3 ΟΙ ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΙ ΚΑΙ ΟΙ ΙΔΙΟΤΗΤΕΣ ΤΟΥΣ

3.1. Θεωρία της πληροφορίας

Το 1948 και το 1949 ο Shannon παρουσίασε δύο εργασίες ορόσημα στις επικοινωνίες και στην ασφάλεια της πληροφορίας. Στο σημείο αυτό θα παρουσιάσουμε τις βασικές ιδέες της θεωρίας του.

3.1.1. Υποδομή: πιθανότητες και πληροφορία

Θεωρούμε μια πηγή πληροφορίας X η οποία μπορεί να παράγει n σύμβολα από το σύνολο $\boldsymbol{F} = \{x_1, x_2, \ldots, x_n\}$. Το σύνολο αυτό αποτελεί το αλφάβητο της πηγής X. Έστω $p(x_i)$ η πιθανότητα εμφάνισης του συμβόλου x_i, για $1 \le i \le n$. Το σύνολο με στοιχεία τις πιθανότητες όλων των συμβόλων αποτελεί την κατανομή πιθανότητας της πηγής X:

$$\{p(x_1), p(x_2), \ldots, p(x_n)\}$$

όπου φυσικά:

$$\sum_{i=1}^{n} p(x_i) = 1 .$$

Θεωρούμε αντίστοιχα και μια δεύτερη πηγή πληροφορίας Y με αλφάβητο $\boldsymbol{G} = \{y_1, y_2, \ldots, y_m\}$ και κατανομή πιθανότητας:

$$\{q(y_1), q(y_2), \ldots, q(y_m)\} .$$

Η πιθανότητα όπου η πηγή X παράγει ένα σύμβολο x_i ενώ ταυτόχρονα η πηγή Y παράγει ένα σύμβολο y_j, ονομάζεται ***από κοινού πιθανότητα*** (joint probability) και συμβολίζεται με $p(x_i, y_j)$. Εάν οι πηγές X και Y είναι ανεξάρτητες, τότε:

$p(x_i, y_j) = p(x_i)q(y_j)$, για κάθε i, j.

Η πιθανότητα όπου η πηγή X παράγει ένα σύμβολο x_i δοθέντος ότι η πηγή Y παράγει ένα σύμβολο y_j, ονομάζεται ***δεσμευμένη*** ή ***υπό συνθήκη πιθανότητα*** (conditional probability), $p(x_i \mid y_j)$, όπου:

$$p(x_i \mid y_j) = \frac{p(x_i, y_j)}{q(y_j)}, \text{ με } q(y_j) > 0.$$

Η υπό συνθήκη πιθανότητα υποδηλώνει την εξάρτηση της πηγής X από την πηγή Y. Είναι φανερό πως εάν οι πηγές είναι ανεξάρτητες, τότε:

$$p(x_i \mid y_j) = p(x_i).$$

Παρόμοια ορίζεται και η εξάρτηση της πηγής Y από την πηγή X με την υπό συνθήκη πιθανότητα:

$$q(y_j \mid x_i) = \frac{p(x_i, y_j)}{p(x_i)}, \text{ με } p(x_i) > 0.$$

ΟΡΙΣΜΟΣ 3.1 – (Πληροφορία κατά Shannon). Η ποσότητα της πληροφορίας ή αβεβαιότητας με βάση μια πηγή πληροφορίας X, ορίζεται ως:

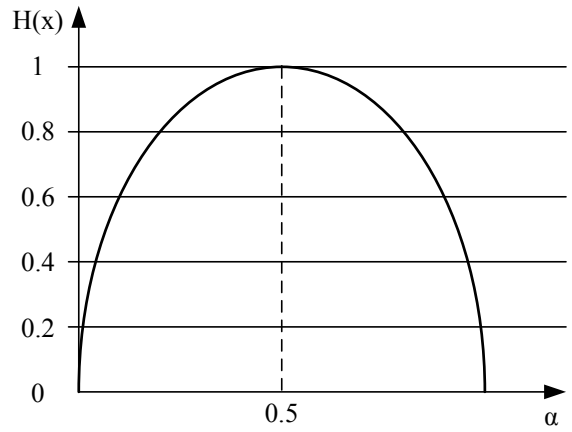
$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i) \ .$$

Δηλαδή, σύμφωνα με τον Shannon, η πληροφορία που περιέχει ένα γεγονός μπορεί να μετρηθεί σχετίζοντάς την άμεσα με την πιθανότητα που έχει αυτό το γεγονός να πραγματοποιηθεί (ή να εμφανισθεί). Έτσι η πληροφορία και η αβεβαιότητα καθίστανται δυο ταυτόσημες έννοιες.

ΠΑΡΑΔΕΙΓΜΑ 3.1 – Δυαδική πηγή πληροφορίας. Έστω ότι η πηγή παράγει σύμβολα από το αλφάβητο δύο συμβόλων $\{0,1\}$, με $p(0) = a$ και $p(1) = 1 - a$. Τότε η αβεβαιότητα της πηγής θα είναι:

$$H(X) = -a \log_2 a - (1-a) \log_2 (1-a).$$

Εάν παραστήσουμε τις τιμές της συνάρτησης $H(X)$ ως προς το a, θα έχουμε την καμπύλη του Σχήματος 3.1. Η καμπύλη αυτή συμφωνεί με τη διαίσθησή μας σχετικά με την αβεβαιότητα. Εάν η πιθανότητα a είναι 0 ή 1, τότε η πηγή θα παράγει μόνον **1** ή **0** αντίστοιχα. Εάν γνωρίζουμε ότι η πηγή πάντα θα παράγει το ίδιο σύμβολο, τότε η αβεβαιότητα θα είναι μηδενική. Αντίθετα, στην περίπτωση όπου η πιθανότητα είναι 0.5, τότε η αβεβαιότητα θα είναι και η μέγιστη, αφού δεν θα είμαστε σε θέση να γνωρίζουμε πιο σύμβολο θα εμφανιστεί οποιαδήποτε χρονική στιγμή. Στην περίπτωση που η πιθανότητα είναι μεταξύ των διαστημάτων (0, 0.5) ή (0.5, 1), γνωρίζουμε απλώς ότι ένα σύμβολο θα εμφανίζεται πιο συχνά από το άλλο, οπότε και η αβεβαιότητα είναι μικρότερη.



Σχήμα 3.1 Γραφική παράσταση της αβεβαιότητας μιας πηγής δύο συμβόλων.

Σε συμφωνία με την από κοινού πιθανότητα που αναφέρθηκε παραπάνω, ορίζεται η από κοινού αβεβαιότητα ή πληροφορία ως εξής:

ΟΡΙΣΜΟΣ 3.2 – Η ***από κοινού αβεβαιότητα*** δύο πηγών X και Y ορίζεται ως η ποσότητα:

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j)\log_2 p(x_i, y_j),$$

όπου $p(x_i, y_j)$ η από κοινού πιθανότητα παραγωγής του συμβόλου x_i και του συμβόλου y_j από τις πηγές X και Y, αντίστοιχα.
Εάν οι πηγές X και Y είναι ανεξάρτητες, τότε:

$$\begin{aligned} H(X,Y) &= -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i)q(y_j)\log_2(p(x_i)q(y_j)) \\ &= -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i)q(y_j)\log_2 p(x_i) - \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i)q(y_j)\log_2 q(y_j) \\ &= -\sum_{j=1}^{m} q(y_j)\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) - \sum_{i=1}^{n} p(x_i)\sum_{j=1}^{m} q(y_j)\log_2 q(y_j) \\ &= H(X) + H(Y). \end{aligned}$$

Αντίστοιχα ορίζεται και η υπό συνθήκη αβεβαιότητα, σε σχέση με την υπό συνθήκη πιθανότητα $p(x_i|y_j)$:

ΟΡΙΣΜΟΣ 3.3 – Η ***υπό συνθήκη αβεβαιότητα*** δύο πηγών X και Y ορίζεται ως η ποσότητα:

$$H(X \mid Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j)\log_2 p(x_i \mid y_j).$$

Αποδεικνύεται ότι:

$$H(X,Y) = H(X) + H(Y \mid X) = H(Y) + H(X \mid Y).$$

Με βάση τα παραπάνω, αποδεικνύονται οι ακόλουθες σχέσεις για τρεις πηγές *X,Y,Z*:

$H(\varnothing) = 0$	«Δεν υπάρχει αβεβαιότητα στο κενό σύνολο γεγονότων»
$H(X) \geq H(X \mid Y)$ $H(X \mid Y) \geq H(X \mid Y,Z)$	«Η αβεβαιότητα μειώνεται όσο μαθαίνουμε»
$H(X \mid Y) \leq H(X,Z \mid Y)$	«Η αβεβαιότητα αυξάνεται με την αύξηση του πλήθους των στοιχείων του συνόλου των γεγονότων»
$H(X,Y \mid Z) = H(X \mid Y,Z) + H(Y \mid Z)$	«Τα σύνολα των γεγονότων έχουν αθροιστική σχέση μεταξύ τους ως προς την αβεβαιότητα»

Επιπλέον, μια ποσότητα με ιδιαίτερο ενδιαφέρον είναι η ***αμοιβαία πληροφορία*** (mutual information) η οποία ορίζεται ως η διαφορά:

$$I(X;Y) = H(X) - H(X \mid Y).$$

Η αμοιβαία πληροφορία αποκαλύπτει εάν και πόσο μειώνεται η αβεβαιότητα του *X*, εάν γνωστοποιηθεί το *Y*. Από πλευράς ασφάλειας αυτή η ποσότητα είναι πολύ σημαντική γιατί χρησιμοποιείται στη μέτρηση της διαρροής πληροφορίας.

Οι σχέσεις αυτές και γενικότερα η θεωρία της πληροφορίας είναι ένα αποτελεσματικό εργαλείο στη ανάλυση των συστημάτων για τη μετάδοση και αποθήκευση της πληροφορίας. Η ανάλυση της ασφάλειας των κρυπτοσυστημάτων από πλευράς θεωρίας της πληροφορίας μπορεί να βοηθήσει τον κρυπτογράφο στη σχεδίαση ενός κρυπτοσυστήματος, συνεισφέροντας στην κατανόηση του επιπέδου ασφάλειας αυτού. Ένα από τα πιο αντιπροσωπευτικά παραδείγματα είναι αυτό της δημιουργίας και της απόδειξης ενός άνευ όρων ασφαλούς κρυπτοσυστήματος, που παραθέτουμε σε επόμενη ενότητα.

3.1.2. Η θεωρία της πληροφορίας και το κρυπτοσύστημα

Προκειμένου να μελετήσουμε ένα κρυπτοσύστημα από πλευράς θεωρίας της πληροφορίας, θεωρούμε τρεις πηγές που αντιστοιχούν στο απλό κείμενο *P*, στο κλειδί *K* και στο κρυπτοκείμενο *C*. Τα σύμβολα που παράγει η κάθε πηγή προέρχονται από τα αντίστοιχα σύνολα συμβόλων των *P*, *K* και *C*.

Αρχικά μπορούμε να δηλώσουμε τις ακόλουθες αβεβαιότητες:

$H(K) \le H(K \mid P)$	«διαρροή πληροφορίας κλειδιού από το απλό κείμενο»
$H(K) \le H(K \mid C)$	«διαρροή πληροφορίας κλειδιού από το κρυπτοκείμενο»
$H(C) \le H(C \mid P)$	«διαρροή πληροφορίας κρυπτοκειμένου από το απλό κείμενο»
$H(C) \le H(C \mid K)$	«διαρροή πληροφορίας κρυπτοκειμένου από το κλειδί»
$H(P) \le H(P \mid K)$	«διαρροή πληροφορίας απλού κειμένου από το κλειδί»
$H(P) \le H(P \mid C)$	«διαρροή πληροφορίας απλού κειμένου από το κρυπτοκείμενο»

Για να είναι δυνατή η κρυπτογράφηση, θα πρέπει να γνωρίζουμε το απλό κείμενο και το κλειδί. Η γνώση αυτών των δύο οδηγεί σε ένα και μόνο κρυπτοκείμενο, δηλαδή:

$$H(C \mid P, K) = 0 .$$

Παρόμοια, για να είναι δυνατή η αποκρυπτογράφηση, απαιτείται η γνώση του κρυπτοκειμένου, του κλειδιού, και επίσης θα πρέπει το κρυπτοσύστημα να είναι ενριπτικό (injective), δηλαδή:

$$H(P \mid C, K) = 0 .$$

Με βάση τις παραπάνω αβεβαιότητες που διέπουν ένα κρυπτοσύστημα, αποδεικνύεται ότι:

- για την κρυπτογράφηση ισχύει:

$$H(C \mid K) \le H(P \mid K) ,\ H(C \mid P) \le H(K \mid P)$$

- για την αποκρυπτογράφηση ισχύει:

$$H(P \mid C) \le H(K \mid C) ,\ H(P \mid K) \le H(C \mid K)$$

Σε ένα κρυπτοσύστημα όπου το κρυπτοκείμενο και το απλό κείμενο έχουν το ίδιο μήκος, θα πρέπει να ισχύουν συγχρόνως όλες οι σχέσεις, γεγονός που οδηγεί στην ισότητα:

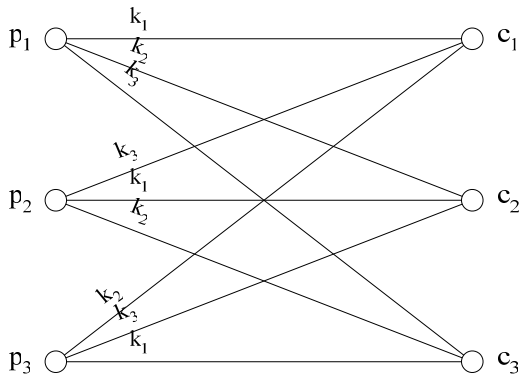
$$H(C \mid K) = H(P \mid K) ,$$

δηλαδή όταν είναι γνωστό το κλειδί η αβεβαιότητα του απλού κειμένου είναι ίδια με αυτήν του κρυπτοκειμένου.

3.1.3. Τέλεια μυστικότητα

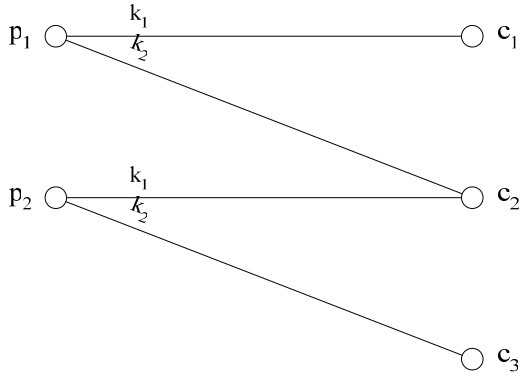
Η έννοια ενός τέλεια μυστικού (perfect secret) συστήματος σχετίζεται με το άνευ όρων ασφαλές κρυπτοσύστημα. Αν θεωρήσουμε ένα κρυπτοσύστημα με 3 σύμβολα απλού κειμένου, τα οποία αντιστοιχίζονται σε 3 σύμβολα κρυπτοκειμένου με βάση το κλειδί, τότε η τέλεια μυστικότητα θα είναι αυτή όπως φαίνεται στο Σχήμα

3.2. Το κλειδί μπορεί να πάρει 3 τιμές, οπότε ανάλογα με την τιμή το σύμβολο του απλού κειμένου p_i, μπορεί να κρυπτογραφηθεί ως c_1, c_2 ή c_3.



Σχήμα 3.2 Τέλεια μυστικότητα (Shannon (1949)).

Στην περίπτωση όμως που το κλειδί είναι μικρότερο, δηλαδή μπορεί να πάρει λιγότερες τιμές, το σύμβολο του απλού κειμένου p_i δεν θα μπορεί να κρυπτογραφηθεί σε οποιοδήποτε από τα c_1, c_2 ή c_3, αλλά μόνον σε τόσα σύμβολα, όσες είναι οι δυνατές τιμές του κλειδιού. Αυτή η μείωση των επιλογών δίνει πολύτιμη πληροφορία στον αντίπαλο ως προς τα υποψήφια σύμβολα του απλού κειμένου. Ένα τέτοιο κρυπτοσύστημα δεν προσφέρει τέλεια μυστικότητα. Στο παράδειγμα του Σχήματος 3.3, το p_2 μπορεί να κρυπτογραφηθεί μόνον ως c_2 ή c_3, οπότε όταν ο αντίπαλος συναντήσει το σύμβολο c_1, αποκλείει την πιθανότητα το απλό κείμενο να είναι το p_2.



Σχήμα 3.3 Μη τέλεια μυστικότητα.

Για να χαρακτηρισθεί ένα κρυπτοσύστημα ως άνευ όρων ασφαλές, θα πρέπει να προσφέρει τέλεια μυστικότητα, διότι στην αντίθετη περίπτωση το κρυπτοκείμενο «προδίδει» πληροφορίες σχετικά με το κλειδί η το απλό κείμενο. Όπως θα δούμε, τα άνευ όρων ασφαλή συστήματα δεν είναι πρακτικά εφαρμόσιμα. Επομένως, μας ενδιαφέρει να γνωρίζουμε πόση είναι η διαρροή πληροφορίας του απλού κειμένου ή του κλειδιού, ή ακόμη καλύτερα, πόση προσπάθεια θα πρέπει να καταβάλλει ο αντίπαλος προκειμένου να εκμεταλλευτεί τη διαρροή και να ανακτήσει το απλό κείμενο ή το κλειδί.

