Κεφάλαιο 6. Εισαγωγή στην κρυπτολογία

Σύνοψη
Το κεφάλαιο αποτελεί εισαγωγή στη γνωστική περιοχή της κρυπτολογίας, ως μιας γενικότερης περιοχής που περιλαμβάνει την κρυπτογραφία και την στεγανογραφία. Θα παρατεθούν και θα εξεταστούν συνοπτικά οι δύο αυτές βασικές υποπεριοχές και θα γίνει αναφορά σε έννοιες της θεωρίας πληροφορίας που θα μας χρειαστούν στη συνέχεια. Ο αναγνώστης θα έχει την ευκαιρία να κατανοήσει βασικές έννοιες τη εφαρμοσμένης κρυπτογραφίας, καθώς και να κάνει τα πρώτα βήματα στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης, καθώς και προσπάθειες κρυπτανάλυσης, χρησιμοποιώντας απλούς κλασσικούς αλγόριθμους με τη βοήθεια του εκπαιδευτικού εργαλείου Cryptool.

Προαπαιτούμενη γνώση
Για την κατανόηση των εννοιών που περιλαμβάνονται στο κεφάλαιο δεν απαιτείται κάποια εξειδικευμένη προηγούμενη γνώση.

6.1 Εισαγωγή

Ο όρος κρυπτολογία (cryptology) είναι ετυμολογικά μια σύνθετη λέξη που αποτελείται από τα λήμματα «κρυπτός» και «λόγος» και δηλώνει τη μυστικότητα του λόγου που μπορεί να είναι προφορικός ή με τη μορφή ενός γραπτού κειμένου. Η μυστικότητα των περιεχομένων αφορά την προστασία της εμπιστευτικότητας (confidentiality) της πληροφορίας που περιέχεται σε αυτά. Σήμερα, με τον όρο κρυπτολογία ορίζεται η επιστημονική περιοχή που περιλαμβάνει την **κρυπτογραφία** (cryptography) και την **κρυπτανάλυση** (cryptanalysis).

Η κρυπτογραφία ασχολείται με την μετατροπή των δεδομένων με τέτοιο τρόπο ώστε να καθίσταται αδύνατη η ανάγνωση και ερμηνεία του μεταδιδόμενου κρυπτογραφημένου μηνύματος. Σχετική με την κρυπτογραφία είναι η περιοχή της **στεγανογραφίας (steganography)**. Η λέξη προέρχεται από τις λέξεις «στεγανός» και «γραφή» και δηλώνει την προσπάθεια απόκρυψης της ύπαρξης ενός μηνύματος που είναι κρυμμένο μέσα στα μηνύματα μιας φανερής (φαινομενικά απροστάτευτης) επικοινωνίας μεταξύ δυο οντοτήτων. Η κύρια διαφορά με την κρυπτογραφία είναι ότι η στεγανογραφία στοχεύει στην απόκρυψη της ύπαρξης του κρίσιμου μηνύματος, το οποίο δεν είναι απαραίτητο να είναι κρυπτογραφημένο.

Η πρώτη εμφάνιση τεχνικών κρυπτογραφίας συναντάται περίπου 4.000 χρόνια πριν, στα πρώιμα στάδια του Αιγυπτιακού πολιτισμού, όταν οι συγγραφείς της εποχής περιέγραφαν τη ζωή των βασιλιάδων με ασυνήθιστες ιερογλυφικές αναπαραστάσεις. Ως αποτέλεσμα αυτής της ενέργειας, η ανάγνωση των ιερογλυφικών ήταν δυνατή μόνο από όσους γνώριζαν τον μυστικό κώδικα που είχε χρησιμοποιηθεί κατά τη συγγραφή τους, ενώ για όλους τους άλλους οι παραστάσεις ήταν ακατανόητες. Η διεργασία μετασχηματισμού ενός **αρχικού κειμένου** (plaintext) σε μια ακατάληπτη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου ονομάζεται **κρυπτογράφηση.**

Ένας **κρυπτογραφικός αλγόριθμος** (Cipher/Encryption algorithm) περιγράφει τη μέθοδο μετασχηματισμού μηνυμάτων σε μια μορφή τέτοια που να μην επιτρέπεται σε μη εξουσιοδοτημένα μέρη η αποκάλυψη του περιεχομένου τους. Οι αρχαίοι Σπαρτιάτες χρησιμοποίησαν την κρυπτογραφία και εκμεταλλεύτηκαν τις τεχνικές της για στρατιωτικούς σκοπούς. Αναφέρεται χαρακτηριστικά η χρήση της «σκυτάλης», η οποία ήταν μια ξύλινη ράβδος πάνω στην οποία περιτυλίγονταν ένας πάπυρος σε μορφή ταινίας. Το μήνυμα αποτυπωνόταν στον τυλιγμένο γύρω από την σκυτάλη πάπυρο, κατά μήκος της ράβδου, οπότε όταν ο πάπυρος ξετυλίγονταν, η ανάγνωση του κειμένου κατά μήκος του πάπυρου κατέληγε να μην αποδίδει ένα καταληπτό νόημα. Το αρχικό μήνυμα ήταν δυνατό να διαβαστεί μόνο από κάποιον ο οποίος διέθετε σκυτάλη ίδιας διαμέτρου, ώστε να προσαρμόσει πάνω της εκ νέου τον πάπυρο και να αποκρυπτογραφήσει το μήνυμα. Σε αυτή την περίπτωση, η διάμετρος της σκυτάλης αποτελεί το **κλειδί** (key) κρυπτογράφησης, το οποίο μαζί με τον κρυπτογραφικό αλγόριθμο αποτελεί το μέσο για το μετασχηματισμό του αρχικού μηνύματος σε **κρυπτοκείμενο** (cipher text).

Στην Εικόνα 6.1 (Πηγή: https://commons.wikimedia.org/wiki/File:Skytale.png) παρουσιάζεται η λειτουργία της Σπαρτιατικής σκυτάλης.

Εικόνα 6.1 *Λειτουργία Σπαρτιατικής σκυτάλης.*

Η διαδικασία που εκτελείται από μια εξουσιοδοτημένη οντότητα για την ανάκτηση του αρχικού κειμένου από το κρυπτοκείμενο, ονομάζεται **αποκρυπτογράφηση** (Decryption/Decipherment).

6.2 Κρυπτογραφία

Στόχος της κρυπτογραφίας είναι να παρέχει υπηρεσίες ασφάλειας, όπως:

- Εμπιστευτικότητα (confidentiality).
- Ακεραιότητα (integrity).
- Αυθεντικοποίηση (authentication).
- Αδυναμία αποποίησης (non-repudiation).

Επιπλέον, είναι επιθυμητές οι παρακάτω ιδιότητες για ένα κρυπτοσύστημα και τα συστατικά μέρη του:

- Πρέπει να χρησιμοποιούνται αποδοτικοί αλγόριθμοι για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης.

- Το σύστημα πρέπει να είναι εύχρηστο και να μην προκαλεί σύγχυση στον χρήστη.

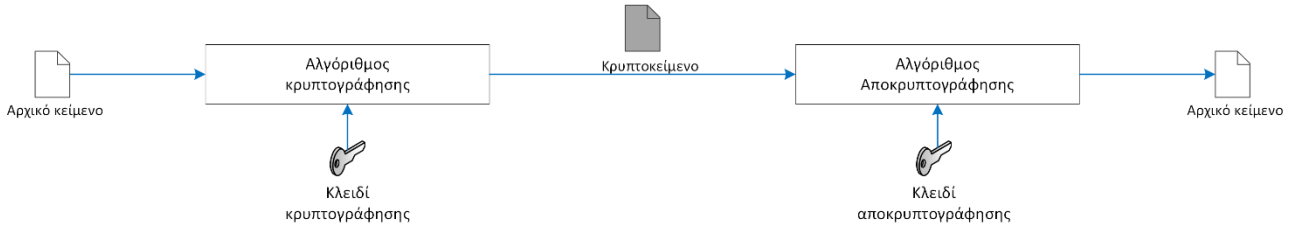
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών και όχι των αλγορίθμων που χρησιμοποιούνται.

Η τελευταία ιδιότητα, γνωστή ως αρχή του Kerckhoff, εκφράστηκε το 1883 από τον Auguste Kerckhoff (1853-1903) και ορίζει πως σε αντίθεση με την αντίληψη πως σε ένα **κρυπτογραφικό σύστημα** οι λεπτομέρειες σχεδιασμού και υλοποίησης πρέπει να είναι κρυφές (security through obscurity), αυτό θα πρέπει να σχεδιάζεται έτσι ώστε να είναι ασφαλές όταν ο «αντίπαλος» γνωρίζει κάθε λεπτομέρεια, εκτός από τις παραμέτρους που σχεδιάζονται να είναι μυστικές, όπως τα κλειδιά κρυπτογράφησης / αποκρυπτογράφησης.

6.2.1 Κρυπτογραφικό σύστημα

Σε ένα κρυπτογραφικό σύστημα, τα δεδομένα που περιέχονται σε ένα μήνυμα με τη μορφή ενός αρχικού κειμένου (plaintext), κρυπτογραφούνται και το παραγόμενο μήνυμα αποτελεί το κρυπτοκείμενο (ciphertext).

Στη συνέχεια, το κρυπτοκείμενο αποστέλλεται στον παραλήπτη, όπου αποκρυπτογραφείται για να αναπαραχθεί το αρχικό κείμενο. Η κρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης που χρησιμοποιεί ένα κλειδί κρυπτογράφησης. Ανάλογα, κατά την αποκρυπτογράφηση χρησιμοποιείται ένας αλγόριθμος αποκρυπτογράφησης και είτε το ίδιο είτε ένα άλλο κλειδί αποκρυπτογράφησης. Ένα τυπικό κρυπτοσύστημα απεικονίζεται στο σχήμα της Εικόνας 6.2:



Εικόνα 6.2 *Τυπικό κρυπτοσύστημα.*

Ένα κρυπτογραφικό σύστημα θεωρείται ασφαλές όταν ικανοποιούνται τα ακόλουθα κριτήρια:

- Το **κόστος** της παραβίασης του κρυπτομηνύματος, δηλαδή της ανάκτησης του κλειδιού αποκρυπτογράφησης, υπερβαίνει την αξία των πληροφοριών που τελικά λαμβάνονται ως αποτέλεσμα της κρυπτανάλυσης.

- Ο **χρόνος** που απαιτείται για τη διαδικασία της κρυπτανάλυσης υπερβαίνει την ωφέλιμη διάρκεια ζωής των λαμβανομένων πληροφοριών.

6.2.2 Κρυπτανάλυση

Στόχος της κρυπτανάλυσης είναι η εύρεση του κλειδιού αποκρυπτογράφησης που χρησιμοποιήθηκε για την ασφαλή ανταλλαγή μηνυμάτων με τη χρήση ενός κρυπτοσυστήματος. Ο ρόλος του **κρυπταναλυτή**, επομένως, έρχεται σε πλήρη αντίθεση με το ρόλο του **κρυπτογράφου**, καθώς ο πρώτος προσπαθεί να παραβιάσει ένα κρυπτοσύστημα το οποίο χρησιμοποιεί ο δεύτερος.

Για την εύρεση του κλειδιού αποκρυπτογράφησης, ο κρυπταναλυτής μπορεί να χρησιμοποιήσει τεχνικές όπως:

- **Επίθεση Ωμής Βίας (Brute-Force Attack)**: Ο επιτιθέμενος, μέσω εξαντλητικής αναζήτησης, προσπαθεί να αποκαλύψει το κλειδί αποκρυπτογράφησης, δοκιμάζοντας όλους τους πιθανούς συνδυασμούς στοιχείων του αλφαβήτου που χρησιμοποιήθηκε κατά τον ορισμό του. Ξεκινώντας από το ελάχιστο δυνατό μήκος κλειδιού (εφόσον το μήκος κλειδιού μπορεί να είναι μεταβλητό), δοκιμάζει να αποκρυπτογραφήσει το κρυπτοκείμενο με όλες τις πιθανές τιμές του κλειδιού. Μόλις τις εξαντλήσει, αυξάνει κατά ένα το μήκος του δοκιμαζόμενου κλειδιού και συνεχίζει με τον ίδιο τρόπο. Η υπολογιστική ισχύς των σημερινών υπολογιστών, παρέχει σημαντικά πλεονεκτήματα τα οποία μπορούν να πολλαπλασιαστούν με διατάξεις υπολογιστών που εκτελούν μια τέτοια επίθεση παράλληλα (π.χ. με κατανομή του πεδίου ορισμού του κλειδιού). Για αυτό, λαμβάνοντας υπόψη την τρέχουσα τεχνολογική στάθμη και εξέλιξη, επιβάλλεται η χρήση κλειδιών μεγάλου μήκους για την ενίσχυση της ανθεκτικότητας των κρυπτογραφικών αλγορίθμων (αυτό κυρίως αφορά τους λεγόμενους συμμετρικούς αλγορίθμους).

- **Επίθεση Στατιστικής Ανάλυσης (Statistical Analysis Attack)**: Ο κρυπταναλυτής προσπαθεί να εκμεταλλευτεί, προς όφελός του, εγγενή χαρακτηριστικά της γλώσσας στην οποία έχει γραφτεί το αρχικό κείμενο. Για παράδειγμα, έστω ότι το γράμμα Ε είναι το πλέον χρησιμοποιούμενο στην Αγγλική γλώσσα. Ξεκινώντας από αυτή τη γνώση, ο κρυπταναλυτής αναλύει στατιστικά το κρυπτοκείμενο και προσπαθεί να αντιστοιχίσει το συχνότερα

εμφανιζόμενο γράμμα με το γράμμα Ε. Συνεχίζει με παρόμοιο τρόπο, χρησιμοποιώντας παρόμοια στατιστικά χαρακτηριστικά, π.χ. για άλλα γράμματα ή συνδυασμούς γραμμάτων (όπως δυάδες, τριάδες κ.λπ.), ώστε σε συνδυασμό με άλλες τεχνικές, όπως η αυτοσυσχέτιση (autocorrelation), να οδηγηθεί σε χρήσιμες πληροφορίες και συμπεράσματα για τα χαρακτηριστικά του κλειδιού (π.χ. μέγεθος) και τελικά στην εύρεση της τιμής του. Μια ακόμη τεχνική που μπορεί να τον βοηθήσει, στο πλαίσιο της γενικότερης ανάλυσης που πραγματοποιεί ο κρυπταναλυτής, είναι η αναζήτηση και ο εντοπισμός επαναλαμβανόμενων μοτίβων (pattern) που έχουν σχέση, για παράδειγμα, με τυπικές εκφράσεις που χρησιμοποιούνται στη σύνταξη επαγγελματικών επιστολών (π.χ. τυπική έκφραση του αρχικού χαιρετισμού).

