχνικές οι οποίες, δοθέντος ενός πίνακα γεννήτορα G ενός γραμμικού κώδικα, υπολογίζουν τις κωδικές λέξεις του κώδικα με το μικρότερο δυνατό βάρος [13]. Αυτές οι τεχνικές μπορούν να χρησιμοποιηθούν για την κρυπτανάλυση του McEliece, αν παρατηρήσει κανείς ότι για τον κώδικα με πίνακα γεννήτορα τον εξής (k+1) x n πίνακα

$$\begin{pmatrix} G' \\ c \end{pmatrix}$$

η κωδική λέξη με το ελάχιστο βάρος είναι εκείνο το διάνυσμα z το οποίο ικανοποιεί τη σχέση

$$c = mG' + z$$

Ως εκ τούτου, γνωρίζοντας το c μπορεί κανείς, με τον υπολογισμό του z, να ανακαλύψει το m. Και αυτή η επίθεση ωστόσο, για κατάλληλες επιλογές των παραμέτρων n,k, είναι πρακτικά ανέφικτη.

Επίθεση ανεύρεσης σφάλματος

Μια άλλη προσέγγιση είναι αυτή στην οποία βασίζεται στην υπόθεση ότι ο παραλήπτης του κρυπτογραφημένου μηνύματος, αν δεν μπορέσει να αποκρυπτογραφήσει σωστά (π.χ. μη έγκυρο κρυπτοκείμενο) αντιδρά εκπέμποντας κάποιο συγκεκριμένο μήνυμα (π.χ. «Invalid»). Αξιοποιώντας αυτές τις απαντήσεις, μπορεί ο επιτιθέμενος να ανακαλύψει το σφάλμα e που έχει εισαχθεί κατά την κρυπτογράφηση – οπότε, αν βρεθεί το e, μπορεί εν συνεχεία να βρει και το m (λόγω της σχέσης m*G'+e =c). [13]

Συγκεκριμένα, ο επιτιθέμενος παίρνει το κρυπτοκείμενο c και αλλάζει τυχαία ένα ψηφίο σε αυτό, αλλοιώνοντάς το. Προφανώς, τροποποιώντας ψηφίο του c, είτε προσθέτει επιπλέον σφάλμα είτε «διορθώνει» κάποιο από τα σφάλματα που ηθελημένα εισήγαγε ο αποστολέας του

μηνύματος με το διάνυσμα σφάλματος e. Εάν ο παραλήπτης του παραποιημένου c αποκριθεί «Invalid», σημαίνει ότι το σφάλμα εισήχθη σε νέα θέση και ο παραλήπτης δεν μπόρεσε να κάνει αποκωδικοποίηση (δηλ. αποκρυπτογράφηση) – άρα συμπεραίνουμε ότι στη θέση που εισαγάγαμε το σφάλμα, το διάνυσμα e είχε την τιμή 0: διαφορετικά, συμπεραίνουμε ότι το e στη θέση αυτή έχει την τιμή 1. Επαναλαμβάνοντας αυτή τη διαδικασία μπορούμε σταδιακά να ανακαλύψουμε ολόκληρο το e.

Παρά τις όλες προσπάθειες κρυπτανάλυσης του McEliece, ο αλγόριθμος παραμένει ακόμη ασφαλής. Τίθενται όμως θέματα υλοποίησης (λόγω των μεγεθών των κλειδιών), και αυτός είναι και ο κύριος λόγος που δεν έχει τύχει ευρείας εφαρμογής.

5.2 Κρυπτοσύστημα Niederreiter

Το κρυπτοσύστημα Niederreiter είναι μια παραλλαγή του McEliece όπου παρουσιάστηκε το 1986 από τον Harald Niederreiter. Βασίζεται στην ίδια λογική δημιουργίας ενός (n,k) κώδικα (επίσης Goppa ήταν ο κώδικας που προτάθηκε στο αρχικό σχήμα) και μετέπειτα παραγωγής άλλου κώδικα μέσω πινάκων μετατροπής.