3.1.4. Περίσσεια της γλώσσας και unicity distance

Ως ***περίσσεια*** (redundancy) μιας γλώσσας εννοούμε το ποσοστό των συνδυασμών των γραμμάτων της γλώσσας αυτής που δεν οδηγούν σε μηνύματα τα οποία να ανήκουν στη γλώσσα αυτή. Για παράδειγμα, το ελληνικό αλφάβητο αποτελείται από 24 γράμματα. Ο ελάχιστος αριθμός των bits που χρειαζόμαστε για να αναπαραστήσουμε τα 24 αυτά γράμματα είναι $\lceil \log_2 24 \rceil = 5$. Βέβαια, με λέξεις μήκους 5 bits μπορούμε να αναπαραστήσουμε $2^5 = 32$ διαφορετικά σύμβολα (γράμματα), αλλά με 4 bits είναι μόνο $2^4 = 16$. Η ποσότητα $A = \lceil \log_2(n) \rceil$, όπου n το πλήθος των γραμμάτων του αλφάβητου, ονομάζεται ***απόλυτος ρυθμός*** (absolute rate) μιας γλώσσας.

Ο αριθμός μηνυμάτων μήκους m γραμμάτων, είναι 2^{Am}. Για παράδειγμα, στην ελληνική γλώσσα αν καταγράψουμε όλες τις λέξεις που έχουν μήκος $m = 5$, θα έχουμε 24^5 καταχωρήσεις. Μέσα σε αυτές υπάρχουν ελληνικές λέξεις όπως «ποδια», «ρωταν», «χερια», αλλά και λέξεις που δεν ανήκουν στο ελληνικό λεξιλόγιο όπως «αααααα», «αβαβα», «κσδδφ» κτλ. Έστω 2^{Rm} ο αριθμός των μηνυμάτων που ανήκουν στην ελληνική γλώσσα. Αυτά τα μηνύματα τα ονομάζουμε ***έγκυρα***. Η περίσσεια της γλώσσας ορίζεται ως η ποσότητα:

$$D = A - R$$

η οποία μετριέται σε bits.

Από πλευράς ασφάλειας της πληροφορίας, είναι επιθυμητό η περίσσεια D μιας γλώσσας να είναι όσο το δυνατόν μικρότερη. Αν η περίσσεια είναι μικρή, τότε ο αντίπαλος που έχει στην κατοχή του το κρυπτοκείμενο, κατά την αποκρυπτογράφηση το κρυπτοκείμενο αυτό θα έχει μεγαλύτερη πιθανότητα να αντιστοιχίζεται σε πολλά έγκυρα απλά κείμενα. Αν όμως η περίσσεια είναι μεγάλη, τότε ο αντίπαλος θα μπορεί πιο εύκολα να αναγνωρίσει το ζητούμενο απλό κείμενο, αφού τα λάθος κλειδιά θα αποκρυπτογραφούν το κρυπτοκείμενο σε μη έγκυρα απλά κείμενα με μεγάλη πιθανότητα.

Μπορούμε να δεχτούμε ότι όσο περισσότερο κρυπτοκείμενο διαθέτει ο αντίπαλος, τόσο πιο αποτελεσματικά μπορεί να συσχετίσει τις αποκρυπτογραφήσεις και να οδηγηθεί στο σωστό απλό κείμενο. Επειδή όμως και η περίσσεια της γλώσσας επηρεάζει την επιτυχία της κρυπτανάλυσης, μπορούμε να φανταστούμε ότι υπάρχει εξάρτηση μεταξύ του μεγέθους του κρυπτοκειμένου που χρειάζεται για να ανακτήσει ο αντίπαλος το απλό κείμενο, και της περίσσειας της γλώσσας. Ο Shan-

non υπολόγισε ακριβώς αυτήν την ποσότητα του κρυπτοκειμένου που χρειάζεται για την ανάκτηση του απλού κειμένου, την οποία ονόμασε ***unicity distance.*** Όπως είναι γνωστό, η ποσότητα:

$$H(P|C)$$

αντιπροσωπεύει την αβεβαιότητα του απλού κειμένου, εφόσον είναι γνωστό το κρυπτοκείμενο. Η unicity distance (*UD*) είναι το μικρότερο εκείνο μήκος του κρυπτοκειμένου κατά το οποίο η παραπάνω αβεβαιότητα είναι ίση με 0. Ο Shannon απέδειξε ότι:

$$UD = \frac{H(K)}{D},$$

όπου $H(K)$ η αβεβαιότητα του κλειδιού και D η περίσσεια της γλώσσας. Όπως είναι φανερό στον παραπάνω λόγο, όσο μικρότερη είναι η περίσσεια της γλώσσας, τόσο περισσότερο κρυπτοκείμενο απαιτείται για να εντοπισθεί το κλειδί. Στην περίπτωση που το κρυπτοσύστημα μπορεί να χρησιμοποιεί όλα τα μηνύματα της γλώσσας του απλού κειμένου, τότε κάθε απόπειρα αποκρυπτογράφησης θα οδηγεί σε έγκυρο απλό κείμενο, οπότε ο αντίπαλος δεν θα είναι σε θέση να ξεχωρίσει τα λάθος κλειδιά από τα σωστά, όσο κρυπτοκείμενο και αν έχει στη διάθεσή του ($UD = \infty$).

3.2. Ορολογία - παραστάσεις

Έστω $\mathcal{F}$ το σύνολο των συμβόλων που απαρτίζουν το απλό κείμενο P, δηλαδή $P = [p_1p_2\ldots]$, όπου $p_i \in \mathcal{F}$, για i = 1, 2, … . Αντίστοιχα, έστω $\mathcal{G}$ το σύνολο των συμβόλων που απαρτίζουν το κρυπτοκείμενο C, όπου $C = [c_1c_2\ldots]$, με $c_i \in \mathcal{G}$, για i = 1, 2, … . Το σύνολο όλων των δυνατών απλών κειμένων ονομάζεται ***χώρος των απλών κειμένων*** και συμβολίζεται με $\mathcal{F}^*$, ενώ το σύνολο όλων των δυνατών κρυπτοκειμένων ονομάζεται ***χώρος των κρυπτοκειμένων*** και συμβολίζεται με $\mathcal{G}^*$.

Έστω $\mathcal{F}^n$ το σύνολο των απλών κειμένων μήκους n και $\mathcal{G}^m$ το σύνολο των κρυπτοκειμένων μήκους m. Τότε εάν $\mathcal{F}^{(n)}$ είναι το σύνολο των απλών κειμένων μήκους από 0 μέχρι n, θα είναι $\mathcal{F}^{(n)} = \varnothing \cup \mathcal{F} \cup \mathcal{F}^2 \cup \ldots \cup \mathcal{F}^n$, όπου $\varnothing$ το κενό σύνολο. Παρομοίως, εάν $\mathcal{G}^{(m)}$ είναι το σύνολο των απλών κειμένων μήκους από 0 μέχρι m, θα είναι $\mathcal{G}^{(m)} = \varnothing \cup \mathcal{G} \cup \mathcal{G}^2 \cup \ldots \cup \mathcal{G}^m$. Το κάθε ένα από τα επιμέρους σύνολα του $\mathcal{F}^{(n)}$ είναι ένα αλφάβητο του απλού κειμένου. Συνολικά το $\mathcal{F}^{(n)}$ περιέχει n αλφάβητα, αν εξαιρέσουμε το κενό σύνολο. Αντίστοιχα, το $\mathcal{G}^{(m)}$ αποτελείται από m αλφάβητα κρυπτοκειμένου.

ΠΑΡΑΔΕΙΓΜΑ 3.2 Έστω ότι τα σύμβολα του απλού κειμένου είναι τα πεζά ελληνικά γράμματα και τα σύμβολα του κρυπτοκειμένου είναι τα αντίστοιχα κεφαλαία.

$\mathcal{F}$ = {α, β, γ, δ, ε, ζ, η, θ, ι, κ, λ, μ, ν, ξ, ο, π, ρ, σ, τ, υ, φ, χ, ψ, ω}
$\mathcal{G}$ = {Α, Β, Γ, Δ, Ε, Ζ, Η, Θ, Ι, Κ, Λ, Μ, Ν, Ξ, Ο, Π, Ρ, Σ, Τ, Υ, Φ, Χ, Ψ, Ω}
$\mathcal{F}^2$ = {αα, αβ, αγ, …, βα, ββ, βγ, …, ωω}
Πλήθος στοιχείων του αλφάβητου $\mathcal{F}^2$: $|\mathcal{F}^2| = 24^2$.

Εφόσον το αλφάβητο του απλού κειμένου του παραδείγματος περιέχει μόνον τα γράμματα του ελληνικού αλφάβητου, δεν επιτρέπονται κενά ή σημεία στίξης στο απλό κείμενο:

P = [θασυναντηθουμεταμεσανυχτα].

Με βάση τα παραπάνω η κρυπτογράφηση ορίζεται ως μια απεικόνιση $\boldsymbol{S}$: $\mathcal{F}^* \rightarrow \mathcal{G}^*$ που απεικονίζει το σύνολο $\mathcal{F}^*$ στο $\mathcal{G}^*$. Αν ορίζεται και η αντίστροφη απεικόνιση $\boldsymbol{S}^{-1}$: $\mathcal{G}^* \rightarrow \mathcal{F}^*$ τότε η $\boldsymbol{S}^{-1}$ είναι η αποκρυπτογράφηση.

Έστω το σύνολο $\boldsymbol{E}$ = {e_1, e_2, …, e_k} όπου το στοιχείο e_i: $\mathcal{F}^{(n)} \rightarrow \mathcal{G}^{(m)}$ ορίζει αντιστοιχίες μεταξύ του συνόλου του απλού κειμένου μήκους έως n και του συνόλου του κρυπτοκειμένου μήκους έως m. Το e_i είναι μια πράξη κρυπτογράφησης. Εάν το e_i είναι ένριψη (injective), τότε ορίζεται η πράξη αποκρυπτογράφησης $d_i = e_i^{-1}$: $\mathcal{G}^{(m)} \rightarrow \mathcal{F}^{(n)}$, η οποία είναι στοιχείο του συνόλου $\boldsymbol{D}$ = {d_1, d_2, …, d_k}. Το κλειδί χρησιμοποιείται για να επιλέξουμε μια πράξη κρυπτογράφησης από το $\boldsymbol{E}$**.** Το πλήθος των στοιχείων του $\boldsymbol{E}$ ορίζει τον *κλειδοχώρο* $\boldsymbol{K}$ = {1, 2, …, k}.

Ένα κρυπτοσύστημα ορίζεται από την πεντάδα $\mathcal{F}^{(n)}$, $\mathcal{G}^{(m)}$, $\boldsymbol{E}$, $\boldsymbol{D}$**,** $\boldsymbol{K}$. Ο αλγόριθμος κρυπτογράφησης δέχεται ως εισόδους το $\boldsymbol{P} \in \mathcal{F}^{(n)}$ και το $i \in \boldsymbol{K}$ και επιλέγει και υλοποιεί το $e_i \in \boldsymbol{E}$ και $d_i \in \boldsymbol{D}$, ώστε $e_i(p) = c$ και $d_i(c) = p$.

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, το κλειδί θα πρέπει να είναι αρκετά μεγάλο ώστε να αποτρέπει την επίθεση της εξαντλητικής αναζήτησης. Επιπλέον, η ασφάλεια του κρυπτοσυστήματος θα πρέπει να εξαρτάται μόνον από τη μυστικότητα του κλειδιού. Σε ψηφιακά συστήματα επικοινωνίας όπου τα κλειδιά είναι δυαδικές λέξεις, ένα τυπικό μήκος κλειδιού για υποψήφιο ασφαλές κρυπτοσύστημα είναι 128 bits. Αυτό σημαίνει ότι το σύνολο $\boldsymbol{E}$ περιέχει ακριβώς 2^{128} στοιχεία. Ένας αφελής τρόπος για να υλοποιήσουμε το κρυπτοσύστημα θα ήταν να αποθηκεύσουμε πίνακες των πράξεων κρυπτογράφησης e_i, για όλα τα i. Δηλαδή, η συσκευή κρυπτογράφησης θα πρέπει να προβλέψει χώρο της τάξης του $2^{128} \approx 10^{38}$. Στην πραγματικότητα, ο χώρος θα είναι πολλαπλάσιος της τιμής αυτής, αφού η κάθε πράξη κρυπτογράφησης θα καταλαμβάνει χώρο μεγαλύτερο του ενός bit. Έτσι λοιπόν είναι αναγκαία η δημιουργία αλγόριθμων κρυπτογράφησης ώστε το κλειδί να ελέγχει και να συμμετέχει σε μια σειρά μετασχηματισμών που θα αντιστοιχούν στο e_i.

Η πράξη της αποκλειστικής διάζευξης (exclusive OR, XOR)

Μια από τις πιο δημοφιλείς πράξεις στα ψηφιακά κρυπτοσυστήματα είναι αυτή της αποκλειστικής διάζευξης. Η πράξη αυτή συμβολίζεται με το σύμβολο ⊕ και ο πίνακας αληθείας στο σύνολο {0, 1} φαίνεται στον Πίνακα 3.1.

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Πίνακας 3.1 Πίνακας αληθείας για την αποκλειστική διάζευξη

Η αποκλειστική διάζευξη είναι, όπως είδαμε στο προηγούμενο κεφάλαιο, ισοδύναμη πράξη με την πρόσθεση modulo 2. Η δημοτικότητα της αποκλειστικής διάζευξης οφείλεται στην ιδιότητα της ακύρωσης που διατηρεί, όπως φαίνεται στο ακόλουθο παράδειγμα.

ΠΑΡΑΔΕΙΓΜΑ 3.3 – Κρυπταλγόριθμος *XOR*. Έστω ένα κρυπτοσύστημα όπου $\mathcal{F} = \mathcal{G} = \{0,1\}$ και $P = [01001] \in \mathcal{F}^{(5)}$. Έστω ότι $K = [11100]$ το μυστικό κλειδί κρυπτογράφησης. Η κρυπτογράφηση ορίζεται ως:

$$C = P \oplus K = 01001 \oplus 11100 = 10101 .$$

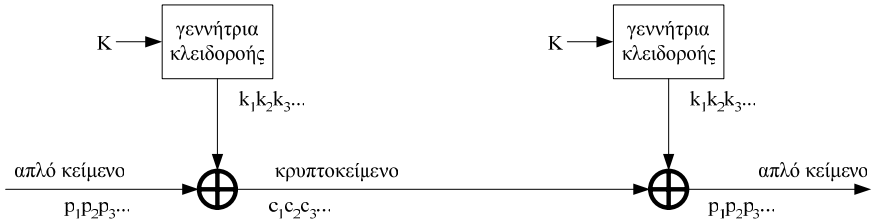
Κατά την αποκρυπτογράφηση ισχύει:

$$P = C \oplus K = (P \oplus K) \oplus K = 10101 \oplus 11100 = 01001$$

Αν και ο κρυπταλγόριθμος αυτός είναι πολύ απλός σε περιγραφή και σε εκτέλεση, μπορεί υπό συγκεκριμένες συνθήκες να μας οδηγήσει σε άνευ όρων ασφαλές κρυπτοσύστημα, όπως θα δούμε σε επόμενη ενότητα.

3.2.1. Κρυπταλγόριθμοι ροής και κρυπταλγόριθμοι τμήματος

Οι κρυπταλγόριθμοι ροής ενεργούν σε ένα σύμβολο απλού κειμένου τη φορά. Η αρχή λειτουργίας φαίνεται στο Σχήμα 3.4. Σε ένα ψηφιακό κρυπτοσύστημα τα αλφάβητα του απλού κειμένου, του κρυπτοκειμένου καθώς και της κλειδοροής αποτελούνται από bits.



Σχήμα 3.4 Αρχή λειτουργίας κρυπταλγόριθμου ροής

Βασικό συστατικό ενός κρυπταλγόριθμου ροής είναι η γεννήτρια της κλειδοροής. Η κλειδοροή είναι μια περιοδική ακολουθία κλειδιών. Η αρχή της περιόδου καθορίζεται από το κλειδί εκκίνησης K το οποίο είναι και το μυστικό κλειδί του κρυπτοσυστήματος. Δύο είναι οι βασικοί και αλληλένδετοι λόγοι της περιοδικής φύσης της κλειδοροής. Πρώτον, η γεννήτρια κλειδοροής θα πρέπει να έχει τη δυ-

νατότητα να παράγει την ίδια ακολουθία σε δύο διαφορετικές τοποθεσίες την ίδια χρονική στιγμή. Επομένως η υλοποίηση των γεννητριών αυτών πρέπει να γίνεται με συσκευές οι οποίες μπορούν με αξιοπιστία να αναπαράγουν την ίδια ακολουθία. Δεύτερον, οι μόνες γνωστές συσκευές σήμερα που μπορούν να αντεπεξέλθουν στον περιορισμό αυτό είναι οι μηχανές πεπερασμένων καταστάσεων, στην κατηγορία των οποίων ανήκουν και οι ηλεκτρονικοί υπολογιστές. Εάν δεν υπήρχε ο περιορισμός της αξιόπιστης αναπαραγωγής της κλειδοροής, τότε από τη μια θα έπρεπε να υπάρχει ένα ασφαλές κανάλι για τη μετάδοση της κλειδοροής η οποία έχει μέγεθος ίσο με το απλό κείμενο, ενώ από την άλλη ως γεννήτρια κλειδοροής θα μπορούσε να ήταν μια οποιαδήποτε πηγή τυχαίων αριθμών, ή γενικότερα συμβόλων.

Από πλευράς κρυπτογραφικής ασφάλειας, η ανεξάρτητη κρυπτογράφηση των συμβόλων έχει σοβαρά μειονεκτήματα. Επειδή το κάθε σύμβολο του απλού κειμένου κρυπτογραφείται χωριστά, όλη η πληροφορία του συμβόλου αυτού περικλείεται σε ένα μόνο σύμβολο του κρυπτοκειμένου. Συνεπώς η διάχυση ενός αλγόριθμου ροής είναι πολύ χαμηλή.