Μπορούμε να διακρίνουμε τις επιθέσεις κρυπτανάλυσης, με βάση την πληροφορία που διαθέτει ο κρυπταναλυτής, ως εξής:

- **Μόνο κρυπτοκειμένου (ciphertext only)**: Ο επιτιθέμενος γνωρίζει μόνο τον αλγόριθμο κρυπτογράφησης και το σύνολο ή μέρος του κρυπτοκειμένου. Αυτό το είδος επίθεσης είναι και το πιο συνηθισμένο, καθώς ο επιτιθέμενος σχετικά εύκολα μπορεί να υποκλέψει το κρυπτοκείμενο, παρακολουθώντας το κανάλι επικοινωνίας μεταξύ των δύο οντοτήτων που επικοινωνούν με χρήση κρυπτογραφίας

- **Γνωστού αρχικού κειμένου (known plaintext)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο κρυπτογράφησης και καταφέρνει επιπροσθέτως να αποκτήσει ένα ή περισσότερα ζεύγη από το σύνολο ή μέρος του αρχικού κειμένου και κρυπτοκειμένου, που έχουν κρυπτογραφηθεί με το κλειδί κρυπτογράφησης.

- **Επιλεγμένου αρχικού κειμένου (chosen plaintext)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο κρυπτογράφησης και καταφέρνει να εισάγει ένα δικό του αρχικό κείμενο, το οποίο αφού κρυπτογραφηθεί με το κλειδί κρυπτογράφησης, θα πάρει τη μορφή ενός κρυπτοκειμένου το οποίο, στη συνέχεια, θα επιδιώξει π.χ. να υποκλέψει. Με κατάλληλη διαμόρφωση του αρχικού κειμένου, ο κρυπταναλυτής μπορεί να καταφέρει να οδηγηθεί σε συμπεράσματα σχετικά με την τιμή του κλειδιού.

- **Επιλεγμένου κρυπτοκειμένου (chosen ciphertext)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο αποκρυπτογράφησης και καταφέρνει να εισάγει επιλεγμένα κρυπτοκείμενα τα οποία αφού αποκρυπτογραφηθούν παράγουν αρχικά κείμενα που μπορεί να τον οδηγήσουν σε συμπεράσματα σχετικά με την τιμή του κλειδιού.

- **Επιλεγμένου κειμένου (chosen text)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο κρυπτογράφησης και καταφέρνει να εισάγει δικά του αρχικά κείμενα τα οποία κρυπτογραφούνται, ενώ καταφέρνει να εισάγει και επιλεγμένα κρυπτοκείμενα τα οποία αποκρυπτογραφούνται με γνωστό αλγόριθμο αποκρυπτογράφησης για να παράγουν αρχικά κείμενα τα οποία μαζί με τα κρυπτοκείμενα των δικών του αρχικών κειμένων μπορεί να τον οδηγήσουν σε συμπεράσματα σχετικά με την τιμή του κλειδιού.

6.2.3 Κλειδί

Σε ένα κρυπτογραφικό σύστημα, η ανάκτηση του αρχικού κειμένου, το οποίο πρέπει να παραμείνει μυστικό από τρίτους, προϋποθέτει την ανάκτηση του κλειδιού αποκρυπτογράφησης. Όπως αναφέρθηκε προηγουμένως, μια μη εξουσιοδοτημένη οντότητα μπορεί να έχει τη δυνατότητα π.χ. να εκτελέσει μια εξαντλητική αναζήτηση έτσι ώστε:

- Στην περίπτωση που έχει αποκτήσει δεδομένα που αποτελούν μέρος του αρχικού κειμένου και του κρυπτοκειμένου να δοκιμάσει όλα τα πιθανά κλειδιά μέχρι να βρει το σωστό το οποίο, στη συνέχεια, θα χρησιμοποιήσει για την αποκρυπτογράφηση κάθε επόμενου κρυπτοκειμένου.

- Στην περίπτωση που έχει αποκτήσει μόνο δεδομένα που αποτελούν μέρος του κρυπτοκειμένου, να δοκιμάσει όλα τα πιθανά κλειδιά μέχρι να βρει ένα με το οποίο το παραγόμενο αποτέλεσμα της αποκρυπτογράφησης να έχει λογική σημασία. Εικάζοντας πως αυτό είναι το σωστό κλειδί, στη συνέχεια, θα το χρησιμοποιήσει για την αποκρυπτογράφηση των υπόλοιπων τμημάτων κρυπτοκειμένου.

Ένα κλειδί αποτελείται από μια σειρά bit. Για την αποφυγή του εντοπισμού του κλειδιού μέσω της εξαντλητικής αναζήτησης (brute force attack), το πλήθος των πιθανών τιμών (συνδυασμών από bit) που μπορεί να πάρει ένα κλειδί, πρέπει να είναι τεράστιο προκειμένου να αντιμετωπίζονται οι επιθέσεις αυτές στη βάση των κριτηρίων κόστους και χρόνου που αναφέρθηκαν προηγουμένως. Έτσι, για μήκος κλειδιού της τάξης των 64bit, οι πιθανές τιμές κλειδιού είναι 2^{56}, δηλαδή μπορούν να παραχθούν περισσότερα από $7x10^{16}$ διαφορετικά κλειδιά.

Αν θεωρήσουμε πως ένας επεξεργαστής έχει τη δυνατότητα δοκιμής 60 εκατομμυρίων κλειδιών το δευτερόλεπτο, τότε ένα κλειδί μήκους 56 bit θα ανακτηθεί σε περίπου από 1.200.000.000 δευτερόλεπτα. Όμως, μοιράζοντας το χώρο αναζήτησης σε περισσότερους επεξεργαστές (π.χ. 1536 του Deep Crack που χρησιμοποιήθηκε για παρόμοιο σκοπό το 1998) ο χρόνος μειώνεται σε 781.875 δευτερόλεπτα, δηλαδή 217 ώρες, άρα μόλις 9 μέρες. Η αύξηση του μήκους του κλειδιού στα 64bit, αυξάνει το χώρο αναζήτησης σε περισσότερα από 10^{19} κλειδιά και τον απαιτούμενο χρόνο στις 2317 μέρες (περίπου 6 έτη)!

Στον πίνακα 6.1 μπορείτε να δείτε ενδεικτικά την αύξηση του χρόνου αναζήτησης σε σχέση με το μήκος του κλειδιού και τον αριθμό n των επεξεργαστικών μονάδων.

Μήκος κλειδιού	**Χώρος αναζήτησης**	**Απαιτούμενος χρόνος με $6x10^7$ κλειδιά ανά sec**
56	$7,2x10^{16}$	38 έτη / n
64	$1,8x10^{19}$	9749 έτη / n
128	$3,4x10^{38}$	$1,8x10^{23}$ έτη / n
256	$1,16x10^{77}$	$6,1x10^{61}$ έτη / n
512	$1,36x10^{154}$	$7,1x10^{138}$ έτη / n

Πίνακας 6.1 *Χρόνοι εξαντλητικής αναζήτησης κλειδιών.*

6.2.4 Αλγόριθμοι κρυπτογράφησης

Οι κρυπτογραφικοί αλγόριθμοι διακρίνονται ως προς:

- το είδος των κλειδιών που χρησιμοποιούν και
- τον τρόπο επεξεργασίας του αρχικού και του κρυπτογραφημένου κειμένου.

6.2.4.1 Είδος κλειδιών

Κατηγοριοποιώντας τους αλγορίθμους κρυπτογράφησης ως προς το είδος των κλειδιών, διακρίνουμε τους συμμετρικούς (symmetric) αλγορίθμους και τους ασύμμετρους (asymmetric) ή δημοσίου κλειδιού (public key).

Στους συμμετρικούς κρυπτογραφικούς αλγορίθμους, η κρυπτογράφηση και η αποκρυπτογράφηση γίνεται χρησιμοποιώντας (συμμετρικά) το ίδιο κλειδί, αλλά με αντίστροφες λειτουργίες. Η οντότητα Α κρυπτογραφεί το αρχικό κείμενο με το κλειδί Κ και αποστέλλει το κρυπτοκείμενο, ενώ η οντότητα Β παραλαμβάνει το κρυπτοκείμενο και χρησιμοποιεί το ίδιο κλειδί Κ για να το αποκρυπτογραφήσει και να ανακτήσει το αρχικό κείμενο (Εικόνα 6.3). Η συμμετρική κρυπτογραφία ονομάζεται και κρυπτογραφία μυστικού κλειδιού.

Εικόνα 6.3 *Συμμετρική κρυπτογραφία.*

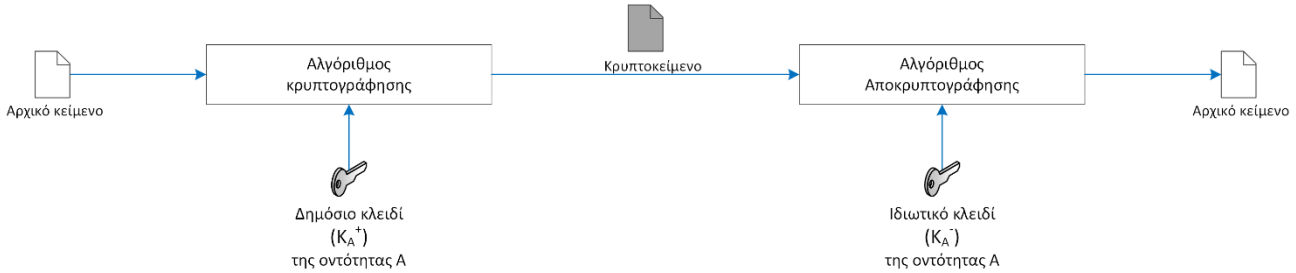
Έστω, P είναι το αρχικό κείμενο το οποίο επιθυμεί να κρυπτογραφήσει η οντότητα A, C είναι το κρυπτοκείμενο που παράγεται και K το κοινό μυστικό κλειδί που χρησιμοποιεί ο αλγόριθμος κρυπτογράφησης E. Η διαδικασία $E_k(P)$ δημιουργεί το κρυπτοκείμενο C με είσοδο το αρχικό κείμενο P και το κλειδί K, ενώ ο αλγόριθμος αποκρυπτογράφησης D ακολουθεί τη διαδικασία $D_k(C)$ για να ανακτήσει το αρχικό κείμενο P με είσοδο το κρυπτοκείμενο C και το κλειδί K.

Σημαντική προϋπόθεση είναι η πρότερη συμφωνία μεταξύ των δυο οντοτήτων για την τιμή του κοινού μυστικού κλειδιού (secret key), το οποίο θα πρέπει να έχει περιορισμένη διάρκεια ισχύος, συνήθως στα όρια μιας συνόδου επικοινωνίας. Για αυτό και το κλειδί αυτό ονομάζεται κλειδί συνόδου (session key). Επομένως, για να επικοινωνήσουν μεταξύ τους ανά δυο (2) συνολικά n οντότητες, θα χρειαστούν n (n-1) / 2 κλειδιά συνόδων. Ο πιο διαδεδομένος αλγόριθμος συμμετρικής κρυπτογραφίας είναι ο DES, ο οποίος επινοήθηκε το 1977 και θα μελετηθεί στο επόμενο κεφάλαιο.

Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν διαφορετικό κλειδί για την κρυπτογράφηση (π.χ. το δημόσιο κλειδί του παραλήπτη) και διαφορετικό για την αποκρυπτογράφηση (π.χ. το ιδιωτικό κλειδί του παραλήπτη). Κάθε οντότητα που συμμετέχει σε ένα κρυπτοσύστημα δημοσίου κλειδιού, διαθέτει ένα δικό της ζεύγος κλειδιών, με μεγάλη διάρκεια ισχύος που εξαρτάται από το σκοπό χρήσης του (π.χ. για κρυπτογράφηση ή για υπογραφή).

Οι ασύμμετροι αλγόριθμοι λειτουργούν ικανοποιώντας δυο (2) βασικές απαιτήσεις:

- **Είναι υπολογιστικά ανέφικτο να υπολογιστεί το ένα κλειδί γνωρίζοντας το άλλο κλειδί του ίδιου κατόχου.** Η ιδιότητα αυτή επιτρέπει να δημοσιοποιηθεί το ένα κλειδί (δημόσιο κλειδί) και να διατηρηθεί το άλλο πραγματικό μυστικό, ώστε να το γνωρίζει μόνον ο ιδιοκτήτης του (ιδιωτικό κλειδί). Λόγω αυτού του σχήματος λειτουργίας, οι αλγόριθμοι αυτοί ονομάζονται αλγόριθμοι δημοσίου κλειδιού, οπότε:
    - Το δημόσιο κλειδί (K^+) κάθε οντότητας είναι διαθέσιμο σε όλες τις άλλες οντότητες.
    - Το ιδιωτικό κλειδί (K^-) είναι αυστηρά γνωστό μόνο στη μια οντότητα που κατέχει το ζεύγος των κλειδιών στο οποίο ανήκει.
- **Κάθε αρχικό κείμενο που κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται μόνο με το άλλο κλειδί του ίδιου ζεύγους.** Έτσι, μια οντότητα A μπορεί να κρυπτογραφήσει ένα μήνυμα το οποίο προορίζεται για την οντότητα B, χρησιμοποιώντας το δημόσιο κλειδί της οντότητας B. Στη συνέχεια, το κρυπτοκείμενο που παράγεται αποστέλλεται στον παραλήπτη (B), όπου μόνον αυτός μπορεί να το αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό κλειδί του. Με τον τρόπο αυτό εξασφαλίζεται η εμπιστευτικότητα του μηνύματος.



Εικόνα 6.4 *Εφαρμογή κρυπτογραφίας δημοσίου κλειδιού για προστασία της εμπιστευτικότητας*.

6.2.4.2 Τρόπος επεξεργασίας

Κατηγοριοποιώντας τους αλγόριθμους κρυπτογράφησης ως προς τον τρόπο επεξεργασίας, διακρίνουμε τις περιπτώσεις αλγορίθμων δέσμης (block) και ροής (stream).

6.2.4.2.1 Επεξεργασία Δέσμης

Οι αλγόριθμοι δέσμης μετατρέπουν το αρχικό κείμενο (μήνυμα) σε δέσμες σταθερού μήκους, π.χ. των 64 bit, τις οποίες στη συνέχεια κρυπτογραφούν. Σε μια σύνοδο κρυπτογράφησης, όλες οι δέσμες δεδομένων ενός μηνύματος κρυπτογραφούνται με το ίδιο κλειδί.

Οι αλγόριθμοι δέσμης προϋποθέτουν ότι είναι γνωστό το αρχικό μήνυμα πριν την κρυπτογράφησή του. Επομένως, δεν μπορούν να χρησιμοποιηθούν π.χ. για την κρυπτογραφημένη μετάδοση μιας συνομιλίας σε πραγματικό χρόνο, χωρίς την εισαγωγή αισθητής καθυστέρησης στη μετάδοσή της.