Για το κρυπτοσύστημα Niederreiter, θεωρούμε τον πίνακα ισοτιμίας H ενός (n,k) κώδικα με ελάχιστη απόσταση d_{min}. Επίσης, κατ' αντιστοιχία με το κρυπτοσύστημα McEliece, επιλέγουμε έναν αντιστρέψιμο πίνακα S διαστάσεων (n-k) x (n-k), καθώς και έναν τυχαίο δυαδικό τετραγωνικό πίνακα P διαστάσεων n x n, όπου κάθε γραμμή αλλά και κάθε στήλη του έχει ακριβώς ένα «1». Η τριπλέτα (H, S, P) αποτελεί το ιδιωτικό κλειδί. Το δημόσιο κλειδί του κρυπτοσυστήματος είναι ένας πίνακας H' ο οποίος προκύπτει από την πράξη H'=SHP. Στο δημόσιο κλειδί επίσης ανήκει και η διορθωτική ικανότητα t του αρχικού κώδικα, όπου βέβαια $t = \lfloor (dmin - 1) / 2 \rfloor$.

Για την κρυπτογράφηση ενός μηνύματος, αυτό μετατρέπεται σε μία δυαδική λέξη m μεγέθους n και βάρους το πολύ t, και το κρυπτοκείμενο παράγεται μέσα από τον πολλαπλασιασμό $c = H'm^T$.

Για την αποκρυπτογράφηση, ο παραλήπτης του μηνύματος κάνει τα εξής:

α) Υπολογίζει τον αντίστροφο πίνακα S^{-1} του S, και το πολλαπλασιάζει από αριστερά με το κρυπτοκείμενο c. Το διάνυσμα που θα προκύψει ισούται με:

$$S^{-1}c = HPm^T.$$

β) Από το HPm^T. ο παραλήπτης, που γνωρίζει τον αρχικό μυστικό κώδικα με πίνακα ισοτιμίας τον H, μπορεί να υπολογίσει, με τεχνικές αποκωδικοποίησης, το διάνυσμα Pm^T (το οποίο ουσιαστικά μπορεί να το δει κανείς ως ένα διάνυσμα που περιγράφει τις θέσεις των λαθών που έχουν λάβει χώρα σε μία μετάδοση, και επειδή το πλήθος αυτών των λαθών είναι εντός της διορθωτικής ικανότητας του κώδικα, οι θέσεις τους μπορούν να υπολογιστούν).

γ) Ξέροντας πλέον το διάνυσμα Pm^T , ο παραλήπτης μπορεί να εξάγει το αρχικό μήνυμα m, επιτελώντας τον πολλαπλασιασμό

$$m^T = P^{-1}Pm^T$$

αφού βέβαια πρώτα έχει υπολογίσει τον αντίστροφο πίνακα P^{-1}.

Αξίζει να σημειωθεί ότι το κρυπτοσύστημα Niederreiter έχει, εκτός από την ικανότητα της κρυπτογράφησης, και την ικανότητα της υπογραφής ενός μηνύματος. Για να επιτευχθεί αυτό, το μήνυμα διέρχεται από μία κρυπτογραφική συνάρτηση κατακερματισμού (hash), η έξοδος αυτής αποτελεί την είσοδο στον αλγόριθμο Niederreiter και το αποτέλεσμα επισυνάπτεται στο μήνυμα ως υπογραφή. Ο παραλήπτης επαναλαμβάνει την συνάρτηση κατακερματισμού, παράλληλα κρυπτογραφεί τη λαμβανόμενη υπογραφή με το δημόσιο κλειδί του αποστολέα και ελέγχει τα δύο αυτά αποτελέσματα: αν συμπίπτουν, τότε το μήνυμα δεν έχει αλλοιωθεί και επιβεβαιώνεται η ταυτότητα του αποστολέα. Στην διαδικασία αυτή προσθέτονται κάποιες επαναλήψεις κατά την κωδικοποίηση λόγω των λαθών μετάδοσης - που όμως δεν θα μελετήσουμε εδώ.

5.2.1 Κρυπτανάλυση στο κρυπτοσύστημα Niederreiter

Οι επιθέσεις που μπορούν να εφαρμοστούν σο κρυπτοσύστημα Niederreiter είναι σε γενικές γραμμές αντίστοιχης λογικής με αυτές για το κρυπτοσύστημα McEliece. Μάλιστα, το 1994 αποδείχτηκε ότι τα δύο αυτά κρυπτοσυστήματα, εφόσον σχεδιαστούν με εφάμιλλες τιμές στις παραμέτρους τους, είναι ισοδύναμα ως προς την ασφάλεια που παρέχουν [14].