Ο συγχρονισμός των δύο γεννητριών κλειδοροής είναι η Αχίλλειος πτέρνα του συστήματος. Ένας αντίπαλος μπορεί να αποσυγχρονίσει το κρυπτοσύστημα παρεμβάλλοντας επιπλέον σύμβολα στο κρυπτοκείμενο, οπότε η αποκρυπτογράφηση θα οδηγεί σε απλό κείμενο άλλο από το αρχικό.

Το πλεονέκτημα του αλγόριθμου ροής είναι η μεγάλη ταχύτητα κρυπτογράφησης. Επειδή το κάθε σύμβολο του απλού κειμένου δεν εξαρτάται από τα υπόλοιπα, μπορεί να κρυπτογραφηθεί και να σταλεί τη στιγμή που θα εισαχθεί στο κρυπτοσύστημα. Για το λόγο αυτόν οι αλγόριθμοι ροής βρίσκουν εφαρμογές στην κρυπτογράφηση τηλεφωνικών συνδιαλέξεων και γενικότερα σε δεδομένα τηλεσυνδυάσκεψης.

Τέλος, το μειονέκτημα της χαμηλής διάχυσης είναι πλεονέκτημα από πλευράς κωδικοποίησης πληροφορίας. Η πληροφορία ενός συμβόλου του απλού κειμένου περιέχεται μόνο σε ένα σύμβολο του κρυπτοκειμένου, οπότε σε περίπτωση σφάλματος μετάδοσης ενός συμβόλου του κρυπτοκειμένου, δεν θα επηρεαστούν τα γειτονικά σύμβολα και το σφάλμα κατά την αποκρυπτογράφηση θα περιοριστεί στο αντίστοιχο σύμβολο του απλού κειμένου.

Οι κρυπταλγόριθμοι τμήματος (block) ενεργούν σε μια ομάδα συμβόλων απλού κειμένου και παράγουν μια ομάδα συμβόλων κρυπτοκειμένου. Το απλό κείμενο που συνήθως έχει μήκος μεγαλύτερο από το μήκος της ομάδας, χωρίζεται σε τμήματα όπου το κάθε τμήμα είναι η ομάδα που θα διοχετευθεί στον αλγόριθμο κρυπτογράφησης. Συνήθως το μήκος του τμήματος είναι σταθερό και συγκεκριμένο για έναν κρυπταλγόριθμο, οπότε υπάρχει το ενδεχόμενο το τελευταίο τμήμα του απλού κειμένου να συμπληρωθεί από μηδενικά σύμβολα προκειμένου να έχει το απαιτούμενο μήκος.

Τα μειονεκτήματα των κρυπταλγόριθμων ροής είναι τα πλεονεκτήματα των κρυπταλγόριθμων τμήματος, ενώ τα πλεονεκτήματα των αλγόριθμων ροής είναι και τα μειονεκτήματα των αλγόριθμων τμήματος. Έτσι οι αλγόριθμοι τμήματος

μπορούν να έχουν υψηλή διάχυση, λόγω του ομαδικού χειρισμού των συμβόλων του απλού κειμένου κατά την κρυπτογράφηση. Επίσης, ο αντίπαλος δεν είναι σε θέση να παρεμβάλλει επιπλέον σύμβολα στο κρυπτοκείμενο, διότι στη περίπτωση αυτή θα μεταβαλλόταν το μέγεθος του τμήματος και η απόπειρα παρεμβολής θα γινόταν αντιληπτή.

Τα μειονεκτήματα των αλγόριθμων ροής είναι η σχετικά χαμηλή ταχύτητα και η διάδοση των σφαλμάτων. Ο αλγόριθμος κρυπτογράφησης απαιτεί την συμπλήρωση του τμήματος του απλού κειμένου προκειμένου να εκτελεστεί η κρυπτογράφηση. Επίσης ένα σφάλμα σε ένα σύμβολο του κρυπτοκειμένου κατά τη μετάδοσή του, επηρεάζει όλο το τμήμα στο οποίο ανήκει με αποτέλεσμα να μην είναι εφικτή η αποκρυπτογράφηση του τμήματος αυτού.

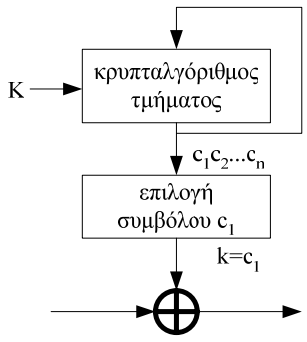
ΠΑΡΑΔΕΙΓΜΑ 3.4 – Μέγιστη διάχυση και σύγχυση κρυπταλγόριθμου τμήματος. Έστω το κρυπτοσύστημα $\mathcal{F}^{(n)} \to \mathcal{G}^{(n)}$ με $\mathcal{F} = \mathcal{G} = \{0, 1\}$, κλειδοχώρο $\boldsymbol{K}$, και $\boldsymbol{E}$, $\boldsymbol{D}$ που ορίζονται από κρυπταλγόριθμο τμήματος μήκους n-bit. Έστω P = $[p_1 p_2 \ldots p_n]$ το τμήμα του απλού κειμένου και C = $[c_1 c_2 \ldots c_n]$ το αντίστοιχο τμήμα του κρυπτοκειμένου. Για να υπάρχει μέγιστη διάχυση θα πρέπει να υπάρχει σχέση μεταξύ του κάθε συμβόλου του απλού κειμένου με όλα τα σύμβολα του κρυπτοκειμένου, για οποιοδήποτε κλειδί:

$$c_i = f_{i,j}(p_j), \quad i, j = 0, 1, \ldots, n$$

ενώ για να υπάρχει μέγιστη σύγχυση θα πρέπει η πιθανότητα αντιστροφής ενός συμβόλου του κρυπτοκειμένου c_i να είναι 0.5 εφόσον υπάρξει αντιστροφή του p_j, για όλα τα i, j:

$$p(c_i \oplus 1 = f_{i,j}(p_j \oplus 1)) = \frac{1}{2}, \quad i, j = 0, 1, \ldots, n$$

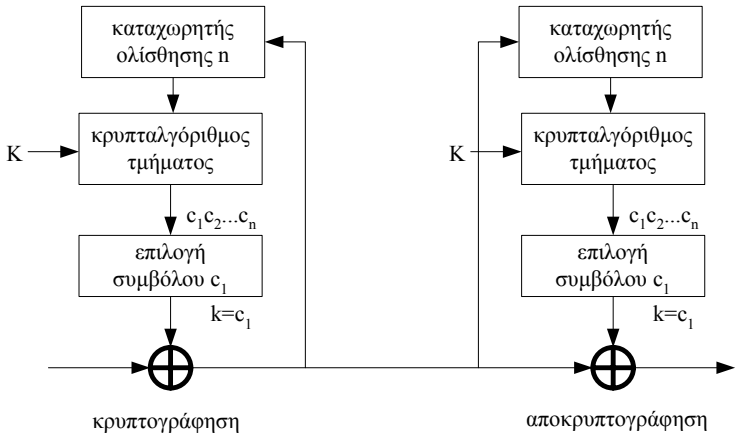
ΠΑΡΑΔΕΙΓΜΑ 3.5 – Δημιουργία κρυπταλγόριθμου ροής από κρυπταλγόριθμο τμήματος. Μπορούμε να εκμεταλλευτούμε την υψηλή διάχυση και σύγχυση ενός κρυπταλγόριθμου τμήματος για να κατασκευάσουμε μια γεννήτρια κλειδοροής για



Σχήμα 3.5 Χρήση κρυπταλγόριθμου τμήματος ως γεννήτρια κλειδοροής

κρυπταλγόριθμο ροής όπως φαίνεται στο Σχήμα 3.5. Η διαδικασία ξεκινά με την κρυπτογράφηση ενός αρχικού απλού κειμένου που εισάγεται στον κρυπταλγόριθμο τμήματος, για παράδειγμα [00…0]. Σε κάθε κρυπτογράφηση, το κρυπτοκείμενο του κρυπταλγόριθμου τμήματος τροφοδοτείται ως απλό κείμενο, ενώ από τα διαδοχικά αποτελέσματα επιλέγεται το πρώτο σύμβολο του τμήματος του κρυπτοκειμένου και εξάγεται από τη γεννήτρια κλειδοροής προς χρήση του κρυπταλγόριθμου ροής.

ΠΑΡΑΔΕΙΓΜΑ 3.6 – Δημιουργία αυτοσυγχρονιζόμενου αλγόριθμου ροής. Παρατηρώντας ότι η γεννήτρια κλειδοροής του Παραδείγματος 3.6 έχει δύο εισόδους, μπορούμε να εκμεταλλευτούμε τη μία από αυτές για να κατασκευάσουμε έναν κρυπταλγόριθμο ροής ο οποίος δεν έχει το μειονέκτημα της απώλειας συγχρονισμού. Στο Σχήμα 3.6 φαίνεται η συνδεσμολογία ενός αυτοσυγχρονιζόμενου κρυπταλγόριθμου ροής**.**



Σχήμα 3.6 Αυτοσυγχρονιζόμενος κρυπταλγόριθμος ροής

Το επιπρόσθετο συστατικό του κρυπταλγόριθμου, ο καταχωρητής ολίσθησης, χρησιμοποιείται ως μέσο αποθήκευσης *n* στοιχείων που απαιτούνται ως είσοδος στον κρυπταλγόριθμο τμήματος. Σε κάθε κρυπτογράφηση του συμβόλου του απλού κειμένου, το σύμβολο που προκύπτει αποθηκεύεται στην πρώτη θέση του καταχωρητή ολίσθησης. Στην επόμενη κρυπτογράφηση, το σύμβολο αυτό θα μεταβεί στη δεύτερη θέση για να δώσει την πρώτη θέση στο νεοεισερχόμενο σύμβολο. Μετά από *n* κρυπτογραφήσεις, το σύμβολό μας αποβάλλεται από τον καταχωρητή. Έτσι, σε περίπτωση που υπάρξει κάποιο σφάλμα ή αυθαίρετη εισαγωγή κρυπτοκειμένου κατά τη μετάδοση, η διαδικασία αποκρυπτογράφησης θα επανέλθει στη σωστή λειτουργία μετά από *n* αποκρυπτογραφήσεις από το τελευταίο σφάλμα.

3.3. Κατηγορίες κρυπτογραφικών πράξεων

Οι κρυπτογραφικές πράξεις χωρίζονται σε δυο κύριες κατηγορίες, στην ***αναδιάταξη*** (transposition) και στην ***αντικατάσταση*** (substitution). Η αναδιάταξη επιδρά αποκλειστικά στη θέση των συμβόλων του απλού κειμένου, ενώ η αντικατάσταση επιδρά στα σύμβολα του απλού κειμένου. Η αντικατάσταση με τη σειρά της χωρίζεται σε δυο κατηγορίες, με κριτήριο το πλήθος των αλφάβητων στα οποία επιδρά μια κρυπτογραφική πράξη: στη ***μονοαλφαβητική αντικατάσταση*** και στην ***πολυαλφαβητική αντικατάσταση***.

3.3.1. Αναδιάταξη

Είναι φανερό πως στην περίπτωση της αναδιάταξης είναι $\mathcal{F} = \mathcal{G}$, δηλαδή τα σύμβολα του κρυπτοκειμένου είναι ίδια με τα σύμβολα του απλού κειμένου, αφού η κρυπτογράφηση αναδιάταξης επιδρά μόνο στις θέσεις των συμβόλων του απλού κειμένου.

ΠΑΡΑΔΕΙΓΜΑ 3.7 – Κρυπτογράφηση με αναδιάταξη. Έστω τα σύνολα του απλού κειμένου και κρυπτοκειμένου:

$\mathcal{F} = \mathcal{G} = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \mu, \nu, \xi, \omicron, \pi, \rho, \sigma, \tau, \upsilon, \varphi, \chi, \psi, \omega\}$

και έστω το απλό κείμενο:

[αλλαγη].

Το κλειδί σε μια αναδιάταξη είναι η αντιστοίχιση των θέσεων των γραμμάτων του απλού κειμένου και του κρυπτοκειμένου. Έστω το κλειδί:

[261453],

το οποίο σημαίνει ότι το πρώτο γράμμα του απλού κειμένου θα εμφανισθεί στη δεύτερη θέση του κρυπτοκειμένου, το δεύτερο στην έκτη, κ.ο.κ. Η κρυπτογράφηση του απλού κειμένου θα δώσει:

[λαηαγλ].

Το κρυπτοκείμενο που προκύπτει είναι στην ουσία ένας αναγραμματισμός του απλού κειμένου. Αν συμβολίσουμε με $\pi(\ )$ την κρυπτογραφική πράξη της αναδιάταξης, για το παράδειγμά μας θα ισχύει:

$\pi: \mathcal{F}^6 \rightarrow \mathcal{G}^6$

με πράξη κρυπτογράφησης:

$\pi([p_1\ p_2\ p_3\ p_4\ p_5\ p_6]) = [\ p_2\ p_6\ p_1\ p_4\ p_5\ p_3]$.

και πράξη αποκρυπτογράφησης:

$\pi^{-1}([p_1\ p_2\ p_3\ p_4\ p_5\ p_6]) = [\ p_3\ p_1\ p_6\ p_4\ p_5\ p_2]$.

Ο αριθμός των ψηφίων του κλειδιού καθορίζει το μέγεθος του κλειδιού. Όπως είναι φανερό, η αναδιάταξη είναι κρυπταλγόριθμος τμήματος, όπου το μέγεθος του κλειδιού καθορίζει το μέγεθος του τμήματος του απλού κειμένου και του κρυπτοκειμένου.

Η αναδιάταξη είναι μια ειδική περίπτωση του κρυπταλγόριθμου του Hill που θα εξετάσουμε σε επόμενη ενότητα.

3.3.2. Μονοαλφαβητική αντικατάσταση

ΟΡΙΣΜΟΣ 3.4 – Μονοαλφαβητική αντικατάσταση είναι η κρυπτογραφική πράξη e_i: $\mathcal{F}^{(n)} \rightarrow \mathcal{G}^{(m)}$, όπου η e_i παραμένει σταθερή σε όλη τη διάρκεια της κρυπτογράφησης ενός απλού κειμένου.

Η ειδική περίπτωση $\mathcal{F}^{(1)} \rightarrow \mathcal{G}$ ονομάζεται απλή αντικατάσταση, όπου οι κρυπτογραφική πράξη αντιστοιχίζει ένα σύμβολο του απλού κειμένου σε ένα σύμβολο του κρυπτοκειμένου. Αυτό το οποίο έχει ιδιαίτερο ενδιαφέρον στην σύγχρονη κρυπτογραφία είναι όταν τα αλφάβητα του απλού κειμένου και του κρυπτοκειμένου είναι τα ίδια, δηλαδή $\mathcal{F} = \mathcal{G}$. Με αυτήν την ισοδυναμία, η υλοποίηση του κρυπτοσυστήματος από υπολογιστικά συστήματα είναι απλούστερη και επιπλέον οι κρυπτογραφικές πράξεις μπορούν με ευκολία να εφαρμοστούν διαδοχικά περισσότερες από μία φορές, ώστε να προκύψουν πιο ισχυροί κρυπταλγόριθμοι.

Κρυπταλγόριθμος μετατόπισης

ΟΡΙΣΜΟΣ 3.5 – Ο κρυπταλγόριθμος μετατόπισης ορίζει το κρυπτοσύστημα $\mathcal{F} = \mathcal{G} = \boldsymbol{K} = \boldsymbol{Z_n}$ και με $e_k \in \boldsymbol{E}$, $d_k \in \boldsymbol{D}$, τέτοια ώστε

$$c = e_k(p) = p + k \mod n$$

και

$$p = d_k(c) = c - k \mod n, \quad \text{για } p \in \mathcal{F},\ c \in \mathcal{G},\ k \in \boldsymbol{K}.$$

Στην περίπτωση που το απλό κείμενο αναφέρεται στο ελληνικό αλφάβητο (μόνον πεζά, χωρίς κενά, όπως στο Παράδειγμα 3.2), n = 24, ενώ τα γράμματα απαριθμούνται:

α,Α = 0, β,Β = 1, …, ω,Ω = 23

και ο κρυπταλγόριθμος εφαρμόζεται στο αριθμητικό ισοδύναμο των γραμμάτων.

ΠΑΡΑΔΕΙΓΜΑ 3.8 – Κρυπταλγόριθμος μετατόπισης του Καίσαρα. Έστω το απλό κείμενο [αγορασεμετοχεσ]. Με κλειδί k = 3, η κρυπτογράφηση θα είναι ως εξής:

$$c = e_k(p) = p + 3 \mod 24$$

και το κρυπτοκείμενο που προκύπτει θα είναι το:

[ΔΖΣΥΔΦΘΟΘΧΣΑΘΦ]

	α	γ	ο	ρ	α	σ	ε	μ	ε	τ	ο	χ	ε	σ
p:	0	2	14	16	0	17	4	11	4	18	14	21	4	17
c:	3	5	17	19	3	20	7	14	7	21	17	0	7	20
	Δ	Ζ	Σ	Υ	Δ	Φ	Θ	Ο	Θ	Χ	Σ	Α	Θ	Φ

Όταν το κλειδί του κρυπταλγόριθμου μετατόπισης έχει την τιμή $k = 3$, όπως στο παράδειγμά μας, ο κρυπταλγόριθμος ονομάζεται «κρυπταλγόριθμος του Καίσαρα», διότι σύμφωνα με την Ιστορία ο Ιούλιος Καίσαρας χρησιμοποιούσε το συγκεκριμένο αλγόριθμο και το συγκεκριμένο κλειδί για την μυστική επικοινωνία με τους στρατιωτικούς του.