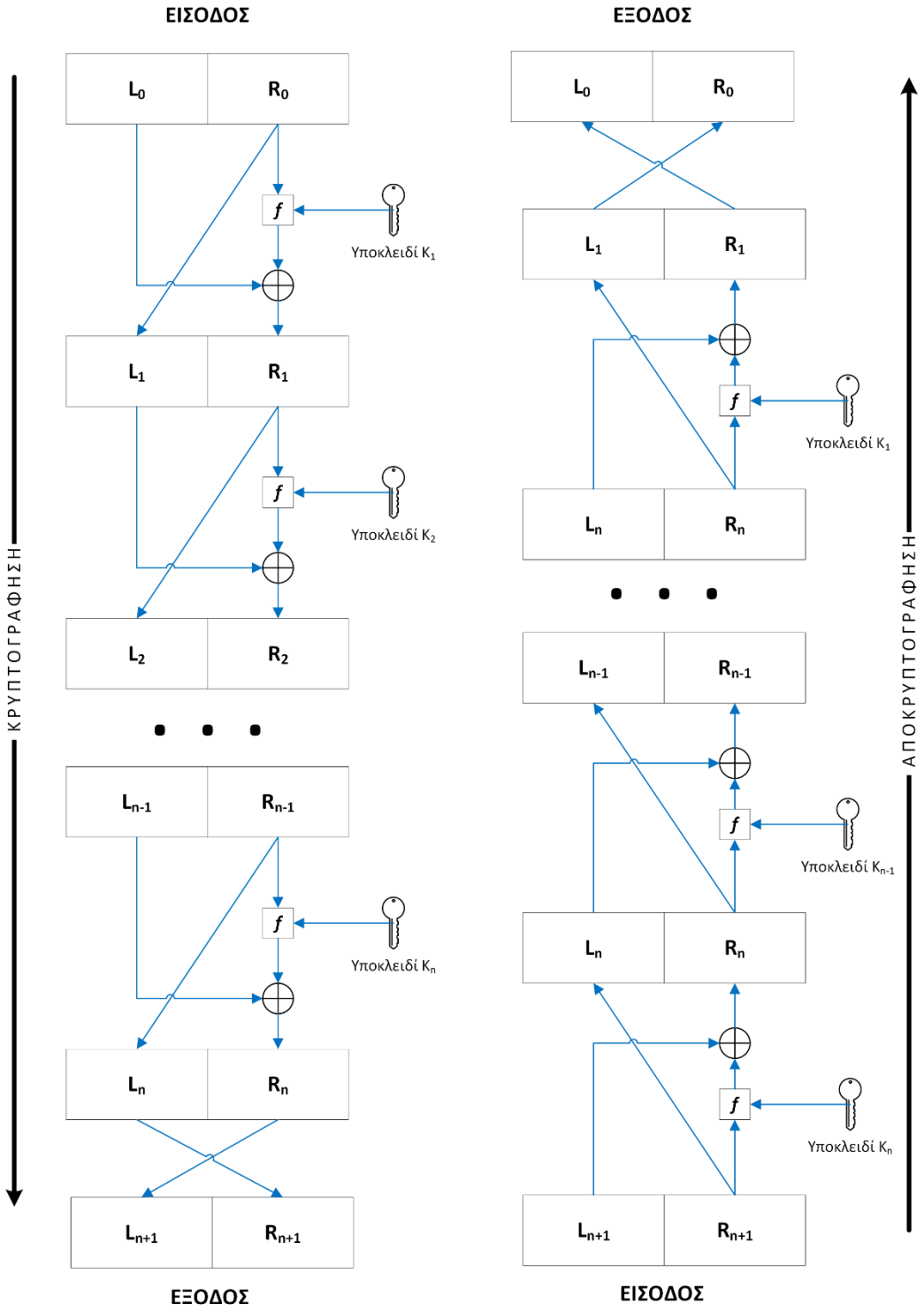
Ορισμένοι συμμετρικοί αλγόριθμοι δέσμης ανήκουν στην οικογένεια αλγορίθμων με δομή Feistel. Η δομή Feistel αποτελείται από μια σειρά πανομοιότυπων κύκλων επεξεργασίας. Σε κάθε κύκλο (round) επεξεργασίας, τα δεδομένα της δέσμης υποβάλλονται σε επεξεργασία, όπου χρησιμοποιείται ένα διαφορετικό υποκλειδί (sub-key), που προκύπτει από το συμμετρικό κλειδί.

Συγκεκριμένα, από το συμμετρικό κλειδί K υπολογίζονται τόσα υποκλειδιά (K_i, i=1 … n), όσοι και οι n κύκλοι επεξεργασίας. Κατά την κρυπτογράφηση, πρώτα χωρίζεται η δέσμη του αρχικού κειμένου σε δυο ίσα μέρη: L_0 και R_0. Στη συνέχεια, εκτελούνται οι κύκλοι επεξεργασίας, όπως φαίνεται στην Εικόνα 6.5. Πιο συγκεκριμένα, σε κάθε κύκλο:

- το τρέχον δεξί μέρος δέσμης γίνεται το επόμενο αριστερό: $L_i = R_{i-1}$
- στο τρέχον δεξί μέρος της δέσμης εφαρμόζεται η συνάρτηση f με το υποκλειδί K_i, ενώ το αποτέλεσμα γίνεται είσοδος μαζί με το τρέχον αριστερό μέρος της δέσμης σε μια πράξη XOR που παράγει στην έξοδό της το επόμενο δεξί μέρος της δέσμης: $R_i = L_{i-1} \oplus f_{Ki}(R_{i-1})$.

Επειδή η κυκλική συνάρτηση είναι αντιστρέψιμη, κατά την αποκρυπτογράφηση ακολουθείται η ακριβώς αντίστροφη διαδικασία:

- το τρέχον αριστερό μέρος δέσμης θα γίνει το επόμενο δεξί: $R_i = L_{i-1}$
- στο τρέχον αριστερό δεξί μέρος της δέσμης εφαρμόζεται η συνάρτηση f με το υποκλειδί K_i, ενώ το αποτέλεσμα γίνεται είσοδος μαζί με το τρέχον δεξί μέρος της δέσμης σε μια πράξη XOR που παράγει στην έξοδό της το επόμενο αριστερό μέρος της δέσμης: $L_i = R_{i-1} \oplus f_{Ki}(L_{i-1})$.

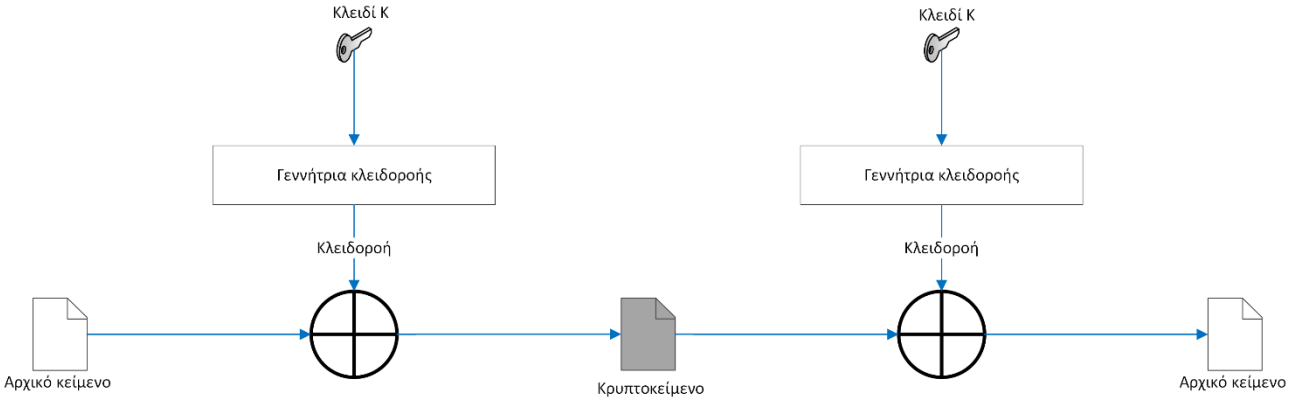


Εικόνα 6.5 *Δομή Feistel.*

6.2.4.2.2 Επεξεργασία Ροής

Οι αλγόριθμοι ροής κρυπτογραφούν το αρχικό κείμενο, το οποίο θεωρείται ότι έχει τη μορφή μιας ροής από bit, εφαρμόζοντας την πράξη XOR μεταξύ κάθε bit της ροής του μηνύματος και μιας άλλης ροής, γνωστής ως κλειδοροής (key stream). Επομένως, η ανθεκτικότητα της παρεχόμενης κρυπτογράφησης εξαρτάται από την γεννήτρια της κλειδοροής, η οποία λειτουργεί επίσης στη βάση της τιμής ενός μυστικού κλειδιού.

Στην Εικόνα 6.6, περιγράφεται η λειτουργία ενός αλγορίθμου ροής, όπου το μυστικό κλειδί K αποτελεί την είσοδο σε μια γεννήτρια κλειδοροής:



Εικόνα 6.6 *Λειτουργία αλγόριθμου ροής.*

Κάθε bit της κλειδοροής συνδυάζεται με ένα bit του αρχικού κειμένου, χρησιμοποιώντας την λογική πράξη XOR, ως εξής:

```
11001100  αρχικό κείμενο
01101100  κλειδοροή
----------
10100000  κρυπτοκείμενο
```

Για τη σωστή αποκρυπτογράφηση απαιτείται η παραγωγή της ίδιας ακριβώς κλειδοροής στη μεριά του παραλήπτη:

```
10100000  κρυπτοκείμενο
01101100  κλειδοροή
----------
11001100  αρχικό κείμενο
```

Μια ανθεκτική σε επίθεση αυτοσυσχέτισης (correlation attack) κλειδοροή θα πρέπει να χαρακτηρίζεται από τις ακόλουθες ιδιότητες:

- Θα πρέπει να έχει μεγάλη περίοδο επανάληψης. Στην πραγματικότητα, η κλειδοροή παράγεται από μια γεννήτρια ψευδοτυχαίων αριθμών, όπως για παράδειγμα οι γεννήτριες Linear Congruence Generator (LCG) και Inverse Congruence Generator (LCG). Μια τέτοια γεννήτρια χρησιμοποιεί μια συνάρτηση που παράγει μια ντετερμινιστική ακολουθία από bit, η οποία είναι αναπόφευκτο από κάποια στιγμή και μετά να επαναλαμβάνεται. Όσο πιο αργά έρθει αυτή η στιγμή, τόσο μεγαλύτερη είναι η περίοδος επανάληψης.

- Θα πρέπει να ομοιάζει όσο γίνεται περισσότερο τις ιδιότητες μιας ακολουθίας πραγματικά τυχαίων αριθμών. Για παράδειγμα, θα πρέπει να επιδιώκεται ώστε να περιέχει ίσο περίπου αριθμό από 0 και 1. Το NIST έχει ορίσει στο Special Publication 800-22 ένα εκτενές σύνολο στατιστικών ελέγχων για την επιβεβαίωση της τυχαιότητας (randomness tests) μιας ακολουθίας bit που παράγεται από μια γεννήτρια.

- Θα πρέπει να έχει μεγάλη γραμμική ισοδυναμία (linear equivalence). Επειδή η παραγωγή μιας τέτοιας ακολουθίας γίνεται με τη χρήση γραμμικών μεθόδων, όπου κάθε επόμενο bit προκύπτει από το γραμμικό συνδυασμό των bit ενός ή περισσότερων καταχωρητών (όπως π.χ. στην

περίπτωση του LCG) της γεννήτριας, όσο μεγαλύτερο το πλήθος αυτών των bit, τόσο μεγαλύτερη η γραμμική ισοδυναμία.

Με μια προσεκτικά σχεδιασμένη γεννήτρια ψευδοτυχαίων αριθμών, ένας αλγόριθμος ροής μπορεί να είναι το ίδιο ασφαλής όσο και ένας αλγόριθμος δέσμης ίδιου μήκους κλειδιού. Ένα ακόμη πλεονέκτημα των αλγόριθμων ροής σχετίζεται με το γεγονός ότι είναι πιο γρήγοροι, σε σχέση με τους αλγορίθμους δέσμης.

Καταλήγοντας, θα λέγαμε ότι για εφαρμογές που χειρίζονται ροές δεδομένων, όπως για παράδειγμα δεδομένα τα οποία διακινούνται σε ένα κανάλι επικοινωνίας ή δεδομένα τα οποία μεταφέρονται από έναν φυλλομετρητή (Web browser), ένας αλγόριθμος ροής είναι η προτιμότερη επιλογή. Για εφαρμογές οι οποίες διαχειρίζονται δέσμες δεδομένων, όπως οι εφαρμογές μεταφοράς αρχείων, εφαρμογές email και εφαρμογές διαχείρισης βάσεων δεδομένων, οι αλγόριθμοι δέσμης είναι καταλληλότεροι.

6.2.4.3 Ανθεκτικότητα

Με βάση τις υποθέσεις για την χειρότερη περίπτωση, γίνονται δοκιμές με σκοπό να βρεθούν τρόποι για να «σπάσει» το κρυπτογραφημένο κείμενο, δηλαδή να βρεθεί το μυστικό κλειδί αποκρυπτογράφησής του. Σε αυτή την περίπτωση, ο σχεδιαστής ή ο χρήστης που προτίθεται να χρησιμοποιήσει ένα προϊόν κρυπτογράφησης παίζει το ρόλο του κρυπταναλυτή.

Οι κρυπτογραφικοί αλγόριθμοι θεωρείται ότι είναι ισχυροί, εφόσον οι προσπάθειες εξειδικευμένων κρυπταναλυτών δεν μπορούν να καταλήξουν σε τρόπους για να τους σπάσουν με συμβατικά μέσα και σε λογικούς χρόνους, καθώς δεν υπάρχουν φορμαλιστικές μέθοδοι που να αποδεικνύουν την ασφάλεια που παρέχουν οι περισσότεροι κρυπτογραφικοί αλγόριθμοι.

Νέοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται συνεχώς και είτε σπάζουν ή αντέχουν καλά. Για το λόγο αυτό η επιλογή του κατάλληλου αλγόριθμου αποκτά ιδιαίτερη βαρύτητα στην υλοποίηση ενός κρυπτογραφικού συστήματος.

6.3 Στεγανογραφία

Η στεγανογραφία, αποτελεί έναν κλάδο της κρυπτολογίας όπου, σε αντίθεση με την κρυπτογραφία, στόχος δεν είναι η μετατροπή του μηνύματος σε ακατανόητη μορφή αλλά η απόκρυψη της ύπαρξής του.