5.3 Σύγκριση RSA , McEliece , Niederreiter

	McEliece [1024,524,101] binary code	Niederreiter [1024,524,101] binary code	RSA 1024-bit modulus public exponent = 17
public-key size	67,072 bytes	32,750 bytes	256 bytes
number of information bits transmitted per encryption	512	276	1024
transmission rate	51.17 %	56.81 %	100 %
number of binary operations performed by the encryption per information bit	514	50	2,402
number of binary operations performed by the decryption per information bit	5,140	7,863	738,112

Σχήμα 5.2 συγκριτικός πίνακας αλγορίθμων δημοσίου κλειδιού

Στο σχήμα 5.2 [15] βλέπουμε ένα συγκριτικό πίνακα αλγορίθμων δημοσίου κλειδιού. Βλέπουμε ότι ο McEliece υστερεί ως προς το ότι απαιτεί ένα τεράστιο κλειδί. Στο συγκριτικό πίνακα παράλληλα βλέπουμε τις αναγκαίες πράξεις για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος μεγέθους 1 bit. Εδώ βλέπουμε την υψηλή ταχύτητα του McEliece συγκριτικά με το τον RSA που περιγράψαμε πριν και βλέπουμε πόσο πιο γρήγορος είναι ο McEliece και πόσο λιγότερο απαιτητικός είναι σε υπολογιστική ανάγκη. Ο Niederreiter είναι βελτιωμένος συγκριτικά με τον McEliece σε σχέση με το μέγεθος του κλειδιού . Βλέπουμε ότι το δημόσιο κλειδί του McEliece είναι 67072 bytes ενώ του Niederreiter 32750 byte: από την άλλη πλευρά βλέπουμε την αύξηση στις αναγκαίες πράξεις τόσο κατά την κωδικοποίηση αλλά και κατά την αποκωδικοποίηση.

Σημειώνεται ότι τόσο ο αλγόριθμος McEliece όσο και αυτός του Niederreiter έχει αποδεικτεί ότι είναι ασφαλείς απέναντι και σε επιθέσεις Κβαντικής δειγματοληψίας Fourier (Quantum Fourier Sampling), οι οποίες δεν μπορούν να γίνουν στο παρόν στάδιο με την υπολογιστική δύναμη που διαθέτουν τα υπολογιστικά συστήματα – κανείς όμως δεν γνωρίζει για το προσεχές μέλλον. Ο RSA όμως έχει αποδειχθεί ότι είναι μη ασφαλής σε τέτοιες επιθέσεις - η δυνατότητα

πραγματοποίησης τέτοιων επιθέσεων θα σήμαινε το τέλος του RSA, όπως και των άλλων αλγόριθμων δημοσίου κλειδιού που βασίζονται στην ίδια λογική.

Επίλογος

Στη συγκεκριμένη εργασία μελετήσαμε θέματα κωδικοποίησης καναλιού και κρυπτογράφησης, από τη σκοπιά της ενιαίας θεώρησής τους. Τα αποτελέσματα που επιφέρει μία τέτοια ενιαία θεώρηση είναι τα εξής: α) Υλοποιώντας τη διαδικασία της κρυπτογράφησης στο φυσικό επίπεδο, μπορούμε να προσδώσουμε πρόσθετα χαρακτηριστικά ασφαλείας σε ένα σύστημα ή και να βελτιώσουμε τη συνολική του απόδοση, αφού ενδεχομένως – αναλόγως και την εφαρμογή όπου εργαζόμαστε - να μη χρειάζεται πλέον η υλοποίηση κρυπτογραφικού αλγορίθμου σε υψηλότερο επίπεδο, η οποία πάντα επιβαρύνει τη συνολική απόδοση (βλ. Κεφάλαιο 4), β) Αξιοποιώντας τη θεωρία κωδίκων, μπορεί κανείς να κατασκευάσει ισχυρούς κρυπτογραφικούς αλγορίθμους (βλ. Κεφάλαιο 5). Το εν λόγω επιστημονικό πεδίο έχει ήδη διανύσει δεκαετίες ζωής, ωστόσο παραμένει - όπως είδαμε - εξαιρετικά ενεργό.