Ασφάλεια του κρυπταλγόριθμου μετατόπισης

Όπως μπορούμε να αντιληφθούμε, το εξαιρετικά μικρό μέγεθος του κλειδοχώρου επιτρέπει σε κάποιον αντίπαλο να βρει το κλειδί ακόμη και χωρίς τη βοήθεια ηλεκτρονικού υπολογιστή. Στο παράδειγμά μας, όπου το κλειδί μπορεί να πάρει 23 τιμές (θεωρούμε ότι δεν θα πάρει ποτέ την τιμή 0, αφού το κρυπτοκείμενο θα είναι το ίδιο με το απλό κείμενο), αναμένουμε ότι ένας αντίπαλος θα μπορέσει να το ανακαλύψει σε 12 προσπάθειες. Ο αριθμός αυτός είναι ο μέσος όρος της χειρότερης και καλύτερης περίπτωσης.

Γενίκευση μονοαλφαβητικής απλής αντικατάστασης

Ο κρυπταλγόριθμος μετατόπισης χρησιμοποιεί αλφάβητα κρυπτοκειμένου τα οποία ορίζονται από την πράξη $c = p+k \bmod n$. Αυτό σημαίνει ότι το πλήθος των αλφάβητων του κρυπτοκειμένου είναι n**.** Το κλειδί καθορίζει το αλφάβητο το οποίο αντιστοιχεί το απλό κείμενο σε κρυπτοκείμενο. Όμως όλα τα πιθανά αλφάβητα του κρυπτοκειμένου είναι $n!$. Επομένως ένα κρυπτοσύστημα το οποίο μπορεί να επιλέξει οποιοδήποτε από τα αλφάβητα αυτά, θα έχει κλειδοχώρο ίσο με $n!$. Στην περίπτωση του ελληνικού αλφάβητου του Παραδείγματος 3.8, ο κλειδοχώρος θα έχει μέγεθος 24!.

Ασφάλεια μονοαλφαβητικής απλής αντικατάστασης

Φαινομενικά η χρησιμοποίηση όλων των δυνατών αλφάβητων του κρυπτοκειμένου δίνει την εντύπωση ενός ασφαλούς κρυπτοσυστήματος, αφού ο κλειδοχώρος είναι απαγορευτικά μεγάλος σε μια προσπάθεια του αντιπάλου να εκτελέσει εξαντλητική αναζήτηση. Όμως όπως αναφέραμε στο προηγούμενο κεφάλαιο, η εξαντλητική αναζήτηση είναι η προφανής (και πολλές φορές αφελής) επίθεση σε ένα κρυπτοσύστημα, και ο αντίπαλος προσπαθεί να βρει άλλες επιθέσεις οι οποίες τον οδηγούν συντομότερα στην ανακάλυψη του απλού κειμένου ή του κλειδιού. Η μονοαλφαβητική αντικατάσταση έχει μια σοβαρή αδυναμία, όπου ο αντίπαλος

μπορεί να ανακαλύψει με σχετική ευκολία το απλό κείμενο, ακόμη και χωρίς τη χρήση ηλεκτρονικού υπολογιστή.

Η αδυναμία της μονοαλφαβητικής αντικατάστασης αφορά την διατήρηση της πληροφορίας σχετικά με τη συχνότητα εμφάνισης των γραμμάτων σε μια γλώσσα. Στον Πίνακα 3.2, φαίνεται η συχνότητα εμφάνισης των γραμμάτων της ελληνικής γλώσσας, όπως προέκυψε από μέτρηση δείγματος λογοτεχνικού κειμένου 194.304 χαρακτήρων.

Γράμμα	Συχνότητα εμφάνισης (%)	Γράμμα	Συχνότητα εμφάνισης (%)
α	12	**ν**	7,9
β	0,8	**ξ**	0,6
γ	2	**ο**	9,8
δ	1,7	**π**	5,024
ε	8	**ρ**	5,009
ζ	0,5	**σ**	4,9
η	2,9	**τ**	9,1
θ	1,3	**υ**	4,3
ι	7,8	**φ**	1,2
κ	4,2	**χ**	1,4
λ	3,3	**ψ**	0,2
μ	4,4	**ω**	1,6

Πίνακας 3.2 Συχνότητα εμφάνισης των γραμμάτων της ελληνικής γλώσσας (Πηγή: Simon Singh, «Κώδικες και Μυστικά»).

Ο υπολογισμός της συχνότητας εμφάνισης των γραμμάτων σε μια γλώσσα είναι μια διαδικασία που μπορεί να εκτελεσθεί ανεξάρτητα από οποιονδήποτε. Οι συχνότητες που θα προκύψουν εξαρτώνται τόσο από το είδος του δείγματος (λογοτεχνικό, επιστημονικό, εφημερίδα, περιοδικό), όσο και από το μέγεθός του. Γενικά όμως όσο μεγαλώνει το δείγμα, τόσο οι συχνότητες των ανεξάρτητων μετρήσεων συγκλίνουν μεταξύ τους.

Ο αντίπαλος έχει στη διάθεσή του το κρυπτοκείμενο, τον Πίνακα 3.2, και μπορεί να υπολογίσει την συχνότητα εμφάνισης των συμβόλων του κρυπτοκειμένου. Το πιο συχνό γράμμα στην ελληνική γλώσσα είναι το **α**, και ακολουθούν το **ο**, το **ε** και το **ι**. Επιπλέον ο αντίπαλος μπορεί να κατασκευάσει έναν πίνακα συχνοτήτων του κρυπτοκειμένου και να αντιπαραθέσει τις συχνότητες εμφάνισης του κρυπτοκειμένου με αυτές της ελληνικής γλώσσας. Για τα πιο συχνά γράμματα μπορεί να βρει τις αντιστοιχίες των συμβόλων του απλού κειμένου με το κρυπτοκείμενο. Αντικαθιστώντας στο κρυπτοκείμενο τα σύμβολα τα οποία έχει βρει τις αντιστοιχίες, μπορεί να εργαστεί δοκιμάζοντας σταδιακά πιθανές αντιστοιχίες συμβόλων, με μια διαδικασία παρόμοια με αυτήν του γνωστού παιχνιδιού της κρεμάλας. Παράλληλα, η ελληνική γλώσσα όπως και όλες οι φυσικές γλώσσες έχουν το χαρα-

κτηριστικό των περιττών συνδυασμών, το οποίο μπορεί να χρησιμοποιήσει ο αντίπαλος προς όφελός του. Για παράδειγμα, εάν κάποια στιγμή στο απλό κείμενο εμφανισθούν λέξεις που περιέχουν ακολουθίες γραμμάτων όπως «τγ», «κγ», «ψσ» κ.ο.κ. τότε κάποια από τις αντιστοιχίες είναι λάθος και χρειάζεται επανεξέταση. Βασική παράμετρος στην επιτυχία της μεθόδου αυτής είναι και το μέγεθος του κρυπτοκειμένου. Το κρυπτοκείμενο θα πρέπει να είναι αρκετά μεγάλο ώστε να μπορέσουν να διακριθούν τα γράμματα τα οποία έχουν μεγάλη συχνότητα εμφάνισης.

Για λόγους πληρότητας, παραθέτουμε τη συχνότητα εμφάνισης των γραμμάτων του λατινικού αλφάβητου για την αγγλική γλώσσα στον Πίνακα 3.3. Η πλειοψηφία των παραδειγμάτων των κρυπτοκειμένων στη βιβλιογραφία είναι φυσικά στην αγγλική, και επομένως κρίθηκε σκόπιμο να συμπεριληφθεί ο παρακάτω πίνακας.

Γράμμα	Συχνότητα εμφάνισης (%)	Γράμμα	Συχνότητα εμφάνισης (%)
a	8.167	**n**	6.749
b	1.492	**o**	7.507
c	2.782	**p**	1.929
d	4.253	**q**	0.095
e	12.702	**r**	5.987
f	2.228	**s**	6.327
g	2.015	**t**	9.056
h	6.094	**u**	2.758
i	6.966	**v**	0.978
j	0.153	**w**	2.360
k	0.772	**x**	0.150
l	4.025	**y**	1.974
m	2.406	**z**	0.074

Πίνακας 3.3 Συχνότητα εμφάνισης των γραμμάτων της αγγλικής γλώσσας (Πηγή: Lewand, 2000)

Ο γραμμικός κρυπταλγόριθμος

Ο γραμμικός κρυπταλγόριθμος είναι και αυτός μια ειδική περίπτωση μονοαλφαβητικής απλής αντικατάστασης, αλλά δίνει τη δυνατότητα πρόσβασης σε παραπάνω από n αλφάβητα κρυπτοκειμένου.

ΟΡΙΣΜΟΣ 3.6 – Ο γραμμικός κρυπταλγόριθμος ορίζει το κρυπτοσύστημα $\boldsymbol{\mathcal{F}} = \boldsymbol{\mathcal{G}} = \boldsymbol{K} = \boldsymbol{Z}_n$, $\boldsymbol{K} = \{(a, b) \in \boldsymbol{Z}_n \times \boldsymbol{Z}_n : \gcd(a, n) = 1\}$ και με $e_k \in \boldsymbol{E}$, $d_k \in \boldsymbol{D}$ τέτοια ώστε:

$$c = e_k(p) = ap + b \mod n$$

και

$$p = d_k(c) = a^{-1}(c-b) \mod n, \text{ για } p \in \mathcal{P},\ c \in \mathcal{C},\ k = (a,b) \in \mathcal{K}.$$

Για $a = 1$ έχουμε την περίπτωση του κρυπταλγόριθμου μετατόπισης.

Ο περιορισμός που τίθεται στα *a* και *n* να έχουν μέγιστο κοινό διαιρέτη 1, δηλαδή οι ακέραιοι *a*, *n* να είναι σχετικώς πρώτοι, απαιτείται προκειμένου η αποκρυπτογράφηση να είναι εφικτή και να έχει μία μόνο λύση.

ΠΑΡΑΔΕΙΓΜΑ 3.9 – Έλεγχος εγκυρότητας συνάρτησης γραμμικού κρυπταλγόριθμου. Θεωρούμε την κρυπτογραφική πράξη

$$e_k(p) = 4p + 5 \mod 24$$

Επειδή gcd(4,24)=4, η κρυπτογράφηση του *p* και του *p* + 24/4 θα οδηγεί στο ίδιο κρυπτοκείμενο:

$$e_k(3) = 12 + 5 = 17 \mod 24$$
$$e_k(9) = 36 + 5 = 41 \equiv 17 \pmod{24}$$

Επομένως η κρυπτογραφική πράξη δεν μπορεί να χρησιμοποιηθεί ως γραμμικός κρυπταλγόριθμος.

Ασφάλεια του γραμμικού κρυπταλγόριθμου

Η ασφάλεια του γραμμικού κρυπταλγόριθμου υπόκειται στην ασφάλεια της μονοαλφαβητικής απλής αντικατάστασης. Ο αντίπαλος έχοντας στη διάθεσή του το κρυπτοκείμενο, θα πρέπει να ανακαλύψει το ζευγάρι *a* και *b* που απαρτίζουν το κλειδί. Με βάση τη συχνότητα εμφάνισης των συμβόλων του κρυπτοκειμένου, επιλέγει τα δυο πιο συχνά εμφανιζόμενα σύμβολα για να σχηματίσει ένα σύστημα δυο εξισώσεων με δυο αγνώστους, το οποίο μπορεί να λυθεί.

Έστω ότι τα σύμβολα c_i και c_j είναι τα πιο συχνά εμφανιζόμενα σύμβολα στο κρυπτοκείμενο, με το c_i να κατέχει τη μέγιστη συχνότητα. Αντίστοιχα, από τον πίνακα συχνότητας εμφάνισης των γραμμάτων της φυσικής γλώσσας, έστω ότι p_i και p_j είναι τα πιο συχνά εμφανιζόμενα σύμβολα. Τότε θα ισχύει:

$$\left.\begin{aligned} c_i &= ap_i + b \\ c_j &= ap_j + b \end{aligned}\right\} \mod n$$

Το σύστημα εξισώσεων λύνεται με αγνώστους τα *a* και *b*.

ΠΑΡΑΔΕΙΓΜΑ 3.10 – Κρυπτανάλυση γραμμικού κρυπταλγόριθμου. Έστω ότι ο αντίπαλος έχει συλλέξει το ακόλουθο κρυπτοκείμενο:

[ΓΦΖΕΓΟΡΦΣΝΦΥΡΥΝΦΟΜΟΤΦΗΡΧΦΔΟΦΑΖΑΦΝΣΝΜΧΝΕΝΔΟΛΟΒ
θΡΦΤΝΦΜΤΡΑΝΝΧΟΧΝΕΝΧΟΛΛΟΒΜΔΕΒΧΤΝΑΝΛΒΤΡΜ]

Είναι φανερό από τα σύμβολα ότι η γλώσσα που χρησιμοποιείται είναι η ελληνική. Με μια καταμέτρηση της συχνότητας εμφάνισης των γραμμάτων, προκύπτει ότι **Ν**:13, **Φ**:10, **Ο**:9, **Ρ**:6, **Χ**:6, **Μ**:5, **Τ**:5 . Υποθέτουμε ότι **Ν** είναι η κρυπτογράφηση του **α** και **Φ** είναι η κρυπτογράφηση του **ο**. Έτσι λοιπόν θα έχουμε:

$$\left.\begin{aligned} 12 &= a\cdot 0 + b \\ 20 &= a\cdot 14 + b \end{aligned}\right\} \mod 24$$

το οποίο δίνει $b = 12$ και $a = 8 \cdot 14^{-1} \bmod 24$, εφόσον υπάρχει το $14^{-1} \bmod 24$ (= αντίστροφο του 14, modulo 24). Όμως gcd(14, 24) = 2 ≠ 1, που σημαίνει ότι δεν υπάρχει το αντίστροφο του 14. Επομένως θα πρέπει να χρησιμοποιήσουμε γράμμα το οποίο αντιστοιχεί σε περιττό αριθμό ο οποίος είναι σχετικώς πρώτος με το 24. Η επόμενη καλύτερη επιλογή είναι το **Μ** ($c = 11$) το οποίο εμφανίζεται με συχνότητα 6%. Σύμφωνα με τον Πίνακα 3.2, τα πιο κοντινά γράμματα σε αυτήν την συχνότητα είναι τα **π** ($p = 15$)**, ρ** ($p = 16$)**, σ** ($p = 17$). Αυτό μας δίνει τις ακόλουθες τρεις πιθανές τιμές για το a:

$$a_1 = (15-12)\cdot 11^{-1} = 9 \mod 24$$
$$a_2 = (16-12)\cdot 11^{-1} = 20 \mod 24$$
$$a_3 = (17-12)\cdot 11^{-1} = 7 \mod 24$$

όπου χρησιμοποιήσαμε ότι, $11^{-1} \equiv 11 \pmod{24}$. Οι τιμές a_1 και a_2 απορρίπτονται επειδή gcd(20, 24) ≠ 1 και gcd(9, 24) ≠ 1. Για $a = 7$, η αποκρυπτογράφηση δίνει:

[γιωργοειμαιβεβαιοσοτιηεπικοινωνιαμασπαρακολουθειταιστενααποπαραπολλουσκρυπταναλυτες]

Συνεπώς το κλειδί του γραμμικού κρυπταλγόριθμου είναι το (7, 12), και η πράξη αποκρυπτογράφησης είναι η:

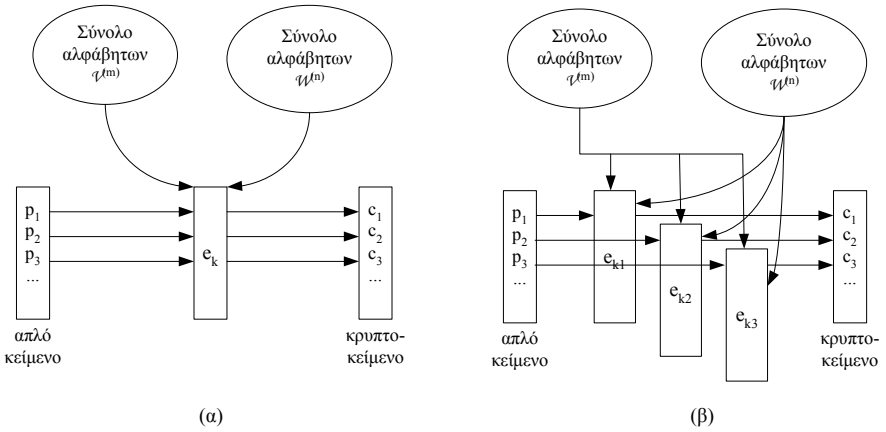
$$d_k(c) = 7c - 12 \mod 24$$

3.3.3. Πολυαλφαβητική αντικατάσταση

ΟΡΙΣΜΟΣ 3.7 – Πολυαλφαβητική αντικατάσταση είναι η κρυπτογραφική πράξη e_i: $\mathcal{F}^{(n)} \to \mathcal{G}^{(m)}$, όπου το i παίρνει τουλάχιστον δύο διαφορετικές τιμές κατά την κρυπτογράφηση ενός απλού κειμένου**.**

Σε αντίθεση με τη μονοαλφαβητική αντικατάσταση όπου η κρυπτογραφική πράξη e_i επιλέγει μια αντιστοιχία του αλφάβητου του απλού κειμένου με ένα συγκεκριμένο αλφάβητο του κρυπτοκειμένου, στην πολυαλφαβητική αντικατάσταση η κρυπτογράφηση μεταπηδά μεταξύ πολλών αλφάβητων του κρυπτοκειμένου όπως φαίνεται στο Σχήμα 3.7. Έτσι ένα γράμμα του απλού κειμένου μπορεί να αντιστοιχισθεί σε περισσότερα από ένα γράμματα του κρυπτοκειμένου. Αυτό έχει ως αποτέλεσμα όλες οι συχνότητες εμφάνισης των γραμμάτων να προσεγγίζουν

την τιμή 1/*n*, δηλαδή αίρεται η έμφυτη αδυναμία του μονοαλφαβητικού κρυπταλγόριθμου να κρύψει την πληροφορία περί συχνότητας των γραμμάτων. Όπως θα δούμε στη συνέχεια, η δυνατότητα αυτή που μας παρέχει η πολυαλφαβητική αντικατάσταση μπορεί να μας οδηγήσει σε άνευ όρων ασφαλή κρυπταλγόριθμο.