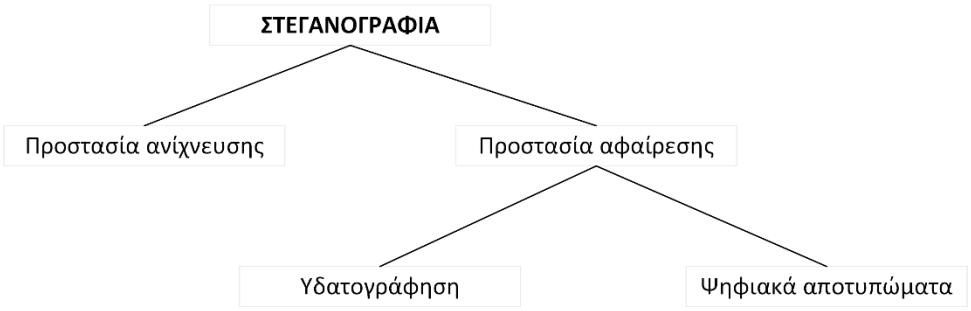
Ένα από τα αρχαιότερα παραδείγματα στεγανογραφικής τεχνικής αναφέρεται στον Ηρόδοτο, όπου περιγράφει την περίπτωση ενός σκλάβου, ο οποίος στάλθηκε στην Ιωνία με ένα μυστικό μήνυμα ζωγραφισμένο στο κεφάλι του. Ο σκλάβος απέκρυψε το μήνυμα αφήνοντας τα μαλλιά του να αποκτήσουν ικανό μάκρος έτσι ώστε να είναι αδύνατη η θέαση του μηνύματος. Στη συνέχεια, ταξίδεψε στη Μίλητο, όπου ξυρίζοντας εκεί το κεφάλι του φανέρωσε το μυστικό μήνυμα στον Αρισταγόρα που ήταν και ο τελικός αποδέκτης του. Ένα άλλο παράδειγμα στεγανογραφικής τεχνικής αποτελεί η χρήση του αόρατου μελανιού. Σε αυτή την περίπτωση, η ύπαρξη του μηνύματος αποκρύπτεται αξιοποιώντας την ιδιότητα του ειδικού μελανιού να μην γίνεται αντιληπτό από το ανθρώπινο μάτι σε κανονικές συνθήκες. Σήμερα, χρησιμοποιούνται τεχνικές με παρόμοιο αποτέλεσμα, ώστε να αποκρύπτεται η ύπαρξη των μεταδιδόμενων ηλεκτρονικών μηνυμάτων.

Οι στεγανογραφικές τεχνικές μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, όπως:

- Διαφύλαξη της εμπιστευτικότητας ενός μηνύματος.
- Προστασία πληροφορίας από μη εξουσιοδοτημένη τροποποίηση.
- Έλεγχος πρόσβασης κατά τη διανομή ηλεκτρονικού περιεχομένου.

Μια ακόμη χρήση της στεγανογραφίας στις μέρες μας, είναι η προστασία των πνευματικών δικαιωμάτων ηλεκτρονικού περιεχομένου, όπου το κρυφό μήνυμα επιβεβαιώνει την ταυτότητα του νόμιμου ιδιοκτήτη του. Η Ψηφιακή Υδατογράφηση (Digital Watermarking) και τα Ψηφιακά Αποτυπώματα (Digital Fingerprinting) είναι δύο κατηγορίες στις οποίες διαχωρίζεται η τεχνική του ηλεκτρονικού «σημαδέματος» ενός ηλεκτρονικού αρχείου με τεχνικές στεγανογραφίας.

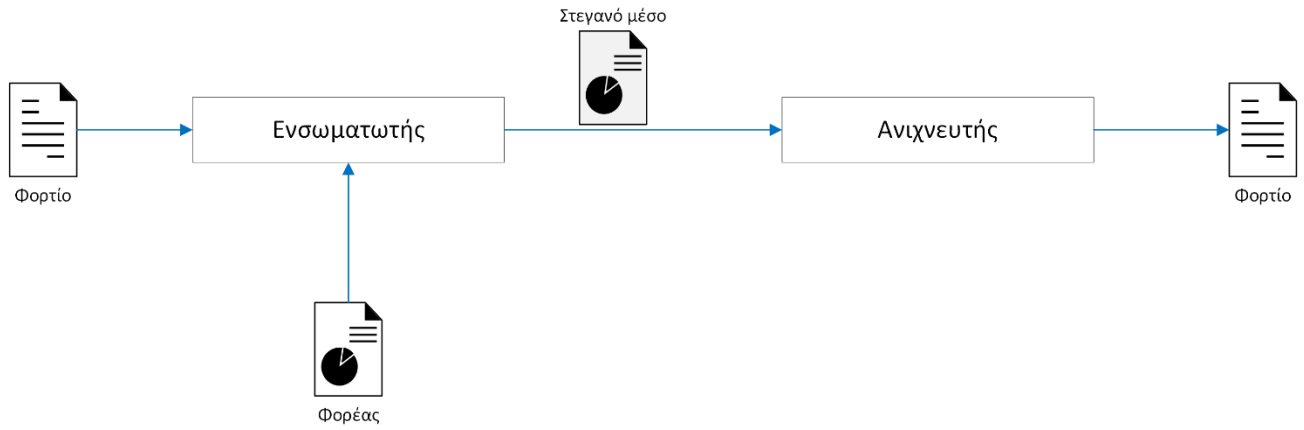
Στην Εικόνα 6.7 απεικονίζεται μια κατηγοριοποίηση των σύγχρονων στεγανογραφικών τεχνικών.



Εικόνα 6.7 *Κατηγοριοποίηση σύγχρονων στεγανογραφικών τεχνικών.*

Το κριτήριο, με βάση το οποίο γίνεται ο διαχωρισμός, προκύπτει από το στόχο της στεγανογραφικής μεθόδου. Στόχος μπορεί να είναι η προστασία ανίχνευσης της ύπαρξης των δεδομένων στο μήνυμα ή η προστασία της αφαίρεσής τους από το μήνυμα (τα ίδια τα δεδομένα δηλώνουν το νόμιμο ιδιοκτήτη τους). Στην περίπτωση κατά την οποία στόχος είναι η προστασία αφαίρεσης, οι τεχνικές διακρίνονται σε παραγωγή υδατογραφημάτων (watermarking), που αφορούν το σύνολο των δεδομένων, ή αποτυπωμάτων (fingerprinting), που προσδιορίζουν μοναδικά κάθε αντικείμενο. Το αποτύπωμα, συνήθως, παράγεται με τη βοήθεια μιας **συνάρτησης συνόψισης**. Οι συναρτήσεις αυτές θα μελετηθούν στο Κεφάλαιο 8.

Ένα γενικό περιγραφικό σχήμα για τη διαδικασία ψηφιακής υδατογράφησης παρατίθεται στην Εικόνα 6.8. Παρατηρούμε ότι στον **ενσωματωτή** (embedder) υπάρχουν δύο είσοδοι: μια για το **φορτίο** (payload), το οποίο αποτελεί το κυρίως μήνυμα που επιθυμούμε να μεταφέρουμε, καθώς και μια για τον **φορέα** (cover work), στον οποίο θέλουμε να ενσωματώσουμε το φορτίο (ώστε να αποκρυφτεί η ύπαρξή του). Η παραγόμενη έξοδος, γνωστή ως **στεγανό μέσο** (stego work), μεταφέρεται στον παραλήπτη και αποτελεί την είσοδο στον **ανιχνευτή** (detector), ο οποίος είναι επιφορτισμένος με την ευθύνη ανίχνευσης της ύπαρξης φορτίου. Αν ανιχνευτεί φορτίο, τότε αυτό παρουσιάζεται στον παραλήπτη.



Εικόνα 6.8 *Διαδικασία ψηφιακής υδατογράφησης.*

Η στεγανογραφία βασίζεται σε τρεις κύριες αρχές, οι οποίες αποτελούν και ένα μέτρο της αποδοτικότητας μιας στεγανογραφικής τεχνικής:

- **Ποσότητα Πληροφορίας:** Όσο περισσότερη πληροφορία (μεγαλύτερο φορτίο) μπορούμε να αποκρύψουμε, τόσο πιο αποδοτική είναι η στεγανογραφική τεχνική.

- **Δυσκολία Ανίχνευσης:** Μια στεγανογραφική τεχνική θα πρέπει να είναι ανθεκτική σε προσπάθειες ανίχνευσης. Υπάρχει οπωσδήποτε μια άμεση σχέση μεταξύ της ποσότητας πληροφορίας που μπορούμε να κρύψουμε και της δυσκολίας ανίχνευσης που προσφέρει η μέθοδος που χρησιμοποιούμε. Όσο περισσότερη πληροφορία, για παράδειγμα, προσπαθούμε

να κρύψουμε ενσωματώνοντάς την στο στεγανό μέσο, τόσο πιο εύκολη γίνεται η ανίχνευση της κρυμμένης πληροφορίας.

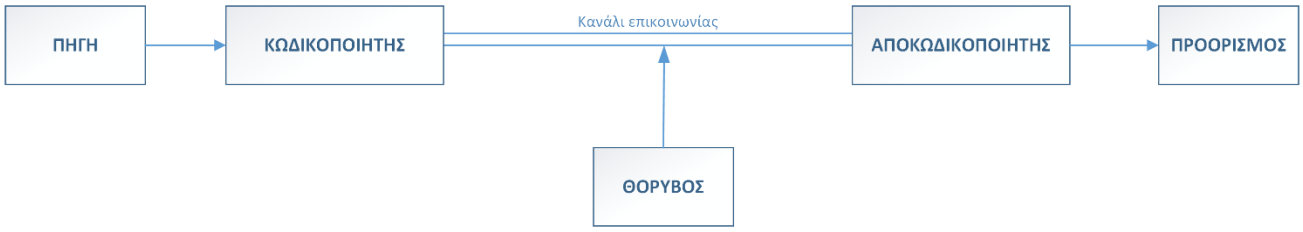
- **Δυσκολία Αφαίρεσης Πληροφορίας**: Πρέπει να είναι πολύ δύσκολη, αν όχι αδύνατη, η αφαίρεση του κρυμμένου μηνύματος (φορτίου) από το στεγανό μέσο, χωρίς αυτό να γίνεται αντιληπτό από το νόμιμο παραλήπτη.

6.4 Χρήσιμες Έννοιες από τη Θεωρία Πληροφορίας

Το 1948 και το 1949 ο Claude Shannon δημοσίευσε δύο εργασίες του με τίτλους: «The Mathematical Theory of Communication» και «Communication Theory of Secrecy Systems», οι οποίες αποτέλεσαν τα θεμέλια για τη γνωστική περιοχή που σήμερα ονομάζεται Θεωρία Πληροφορίας (Information Theory). Η Θεωρία Πληροφορίας διαδραματίζει σπουδαίο ρόλο στη σύγχρονη κρυπτογραφία, καθώς μελετάει ζητήματα τα οποία αφορούν άμεσα τις διαδικασίες που εκτελούν οι κρυπτογραφικοί αλγόριθμοι.

Η συνδυασμένη αξιοποίηση της Θεωρίας Πληροφορίας και της Πολυπλοκότητας Αλγορίθμων, στο πλαίσιο μελέτης της ανθεκτικότητας των κρυπτογραφικών αλγόριθμων, είναι η αναζήτηση και απόδειξη των ελάχιστων ορίων σε χρόνο και χώρο οι οποίοι απαιτούνται προκειμένου να επιλυθεί ένα δεδομένο υπολογιστικό πρόβλημα. Όπως αναφέρθηκε προηγουμένως, ένα κρυπτογραφικό σύστημα είναι ασφαλές αν ο κρυπτογραφικός αλγόριθμος το προστατεύει με τέτοιο τρόπο ώστε να είναι **υπολογιστικά ανέφικτο** να καταφέρει κάποιος τρίτος να υπερνικήσει αυτή την προστασία με λογικούς πόρους (δηλαδή, σε εύλογο χρονικό διάστημα και χρησιμοποιώντας περιορισμένο χώρο αποθήκευσης). Επομένως, η εύρεση των ελάχιστων αυτών ορίων είναι σημαντική για να διασφαλιστεί ότι ο κρυπτογραφικός αλγόριθμος εξυπηρετεί το σκοπό του, ακόμη και αν αποδεδειγμένα μπορεί με κάποιο τρόπο να υπερνικηθεί. Αν οι πόροι που απαιτούνται ικανοποιούν τις απαιτήσεις, τότε ο κρυπτογραφικός αλγόριθμος κρίνεται ανθεκτικός.

Η Θεωρία Πληροφορίας εστιάζει στην επικοινωνία μεταξύ των οντοτήτων, οι οποίες συμμετέχουν σε ένα επικοινωνιακό σύστημα, όπως απεικονίζεται στην Εικόνα 6.9.



Εικόνα 6.9 *Επικοινωνιακό σύστημα.*

Ο σκοπός ενός επικοινωνιακού συστήματος είναι η μεταφορά πληροφορίας από μια πηγή (source) σε ένα συγκεκριμένο προορισμό (destination). Οι οντότητες που συμμετέχουν σε ένα επικοινωνιακό σύστημα, όπως αυτές εμφανίζονται στην αφαιρετική αναπαράσταση της Εικόνας 6.9, είναι οι παρακάτω:

- **Πηγή (Source)**: Είναι η οντότητα η οποία παράγει το μήνυμα πληροφορίας το οποίο πρέπει να μεταδοθεί.

- **Κωδικοποιητής (Encoder)**: Μεταφράζει το μήνυμα σε μια μορφή κατάλληλη για μεταφορά μέσω του **καναλιού επικοινωνίας (communication channel)**. Για παράδειγμα, στις ψηφιακές επικοινωνίες η μορφή αυτή είναι μια ακολουθία δυαδικών ψηφίων.

- **Κανάλι επικοινωνίας (communication channel)**: Είναι το μέσο (ο δίαυλος επικοινωνίας), το οποίο χρησιμοποιείται για τη μεταφορά του κωδικοποιημένου μηνύματος, όπως αυτό έχει προκύψει από τον κωδικοποιητή.

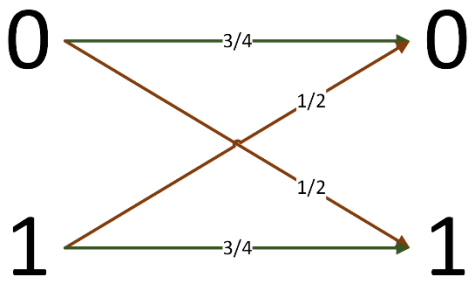
- **Κανάλι μεταφοράς**: Μπορεί να υπόκειται σε παρέμβαση **θορύβου (noise)**, με αποτέλεσμα να υπάρχουν αλλοιώσεις του μηνύματος κατά τη μεταφορά του. Για παράδειγμα, η επιθυμητή μεταφορά του bit με τιμή 1 μπορεί να έχει ως αποτέλεσμα να φτάσει στον προορισμό το bit με τιμή 0.

- **Αποκωδικοποιητής (Decoder)**: Παραλαμβάνει το κωδικοποιημένο μήνυμα από την έξοδο του καναλιού και το αποκωδικοποιεί έτσι ώστε να είναι καταληπτό από τον προορισμό.