Υπάρχουν διάφορες άλλες προσεγγίσεις οι οποίες αποσκοπούν επίσης στον εποικοδομητικό συνδυασμό κωδικοποίησης και κρυπτογράφησης. Μία τέτοια προσέγγιση υπάρχει [16] όπου προτείνεται ένα σχήμα που επιτυγχάνει ταυτόχρονα διόρθωση σφαλμάτων και αυθεντικοποίηση μηνύματος (message authentication), ενώ συστήματα που επιτελούν ταυτόχρονα κρυπτογράφηση και κωδικοποίηση έχουν επίσης προταθεί στα [17], [18]. Επίσης, στο [19] προτείνεται η αντικατάσταση δομικών συστατικών κρυπτογραφικών αλγορίθμων (όπως είναι τα S-boxes στους κρυπταλγόριθμους τμήματος) από άλλες αντίστοιχες μονάδες που έχουν επιθυμητά χαρακτηριστικά ως προς τη διόρθωση σφαλμάτων (τέτοιο χαρακτηριστικό είναι η υψηλή διάχυση). Τέλος, στο [20]προτείνεται η χρήση μίας γεννήτριας ψευδοτυχαίας κλειδοροής (ακολουθίας από bit), σε κατάλληλο συνδυασμό με έναν κώδικα διόρθωσης σφαλμάτων, προκειμένου να μπορεί μόνο ο νόμιμος παραλήπτης να αποκωδικοποιεί τα σφάλματα που εισάγει η κλειδοροή (η οποία έχει το ρόλο του «θορύβου» του καναλιού) και όχι κάποιος τρίτος. Παρόλα αυτά, όλες οι παραπάνω τεχνικές εμφανίζουν προβλήματα ως προς την υλοποίησης ενώ σε πολλές περιπτώσεις η ασφάλειά τους δεν θεμελιώνεται μαθηματικά.

Από τη μελέτη όλων των προσεγγίσεων, και λαμβάνοντας υπόψη ότι αυξάνονται διαρκώς οι εφαρμογές που απαιτούν ταυτόχρονα υψηλή ταχύτητα, χαμηλή κατανάλωση ενέργειας αλλά και ασφάλεια (π..χ. δίκτυα αισθητήρων, RFID κτλ.), συμπεραίνουμε ότι η κρυπτογράφηση στο

φυσικό επίπεδο είναι ένας τομέας όπου χρήζει περαιτέρω έρευνας και εμβάθυνσης. Αυτό δεν σημαίνει ότι η κρυπτογράφηση στα υψηλότερα επίπεδα θα καταστεί ποτέ παρωχημένη – τουναντίον μπορούν να δρουν από κοινού, ενισχύοντας ακόμα περισσότερο τη συνολική ασφάλεια. Περαιτέρω, τα πλεονεκτήματα που παρέχουν τα κρυπτοσυστήματα McEliece και Niederreiter είναι τέτοια ώστε καθιστούν σαφές το ότι πρέπει να συνεχιστούν οι ερευνητικές προσπάθειες για περαιτέρω βελτίωσή τους – όσον αφορά τόσο θέματα απόδοσης όσο και θέματα ασφάλειας. Ακριβώς για αυτό το λόγο εξάλλου προτείνονται διαρκώς παραλλαγές αυτών των κρυπτοσυστημάτων (π.χ. χρήση συγκεραστικού κώδικα αντί για κώδικα Goppa), και μελετάται συνεχώς η ασφάλεια αυτών – όπως αποτυπώνεται και από τις πρόσφατες επιστημονικές δημοσιεύσεις του χώρου, π.χ. [21]

Βιβλιογραφία

BIBLIOGRAPHY

1. http://www.medientheorien.hu-berlin.de/vlz/Zufall.pdf.

2. Ευστάθιος, Βίδρα Μαριάνα Παπαδόπουλος. Τεχνικές Κωδικοποίησης,Κώδικες Hamming.

3. Stallings, William. *Ασύρματες Επικοινωνίεσ Και Δίκτυα.* s.l. : Τζιόλα, 2007. ISBN 978-960-418-123-0.

4.http://www.eyliko.gr/htmls/diktya/senario4/theory/files/DiktyMetds1Kef2.pdf.

5. S.Lin.and.D.J.Costello. *Error.Control.Coding.Fundamentals.and.Applications.* s.l. : Prentice.Hall, 1983.

6. John G. Proakis, Masoud Salehi. *Συστήματα Τηλεπικοινωνιών.* Αθήνα : εκδόσεις Εθνικού & Καποδιστριακού Πανεπιστημίου Αθηνών, 2002.

7. *Physical-layer encryption with stream ciphers.* Barros, A. Z´ uquete and J. s.l. : International Symposium on Information Theory, 2008.