Σχήμα 3.7 (α) Μονοαλφαβητική και (β) πολυαλφαβητική αντικατάσταση

Ο Κρυπταλγόριθμος Vigenère

ΟΡΙΣΜΟΣ 3.8 – Ο κρυπταλγόριθμος **Vigenère** ορίζει το κρυπτοσύστημα $\mathcal{F} = \mathcal{G} = \boldsymbol{K} = \boldsymbol{Z}_n^l$ και με $\boldsymbol{e_k} \in \boldsymbol{E}^l$, $\boldsymbol{d_k} \in \boldsymbol{D}^l$ τέτοια ώστε

$$\boldsymbol{c} = \boldsymbol{e_k}(\boldsymbol{p}) = (e_{k_1}(p_1), e_{k_2}(p_2), ..., e_{k_l}(p_l))$$

και

$$\boldsymbol{p} = \boldsymbol{d_k}(\boldsymbol{c}) = (d_{k_1}(c_1), d_{k_2}(c_2), ..., d_{k_l}(c_l)),$$

για

$$\boldsymbol{p} \in \mathcal{F}, \mathbf{c} \in \mathcal{G}, \boldsymbol{k} = (k_1, k_2, ..., k_l) \in \boldsymbol{K}$$

και όπου

$$e_k(p) = p + k \mod n$$

και

$$d_k(p) = p - k \mod n.$$

Η κρυπτογραφική πράξη e_k είναι αυτή του κρυπταλγόριθμου μετάθεσης. Η ποσότητα l προσδιορίζει το μήκος του κλειδιού, καθώς και τον αριθμό των αλφάβητων που συμμετέχουν στην κρυπτογράφηση. Εάν $l = 1$, τότε ο κρυπταλγόριθμος Vigenère εκφυλίζεται στο μονοαλφαβητικό κρυπταλγόριθμο μετάθεσης.

ΠΑΡΑΔΕΙΓΜΑ 3.11 – Κρυπτογράφηση Vigenère. Για να γίνει παραστατικό το παράδειγμα αντιστοιχίζουμε τις αριθμητικές τιμές στα γράμματα του ελληνικού αλφάβητου στο απλό κείμενο και στο κλειδί.

Έστω το απλό κείμενο P = [ναζεικανεισηναμηζει] και το κλειδί k = [αμλετ]. Η κρυπτογράφηση θα είναι ως εξής:

απλό κειμ.	ν	α	ζ	ε	ι	κ	α	ν	ε	ι	σ	η	ν	α	μ	η	ζ	ε	ι
κλειδί	α	μ	λ	ε	τ	α	μ	λ	ε	τ	α	μ	λ	ε	τ	α	μ	λ	ε
κρυπτοκ.	Ν	Μ	Π	Ι	Γ	Κ	Μ	Ψ	Ι	Γ	Σ	Σ	Ψ	Ε	Ζ	Η	Ρ	Ο	Ν

Από το παράδειγμα αυτό μπορούμε να κάνουμε ορισμένες χρήσιμες παρατηρήσεις. Πρώτον, επειδή το κλειδί είναι μικρότερο από το απλό κείμενο, θα πρέπει να επαναλαμβάνεται προκειμένου να κρυπτογραφηθεί όλο το απλό κείμενο. Στο παράδειγμά μας, ο κρυπταλγόριθμος Vigenère εκτελέστηκε τέσσερις φορές. Το

p / κλειδί	α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω
Α	ΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩ
Β	ΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑ
Γ	ΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒ
Δ	ΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓ
Ε	ΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔ
Ζ	ΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕ
Η	ΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖ
Θ	ΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗ
Ι	ΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘ
Κ	ΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙ
Λ	ΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚ
Μ	ΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛ
Ν	ΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜ
Ξ	ΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝ
Ο	ΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞ
Π	ΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟ
Ρ	ΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠ
Σ	ΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡ
Τ	ΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣ
Υ	ΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤ
Φ	ΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥ
Χ	ΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦ
Ψ	ΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧ
Ω	ΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨ

Πίνακας 3.4 Οικογένεια αλφάβητων Vigenère

τελευταίο τμήμα του απλού κειμένου που κρυπτογραφήθηκε ήταν μικρότερο από το κλειδί κατά ένα γράμμα, οπότε παραλήφθηκε και το τελευταίο γράμμα του κλειδιού. Δεύτερον, το **α** κρυπτογραφήθηκε τις δυο φορές σε **Μ** και τη μια φορά σαν **Ε**. Παρόμοια, το **ε** κρυπτογραφήθηκε δυο φορές ως **Ι** και μια φορά ως **Ο**. Μπορούμε να αντιληφθούμε ότι η ασφάλεια του Vigenère εξαρτάται από το μήκος του κλειδιού, όχι μόνον για την αποτροπή της επίθεσης της εξαντλητικής αναζήτησης, γεγονός το οποίο ισχύει σε όλα τα κρυπτοσυστήματα, αλλά και για την απόκρυψη της κατανομής συχνοτήτων των γραμμάτων.

Στο παράδειγμά μας χρησιμοποιήθηκαν 5 αλφάβητα από κάποιο σύνολο αλφάβητων. Η κρυπτογραφική πράξη e_k περιορίζει το σύνολο αυτό στα αλφάβητα τα οποία προκύπτουν με μετατόπιση του αρχικού αλφάβητου (e_0). Επομένως στο παράδειγμα διατίθενται συνολικά 24 διαφορετικά αλφάβητα όπως φαίνεται στον Πίνακα 3.4 και η ακολουθία του κλειδιού καθορίζει τη σειρά που θα επιλεχθούν τα αλφάβητα αυτά.

Ασφάλεια του Vigenère

Λογικά το πρώτο βήμα στην προσπάθεια ανακάλυψης του κλειδιού ενός κρυπταλγόριθμου Vigenère, είναι να βρεθεί το μέγεθος του κλειδιού αυτού. Εάν βρεθεί το μέγεθος, τότε το πρόβλημα μπορεί να αναχθεί σε πολλές μονοαλφαβητικές απλές αντικαταστάσεις, αφού σε ένα κρυπτοκείμενο, όλα τα σύμβολα που απέχουν απόσταση l μεταξύ τους θα ανήκουν στο ίδιο αλφάβητο. Υπάρχουν δύο γνωστές κρυπταναλυτικές μέθοδοι για τον προσδιορισμό του μήκους του κλειδιού: ο έλεγχος του Kasiski και ο δείκτης σύμπτωσης.

Ο έλεγχος του Kasiski εκμεταλλεύεται το γεγονός ότι συχνά επαναλαμβανόμενα μοτίβα του απλού κειμένου θα τύχουν κρυπτογράφησης με τμήματα του κλειδιού, παραπάνω από μια φορά. Στην περίπτωση που συμβεί αυτό, το επαναλαμβανόμενο μοτίβο θα είναι φανερό και στο κρυπτοκείμενο. Για παράδειγμα, στην ελληνική γλώσσα τα μοτίβα «οσ», «στο», «απο», «νοσ», «του» συναντώνται αρκετά συχνά σε ένα κείμενο. Εάν κάποιο από τα μοτίβα αυτά τύχει να κρυπτογραφηθεί δυο φορές από το ίδιο τμήμα του κλειδιού, τα αντίστοιχα τμήματα του κρυπτοκειμένου θα είναι τα ίδια. Έτσι παρατηρώντας το κρυπτοκείμενο, ο αντίπαλος σημειώνει τις θέσεις των μοτίβων που εμφανίζονται παραπάνω από μια φορά. Βέβαια μικρά σε μέγεθος μοτίβα (των δύο γραμμάτων) είναι πιθανότατα τυχαία, αλλά οποιοδήποτε μοτίβο μεγαλύτερο των τριών γραμμάτων είναι σχεδόν βέβαιο ότι δεν είναι τυχαίο και αντιστοιχεί σε μοτίβο του απλού κειμένου. Πράγματι, η πιθανότητα ενός μοτίβου τριών γραμμάτων να είναι τυχαία είναι ίση με $1/(24^3) \cong 0.0007$ και τεσσάρων γραμμάτων είναι ίση με $1/(24^4) \cong 0.00003$.

Έχοντας σημειώσει τις θέσεις του επαναλαμβανόμενου μοτίβου, ο αντίπαλος υπολογίζει τις διαδοχικές αποστάσεις που εμφανίζεται το μοτίβο αυτό. Γνωρίζοντας ότι το κλειδί θα πρέπει να είναι υποπολλαπλάσιο των αποστάσεων αυτών, παραγοντοποιεί τις αποστάσεις, οπότε το κλειδί θα είναι κάποιο από τους κοινούς αυτούς παράγοντες.

ΠΑΡΑΔΕΙΓΜΑ 3.12 – Ο έλεγχος του Kasiski. Θεωρούμε το ακόλουθο κρυπτοκείμενο:

[ΔΘΒΚΗΤΓΓΓΨΗΓΓΘΘΔΥΘΜΨΧΤΥΥΙΚΥΜΔΨΧΤΑΧΓΓΩΜΞ
ΟΜΝΑΞΦΠΝΛΔΨΜΕΜΞΦΠΥΘΗΞΣΕΜΝΝΨΑΥΥΖΔΘΤΥΠΣΘΥΞΝ
ΟΡΚΥΙΘΦΧΕΨΜΗΞΨΣΠΝΤΒΡΚΖΔΟΠΚΖΑΥΣΧΤΒΒΒΜΔΣΒΨΤΡΠ
ΜΗΔΔΧΟΚΔΖΨΩΟΜΗΩΔΑΨΕΠΑΓΜΝΨΚΞΔΑΒΚΣΝΝΠΘΨΟΝΟΚ
ΣΠΝΨΚΨΨΗΞΞΕΛΝΓΗΨΦΗΞΓΓΓΕΞΝΕΤΜΑΘΨΖΑΗΜΗΦΓΓΘΡΣ
ΑΜΥΣΧΓΒΚΣΦΞΣΩΞΣΑΒΥΠΧΓΥΞΝΤΓΟΩΡΚΩΜΘΝΔΑΘΗΓΦΝΑ
ΩΚΜΝΘΛΓΜΕΠΥΘΔΦΜΘΨΧΦΨΚΡΔΧΠΘΕΦΤΑΥΛΔΩΜΝΨΦΡΤΔ
ΨΔΔΜΔΟΜΝΡΥΗΘΑΘΞΗΤΓΒΥΤΥΓΥΚΣ]

Το πρώτο στάδιο είναι η ανακάλυψη των μοτίβων. Όσο περισσότερες επαναλήψεις ενός μοτίβου και όσο μεγαλύτερο το μέγεθος του μοτίβου, τόσο μεγαλύτερη και η πιθανότητα να ανακαλύψουμε το μήκος του κλειδιού. Στο κρυπτοκείμενο του παραδείγματος είναι υπογραμμισμένα ορισμένα μοτίβα τριών χαρακτήρων. Για να θεωρηθεί μια ακολουθία χαρακτήρων ως μοτίβο, θα πρέπει η ακολουθία αυτή να εμφανισθεί στο κείμενο τουλάχιστον δύο φορές. Για τα μοτίβα που ανακαλύψαμε, υπολογίζουμε τις αποστάσεις τους:

μοτίβο	απόσταση	παράγοντες
ΓΓΘ	190	19,10,5,2
ΨΧΤ	10	10,5,2
ΟΜΝ	255	85,51,17,15,5,3.

Οι παράγοντες είναι πολλαπλάσια της απόστασης. Το μήκος του κλειδιού θα πρέπει να είναι κοινό πολλαπλάσιο όλων των αποστάσεων. Από τα πρώτα δύο μοτίβα, το «ΓΓΘ» και το «ΨΧΤ», τα υποψήφια μήκη είναι τρία σε πλήθος (10,5,2). Ωστόσο, το 2 απορρίπτεται διότι είναι πολύ μικρό. Εάν το μήκος του κλειδιού ήταν ίσο με 2, τότε θα εμφανιζόταν πολύ περισσότερα (και μεγαλύτερα σε μέγεθος) μοτίβα. Η κατάσταση ξεκαθαρίζει με το τρίτο μοτίβο το οποίο έχει μόνο ένα κοινό παράγοντα με τα άλλα δυο, το 5. Ανακαλύπτοντας το μέγεθος του κλειδιού, ανάγουμε το κρυπτοσύστημα σε 5 κρυπτοσυστήματα μονοαλφαβητικής αντικατάστασης. Αφήνουμε την κρυπτανάλυση του παραπάνω κρυπτοκειμένου σαν άσκηση στον αναγνώστη (το απλό κείμενο είναι ένα απόσπασμα από το «Θεώρημα του Παπαγάλου», του Ντενί Γκετζ).

Πολλές φορές όμως το μήκος του κλειδιού μπορεί να είναι αρκετά μεγάλο ή το κρυπτοκείμενο που έχουμε στη διάθεσή μας μπορεί να είναι περιορισμένο σε μέγεθος. Στο παραπάνω παράδειγμα το μήκος του κλειδιού αποκαλύφθηκε με μόνο τρία μοτίβα των τριών χαρακτήρων. Κάτι τέτοιο δεν τυχαίνει πάντοτε, με αποτέλεσμα ο έλεγχος του Kasiski να μας δίνει ένα σύνολο από υποψήφια μήκη για το κλειδί.

Στη συνέχεια, θεωρούμε ότι ο έλεγχος του Kasiski δεν κατάφερε να απομονώσει το σωστό μήκος του κλειδιού. Έτσι έχοντας βρει υποψήφια μήκη για το κλειδί,

θα πρέπει να αποκλείσουμε το λάθος και να καταλήξουμε στο σωστό. Ο υπολογισμός του ***δείκτη σύμπτωσης*** (index of coincidence) είναι ένα δυνατό εργαλείο που αποκαλύπτει αν ένα κρυπτοκείμενο περιλαμβάνει ένα ή παραπάνω αλφάβητα. Θα πρέπει να σημειωθεί ότι ο δείκτης σύμπτωσης είναι αποτελεσματικός σε μικρό αριθμό αλφάβητων, οπότε θα πρέπει να χρησιμοποιείται σε συνδυασμό με τον έλεγχο του Kasiski, για να εφαρμόζεται σε όσον το δυνατόν λιγότερα αλφάβητα.

Έστω ότι το πιθανό μήκος του κλειδιού βρέθηκε να είναι ίσο με l. Αυτό σημαίνει ότι το κρυπτοκείμενο δημιουργήθηκε από l αλφάβητα, που μπορούν να ξεχωρίσουν σε ομάδες κρυπτοκειμένων:

ομάδα 1: $\{c_1, c_{l+1}, c_{2l+1}, ...\}$
ομάδα 2: $\{c_2, c_{l+2}, c_{2l+2}, ...\}$
…
ομάδα l: $\{c_l, c_{2l}, c_{3l}, ...\}$

Εάν όντως έχουμε πετύχει το μήκος του κλειδιού, τότε η κάθε ομάδα περιέχει μόνο στοιχεία από ένα αλφάβητο. Σε περίπτωση όμως που το κλειδί έχει μήκος διαφορετικό του l, κάθε ομάδα θα περιέχει στοιχεία από δύο και πάνω αλφάβητα. Στη χειρότερη περίπτωση θα περιέχει στοιχεία από όλα τα αλφάβητα. Ο δείκτης σύμπτωσης που αναπτύχθηκε από τον Sinkov (1966), εφαρμόζεται σε οποιαδήποτε μια από τις παραπάνω ομάδες και είναι ένας τρόπος μέτρησης της απόκλισης της κατανομής των συχνοτήτων των γραμμάτων μεταξύ του κρυπτοκειμένου και της αντίστοιχης φυσικής γλώσσας που απαρτίζει το απλό κείμενο. Εάν η ομάδα περιέχει μόνον ένα αλφάβητο, η κατανομή των συχνοτήτων θα είναι «κοντά» σε αυτήν του απλού κειμένου. Εάν όμως υπάρχουν παραπάνω από ένα αλφάβητα στο κρυπτοκείμενο, οι κατανομές μεταξύ του απλού κειμένου και του κρυπτοκειμένου θα «απέχουν», με την κατανομή του κρυπτοκειμένου να παρουσιάζει μικρότερες διακυμάνσεις από μια «επίπεδη» κατανομή.