- **Προορισμός (Destination)**: Λαμβάνει το μεταφερθέν μήνυμα πληροφορίας. Είναι ο τελικός αποδέκτης της επικοινωνίας, που λαμβάνει χώρα στο επικοινωνιακό σύστημα.

Η Θεωρία Πληροφορίας αναζητά σε ένα επικοινωνιακό σύστημα και εξετάζει λύσεις για πρακτικά ερωτήματα, όπως για παράδειγμα: «Ποιος είναι ο βέλτιστος τρόπος συμπίεσης των δεδομένων προς αποστολή;», «Ποιο είναι το καταλληλότερο σχήμα κωδικοποίησης που μπορούμε να χρησιμοποιήσουμε;». Οι απαντήσεις σε τέτοιου είδους ερωτήματα βασίζονται σε θεωρίες με ισχυρά μαθηματικά θεμέλια, οι οποίες αναπτύχθηκαν και συνεχίζουν να αναπτύσσονται, ή να βελτιώνονται, καθώς οι ανάγκες αλλάζουν με την πάροδο του χρόνου.

Ας θεωρήσουμε το ακόλουθο παράδειγμα. Έστω ότι υπάρχει μια πηγή, η οποία παράγει μια ακολουθία bit με ρυθμό 1 bit/sec. Τα bit με τιμή 0 και τα bit με τιμή 1 παράγονται με ίσες πιθανότητες και ανεξάρτητα το ένα από το άλλο. Η επικοινωνία λαμβάνει χώρα πάνω σε ένα κανάλι με θόρυβο. Ας υποθέσουμε ότι ο θόρυβος προκαλείται με τρόπο τέτοιο ώστε ένα bit να μπορεί να παραληφθεί στον προορισμό με λάθος τιμή (δηλαδή με τιμή διαφορετική από αυτή με την οποία στάλθηκε από την πηγή) με πιθανότητα ¼ (0,25). Το επικοινωνιακό αυτό σύστημα απεικονίζεται στην Εικόνα 6.10



Εικόνα 6.10 *Επικοινωνία σε κανάλι με θόρυβο*.

Σε ένα τέτοιο σύστημα, μπορεί κάποιος να κρίνει ότι η πιθανότητα λάθους 0,25 είναι πολύ μεγάλη και ότι πρέπει να αντιμετωπίσει αυτό το πρόβλημα. Μια λύση θα ήταν η επαναλαμβανόμενη εκπομπή του ίδιου bit περισσότερες από μια φορές. Έστω, ότι στέλνουμε το bit με τιμή 1 τρεις φορές. Τότε ο προορισμός θα μπορούσε να αποφανθεί ποια είναι η σωστή τιμή του bit που αρχικά στάλθηκε, βασιζόμενος στην πιθανότητα σωστής ή λανθασμένης μετάδοσης. Αν ο προορισμός παραλάβει την ακολουθία bit 110 τότε ακόμη και διαισθητικά αντιλαμβανόμαστε ότι πιθανότερο είναι ότι αρχικά η πηγή είχε ως στόχο να μεταδώσει το bit με τιμή 1, αφού η παραλαβή δύο αλλοιωμένων τιμών έχει λιγότερες πιθανότητες από την παραλαβή δύο σωστών.

Το θεμελιώδες θεώρημα της Θεωρίας Πληροφορίας αναφέρει πως προκειμένου να έχουμε μεγάλη αξιοπιστία κατά τη μετάδοση πληροφοριών, χωρίς να μειώσουμε το ρυθμό μετάδοσης κοντά στο μηδέν, αρκεί να τον μειώσουμε ως την τιμή η οποία ονομάζεται Χωρητικότητα Καναλιού (Channel Capacity). Η κωδικοποίηση έχει ακριβώς αυτό τον στόχο. Να αντιστοιχίσει σε μια ακολουθία πραγματικών bit προς αποστολή μια σειρά συμβόλων, η οποία ονομάζεται κωδική λέξη (code word) και είναι κατάλληλη για τη μετάδοση πάνω από κανάλι με θόρυβο. Για την αποδοτικότερη μετάδοση των πραγματικών bit του μηνύματος είναι σύνηθες η κωδική λέξη να αντιστοιχεί σε μια δέσμη (block) από bit και όχι σε ένα μόνο bit. Στην

κρυπτογραφία, χρησιμοποιείται η έννοια της εντροπίας ως ένα μαθηματικό μέτρο της πληροφορίας που μεταφέρεται μέσω ενός μηνύματος.

Με την εργασία του 1949, ο Shannon κατάφερε να μετρήσει τη «μυστικότητα» ενός αλγόριθμου κρυπτογράφησης χρησιμοποιώντας την αβεβαιότητα του αρχικού κειμένου, δεδομένης της κατοχής του κρυπτοκειμένου. Ένα κρυπτοσύστημα, από το οποίο έχουμε στη διάθεση μας όση ποσότητα κρυπτοκειμένου επιθυμούμε αλλά παρόλα αυτά δεν μπορούμε να μάθουμε κάτι παραπάνω για το αρχικό κείμενο, λέμε ότι προσφέρει «τέλεια μυστικότητα» (**perfect secrecy**).

Συνήθως, όσο μεγαλύτερη ποσότητα κρυπτοκειμένου έχουμε στη διάθεση μας, τόσο μειώνεται η αβεβαιότητα του αρχικού κειμένου, μέχρι του σημείου που γίνεται μηδενική, οπότε μπορούμε να ανακτήσουμε το αρχικό κείμενο. Ωστόσο, από έναν κρυπτογραφικό αλγόριθμο απαιτείται να είναι υπολογιστικά ανέφικτη δυνατότητα εξαγωγής συμπερασμάτων για το αρχικό κείμενο, λαμβάνοντας υπόψη τους υπολογιστικούς πόρους που μπορούν να διατίθενται στους κρυπταναλυτές.

Η Θεωρία Πληροφορίας μετράει την ποσότητα πληροφορίας που περιέχεται σε ένα μήνυμα με το πλήθος των bit που απαιτούνται για να κωδικοποιήσουμε όλα τα ενδεχόμενα μηνύματα. Για παράδειγμα, για να κωδικοποιήσουμε το σύνολο {ΑΣΠΡΟ, ΜΑΥΡΟ} χρειαζόμαστε 1 bit. Η ποσότητα αυτή της πληροφορίας ενός μηνύματος μετριέται με την εντροπία, η οποία είναι μία συνάρτηση της κατανομής πιθανοτήτων πάνω σε όλες τις ενδεχόμενες τιμές που μπορεί να έχει ένα μήνυμα.

Έστω X_1, …, X_n όλες οι πιθανές εκδοχές ενός μηνύματος *m* με αντίστοιχες πιθανότητες εμφάνισης $p(X_1)$, … , $p(X_n)$, όπου το άθροισμα των $p(X_i)$ είναι 1. Η εντροπία του μηνύματος *m* δίνεται από τον ακόλουθο τύπο:

$$H(X) = -\sum_{i=1}^{n} p(X_i) \log_2 p(X_i) \tag{6.1}$$

όπου για το λογάριθμο χρησιμοποιούμε ως βάση το 2 και για αυτό το λόγο η μονάδα μέτρησης της εντροπίας είναι το bit.

Ο παραπάνω τύπος, ερμηνευτικά μας λέει ότι με πιθανότητα $p(X_i)$ η εκδοχή μηνύματος X_i μπορεί να αναπαρασταθεί με $\log_2 p(X_i)$ bit πληροφορίας. Για παράδειγμα, έστω η τυχαία μεταβλητή X η οποία παίρνει τιμές από το σύνολο X = {Α, Β, Γ}, με p(Α) = 1/2, p(Β) = 1/4 και p(Γ) = 1/4. Τότε, σύμφωνα με τον ορισμό της εντροπίας, θα έχουμε:

$$H(X) = -\frac{1}{2}\log_2\left(\frac{1}{2}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) = 1,5\,bit \tag{6.2}$$

Η εντροπία, στην περίπτωσή μας η τιμή 1.5, μας δίνει και ένα μέτρο των ελάχιστων bit που απαιτούνται προκειμένου να περιγράψουμε πλήρως την τυχαία μεταβλητή X. Ο αριθμός αυτός των bit είναι πάντα μεταξύ των τιμών H(X) και H(X) + 1. Για το παράδειγμά μας, οι τιμές Α, Β και Γ της μεταβλητής απαιτούν τελικά 2 bit για να περιγράφουνε, αφού H(X) < 2 < H(X)+1. Άρα, η εντροπία παρέχει το κάτω όριο του αριθμού των bit που απαιτούνται για να περιγράψουμε την τιμή που έλαβε μια τυχαία διακριτή μεταβλητή.

Παρατηρώντας τον τύπο υπολογισμού της εντροπίας, καταλήγουμε στο συμπέρασμα ότι αυτή γίνεται μέγιστη όταν όλα τα ενδεχόμενα της τυχαίας μεταβλητής X είναι ισοπίθανα. Ενώ, αντίστοιχα, η εντροπία γίνεται ελάχιστη (ίση με το μηδέν) όταν υπάρχει ενδεχόμενο X_i το οποίο έχει πιθανότητα εμφάνισης ίσο με τη μονάδα (σίγουρο ότι θα συμβεί).

Ο κρυπτογράφος και ο κρυπταναλυτής χρησιμοποιούν την έννοια της εντροπίας με διαφορετικό σκοπό. Ο κρυπτογράφος χρησιμοποιεί έναν αλγόριθμο τέτοιο ώστε να αυξήσει την εντροπία του παραγόμενου κρυπτοκειμένου με σκοπό να καταστήσει δυσκολότερη την αποκρυπτογράφηση, καθώς η αύξηση της εντροπίας σημαίνει μείωση της συντακτικής δομής του παραγόμενου κρυπτοκειμένου. Από την άλλη, ο κρυπταναλυτής επιθυμεί να αναγνωρίσει μια λογική δομή στο κρυπτοκείμενο προκειμένου να οδηγηθεί σε συμπεράσματα, άρα χρησιμοποιεί τεχνικές και μεθόδους τέτοιες ώστε να οδηγηθεί σε ένα κρυπτοκείμενο μειωμένης εντροπίας, δηλαδή αυξημένης λογικής δομής. Για παράδειγμα, όταν ο κρυπταναλυτής γνωρίζει ότι το κρυπτοκείμενο FS%S^# αντιστοιχεί είτε στην τιμή ΑΣΠΡΟ είτε στην τιμή ΜΑΥΡΟ τότε η αβεβαιότητα

είναι μόλις 1 bit. Δηλαδή, ο κρυπταναλυτής χρειάζεται να γνωρίσει μόλις 1 bit προκειμένου να αποφανθεί για την πραγματική τιμή που αντιστοιχεί στο κρυπτοκείμενο που έχει στη διάθεσή του. Στην περίπτωσή μας, το πρώτο bit και μόνο θα αρκούσε για να καταλάβει ο κρυπταναλυτής ποιος είναι ο πρώτος χαρακτήρας: **Α**(ΣΠΡΟ) ή **Μ**(ΑΥΡΟ).

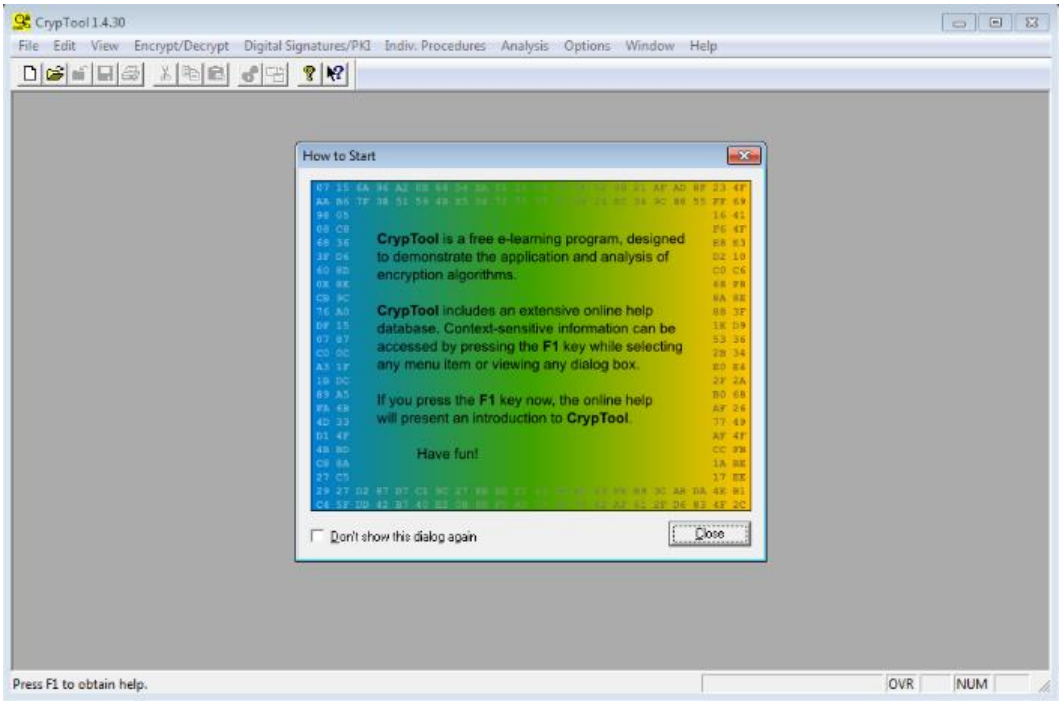
6.5 Μελέτη κλασσικών κρυπτογραφικών αλγορίθμων με το Cryptool

Το Cryptool είναι ένα εκπαιδευτικό λογισμικό που αναπτύχθηκε από τη συνεργασία πανεπιστημίων, στο πλαίσιο ενός εσωτερικού προγράμματος ευαισθητοποίησης μιας τράπεζας. Από τις αρχές της δεκαετίας του 2000 διατίθεται ελευθέρα για χρήση.

Το Cryptool περιλαμβάνει μεταξύ άλλων την υλοποίηση:

- Κλασσικών και σύγχρονων κρυπτογραφικών αλγορίθμων.
- Εργαλείων κρυπτανάλυσης.
- Διαδραστικών παρουσιάσεων αλγορίθμων και κρυπτοσυσκευών.
- Μηχανισμού online βοήθειας.

Στη συνέχεια αυτού του κεφαλαίου, το εργαλείο Cryptool θα χρησιμοποιηθεί για την εφαρμογή και κρυπτανάλυση κλασσικών αλγορίθμων κρυπτογράφησης. Το Cryptool είναι διαθέσιμο στη σελίδα: https://www.cryptool.org/en/ct1-downloads, όπου πέρα από την Αγγλική γλώσσα παρέχεται και στην Ελληνική γλώσσα, μεταφρασμένο από την επιστημονική ομάδα για την έρευνα και ανάπτυξη στην Ασφάλεια Πληροφοριών InfoSec του Πανεπιστημίου Μακεδονίας (http://infosec.uom.gr).