8. February., R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. 1978.

9. *Physical layer security via secret trellis pruning", IEEE Int. Symp. on Personal Indoor and Mobile Communications.* A. Katsiotis, N. Kolokotronis and N. Kalouptsidis. 2013.

10. *Semantically Secure McEliece Public-Key Cryptosystems - Conversions for McEliece PKC. Practice and Theory in Public Key Cryptography.* K. Kobara, H. Imai. s.l. : Springer, 2001.

11.http://www.math.ucdenver.edu/~wcherowi/courses/m5410/ctcmcel.html.

12. *On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory IT-24(3).* Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A. 1978.

13. P. Loidreau and N. Sendrier. “Some weak keys in McEliece public-key cryptosystem”. In Proc. of IEEE International Symposium on Information Theory, ISIT ’98, page 382, 1998.

14. A. Canteaut and N. Sendrier. “Cryptoanalysis of the Original McEliece Cryptosystem”, In Proc. of ASIACRYPT ’98, pages 187–199, 1998.

15. Y.X. Li, R.H. Deng, and X. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems", IEEE Transactions on Information Theory, 1994, pp.271-273.

16. *Cryptanalysis of the Original McEliece.* Nicolas, Canteaut and Sendrier. 1998.

17. Bossert, Mahr, Heilig, “Concatenation of error correcting codes and cryptography”, in Proc. Sixth joint Swedish-Russian Int. workshop on Information theory, 1993.

18. A. Payandeh, M. Ahmadian and M. Reza Aref, “Adaptive secure channel coding based on punctured turbo codes”, IEE Proc.-Commun., 2006.

19. O. Adamo and M. R. Varanasi, “Joint Scheme for Physical Layer Error Correction and Security”, ISRN Communications and Networking, vol. 2011, Article ID 502987, 9 pages, 2011. doi:10.5402/2011/502987.

20. C. N. Mathur, K. Narayan, and K. P. Subbalakshmi, “On the design of error correcting ciphers”, EURASIP Journal on Wireless Communications and Networking, 2006.

21. O. Kara and I. Erguler, “A New Approach to Keystream Based Cryptosystems”, SASC 2008.

22. G. Landais and J Tillich, “An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes”, Post-Quantum Cryptography, Springer, vol. 7932, pp. 102-117, 2013.

23.http://xanthippi.ceid.upatras.gr/courses/advcomm/Presentations/Block_Coding8.pdf. [Online]

Παράρτημα Α
Ορολογίες

- Βάρος Hamming ή απλά βάρος, wt(x), μιας λέξης x μήκους n ψηφίων ονομάζεται το πλήθος των ψηφίων της λέξης, τα οποία είναι ίσα με το ≪1≫. Το βάρος παίρνει τιμές από 0 έως n.
- Απόσταση Hamming ή απλά απόσταση, d(x, y), μεταξύ δύο λέξεων x και y του ιδίου μήκους n ονομάζεται το πλήθος των θέσεων, στις οποίες οι δύο λέξεις εμφανίζουν ασυμφωνία του δυαδικού ψηφίου. Η απόσταση παίρνει τιμές από 0 έως n.
- Απλό κείμενο (plaintext) – το μη κρυπτογραφημένο μήνυμα
- Κρυπτογραφημένο Κείμενο (ciphertext) – το κρυπτογραφημένο μήνυμα
- Αλγόριθμος κρυπτογράφησης (cipher) - Μετατρέπει το plaintext σε ciphertext
- Κλειδί (key) – πληροφορία που χρησιμοποιείται από τον αλγόριθμο
- κρυπτογράφησης και είναι γνωστή μόνο στο μεταδότη και τον αποδεκτή
- Κρυπτογράφηση (encryption, enciphering) – η μετατροπή του plaintext σε ciphertext
- Αποκρυπτογράφηση (decryprion, deciphering) – η μετατροπή του ciphertext σε plaintext
- Κρυπτογραφία (cryptography) – η μελέτη των μεθόδων κρυπτογράφησης και των αρχών της κρυπτογραφίας και των αρχών που τις διέπουν
- Κρυπταναλυση (cryptanalysis) – μελέτη των αρχών και των μεθόδων που αποσκοπούν στην αποκρυπτογράφηση χωρίς να είναι γνωστό το κλειδί.

- Κρυπτολογια (cryptology) – το επιστημονικό πεδίο που περιλαμβάνει την κρυπτογραφία και την κρυπταναλυση