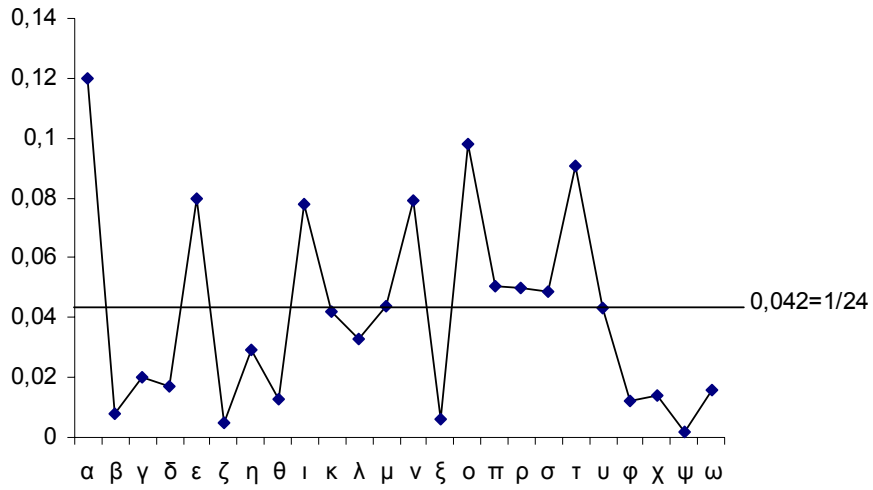
Με βάση τη συχνότητα εμφάνισης των γραμμάτων στην ελληνική γλώσσα του Πίνακα 3.2, κατασκευάζουμε το ιστόγραμμα όπως φαίνεται στο Σχήμα 3.8.

Έστω P_i η πιθανότητα να επιλέξουμε τυχαία ένα γράμμα από κάποιο (απλό) κείμενο. Σύμφωνα με το Σχήμα 3.8, $P_\alpha = 0{,}12$, $P_\beta = 0{,}008$, $P_\gamma = 0{,}02$, κ.ο.κ., με

$$\sum_{i=\alpha}^{i=\omega} P_i = 1 .$$

Στην περίπτωση που όλα τα γράμματα εμφανίζονταν με την ίδια συχνότητα, θα είχαμε:

$$P_\alpha = P_\beta = ... = P_\omega = \frac{1}{24} \cong 0{,}042 .$$



Σχήμα 3.8 Κατανομή συχνότητας εμφάνισης γραμμάτων στην ελληνική γλώσσα.

Μια τέτοια φυσική γλώσσα δεν υπάρχει, αλλά όπως αναφέραμε η χρησιμοποίηση πολλών αλφάβητων έχει αυτόν το στόχο. Από τη στατιστική μπορούμε να δανεισθούμε το μέτρο της διακύμανσης, το οποίο είναι το μέσο άθροισμα των τετραγώνων των διαφορών των παρατηρήσεων από τη μέση τους τιμή. Ως παρατηρήσεις εδώ, θεωρούμε τις πιθανότητες P_i των γραμμάτων, ενώ ως μέση τιμή θεωρούμε την ομοιόμορφη κατανομή 1/24:

$$
\begin{aligned}
24 \cdot \mathrm{Var}[P] &= \sum_{i=a}^{i=\omega} \left(P_i - \frac{1}{24} \right)^2 \\
&= \sum_{i=a}^{i=\omega} \left(P_i^2 - \frac{2}{24} P_i + \left(\frac{1}{24} \right)^2 \right) \\
&= \sum_{i=a}^{i=\omega} P_i^2 - \frac{2}{24} \sum_{i=a}^{i=\omega} P_i + \sum_{i=a}^{i=\omega} \left(\frac{1}{24} \right)^2 \\
&= \sum_{i=a}^{i=\omega} P_i^2 - \frac{2}{24} \cdot 1 + 24 \cdot \left(\frac{1}{24} \right)^2 \\
&= \sum_{i=a}^{i=\omega} P_i^2 - 0,0417
\end{aligned}
$$

Από τον Πίνακα 3.2, η διακύμανση της ελληνικής γλώσσας υπολογίζεται $\mathrm{Var}_{ελληνικά}$=(0.0675–0.0417)/24=0.001. Στην πραγματικότητα, η ποσότητα που μας

ενδιαφέρει είναι το άθροισμα των τετραγώνων των πιθανοτήτων, δηλαδή η τιμή 0.0675, για την ελληνική γλώσσα. Για να υπολογίσουμε το αντίστοιχο άθροισμα στο κρυπτοκείμενο, θα πρέπει πρώτα να κατανοήσουμε την ποσότητα P_i^2. Το τετράγωνο της πιθανότητας σημαίνει ότι δύο γεγονότα συμβαίνουν συγχρόνως. Στην περίπτωσή μας η ποσότητα αυτή εκφράζει την πιθανότητα επιλογής δύο οποιωνδήποτε χαρακτήρων από το κρυπτοκείμενο να είναι *i*. Επομένως το πρόβλημα είναι να υπολογίσουμε την πιθανότητα αυτή στο κρυπτοκείμενο.

Έστω F_i ο αριθμός εμφανίσεων του γράμματος *i* στο κρυπτοκείμενο. Η πιθανότητα να επιλέξουμε δύο φορές το γράμμα *i* θα είναι το πλήθος των δυνατών δυάδων (*i*, *i*), προς το συνολικό πλήθος των δυάδων. Το συνολικό πλήθος των δυνατών δυάδων (*i*, *i*) θα είναι $F_i(F_i - 1)/2$, ενώ εάν το κρυπτοκείμενο έχει μέγεθος *n*, το συνολικό πλήθος των δυάδων θα είναι αντίστοιχα $n(n - 1)/2$. Έτσι, η ποσότητα

$$\frac{F_i(F_i-1)}{n(n-1)}$$

αντιπροσωπεύει την πιθανότητα να επιλέξουμε δυο φορές το γράμμα *i*. Εάν όντως το κλειδί είναι το σωστό, τότε η πιθανότητα αυτή θα πρέπει να είναι κοντά στην πιθανότητα P_i του απλού κειμένου. Αν όμως το κλειδί δεν είναι το σωστό, τότε η επιλογή ίδιων γραμμάτων από το κρυπτοκείμενο δεν θα αντιστοιχεί στο ίδιο γράμμα του απλού κειμένου, με αποτέλεσμα οι δύο πιθανότητες να απέχουν. Προκειμένου να συγκρίνουμε τη διακύμανση του κρυπτοκειμένου με αυτήν της φυσικής γλώσσας (του απλού κειμένου), ορίζουμε ως δείκτη σύμπτωσης (*IC*) την ποσότητα:

$$IC = \sum_{i=\alpha}^{i=\omega} \frac{F_i(F_i-1)}{n(n-1)}$$

Ο δείκτης σύμπτωσης υπολογίζεται σε κάθε ομάδα κρυπτοκειμένου χωριστά. Αν το μήκος του κλειδιού είναι σωστό, τότε το κρυπτοκείμενο περιέχει μόνον ένα αλφάβητο και ο δείκτης σύμπτωσης θα είναι κοντά στην ποσότητα 0.0675. Όσο προστίθενται αλφάβητα και η κατανομή των πιθανοτήτων προσεγγίζει την ομοιόμορφη κατανομή, ο δείκτης σύμπτωσης με τη σειρά του προσεγγίζει την τιμή 0.0417. Επομένως, οι τιμές του δείκτη σύμπτωσης βρίσκονται μεταξύ 0.0417 και 0.0675. Στην περίπτωση που υπάρχουν πάνω από ένα υποψήφια μήκη κλειδιών, η σύγκριση των δεικτών σύμπτωσής τους φανερώνει και το πραγματικό κλειδί.

Σημειωματάρια μιας χρήσης και ο κρυπταλγόριθμος του Vernam

Είναι φανερή η ευαισθησία του κρυπταλγόριθμου Vigenère στο μήκος του κλειδιού, όπως και η αποτελεσματικότητα των κρυπταναλυτικών επιθέσεων του Kasiski και του δείκτη σύμπτωσης. Όσο μεγαλύτερο το κλειδί, τόσο πιο λίγες οι επαναλήψεις των μοτίβων σε ένα κρυπτοκείμενο, τόσο περισσότερα τα αλφάβητα στο κρυπτοκείμενο. Η ύπαρξη πολλών αλφάβητων στο κρυπτοκείμενο σημαίνει

ότι η συχνότητα κατανομής των γραμμάτων του κρυπτοκειμένου προσεγγίζει την ομοιόμορφη κατανομή 1/*n*, όπου *n* το πλήθος των συμβόλων του αλφάβητου κρυπτογράφησης. Τίθεται λοιπόν το ερώτημα του μήκους του κλειδιού:

«Υπάρχει κάποιο μήκος του κλειδιού σε μια κρυπτογράφηση τύπου Vigenère, που να καθιστά το κρυπτοσύστημα ασφαλές;».

Η απάντηση σε αυτήν την ερώτηση μας οδηγεί στα *σημειωματάρια μιας χρήσης*, τα οποία δεν απαντούν μόνο καταφατικά στην παραπάνω ερώτηση, αλλά επιπλέον μπορούν να συστήσουν κρυπτοσυστήματα τα οποία είναι άνευ όρων ασφαλή. Όπως υποδείξαμε στο Κεφάλαιο 1, ένα άνευ όρων ασφαλές κρυπτοσύστημα μπορεί να αντισταθεί σε οποιαδήποτε κρυπταναλυτική επίθεση, ανεξάρτητα από τις υπολογιστικές δυνατότητες του αντιπάλου.

ΟΡΙΣΜΟΣ 3.9 - Ένα σημειωματάριο μιας χρήσης είναι το κρυπτοσύστημα με τα ακόλουθα χαρακτηριστικά:

- Το μήκος του κλειδιού είναι ίσο με το μήκος του απλού κειμένου.
- Το κλειδί χρησιμοποιείται μόνον για μια κρυπτογράφηση. Η κρυπτογράφηση ενός μελλοντικού απλού κειμένου γίνεται με κλειδί το οποίο δεν έχει συμμετάσχει σε κρυπτογράφηση.
- Τα στοιχεία του κλειδιού δεν συσχετίζονται μεταξύ τους.

Ο ορισμός του σημειωματάριου μιας χρήσης δικαιολογεί σε ένα βαθμό την ονομασία του. Το κλειδί μπορεί να θεωρηθεί ότι είναι μια μεγάλη ακολουθία αριθμών καταγεγραμμένη σε ένα σημειωματάριο, όπου κάθε φορά που χρησιμοποιούνται τμήματα της ακολουθίας, τα τμήματα αυτά διαγράφονται για να μην επαναχρησιμοποιηθούν. Τέτοια σημειωματάρια είχαν δημιουργηθεί και χρησιμοποιηθεί κατά τον Δεύτερο Παγκόσμιο Πόλεμο. Κάθε σημειωματάριο τυπωνόταν εις διπλούν και μοιραζόταν μεταξύ των δυο επικοινωνούντων. Ο αποστολέας επέλεγε μια τυχαία σελίδα και κρυπτογραφούσε το απλό κείμενο με την ακολουθία των αριθμών που περιείχε η επιλεγμένη σελίδα. Στη συνέχεια, αποκολλούσε τη σελίδα από το σημειωματάριο για να μη χρησιμοποιηθεί κατά λάθος δεύτερη φορά, και την κατέστρεφε. Το κρυπτογραφημένο κείμενο συνοδευόταν από τον αριθμό σελίδας του σημειωματάριου μιας χρήσης. Ο παραλήπτης του κρυπτοκειμένου ο οποίος ήταν ο δεύτερος και πλέον μοναδικός κάτοχος της σελίδας αυτής, ήταν σε θέση να εκτελέσει την αποκρυπτογράφηση. Το κρυπτοσύστημα που χρησιμοποιήθηκε είναι γνωστό ως κρυπτοσύστημα Vernam:

ΟΡΙΣΜΟΣ 3.10 – Το κρυπτοσύστημα Vernam είναι ένα κρυπτοσύστημα σημειωματάριου μιας χρήσης, όπου κρυπταλγόριθμος είναι αυτός του Vigenère και το μήκος του κλειδιού είναι ίδιο με το μήκος του κρυπτοκειμένου.

Ίσως η περιγραφή του μήκους του κλειδιού είναι πλεονασμός στον ορισμό, αλλά η σκόπιμη δήλωσή του δίνει έμφαση στο σημαντικό αυτό χαρακτηριστικό.

Ασφάλεια του Vernam

Ο ισχυρισμός ότι ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές δεν είναι δυνατόν να περάσει απαρατήρητος στην κοινότητα των κρυπτολόγων. Θα χρησιμοποιήσουμε τη θεωρία της πληροφορίας του Shannon για να αποδείξουμε ότι το κρυπτοσύστημα Vernam ταξινομείται στην κατηγορία των κρυπταλγόριθμων που είναι άνευ όρων ασφαλή (Preneel, 1998).

Θεωρούμε το κρυπτοσύστημα όπου $\mathcal{F} = \mathcal{G} = \{0,1\}$ και $\boldsymbol{P}, \boldsymbol{C}, \boldsymbol{K} \in \{0,1\}^{(m)}$, δηλαδή αναφερόμαστε σε κρυπτοσύστημα με δυαδικά στοιχεία και δυαδικά μηνύματα μήκους m. Η κρυπτογράφηση ορίζεται ως:

$$y = x \oplus k$$

ενώ η αποκρυπτογράφηση ορίζεται ως:

$$x = y \oplus k\,.$$

με $x \in \boldsymbol{P}$ και $y \in \boldsymbol{C}$. Επιπλέον θεωρούμε ότι όλα τα κλειδιά έχουν ίσες πιθανότητες να επιλεχθούν, επομένως:

$$P(k) = \left(\frac{1}{2}\right)^m$$

Αυτό όμως σημαίνει ότι ένα απλό κείμενο x μπορεί να κρυπτογραφηθεί ως οποιοδήποτε κρυπτοκείμενο y, με πιθανότητα ίδια για όλα τα κρυπτοκείμενα και αντίστροφα, ένα κρυπτοκείμενο y μπορεί να προέρχεται από οποιοδήποτε απλό κείμενο x με την ίδια πιθανότητα. Δηλαδή:

$$P(x \mid y) = P(y \mid x) = \left(\frac{1}{2}\right)^m = P(k)$$

το οποίο ισχύει για κάθε x και y ανεξάρτητα από την κατανομή πιθανότητας του x και σε αυτό οφείλεται η «μίξη» του κλειδιού με το απλό κείμενο. Έτσι τα x και y είναι στατιστικώς ανεξάρτητα και από πλευράς πληροφορίας:

$$H(\boldsymbol{P}, \boldsymbol{C}) = H(\boldsymbol{P}) + H(\boldsymbol{C}) \qquad (3.1)$$

Για ένα άνευ όρων ασφαλές κρυπτοσύστημα θα πρέπει η πληροφορία σχετικά με το κρυπτοσύστημα που έχει ο αντίπαλος ο οποίος γνωρίζει το κρυπτοκείμενο, να είναι ίδια με αυτήν αφότου γίνει γνωστό το αντίστοιχο απλό κείμενο, δηλαδή:

$$H(\boldsymbol{P} \mid \boldsymbol{C}) = H(\boldsymbol{P})$$

Η σχέση αυτή σημαίνει ότι ο αντίπαλος βρίσκεται ακριβώς στην ίδια κατάσταση πριν και μετά από την γνώση της αποκρυπτογράφησης, δηλαδή εάν απόκτησε κάποια γνώση, δεν μπορεί να την χρησιμοποιήσει για ένα κρυπτοκείμενο του οποίου το απλό κείμενο δεν είναι γνωστό. Επομένως, η γνώση που απέκτησε είναι μηδέν.

Πράγματι,

$$H(\boldsymbol{P},\boldsymbol{C}) = H(\boldsymbol{P}) + H(\boldsymbol{C} \mid \boldsymbol{P}) = H(\boldsymbol{C}) + H(\boldsymbol{P} \mid \boldsymbol{C})$$

η οποία λόγω της (3.1) δίνει

$$H(\boldsymbol{P} \mid \boldsymbol{C}) = H(\boldsymbol{P}) .$$

Το κρυπτοσύστημα Vernam είναι πρακτικώς αδύνατο για τις περισσότερες εφαρμογές. Οι υψηλές ταχύτητες μετάδοσης πληροφορίας στις μέρες μας καθιστούν ένα τέτοιο σύστημα ασύμφορο έως απαγορευτικό. Πολλές φορές βρισκόμαστε στην κατάσταση να συναλλασσόμαστε με άτομα τα οποία δεν έχουμε επικοινωνήσει στο παρελθόν και μέσω του Διαδικτύου. Σε ένα τέτοιο περιβάλλον η ανταλλαγή σημειωματάριων μιας χρήσης δεν είναι εφικτό να πραγματοποιηθεί.

Έτσι, για μια ακόμη φορά καλείται η κρυπτογραφία να μετασχηματίσει το πρόβλημα της ασφαλούς επικοινωνίας. Αντί να ανταλλάσσουμε κλειδιά τα οποία να έχουν μήκος ίσο με αυτό του απλού κειμένου, μπορούμε να χρησιμοποιήσουμε κλειδιά μεγέθους ενός κλάσματος του απλού κειμένου. Μας ενδιαφέρει ο κρυπταλγόριθμος να χρησιμοποιεί πράξεις οι οποίες να «εκτείνουν» το μικρό, ως προς το απλό κείμενο κλειδί, με τέτοιον τρόπο ώστε να προσεγγίζουμε τη συμπεριφορά ενός σημειωματάριου μιας χρήσης. Στην πραγματικότητα οποιοδήποτε κρυπτοσύστημα που χρησιμοποιεί κλειδί μικρότερο από το μήκος του απλού κειμένου απέχει σε ασφάλεια από το σημειωματάριο μιας χρήσης. Όμως θα πρέπει να συμβιβαστούμε σε χαμηλότερη ασφάλεια για χάρη της αποτελεσματικότητας της επικοινωνίας. Τα επόμενα κεφάλαια του βιβλίου επικεντρώνονται στη μελέτη των κρυπτοσυστημάτων καθώς και των κρυπτογραφικών πράξεων, που μπορούν να οδηγήσουν στην κατασκευή κρυπταλγόριθμων με αποδεκτό επίπεδο κρυπτογραφικής δύναμης.