Εικόνα 6.11 *Το λογισμικό Cryptool.*

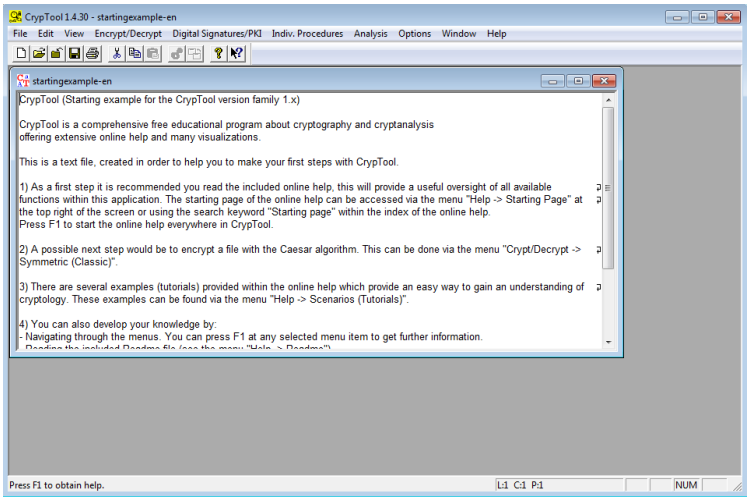
Οι κλασσικοί κρυπτογραφικοί αλγόριθμοι βασίζονται στην εφαρμογή τεχνικών μετατόπισης ή αντικατάστασης χαρακτήρων ενός συγκεκριμένου αλφαβήτου, ώστε το αρχικό κείμενο ως συλλογή χαρακτήρων να μετατραπεί στο κρυπτοκείμενο το οποίο θα έχει μια μορφή ακατανόητη πάλι όμως ως συλλογή χαρακτήρων του ίδιου αλφαβήτου. Ακολουθεί η παρουσίαση ορισμένων από τους πιο γνωστούς κλασσικούς κρυπτογραφικούς αλγορίθμους, με χρήση του εκπαιδευτικού εργαλείου Cryptool.

6.5.1 Αλγόριθμος του Καίσαρα

Ο αλγόριθμος του Καίσαρα ανήκει στην κατηγορία κρυπτογραφικών αλγορίθμων μονοαλφαβητικής αντικατάστασης, όπου το κλειδί είναι ένας χαρακτήρας του οποίου ο αύξων αριθμός θέσης στο αλφάβητο προκαλεί μια μετάθεση όλων των χαρακτήρων στο αλφάβητο. Ο Ιούλιος Καίσαρας στο βιβλίο «The Gallic Wars» περιγράφει έναν αλγόριθμο όπου κάθε γράμμα της αλφαβήτου μετατίθεται τρεις θέσεις δεξιότερα στο αλφάβητο. Η κρυπτογράφηση υλοποιείται με αντικατάσταση κάθε γράμματος του αρχικού κειμένου με το γράμμα που προκύπτει μετά τη μετάθεση. Αντίστοιχα, η αποκρυπτογράφηση γίνεται με αντικατάσταση του κάθε χαρακτήρα σύμφωνα με την αντίστροφη μετάθεση του αρχικού αλφαβήτου.

6.5.1.1 Κρυπτογράφηση

Μετά την εκκίνηση του ανοίγει ένα παράθυρο όπου περιέχεται ένα δείγμα αγγλικού κειμένου (startingexample-en.txt), όπως φαίνεται στην Εικόνα 6.12, το οποίο θα χρησιμοποιηθεί στη συνέχεια ως αρχικό κείμενο.



Εικόνα 6.12 *Το αρχικό κείμενο.*

Από το μενού επιλέγουμε κατά σειρά **Encrypt/Decrypt → Symmetric (classic) → Caesar / Rot13** και βεβαιωνόμαστε ότι:

- Στο πεδίο Select Variant είναι επιλεγμένη η επιλογή Caesar.
- Στο πεδίο Options to interpret the alphabet characters είναι επιλεγμένη η πρώτη επιλογή που καθορίζει πως η αρίθμηση ξεκινά από το 0.
- Στο πεδίο Key entry as επιλέγουμε Alphabet character και δίνουμε ως χαρακτήρα-κλειδί τον χαρακτήρα K.

Παρατηρούμε ότι στο κάτω μέρος του παραθύρου εμφανίζεται (και ανανεώνεται καθώς πληκτρολογούμε) η αντιστοίχιση κάθε χαρακτήρα του αλφαβήτου με αυτόν με τον οποίο θα αντικατασταθεί κατά την παραγωγή του κρυπτοκειμένου (κρυπτογράφηση), σύμφωνα με την επιλογή που έχει γίνει για το χαρακτήρα-κλειδί.

Στη συνέχεια, επιλέγουμε Encrypt, οπότε εμφανίζεται ένα νέο παράθυρο με το κρυπτογραφημένο κείμενο. Τι παρατηρείτε στο κείμενο αυτό; Είναι δυνατή η ανάγνωση και κατανόησή του;

- Έχοντας ως ενεργό το παράθυρο με το κρυπτοκείμενο, επιλέγουμε διαδοχικά από το μενού: **Encrypt/Decrypt → Symmetric (classic) → Caesar / Rot13**. Χωρίς καμία αλλαγή στις προτεινόμενες (default) ρυθμίσεις, επιλέγουμε Decrypt.

Εμφανίζεται ένα νέο παράθυρο με το αποκρυπτογραφημένο κείμενο, το οποίο όμως δεν είναι όμοιο με το αρχικό μας κείμενο. Γιατί συνέβη αυτό; Γιατί δεν αποκρυπτογραφήθηκε σωστά το κρυπτοκείμενο;

- Κλείνουμε το παράθυρο με το ανεπιτυχώς αποκρυπτογραφημένο κείμενο και επιλέγουμε να είναι ενεργό εκ νέου το παράθυρο με το κρυπτογράφημα.

- Επιλέγουμε διαδοχικά από το μενού**: Encrypt/Decrypt → Symmetric (classic) → Caesar / Rot13**.

- Στο πεδίο Key entry as, επιλέγουμε Alphabet character και δίνουμε το χαρακτήρα-κλειδί που είχαμε επιλέξει κατά την κρυπτογράφηση (K).

- Στη συνέχεια, επιλέγουμε Decrypt.

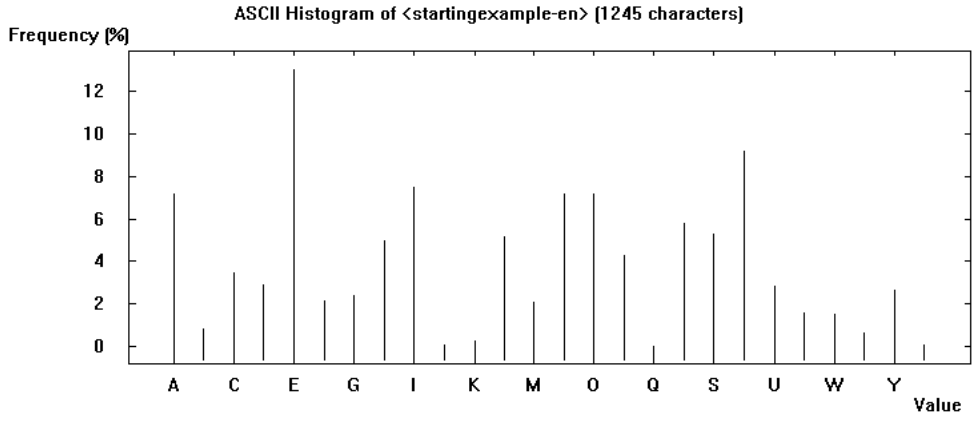
Εμφανίζεται ένα νέο παράθυρο με το αποκρυπτογραφημένο κείμενο. Αυτή τη φορά η αποκρυπτογράφηση έγινε σωστά. Γιατί;

- Επαναλαμβάνουμε τη διαδικασία κρυπτογράφησης / αποκρυπτογράφησης του αρχικού μας κειμένου δίνοντας στο πεδίο Key entry για την επιλογή Number Value την τιμή 8.

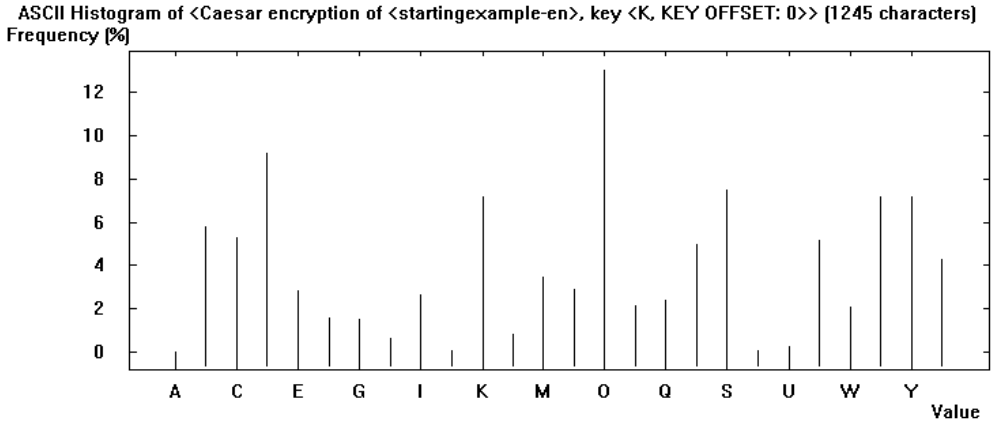
- Επιλέγουμε να είναι ενεργό το παράθυρο με το κρυπτογραφημένο μήνυμα και επιλέγουμε από το μενού κατά σειρά: **Analysis → Tools for Analysis → Histogram**.

- Επιλέγουμε να είναι ενεργό το παράθυρο με το αρχικό κείμενο και επιλέγουμε διαδοχικά από το μενού: **Analysis → Tools for Analysis → Histogram**.

Τι παρατηρείτε συγκρίνοντας τα δύο ιστογράμματα; Μπορείτε να εξάγετε κάποια χρήσιμη πληροφορία κρυπταναλυτικού ενδιαφέροντος (δηλαδή, για το κλειδί αποκρυπτογράφησης);



Εικόνα 6.13 *Ιστόγραμμα αρχικού κειμένου.*



Εικόνα 6.14 *Ιστόγραμμα κρυπτοκειμένου Καίσαρα.*

6.5.1.2 Κρυπτανάλυση μόνο με κρυπτοκείμενο

Η κρυπταναλυτική προσπάθεια έχοντας γνωστό μόνο το υποκλαπέν κρυπτοκείμενο, μπορεί να βοηθηθεί σημαντικά από επιμέρους εργαλεία ανάλυσης που συμπεριλαμβάνει το Cryptool.

Κλείνουμε όλα τα ανοιχτά παράθυρα του Cryptool και από το μενού επιλέγουμε διαδοχικά: **File → New** και εισάγουμε το ακόλουθο κρυπτοκείμενο που γνωρίζουμε ότι προέρχεται από κάποιο αρχικό κείμενο στην Αγγλική γλώσσα, το οποίο έχει κρυπτογραφηθεί με τον αλγόριθμο Caesar. Δυστυχώς όμως, δεν γνωρίζουμε το κλειδί που χρησιμοποιήθηκε:

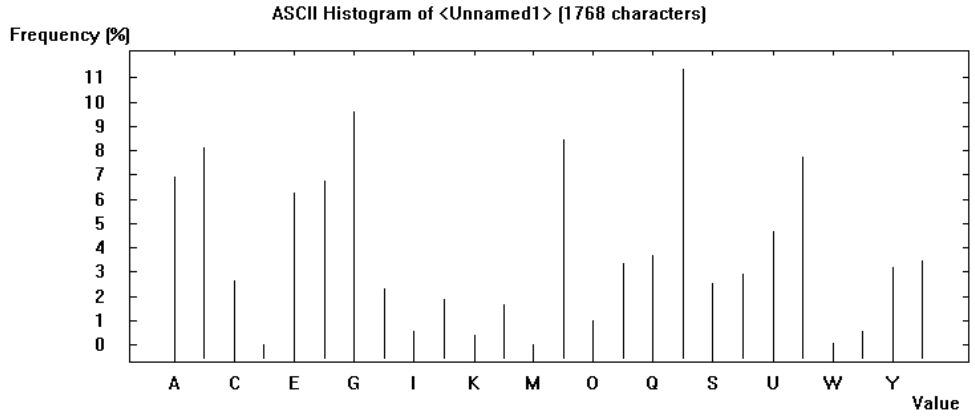
```
Gurer ner n ynetr ahzore bs fgrtnabtencuvp zrgubqf gung zbfg
bs hf ner snzvyvne jvgu (rfcrpvnyyl vs lbh jngpu n ybg bs fcl
zbivrf!), enatvat sebz vaivfvoyr vax naq zvpebqbgf gb frpergvat
n uvqqra zrffntr va gur frpbaq yrggre bs rnpu jbeq bs n ynetr
obql bs grkg naq fcernq fcrpgehz enqvb pbzzhavpngvba. Jvgu
pbzchgref naq argjbexf, gurer ner znal bgure jnlf bs uvqvat
vasbezngvba, fhpu nf:
* Pbireg punaaryf (r.t., Ybxv naq fbzr qvfgevohgrq qravny-bs-
freivpr gbbyf hfr gur Vagrearg Pbageby Zrffntr Cebgbpby, be
VPZC, nf gur pbzzhavpngvbaf punaary orgjrra gur "onq thl" naq
n pbzcebzvfrq flfgrz)
* Uvqqra grkg jvguva Jro cntrf
* Uvqvat svyrf va "cynva fvtug" (r.t., jung orggre cynpr gb
"uvqr" n svyr guna jvgu na vzcbegnag fbhaqvat anzr va gur
p:\jvaqbjf\flfgrz32 qverpgbel?)
* Ahyy pvcuref (r.t., hfvat gur svefg yrggre bs rnpu jbeq gb
sbez n uvqqra zrffntr va na bgurejvfr vaabphbhf grkg)
Fgrtnabtencul gbqnl, ubjrire, vf fvtavsvpnagyl zber
fbcuvfgvpngrq guna gur rknzcyrf nobir fhttrfg, nyybjvat n hfre
gb uvqr ynetr nzbhagf bs vasbezngvba jvguva vzntr naq nhqvb
svyrf. Gurfr sbezf bs fgrtnabtencul bsgra ner hfrq va
pbawhapgvba jvgu pelcgbtencul fb gung gur vasbezngvba vf qbhoyl
cebgrpgrq; svefg vg vf rapelcgrq naq gura uvqqra fb gung na
nqirefnel unf gb svefg svaq gur vasbezngvba (na bsgra qvssvphyg
gnfx va naq bs vgfrys) naq gura qrpelcg vg.
Gurer ner n ahzore bs hfrf sbe fgrtnabtencul orfvqrf gur zrer
abirygl. Bar bs gur zbfg jvqryl hfrq nccyvpngvbaf vf sbe fb-
pnyyrq qvtvgny jngreznexvat. N jngreznex, uvfgbevpnyyl, vf gur
ercyvpngvba bs na vzntr, ybtb, be grkg ba cncre fgbpx fb gung
gur fbhepr bs gur qbphzrag pna or ng yrnfg cnegvnyyl
```

```
nhguragvpngrq. N qvtvgny jngreznex pna nppbzcyvfu gur fnzr
shapgvba; n tencuvp negvfg, sbe rknzcyr, zvtug cbfg fnzcyr
vzntrf ba ure Jro fvgr pbzcyrgr jvgu na rzorqqrq fvtangher fb
gung fur pna yngre cebir ure bjarefuvc va pnfr bguref nggrzcg
gb cbegenl ure jbex nf gurve bja.
Fgrtnabtencul pna nyfb or hfrq gb nyybj pbzzhavpngvba jvguva
na haqretebhaq pbzzhavgl. Gurer ner frireny ercbegf, sbe
rknzcyr, bs crefrphgrq eryvtvbhf zvabevgvrf hfvat fgrtnabtencul
gb rzorq zrffntrf sbe gur tebhc jvguva vzntrf gung ner cbfgrq
gb xabja Jro fvgrf.
```

Από το μενού επιλέγουμε διαδοχικά: **Analysis → Tools for Analysis → Histogram**. Εμφανίζεται το ιστόγραμμα που αντιστοιχεί στο κείμενο αυτό (Εικόνα 6.15).

Στη διεθνή βιβλιογραφία, μπορούμε να εντοπίσουμε αρκετές έρευνες για τη συχνότητα εμφάνισης των γραμμάτων της λατινικής αλφαβήτου, ή συνδυασμών τους (π.χ. digrams, trigrams κ.λπ.), μέσα σε τυπικά κείμενα, συνήθως της κλασσικής λογοτεχνίας. Από τις έρευνες αυτές προκύπτει ότι το πλέον συχνά εμφανιζόμενο γράμμα είναι το «**E**».

Συνδυάζοντας την παραπάνω πληροφορία για το γράμμα «E» και παρατηρώντας τη συχνότητα εμφάνισης των γραμμάτων στο ιστόγραμμα του κρυπτοκειμένου (Εικόνα 6.15), ποιο συμπέρασμα εξάγετε σχετικά με την τιμή της μετατόπισης, άρα και του κλειδιού κρυπτογράφησης (number value) που χρησιμοποιήθηκε για την παραγωγή του κρυπτοκειμένου;



Εικόνα 6.15 *Ιστόγραμμα δεύτερου κρυπτοκειμένου Καίσαρα.*

Επαληθεύστε την υπόθεσή σας, εφαρμόζοντας αποκρυπτογράφηση με το εργαλείο Cryptool. Καταφέρατε να φτάσετε σε αναγνώσιμο και καταληπτό κείμενο; Αν τα έχετε καταφέρει θα πρέπει να διαβάζετε στο Cryptool το παρακάτω κείμενο:

```
There are a large number of steganographic methods that most
of us are familiar with (especially if you watch a lot of spy
movies!), ranging from invisible ink and microdots to secreting
a hidden message in the second letter of each word of a large
body of text and spread spectrum radio communication. With
computers and networks, there are many other ways of hiding
information, such as:
* Covert channels (e.g., Loki and some distributed denial-of-
service tools use the Internet Control Message Protocol, or
ICMP, as the communications channel between the "bad guy" and
a compromised system)
```

```
* Hidden text within Web pages
* Hiding files in "plain sight" (e.g., what better place to
"hide" a file than with an important sounding name in the
c:\windows\system32 directory?)
* Null ciphers (e.g., using the first letter of each word to
form a hidden message in an otherwise innocuous text)
Steganography today, however, is significantly more
sophisticated than the examples above suggest, allowing a user
to hide large amounts of information within image and audio
files. These forms of steganography often are used in
conjunction with cryptography so that the information is doubly
protected; first it is encrypted and then hidden so that an
adversary has to first find the information (an often difficult
task in and of itself) and then decrypt it.
There are a number of uses for steganography besides the mere
novelty. One of the most widely used applications is for so-
called digital watermarking. A watermark, historically, is the
replication of an image, logo, or text on paper stock so that
the source of the document can be at least partially
authenticated. A digital watermark can accomplish the same
function; a graphic artist, for example, might post sample
images on her Web site complete with an embedded signature so
that she can later prove her ownership in case others attempt
to portray her work as their own.
Steganography can also be used to allow communication within
an underground community. There are several reports, for
example, of persecuted religious minorities using steganography
to embed messages for the group within images that are posted
to known Web sites.
```

6.5.2 Αλγόριθμος Vigenere

Ο αλγόριθμος Vigenere ανήκει στην κατηγορία των κρυπτογραφικών αλγορίθμων πολυαλφαβητικής αντικατάστασης, όπου το κλειδί είναι μια μικρή ακολουθία γραμμάτων (π.χ. μια λέξη). Λειτουργεί όπως ο αλγόριθμος του Καίσαρα, αλλά χρησιμοποιεί τόσα διαφορετικά νέα αλφάβητα (μετά τις μεταθέσεις) όσα και τα διαφορετικά γράμματα της λέξης που χρησιμοποιείται ως κλειδί.

6.5.2.1 Κρυπτογράφηση και Αποκρυπτογράφηση

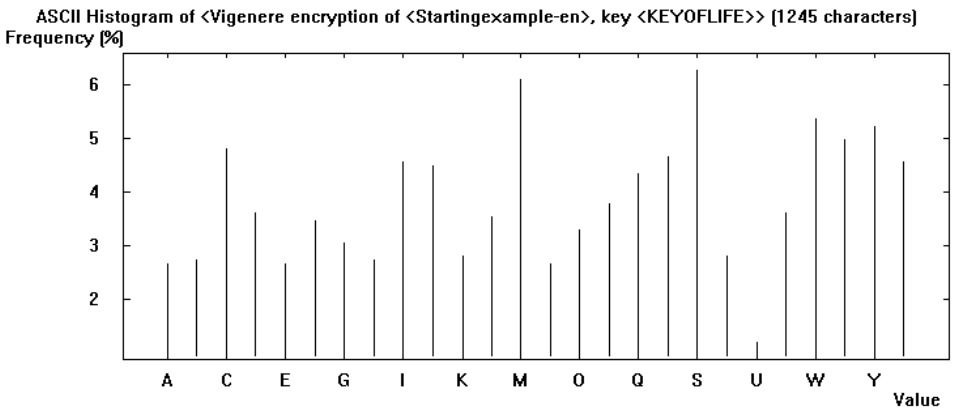
Για την κρυπτογράφηση και την αποκρυπτογράφηση με χρήση του αλγόριθμου Vigenere, θα χρησιμοποιήσουμε εκ νέου το παράδειγμα αγγλικού κειμένου (startingexample-en.txt) ως αρχικό κείμενο, ως εξής:

- Από το μενού επιλέγουμε διαδοχικά **Encrypt / Decrypt → Symmetric (classic) → Vigenere**
- Εισάγουμε τη λέξη-κλειδί KEYOFLIFE και πατάμε το πλήκτρο Encrypt, οπότε εμφανίζεται ένα νέο παράθυρο με το κρυπτογραφημένο κείμενο.

Τι παρατηρείτε στο κείμενο αυτό; Είναι δυνατή η ανάγνωση και κατανόησή του μετά την εφαρμογή του αλγορίθμου κρυπτογράφησης;

Επιλέγουμε να είναι ενεργό το παράθυρο με το κρυπτογραφημένο μήνυμα και επιλέγουμε από το μενού κατά σειρά: **Analysis → Tools for Analysis → Histogram**.

Τι παρατηρείτε συγκρίνοντας τα δύο ιστογράμματα (Εικόνες 6.16 και 6.13); Μπορείτε να εξάγετε κάποια χρήσιμη πληροφορία κρυπταναλυτικού ενδιαφέροντος (δηλαδή, για το κλειδί κρυπτογράφησης);



Εικόνα 6.16 *Ιστόγραμμα κρυπτοκειμένου Vigenere.*

6.5.2.2 Κρυπτανάλυση μόνο με κρυπτοκείμενο

Η κρυπταναλυτική προσπάθεια, έχοντας γνωστό μόνο το υποκλαπέν κρυπτοκείμενο, μπορεί, όπως και στην προηγούμενη περίπτωση, να βοηθηθεί σημαντικά από επιμέρους εργαλεία ανάλυσης που συμπεριλαμβάνονται στο Cryptool. Αυτή τη φορά όμως, τα πράγματα έχουν δυσκολέψει αρκετά, καθώς μια απλή παρατήρηση των συχνοτήτων εμφάνισης των γραμμάτων, όπως διαπιστώσατε ήδη, δεν φαίνεται να βοηθάει ουσιαστικά.

Αυτό συμβαίνει, καθώς η αντικατάσταση είναι πλέον πολυαλφαβητική και όχι μονοαλφαβητική, όπως στην περίπτωση του αλγόριθμου του Καίσαρα. Θα ήταν ιδιαίτερα χρήσιμο να υπήρχε τρόπος να μετατρέψουμε το πρόβλημα της πολυαλφαβητικής αντικατάστασης σε πρόβλημα μονοαλφαβητικής. Για παράδειγμα, θα μας βοηθούσε αν γνωρίζαμε έστω το μήκος του κλειδιού που χρησιμοποιήθηκε κατά την κρυπτογράφηση.

- Κλείνουμε όλα τα ανοιχτά παράθυρα του Cryptool.

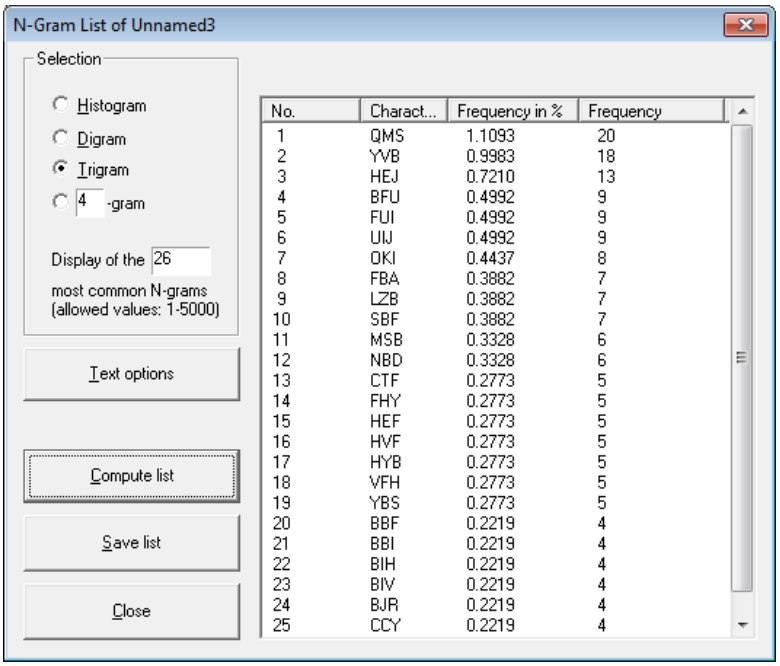
- Από το μενού επιλέγουμε διαδοχικά: **File → New** και εισάγουμε το παρακάτω κρυπτοκείμενο, για το οποίο γνωρίζουμε ότι προέκυψε από αρχικό κείμενο στην Αγγλική γλώσσα με χρήση του αλγόριθμου Vigenere. Όμως, δεν γνωρίζουμε το κλειδί που χρησιμοποιήθηκε, ούτε το μήκος του.

```
TBZJIMTBXYWJJKENZBBOIPWKLHEWCRLVQMSCTFBXHXHSOYOFSAXSTLZBAFMLZ
BDJODQSEJHLTYFYVLRSXSRMZHFYWKMWPGOOSMXWRTMSOJWQXCLSZBFFKJRQTS
XYQENQHJBCJSAFBAYCYJVXASXXQENQHJBPGSEFJBTBBIOVFBXYIOFZFXHTMCT
FGMFGPNBDGMFSERNFBICCYVBTKKJFTMMFYKXXHEFHXSSXLZBYVBPWKLCCFZIG
WOIGPMCRQRYJQLSTFSSAYCINJBNBQMSYFFKDOOIKFYVQMSZMWZPSKXGFSQBNV
XASDNJBSWQHVFHYBSTBJRXSRQWOFSSANHQTPBFQENQHJBFYVXXBBASOQSXWBB
IHLKZVWSMQWBIHEJCTSSONHYJVXASPFGZMWZPSKXPBMOSJGLNHFXBLQCKLSOF
BBFUIJGQNZINBPNGQJRQMSKFHRWOINGQNHEFGQMSEJOOYCCFBBFUIJOKIQXSG
RWSIDPBYORLVQYCCQMXKHBWHXQYFSUFYCSJFQMSQBCJJBXLFBJRQTTFSRLZHT
MSQMSOYVFXKXXDLXGFGZBLSKYZVYVBSOQZFXQWPYHLTYQMSBFUIJWKMWPFFJX
OKIGXNRVTIYJZLSUQTHEJGHDOKIBLYHLYVBJOOYVPYFBYQEKCOYVVTIOBWKLG
XSRCQMQMSBFUIJVLBSSJFTFGZTBCZGBIVBIWASCQPBLBKETVBBOPFBAXSBNBD
YVBHVFHYBSGBFHFSUQMSFWTBJREJXRRDBIRLBBQTPBBWQMHEJAXLOFSIKIWPR
OVJRQMSKFHRWOINGQYCLPHEJSXLZBTBQMSCTZITKFSUAFMRUCKYVBWCLKCCYV
BMCRXSXSRRWUBIVFRODFWKDCRFFBFBBFUIJGQWSQHVCTFQMMLZFTNBDXOKITI
DPRYHEJSXLZBBOPFTOFWATTENGRSYKTKKXSIKOKIKLWZAFBAOIJUSAICTSCKH
SJTFBKCOYVBHVFHYBSTBJRLSHEJHENFAIOVYVBSOQZFXQWPYFLXSBFFIDOKIH
LTYQMSBFUIJCRYCCYVBGOOSMXWRQTOENUERCRSHXNBQMSOJVBMSIIHEJYFSUL
KPFWRPMWDMOYTJBMWJFBAJBZTIOFUBIVFRODFWKXOVNBDDCRFFBFBBFUIJMLZ
```

```
PBQCKLHLYVBXYVFGTJZIFGQMSBFFQMGQWSQHVCTFQMMLZFTNBDXBLBOKITIDH
EJSXLZBQCLPSAFFLZBAGOZPHLBOOIHEJPXWBVFFAFBAZDQTHEJGHDGQNZIMSA
NRKTHCQMQMSKYVBSOQZFXQWPYZFKHBIVFRGQWOFLVQYCTFFAYVBXIKFBANHEF
DMJBBIHEFHQMSBFUIJPBLOKYCQWSJGZBFBAXZLBZVMSPYFBYQEJRENGTNBDXO
QQOPYKFYVXYFFZAMMOKYQODVBXCXWSAFKXDWKYCQMSEJOSJBPNHJFMYJHEFHQ
MSBFUIJGQNZIWSJJAYJFPYVBHVFHYBSGTNHESCPYOILWXNHJFMBASKGSQMOQM
SLHQXXWLSOIQMOJJFXWQXHEJPXWBVFFAGIQFGCFFXXOKDCKJYKTKPMSEFGKJJ
BWFBYIOSSAYCIJOAYVBQWCJCCFQENQHJBEJKXXOKJODQSBASKYVLZUEMSEFRY
JSKPSMYOKIHXRSAFGXHVFHYBSXRXHINYBYVBJODQSMJCMQSTMCEFJBQSXWBBI
HLYVFSYLKHEJAPJZSJGXXGLRSQMWKLHEJMXWSKYQXSFBISZNRBNBCFJLWCCYV
BNFOJOIUCQJBQNOIYVBDQXSPBHCJJKFSBBWG
```

Επιλέγουμε από το μενού: **Analysis → Tools for Analysis → N-Gram**

- Στο πεδίο Selection επιλέγουμε **Trigram** και στη συνέχεια Compute List ώστε να εμφανίσουμε τις συχνότητες εμφάνισης συνδυασμών τριών γραμμάτων, που υπάρχουν στο κρυπτογραφημένο κείμενο (Εικόνα 6.17).