Ο Κρυπταλγόριθμος του Hill

Ο κρυπταλγόριθμος του Hill είναι μια πολυδιάστατη (πολυαλφαβητική) γενίκευση του γραμμικού κρυπταλγόριθμου. Ας ανακαλέσουμε την πράξη κρυπτογράφησης του γραμμικού κρυπταλγόριθμου:

$$c = e_k(p) = ap + b \mod \mathrm{n} .$$

Το κάθε σύμβολο του απλού κειμένου κρυπτογραφείται με βάση τη γραμμική σχέση και με το κλειδί (a, b). Ο κρυπταλγόριθμος του Hill ορίζει ένα σύστημα γραμμικών εξισώσεων, όπου το πλήθος των εξισώσεων είναι ανάλογο του μήκους του απλού κειμένου, του κρυπτοκειμένου και του κλειδιού. Ο κρυπταλγόριθμος δέχεται m σύμβολα του απλού κειμένου όπου αντικαθίστανται με m σύμβολα του κρυπτοκειμένου. Η αντικατάσταση αυτή εκφράζεται με ένα σύστημα γραμμικών ισοδυναμιών, modulo n:

$$
\begin{aligned}
c_1 &\equiv k_{11}p_1 + k_{12}p_2 + ... + k_{1m}p_m \pmod{n} \\
c_2 &\equiv k_{21}p_1 + k_{22}p_2 + ... + k_{2m}p_m \pmod{n} \\
&\vdots \\
c_m &\equiv k_{m1}p_1 + k_{m2}p_2 + ... + k_{mm}p_m \pmod{n}
\end{aligned}
$$

Όπως είδαμε στο προηγούμενο κεφάλαιο, αυτό το γραμμικό σύστημα μπορεί να εκφρασθεί υπό μορφή πινάκων:

$$
\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix} \equiv \begin{pmatrix} k_{11} & k_{12} & ... & k_{1m} \\ k_{21} & k_{22} & ... & k_{2m} \\ \vdots & & \ddots & \\ k_{m1} & k_{m2} & ... & k_{mm} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix} \pmod{n}
$$

ή

$$\boldsymbol{c} \equiv \boldsymbol{K}\boldsymbol{p} \pmod{n}.$$

Η αποκρυπτογράφηση του κρυπτοκειμένου απαιτεί τον υπολογισμό του $\boldsymbol{K}^{-1}$, modulo n, δηλαδή του αντίστροφου πίνακα που ορίζει το κλειδί. Κατά την αποκρυπτογράφηση θα ισχύει:

$$\boldsymbol{P} \equiv \boldsymbol{K}^{-1}\boldsymbol{c} \equiv \boldsymbol{K}^{-1}(\boldsymbol{K}\boldsymbol{p}) \equiv (\boldsymbol{K}^{-1}\boldsymbol{K})\boldsymbol{p} \equiv \boldsymbol{p} \pmod{n}.$$

Όπως είναι γνωστό (§ 2.6), για την ύπαρξη του $\boldsymbol{K}^{-1}$ πρέπει να είναι $\gcd(\det\boldsymbol{K}, n) = 1$, δηλαδή πρέπει οι ακέραιοι $\det\boldsymbol{K}$ και n να είναι σχετικώς πρώτοι.

ΠΑΡΑΔΕΙΓΜΑ 3.13 – Θα παρουσιάσουμε το παράδειγμα του Lewand (2000), το οποίο χρησιμοποιεί το λατινικό αλφάβητο και την Αγγλική γλώσσα (επομένως οι πράξεις θα πραγματοποιούνται modulo 26). Έστω το κρυπτοσύστημα Hill με κλειδί:

$$\mathbf{K} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}.$$

Η κρυπτογράφηση ορίζεται από την πράξη:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \bmod 26 .$$

Έστω ότι θα κρυπτογραφήσουμε το απλό κείμενο:

P = [meetmeathteusualplaceattenratherthaneightoclockq]

Επειδή ο κρυπταλγόριθμος είναι ουσιαστικά κρυπταλγόριθμος τμήματος όπου το κάθε τμήμα έχει μέγεθος ίσο με δύο, έπεται ότι το απλό κείμενο θα πρέπει να είναι πολλαπλάσιο του δύο. Έτσι προσθέτουμε στο τέλος ακόμη ένα σύμβολο (το «**q**»).

Το τελευταίο σύμβολο θα πρέπει να μην επηρεάζει το νόημα του απλού κειμένου, επομένως η επιλογή του γίνεται με βάση το σκεπτικό αυτό. Στη συνέχεια αντιστοιχίζουμε τα γράμματα στα αριθμητικά τους ισοδύναμα ($\mathbf{a}\mapsto 1$, $\mathbf{b}\mapsto 2$,…):

απλό κείμενο	m	e	e	t	m	e	a	t	t	h	e	…
αντιστοίχιση	13	5	5	20	13	5	1	20	20	8	5	…

Η κρυπτογράφηση εφαρμόζεται τμηματικά στο απλό κείμενο. Για τα πρώτα δύο στοιχεία του απλού κειμένου, είναι:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}\begin{pmatrix} 13 \\ 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 137 \\ 100 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 22 \end{pmatrix} \bmod 26.$$

Έτσι το κρυπτοκείμενο που αντιστοιχεί στους αριθμούς 7 και 22 είναι τα γράμματα **G** και **V**. Αν επαναλάβουμε τη διαδικασία για όλο το απλό κείμενο, το κρυπτοκείμενο που προκύπτει είναι το:

C=[GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQRKR].

Για να ορίσουμε την πράξη αποκρυπτογράφησης, θα πρέπει να υπολογίσουμε τον $\boldsymbol{K}^{-1}$. Βρίσκουμε πρώτα την ορίζουσα του $\boldsymbol{K}$:

$$\det\boldsymbol{K} = 9 \cdot 7 - 4 \cdot 5 = 43.$$

Επειδή gcd(43, 26) = 1, ο $43^{-1} \bmod 26$ υπάρχει και εύκολα βρίσκουμε ότι είναι ο 23. Πράγματι, $43 \cdot 23 = 989 \equiv 1 \pmod{26}$. Με τα στοιχεία αυτά μπορούμε να υπολογίσουμε το κλειδί αποκρυπτογράφησης:

$$\boldsymbol{K}^{-1} \equiv 23\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}(\bmod 26) \equiv \begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix}(\bmod 26) \equiv \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}(\bmod 26).$$

Έτσι κατά την αποκρυπτογράφηση αντιστοιχίζουμε τα γράμματα του κρυπτοκειμένου στα αριθμητικά τους ισοδύναμα:

κρυπτοκείμενο	G	V	U	I	G	V	K	O	D	Z	Y	…
αντιστοίχιση	7	22	21	9	7	22	11	15	4	26	25	…

και στη συνέχεια εφαρμόζουμε την πράξη αποκρυπτογράφησης:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \bmod 26$$

στα στοιχεία του κρυπτοκειμένου, ανά δύο. Για τα πρώτα δύο στοιχεία η αποκρυπτογράφηση δίνει:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \begin{pmatrix} 7 \\ 22 \end{pmatrix} \bmod 26 = \begin{pmatrix} 299 \\ 655 \end{pmatrix} \bmod 26 = \begin{pmatrix} 13 \\ 5 \end{pmatrix} \bmod 26$$

που αντιστοιχούν στα δύο πρώτα σύμβολα του απλού κειμένου, **me**.

Ασφάλεια του Hill

Αν και ο κρυπταλγόριθμος Hill έχει τη δυνατότητα να κρύψει τις συχνότητες εμφάνισης των συμβόλων του απλού κειμένου, δεν μπορεί να αντισταθεί σε μια επίθεση γνωστού απλού κειμένου. Ο αντίπαλος έχοντας απλό κείμενο μήκους m^2 και το αντίστοιχο κρυπτοκείμενο, μπορεί να ανακαλύψει το κλειδί. Το απλό κείμενο και το κρυπτοκείμενο εκφράζονται ως δύο πίνακες $m \times m$, όπου θα ισχύει:

$$\begin{pmatrix} c_1 & & c_{m^2-m} \\ c_2 & \cdots & \vdots \\ \vdots & & c_{m^2-1} \\ c_m & & c_{m^2} \end{pmatrix} \equiv \boldsymbol{K} \begin{pmatrix} p_1 & & p_{m^2-m} \\ p_2 & \cdots & \vdots \\ \vdots & & p_{m^2-1} \\ p_m & & p_{m^2} \end{pmatrix} \pmod{n}$$

Αναγκαία συνθήκη για να ανακαλυφθεί το κλειδί είναι ένας από τους δύο αυτούς πίνακες να έχει αντίστροφο. Εάν ο πίνακας του απλού κειμένου έχει αντίστροφο, τότε ο αντίπαλος μπορεί να βρει απευθείας το κλειδί $\boldsymbol{K}$, ενώ στην περίπτωση που ο πίνακας του κρυπτοκειμένου έχει αντίστροφο, τότε ο αντίπαλος μπορεί να υπολογίσει τον $\boldsymbol{K}^{-1}$ και στη συνέχεια να τον αντιστρέψει για να ανακαλύψει το κλειδί. Εάν κανένας από τους πίνακες δεν έχει αντίστροφο τότε θα πρέπει τα στοιχεία των πινάκων του απλού κειμένου και του κρυπτοκειμένου να αναδιαταχθούν κατά τέτοιον τρόπο ώστε κάποιος από τους πίνακες αυτούς να έχει ορίζουσα ίση με ακέραιο σχετικώς πρώτο με τον n. Δηλαδή:

$$\boldsymbol{K} \equiv \begin{pmatrix} c_1 & & c_{m^2-m} \\ c_2 & \cdots & \vdots \\ \vdots & & c_{m^2-1} \\ c_m & & c_{m^2} \end{pmatrix} \begin{pmatrix} p_1 & & p_{m^2-m} \\ p_2 & \cdots & \vdots \\ \vdots & & p_{m^2-1} \\ p_m & & p_{m^2} \end{pmatrix}^{-1} \pmod{n}$$

εάν η ορίζουσα του πίνακα του απλού κειμένου είναι ακέραιος σχετικώς πρώτος με τον n, ή

$$\boldsymbol{K}^{-1} \equiv \begin{pmatrix} c_1 & & c_{m^2-m} \\ c_2 & \cdots & \vdots \\ \vdots & & c_{m^2-1} \\ c_m & & c_{m^2} \end{pmatrix}^{-1} \begin{pmatrix} p_1 & & p_{m^2-m} \\ p_2 & \cdots & \vdots \\ \vdots & & p_{m^2-1} \\ p_m & & p_{m^2} \end{pmatrix} \pmod{n}$$

εάν η ορίζουσα του κρυπτοκειμένου είναι ακέραιος σχετικώς πρώτος με τον n. Η επίθεση που περιγράψαμε φαίνεται στο ακόλουθο παράδειγμα.

ΠΑΡΑΔΕΙΓΜΑ 3.14 – Κρυπτανάλυση του Hill. Θα παρουσιάσουμε το παράδειγμα κρυπτανάλυσης του Lewand (2000), που αναφέρεται στο Παράδειγμα 3.13. Έστω ότι ο αντίπαλος έχει υποκλέψει το κρυπτοκείμενο:

C=[GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQR KR].

Ας υποθέσουμε ότι ο αντίπαλος γνωρίζει το κρυπτοσύστημα το οποίο χρησιμοποιείται (όπως άλλωστε μας επιτρέπει και η αρχή του Kerchoff). Μια επιπλέον παράτολμη υπόθεση είναι να θεωρήσουμε ότι ο αντίπαλος γνωρίζει το μέγεθος του κλειδιού, δηλαδή γνωρίζει τις διαστάσεις του πίνακα $\boldsymbol{K}$. Άλλωστε ο δείκτης σύμπτωσης που περιγράψαμε παραπάνω είναι ένα δυνατό εργαλείο στον εντοπισμό του μεγέθους του κλειδιού.

Ένας έμπειρος κρυπταναλυτής μπορεί να παρατηρήσει ότι το μοτίβο **DZ** εμφανίζεται τρεις φορές στο κρυπτοκείμενο. Επειδή στην αγγλική γλώσσα το πιο συχνό μοτίβο είναι το **th**, υπάρχει μεγάλη πιθανότητα να είναι **DZ** $\leftrightarrow$ **th**. Μια άλλη σημαντική πληροφορία, είναι ότι συνήθως μετά το **th** ακολουθεί το γράμμα **e**. Εάν καταγράψουμε τα δυο σύμβολα που ακολουθούν μετά από το **DZ** στο κρυπτοκείμενο, θα πάρουμε: **YP, MU** και **MY**. Δηλαδή είναι **YP** $\leftrightarrow$ **e#, MU** $\leftrightarrow$ **e#, MY** $\leftrightarrow$ **e#** σύμφωνα με την υπόθεσή μας (όπου # το σύμβολο του απλού κειμένου που δεν μπορούμε στο σημείο αυτό να αντιστοιχίσουμε).

Αλλά ας επιστρέψουμε στην αρχική υπόθεσή μας, **DZ** $\leftrightarrow$ **th**. Εάν όντως ισχύει η αντιστοιχία αυτή, θα είναι:

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix} \bmod 26$$

όπου ο πρώτος πίνακας της σχέσης αποτελεί το κλειδί αποκρυπτογράφησης. Από την παραπάνω σχέση μπορούμε να υπολογίσουμε τα k_{11} και k_{21} ως εξής:

$4k_{11} = 20 \bmod 26$
$4k_{21} = 8 \bmod 26$

από όπου προκύπτει ότι $k_{11} = 5$ ή $k_{11} = 18$, και $k_{21} = 2$ ή $k_{21} = 15$. Εξετάζουμε πρώτα την περίπτωση όπου $k_{11} = 5$. Από τις αντιστοιχίες **YP** $\leftrightarrow$ **e#**, **MU** $\leftrightarrow$ **e#**, **MY** $\leftrightarrow$ **e#**, δημιουργούμε τις ακόλουθες ισότητες:

$$(\alpha)\ \begin{pmatrix} 5 & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} 25 \\ 16 \end{pmatrix} = \begin{pmatrix} 5 \\ * \end{pmatrix} (\bmod 26),$$

$$(\beta)\ \begin{pmatrix} 5 & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} 13 \\ 21 \end{pmatrix} = \begin{pmatrix} 5 \\ * \end{pmatrix} (\bmod 26),$$

$$(\gamma)\ \begin{pmatrix} 5 & k_{12} \\ k_{21} & k_{22} \end{pmatrix}\begin{pmatrix} 13 \\ 25 \end{pmatrix} = \begin{pmatrix} 5 \\ * \end{pmatrix} (\mathrm{mod}\ 26),$$

όπου "*****" τα αριθμητικά ισοδύναμα των άγνωστων συμβόλων #. Από τις τρεις παραπάνω ισότητες προκύπτουν οι εξής ισότητες:

(α) $125 + 16k_{12} = 5 \bmod 26$, με λύσεις $k_{12} = 12$ ή $k_{12} = 25$
(β) $65 + 21k_{12} = 5 \bmod 26$, με λύση $k_{12} = 12$
(γ) $65 + 25k_{12} = 5 \bmod 26$, με λύση $k_{12} = 24$.

Παρατηρούμε από τα παραπάνω ότι εάν δεχθούμε ότι $k_{12} = 12$, τότε **YP** $\leftrightarrow$ **e#**, **MU** $\leftrightarrow$ **e#**, ενώ **MY** $\leftrightarrow$ **##**. Εάν επαναλάβουμε τη διαδικασία αυτή για την περίπτωση όπου $k_{11} = 18$, θα καταλήξουμε στις παρακάτω ισότητες:

(α) $450 + 16k_{12} = 5 \bmod 26$, όπου δεν υπάρχει λύση για το k_{12}
(β) $234 + 21k_{12} = 5 \bmod 26$, με λύση $k_{12} = 25$
(γ) $234 + 25k_{12} = 5 \bmod 26$, με λύση $k_{12} = 21$.

Το γεγονός ότι για μία από τις ισότητες δεν ορίζεται το k_{12}, ενισχύει την αρχική υπόθεσή μας ότι $k_{11} = 5$.