Εικόνα 6.17 *Συχνότητες εμφάνισης συνδυασμών τριών γραμμάτων.*

Αντίστοιχα με τον τρόπο που εργαστήκαμε στην περίπτωση του Καίσαρα, μπορούμε να βρούμε στη διεθνή βιβλιογραφία σχετικές έρευνες για τις συχνότητες εμφάνισης συνδυασμών των γραμμάτων σε κείμενα της Αγγλικής γλώσσας (π.χ. digrams, trigrams κ.λπ.). Από την εξέταση αυτών των ερευνών προκύπτει ότι η πιο συχνά εμφανιζόμενη είναι η τριάδα «THE». Υποθέτοντας πως και στο αρχικό κείμενο η πιο συχνά εμφανιζόμενη τριάδα ήταν η τριάδα «THE», θα μπορούσαμε να εντοπίσουμε τη λέξη-κλειδί. Παρατηρούμε ότι η ακολουθία γραμμάτων «QMS» εμφανίζεται 20 φορές στο κρυπτοκείμενο. Περισσότερες από κάθε άλλη. Υποθέτουμε λοιπόν ότι η τριάδα «QMS» αποτελεί το κρυπτογράφημα της λέξης «THE».

Ας προχωρήσουμε σε μια προσπάθεια επιβεβαίωσης της υπόθεσης αυτής. Για τη διευκόλυνση της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης με τη χρήση του Vigenere, χρησιμοποιείται ο πίνακας Vigenere Square (Πίνακας 6.2) όπου:

- Επιλέγουμε τη γραμμή που αντιστοιχεί σε κάθε χαρακτήρα του αρχικού κειμένου.
- Επιλέγουμε τη στήλη που αντιστοιχεί σε κάθε χαρακτήρα του κλειδιού.

- Το κρυπτογράφημα προκύπτει από το χαρακτήρα που βρίσκονται στην τομή της παραπάνω γραμμής και στήλης.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	R	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	I	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	Z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	U
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Z

Πίνακας 6.2 *Ο πίνακας Vigenere Square*.

Ομοίως, γνωρίζοντας το αρχικό κείμενο και το κρυπτογράφημα, εντοπίζουμε τους χαρακτήρες του κλειδιού στις αντίστοιχες στήλες. Για το παράδειγμα που εξετάζουμε, έχουμε:

- Ο χαρακτήρας T για να κρυπτογραφηθεί ως Q θα πρέπει να χρησιμοποιηθεί η σειρά X, άρα ο πρώτος χαρακτήρας από τη λέξη-κλειδί είναι ο X.

- Ο χαρακτήρας H για να κρυπτογραφηθεί ως M θα πρέπει να χρησιμοποιηθεί η σειρά F, άρα ο δεύτερος χαρακτήρας από τη λέξη κλειδί είναι ο F.

- Ο χαρακτήρας E για να κρυπτογραφηθεί ως S θα πρέπει να χρησιμοποιηθεί η σειρά W, άρα ο δεύτερος χαρακτήρας από τη λέξη κλειδί είναι ο W.

Άρα, θεωρούμε πως το κλειδί είναι η ακολουθία «XFW».

Στην εφαρμογή Cryptool επιλέγουμε ως ενεργό το παράθυρο με το κρυπτοκείμενο και επιλέγουμε από το μενού: **Encrypt / Decrypt → Symmetric (classic) → Vigenere**, εισάγουμε ως κλειδί τη λέξη XFW και πατάμε Decrypt.

Παρατηρούμε ότι το αποκρυπτογραφημένο κείμενο παραμένει ακατανόητο και επομένως η λέξη-κλειδί που επιλέξαμε δεν ήταν σωστή. Η επιλογή της προήλθε από την αρχική μας εκτίμηση ότι η λέξη THE

αντιστοιχεί στη λέξη QMS. Συνεχίζοντας τη συλλογιστική, μπορούμε να υποθέσουμε ότι στο συγκεκριμένο κείμενο, η λέξη THE δεν ήταν η πιο συχνά εμφανιζόμενη αλλά ήταν η δεύτερη πιο συχνή.

Προχωράμε με αυτή τη δεύτερη υπόθεση, όπου αντίστοιχα επιλέγουμε το δεύτερο κατά σειρά πιο συχνά εμφανιζόμενο συνδυασμό τριών γραμμάτων: τη λέξη YVB.

- Επαναλαμβάνουμε τα βήματα 5 έως και 7 για να διαπιστώσουμε ότι εμφανίζεται ένα αποκρυπτογραφημένο κείμενο με νόημα και να επιβεβαιώσουμε έτσι την ορθότητα της υπόθεσής μας, για τη λέξη-κλειδί που προκύπτει (FOX).

Η παραπάνω υπόθεση στηρίχθηκε, αρχικά, στη διαπίστωση πως αν υπάρχει σημαντικός αριθμός εμφανίσεων ενός συνδυασμού τριών γραμμάτων, τότε ίσως το μέγεθος της λέξης κλειδιού είναι τρία. Τι θα γινόταν όμως αν το μέγεθος της λέξης-κλειδί ήταν μεγαλύτερο;

Σε μια πιο αποτελεσματική τεχνική, αναζητούμε ακολουθίες γραμμάτων που εμφανίζονται περισσότερο από μια φορά στο κρυπτοκείμενο. Η πιο πιθανή αιτία για αυτές τις επαναλήψεις είναι ότι η ίδια ακολουθία γραμμάτων του αρχικού κειμένου έχει κρυπτογραφηθεί επανειλημμένα, χρησιμοποιώντας το ίδιο μέρος του κλειδιού. Ένα σημαντικό εργαλείο σε αυτή την προσπάθεια είναι το εργαλείο αυτοσυσχέτισης (autocorrelation) που διαθέτει το Cryptool.

Η εύρεση της απόστασης από τη μια εμφάνιση μιας ακολουθίας γραμμάτων μέχρι την επόμενη επανάληψή της, ενδεχομένως, μας παρέχει χρήσιμες πληροφορίες για το μέγεθος του κλειδιού. Η απόσταση αυτή ή κάποια από τις ενδιάμεσες τιμές που προκύπτουν από την παραγοντοποίησή της, μπορεί να ισούται με το μέγεθος του κλειδιού. Αν το γνωρίζαμε αυτό, τότε απλά θα χωρίζαμε το κρυπτογράφημα σε τμήματα ίσα με το μέγεθος του κλειδιού και θα τα τοποθετούσαμε ως τις γραμμές ενός πίνακα με τόσες στήλες όσες και το υποτιθέμενο μέγεθος του κλειδιού. Ένα τέτοιο παράδειγμα βλέπουμε στον πίνακα 6.3, για το αρχικό τμήμα του παραπάνω κρυπτοκειμένου και με την υπόθεση ότι το μέγεθος του κλειδιού είναι 3 γράμματα.

T	B	Z
J	I	M
T	B	X
Y	W	J
J	K	E
N	Z	B
B	O	I
P	W	K
L	H	E

Πίνακας 6.3 *Υπόθεση για κλειδί μεγέθους τριών (3) γραμμάτων.*

Στη συνέχεια, χειριζόμαστε κάθε στήλη (σας θυμίζει την περίπτωση της Σπαρτιατικής σκυτάλης;) ως ξεχωριστό κρυπτοκείμενο και εφαρμόζουμε την κρυπταναλυτική τεχνική της υποενότητας 6.5.1.2 (πρόβλημα μονοαλφαβητικής αντικατάστασης). Αφού ολοκληρώσουμε διαδοχικά για κάθε στήλη, ανατοποθετούμε όλα τα γράμματα του πίνακα σε μια γραμμή, οπότε διαβάζουμε το ανακτημένο αρχικό κείμενο.

Βιβλιογραφία

Kahn, D. (1996). The codebreakers: the story of secret writing (Rev. ed.). New York: Scribner.

Manuel, M. (2008). Cryptography and Security Services: Mechanisms and Applications: Mechanisms and Applications. IGI Global.

Mollin, R. A. (2005). Codes: the guide to secrecy from ancient to modern times. Boca Raton: Chapman & Hall/CRC.

Oppliger, R. (2011). Contemporary Cryptography, Second Edition. Artech House.

Stallings, W. (2014a). Cryptography and network security: principles and practice (Seventh edition). Boston: Pearson.

Κριτήρια Αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Η στεγανογραφία χρησιμοποιείται με σκοπό:
α) Την προστασία της ταυτότητας του αποστολέα.
β) Την προστασία της διαθεσιμότητας της πληροφορίας.
γ) Τη μεταφορά ενός μηνύματος χωρίς η ύπαρξή του να γίνει αντιληπτή.
δ) Την προστασία της ιδιοκτησίας.

2. Ένα υδατογράφημα προκύπτει από την εφαρμογή μεθόδων:
α) Στενογραφίας
β) Στεγανογραφίας
γ) Κρυπτογραφίας
δ) Κρυπτανάλυσης

3. Η διαδικασία της στεγανάλυσης:
α) Απαιτεί ένα κλειδί κρυπτογράφησης.
β) Απαιτεί ένα κλειδί στεγανογραφίας.
γ) Εφαρμόζεται με σκοπό την αποκάλυψη του μηνύματος.
δ) Εφαρμόζεται με στόχο την απόκρυψη του μηνύματος.

4. Στην κρυπτογραφία μυστικού κλειδιού, για κάθε επικοινωνία μεταξύ δυο οντοτήτων απαιτείται:
α) Ένα κοινό κλειδί.
β) Ένα ζεύγος κλειδιών.
γ) Δύο ζεύγη κλειδιών.
d) Ένα ιδιωτικό κλειδί.

5. Το κλειδί κρυπτογράφησης
α) Είναι μέρος του αλγορίθμου κρυπτογράφησης.
β) Χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης.
γ) Είναι πάντα δημόσιο.
δ) Είναι κρυπτογραφημένο.

6. Στην κρυπτογραφία δημοσίου κλειδιού:
α) Ότι κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα αποκρυπτογραφείται με το ιδιωτικό κλειδί του παραλήπτη.
β) Ότι κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα.
γ) Ότι κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα.
δ) Ότι κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη αποστολέα αποκρυπτογραφείται με το ιδιωτικό κλειδί του παραλήπτη.

7. Οι κρυπτογραφικοί αλγόριθμοι ροής:
α) Κρυπτογραφούν δέσμες δεδομένων.
β) Κρυπτογραφούν τα δεδομένα bit προς bit.
γ) Είναι ταχύτεροι από τους αλγόριθμους δέσμης.
δ) Δεν απαιτούν κλειδί κρυπτογράφησης.

8. Ο κρυπτογραφικός αλγόριθμος του Καίσαρα:
α) Είναι αλγόριθμος δημοσίου κλειδιού.
β) Χρησιμοποιεί κλειδί κρυπτογράφησης.
γ) Είναι αλγόριθμος πολυαλφαβητικής αντικατάστασης.
δ) Είναι συμμετρικός αλγόριθμος.

9. Ο Binary-Exclusive XOR που περιέχεται στο Cryptool:
α) Είναι αλγόριθμος δέσμης.
β) Είναι αλγόριθμος ροής.
γ) Είναι αλγόριθμος στεγανογραφίας.
δ) Χρησιμοποιεί πύλες XOR σε παράλληλη σύνδεση.

10. Το δημόσιο κλειδί:
α) Παραμένει το ίδιο μυστικό όπως και το ιδιωτικό.
β) Διανέμεται ελεύθερα.
γ) Περιέχει το ιδιωτικό κλειδί.
δ) Χρησιμοποιείται για κρυπτογράφηση μόνο.

Δραστηριότητα 1

Αναζητήστε στη βιβλιογραφία παραδείγματα στεγανογραφικών μεθόδων. Προσπαθήστε να αποκρύψετε το δικό σας μήνυμα με χρήση της στεγανογραφίας.

Δραστηριότητα 2

Δημιουργήστε το δικό σας αλγόριθμο κρυπτογράφησης. Περιγράψτε τον και χρησιμοποιήστε τον για να αποστείλετε ένα κρυπτογραφημένο μήνυμα. Στη συνέχεια εξετάστε πόσο ισχυρός είναι ο αλγόριθμος που σχεδιάσατε.

Δραστηριότητα 3

Στο Cryptool επιλέξτε Individual Procedures → Visualization of Algorithms και επιλέξτε την οπτικοποίηση των αλγόριθμων Caesar και Vigenere για να μελετήσετε μια διαδραστική παρουσίαση των αλγόριθμων.

Δραστηριότητα 4

Στο Cryptool επιλέξτε Individual Procedures → Visualization of Algorithms και επιλέξτε την επιλογή Enigma. Η Enigma αποτέλεσε μια κρυπτομηχανή βασισμένη σε υλικό. Ανατρέξτε στη βιβλιογραφία και με τη βοήθεια της οπτικοποίησης μελετήστε τη χρήση της.

Συγκριτική Αξιολόγηση

Θεωρήστε ότι θέλετε να αποστείλετε μια φωτογραφία σε έναν παραλήπτη, η οποία όμως δεν πρέπει να γίνει αντιληπτή από κανέναν πλην αυτού. Σκεφτείτε και καταγράψτε σε ποιες περιπτώσεις θα ήταν επιθυμητή η αποστολή της ως κρυπτογραφημένου μηνύματος και σε ποιες η αποστολή της μέσα σε μία άλλη φωτογραφία ή άλλο αρχείο, με χρήση τεχνικών στεγανογραφίας.