Έχοντας ανακαλύψει τα k_{11} και k_{12}, συνεχίζουμε για τα υπόλοιπα δύο στοιχεία του κλειδιού αποκρυπτογράφησης. Ήδη γνωρίζουμε ότι $k_{21} = 2$ ή $k_{21} = 15$. Αυτό σημαίνει ότι το κλειδί αποκρυπτογράφησης είναι ο πίνακας

$$\begin{pmatrix} 5 & 12 \\ 2 & k_{22} \end{pmatrix}, \text{ ή ο πίνακας } \begin{pmatrix} 5 & 12 \\ 15 & k_{22} \end{pmatrix}.$$

Ας υποθέσουμε ότι το κλειδί είναι ο πρώτος πίνακας. Στο σημείο αυτό έχουμε αποκρυπτογραφήσει παραπάνω από το μισό κρυπτοκείμενο:

13	$14+22k_{22}$	5	$16+9\ k_{22}$	13	$14+22\ k_{22}$	1	$22+15\ k_{22}$
20	8	5	$24+16\ k_{22}$	19	$16+8\ k_{22}$	1	$10+11\ k_{22}$
16	$20+8\ k_{22}$	1	16	5	$20+6\ k_{22}$	20	$6\ k_{22}$
5	$20+19\ k_{22}$	18	$20+19\ k_{22}$	20	8	5	$21\ k_{22}$
20	8	1	$25\ k_{22}$	5	$6+10\ k_{22}$	7	$8+10\ k_{22}$
20	$20+23\ k_{22}$	3	$20+21\ k_{22}$	15	$8+18\ k_{22}$	11	$22+18\ k_{22}$

Τα παραπάνω προέκυψαν εφαρμόζοντας την πράξη αποκρυπτογράφησης:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 2 & k_{22} \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \bmod 26$$

σε όλο το κρυπτοκείμενο. Στη συνέχεια αντικαθιστούμε τους αριθμούς από τα αντίστοιχα γράμματα του απλού κειμένου, εκτός φυσικά από τα σημεία στα οποία περιλαμβάνεται ο άγνωστος k_{22}:

m	$14+22k_{22}$	e	$16+9\,k_{22}$	m	$14+22\,k_{22}$	a	$22+15\,k_{22}$
t	h	e	$24+16\,k_{22}$	s	$16+8\,k_{22}$	a	$10+11\,k_{22}$
p	$20+8\,k_{22}$	a	p	e	$20+6\,k_{22}$	t	$6\,k_{22}$
e	$20+19\,k_{22}$	r	$20+19\,k_{22}$	t	h	e	$21\,k_{22}$
t	h	a	$25\,k_{22}$	e	$6+10\,k_{22}$	g	$8+10\,k_{22}$
t	$20+23\,k_{22}$	c	$20+21\,k_{22}$	o	$8+18\,k_{22}$	k	$22+18\,k_{22}$

Το απλό κείμενο που έχουμε ανακτήσει ως εδώ μπορεί να μας δώσει και άλλες πληροφορίες για το υπόλοιπο άγνωστο κρυπτοκείμενο. Παρατηρούμε ότι η σχέση $14 + 22k_{22}$ εμφανίζεται μετά το γράμμα **m**. Επειδή μετά το συγκεκριμένο γράμμα είναι σχεδόν απίθανο να ακολουθεί σύμφωνο, υποθέτουμε ότι το $14 + 22k_{22}$ αντιπροσωπεύει φωνήεν. Με αυτό το σκεπτικό, εξετάζουμε τις εξής πέντε περιπτώσεις:

1. **a**, ή ισοδύναμα $14 + 22k_{22} = 1 \bmod 26$, όπου δεν υπάρχει λύση για το k_{22}.
2. **e**, ή ισοδύναμα $14 + 22k_{22} = 5 \bmod 26$, όπου δεν υπάρχει λύση για το k_{22}.
3. **i**, ή ισοδύναμα $14 + 22k_{22} = 9 \bmod 26$, όπου δεν υπάρχει λύση για το k_{22}.
4. **o**, ή ισοδύναμα $14 + 22k_{22} = 15 \bmod 26$, όπου δεν υπάρχει λύση για το k_{22}.
5. **u**, ή ισοδύναμα $14+22k_{22}=21 \bmod 26$, όπου δεν υπάρχει λύση για το k_{22}.

Το γεγονός ότι δεν υπάρχει καμία λύση για το στοιχείο k_{22} μας οδηγεί στο συμπέρασμα ότι η υπόθεσή μας ότι $k_{21} = 2$ είναι λανθασμένη. Επομένως επιλέγουμε τη δεύτερη λύση $k_{21} = 15$, και ο πίνακας του κλειδιού αποκρυπτογράφησης είναι ο:

$$\begin{pmatrix} 5 & 12 \\ 15 & k_{22} \end{pmatrix}.$$

Έτσι θα πρέπει να επαναλάβουμε τη διαδικασία αποκρυπτογράφησης με τον δεύτερο υποψήφιο πίνακα. Το απλό κείμενο που προκύπτει (μετά από αντικατάσταση των γνωστών αριθμών με τα σύμβολα του απλού κειμένου) είναι:

m	$1+22k_{22}$	e	$3+9\,k_{22}$	m	$1+22\,k_{22}$	a	$9+15\,k_{22}$
t	h	e	$11+16\,k_{22}$	s	$3+8\,k_{22}$	a	$23+11\,k_{22}$
p	$20+8\,k_{22}$	a	p	e	$7+6\,k_{22}$	t	$6\,k_{22}$
e	$7+19\,k_{22}$	r	$20+19\,k_{22}$	t	h	e	$13+21\,k_{22}$
t	h	a	$13+25\,k_{22}$	e	$19+10\,k_{22}$	g	$21+10\,k_{22}$
t	$12+23\,k_{22}$	c	$7+21\,k_{22}$	o	$21+18\,k_{22}$	k	$9+18\,k_{22}$

Στη συνέχεια επαναλαμβάνουμε τη δοκιμή της υπόθεσης ότι το $1 + 22k_{22}$ είναι φωνήεν, για να εντοπίσουμε τις πιθανές υποψήφιες τιμές για το k_{22}:

1. **a**, ή ισοδύναμα $1 + 22k_{22} = 1 \bmod 26$, με λύση $k_{22} = 0$ ή $k_{22} = 13$
2. **e**, ή ισοδύναμα $1 + 22k_{22} = 5 \bmod 26$, με λύση $k_{22} = 12$ ή $k_{22} = 25$
3. **i**, ή ισοδύναμα $1 + 22k_{22} = 9 \bmod 26$, με λύση $k_{22} = 11$ ή $k_{22} = 24$
4. **o**, ή ισοδύναμα $1 + 22k_{22} = 15 \bmod 26$, με λύση $k_{22} = 3$ ή $k_{22} = 16$
5. **u**, ή ισοδύναμα $1 + 22k_{22} = 21 \bmod 26$, με λύση $k_{22} = 8$ ή $k_{22} = 21$.

Έτσι προκύπτουν 10 πιθανές τιμές για το k_{22}. Από τις τιμές αυτές απορρίπτονται εκείνες οι οποίες έχουν ως αποτέλεσμα ορίζουσα ίση με ακέραιο όχι σχετικώς πρώτο με τον 26, διότι στην περίπτωση αυτή δεν ορίζεται ο πίνακας του κλειδιού κρυπτογράφησης. Συνεπώς καταλήγουμε στις υποψήφιες τιμές: 3, 11, 13, 21 και 25. Με εξαντλητική αναζήτηση επάνω στις πέντε αυτές τιμές, μπορούμε να εντοπίσουμε το αρχικό και σωστό απλό κείμενο:

κλειδί	αποκρυπτογραφημένο κείμενο
$\begin{pmatrix} 5 & 12 \\ 15 & 3 \end{pmatrix}$	moedmoabthegsaadpraceytrelrythexthajewghtccrowkk
$\begin{pmatrix} 5 & 12 \\ 15 & 11 \end{pmatrix}$	miexmiartheesmanpdaceutnehruthejthabeyghtecdokky
$\begin{pmatrix} 5 & 12 \\ 15 & 13 \end{pmatrix}$	maepmaavthekscajptacegtzetrgthezthazesghtyctouki
$\begin{pmatrix} 5 & 12 \\ 15 & 21 \end{pmatrix}$	muejmualtheisoatpfacectveprcthelthareughtacfoikw
$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$	meetmeattheusualplaceattenratherthaneightoclockq

Είναι φανερό ότι το σωστό κλειδί είναι ο τελευταίος από τους παραπάνω πίνακες, όπως προδίδει το απλό κείμενο.

3.3.4. Ανίχνευση της γλώσσας

Στα παραδείγματα και στις κρυπταναλυτικές επιθέσεις που παρουσιάσαμε, υποθέσαμε ότι η γλώσσα το απλού κειμένου ήταν γνωστή στον κρυπταναλυτή. Μια υπόθεση ήταν ότι επειδή πχ. το κρυπτοκείμενο ήταν ελληνικά σύμβολα, τότε το απλό κείμενο θα έπρεπε να είναι σε ελληνικό κείμενο. Η υπόθεση αυτή έγινε χάριν απλούστευσης της παρουσίασης των κρυπτοσυστημάτων. Μια πιο ρεαλιστική υπόθεση είναι ότι ο αντίπαλος που έχει πρόσβαση μόνο στο κρυπτοκείμενο, δεν γνωρίζει την γλώσσα την οποία απεικονίζει το απλό κείμενο. Το λατινικό αλφάβητο για παράδειγμα χρησιμοποιείται σε περισσότερο από μια γλώσσες. Επιπλέον, το

κρυπτοκείμενο θα μπορούσε να αποτελούνταν από σύμβολα τα οποία δεν αντιστοιχούν σε κάποιο από τα γνωστά αλφάβητα. Η ασφάλεια ενός κρυπτοσυστήματος δεν θα πρέπει να εξαρτάται από τα σύμβολα του κρυπτοκειμένου, αλλά μόνον από το κλειδί (αρχή του Kerchoff).

Όπως είδαμε, η αδυναμία ορισμένων κρυπτοσυστημάτων να κρύψουν την κατανομή συχνοτήτων εμφάνισης των συμβόλων του απλού κειμένου, παρέχει αρκετή πληροφορία στον αντίπαλο προκειμένου να επιτύχει σε κάποια κρυπταναλυτική απόπειρα. Η άνιση κατανομή συχνοτήτων των συμβόλων του απλού κειμένου, καθώς και η περίσσεια μιας γλώσσας, είναι έμφυτα χαρακτηριστικά σε κάθε γλώσσα και ένα ασφαλές κρυπτοσύστημα θα πρέπει να έχει την ικανότητα να αποκρύπτει τα χαρακτηριστικά αυτά στο κρυπτοκείμενο.

Στη συνέχεια θα παρουσιάσουμε δύο ελέγχους που εκμεταλλεύονται στατιστικά χαρακτηριστικά του κρυπτοκειμένου για να προσδιορίσουν τη γλώσσα του απλού κειμένου. Ειδικά σε μονοαλφαβητική αντικατάσταση, ο καθορισμός της γλώσσας είναι πολύ ευκολότερος από την ίδια την αποκρυπτογράφηση του κρυπτοκειμένου με τις μεθόδους αυτές.

Ο έλεγχος Κάπα

Ο έλεγχος Κάπα είναι μια ισχυρή μέτρηση η οποία αφορά τη σχετική συχνότητα εμφάνισης ενός συμβόλου στην ίδια θέση, σε δυο διαφορετικά κείμενα.

ΟΡΙΣΜΟΣ 3.11 – Έστω $M=[m_1 \ldots m_2 \ldots m_n]$ και $M'=[m_1' m_2' \ldots m_n']$ δυο κείμενα μήκους n. Ορίζεται η ποσότητα Κάπα ως:

$$\kappa(M, M') = \frac{1}{n} \sum_{i=1}^{n} \delta(m_i, m_i') ,$$

όπου:

$$\delta(x, y) = \begin{cases} 1 & \text{εάν } x = y \\ 0 & \text{εάν } x \neq y \end{cases} .$$

ΠΑΡΑΔΕΙΓΜΑ 3.15 – Υπολογισμός Κάπα σε δείγμα κειμένου.

ΟΠΩΣ Ε Ι Δ ΑΜΕ Η Α Δ Υ ΝΑΜ Ι Α Ο Ρ Ι Σ ΜΕ Ν ΩΝ Κ Ρ Υ Π Τ Ο Σ Υ Σ Τ ΗΜ
ΗΑΝ Ι Σ Η Κ Α Τ Α Ν Ο ΜΗ Σ Υ Χ Ν Ο Τ Η Τ Ω Ν Τ Ω Ν Σ Υ Μ Β Ο Λ Ω Ν Τ Ο Υ Α Π
*
Α Τ Ω Ν Ν Α Κ Ρ Υ Ψ Ο Υ Ν Τ Η Ν Κ Α Τ Α Ν Ο ΜΗ Σ Υ Χ Ν Ο Τ Η Τ Ω Ν Ε Μ Φ Α Ν Ι
Λ Ο Υ Κ Ε Ι Μ Ε Ν Ο Υ Κ Α Θ Ω Σ Κ Α Ι Η Π Ε Ρ Ι Σ Σ Ε Ι Α Μ Ι Α Σ Γ Λ Ω Σ Σ Α Σ
* * *

Ε ΤΗΠΛΗΡΟΦΟΡ Ι Α ΣΤΟΝΑΝΤ Ι ΠΑΛΟΠΡΟΚΕ ΙΜΕΝΟΥΝΑΕΠ
ΕΝΑΑΣΦΑΛΕΣΚΡΥΠΤΟΣΥΣΤΗΜΑΘΑΠΡΕΠΕ Ι ΝΑΕΧΕ Ι ΤΗΝ
* ** * * ** **
ΣΗΣ ΤΩΝΣΥΜΒΟΛΩΝΤΟΥΑΠΛΟΥΚΕ ΙΜΕΝΟΥΠΑΡΕΧΕ Ι ΑΡΚ
Ε Ι ΝΑ Ι ΕΜΦΥΤΑΧΑΡΑΚΤΗΡ Ι Σ Τ Ι ΚΑΣΕΚΑΘΕΓΛΩΣΣΑΚΑ Ι
*

Στο δείγμα βρέθηκαν να υπάρχουν κοινά γράμματα σε 14 θέσεις. Συνεπώς το Κάπα θα είναι $\kappa(M, M') = 14/160 = 8.75\%$. Με στατιστικές μετρήσεις έχει βρεθεί ότι το Κάπα εξαρτάται από τη γλώσσα στην οποία είναι τα κείμενα M, M' και είναι διαφορετικό για κάθε γλώσσα. Στον Πίνακα 3.5 παραθέτονται τα Κάπα διαφόρων γλωσσών. Όπως είναι αναμενόμενο, όσο περισσότερα γράμματα του αλφαβήτου υπάρχουν σε ένα αλφάβητο, τόσο μικρότερο αναμένεται να είναι το Κάπα, αφού η πιθανότητα να συμπέσει το ίδιο γράμμα σε δυο κείμενα στην ίδια θέση είναι μικρότερη.

Γλώσσα	Πλήθος γραμμάτων αλφάβητου	Κάπα (%)
Ελληνικά*	24	8,75
Αγγλικά	26	6,61
Γερμανικά	26	7,62
Γαλλικά	26	7,78
Ιταλικά	26	7,38
Ισπανικά	26	7,75
Ιαπωνικά (Romaji)	26	8,19
Ρώσικα	32	5,29

Πίνακας 3.5 – Τυπικές τιμές Κάπα για διαφορετικές γλώσσες (Πηγή: Kullback, 1976, εκτός από *).

Πειραματικές μετρήσεις έδειξαν ότι για όλες τις μονοαλφαβητικές αντικαταστάσεις καθώς και όλες τις πολυαλφαβητικές αντικαταστάσεις γραμμικής φύσης, οι ποσότητες Κάπα δύο κρυπτοκειμένων που προκύπτουν από κρυπτογράφηση δύο απλών κειμένων με ίδιο κλειδί, είναι στατιστικώς ίσες.

Ο έλεγχος Χι

Ο έλεγχος *Χι* αναφέρεται στις συχνότητες εμφάνισης των γραμμάτων σε ένα μήνυμα και είναι πιο κρυπταναλυτικά αδύναμος σε σχέση με τον έλεγχο Κάπα, αφού ισχύει μόνο για μονοαλφαβητικές αντικαταστάσεις.

ΟΡΙΣΜΟΣ 3.12 – Έστω $M = [m_1 m_2 ... m_n]$ και $M' = [m'_1 m'_2 ... m'_n]$ δυο κείμενα μήκους n, και $\{x_1, x_2, ..., x_l\}$ το αλφάβητο των παραπάνω μηνυμάτων . Έστω f_i και

f_i' οι συχνότητες εμφάνισης του συμβόλου x_i στα κείμενα M και M' αντίστοιχα. Ορίζεται η ποσότητα $Xι$ ως:

$$\chi(M,M') = \frac{1}{n^2}\sum_{i=1}^{n} f_i f_i' .$$

Παρόμοια με τον έλεγχο Κάπα, πειραματικές μετρήσεις έδειξαν ότι για όλες τις μονοαλφαβητικές αντικαταστάσεις οι ποσότητες $Xι$ δύο κρυπτοκειμένων που προκύπτουν από κρυπτογράφηση δύο απλών κειμένων με ίδιο κλειδί, είναι στατιστικώς ίσες.

3.3.5. Κρυπτογράφηση γινομένου

Η κρυπτογράφηση γινομένου είναι ένας όρος που επινοήθηκε από τον Shannon για να περιγράψει τη σύνθεση δύο η περισσοτέρων κρυπτογραφικών πράξεων για τη δημιουργία ενός κρυπταλγόριθμου, ο οποίος είναι κρυπτογραφικά δυνατότερος από τις δυο πράξεις. Η κρυπτογράφηση γινομένου ορίζεται σε ενδομορφικά κρυπτοσυστήματα:

ΟΡΙΣΜΟΣ 3.13 – Ένα κρυπτοσύστημα $\{\mathcal{F},\mathcal{G},\mathbf{E},\mathbf{D},\mathbf{K}\}$ ονομάζεται ***ενδομορφικό***, όταν $\mathcal{F}=\mathcal{G}$.

Σήμερα τα περισσότερα κρυπτοσυστήματα σε ψηφιακά υπολογιστικά συστήματα είναι ενδομορφικά για λόγους συμβατότητας και ευκολίας υλοποίησής των.

ΟΡΙΣΜΟΣ 3.14 – Έστω δύο ενδομορφικά κρυπτοσυστήματα $S_1 = \{\mathcal{F}_1, \mathcal{G}_1, \boldsymbol{E}_1, \boldsymbol{D}_1, \boldsymbol{K}_1\}$ και $S_2 = \{\mathcal{F}_2, \mathcal{G}_2, \boldsymbol{E}_2, \boldsymbol{D}_2, \boldsymbol{K}_2\}$ με $\mathcal{F}_1 = \mathcal{F}_2$ και κρυπτογραφικές πράξεις $e_1 \in \boldsymbol{E}_1$, $d_1 \in \boldsymbol{D}_1$ και $e_2 \in \boldsymbol{E}_2$, $d_2 \in \boldsymbol{D}_2$ αντίστοιχα. Το κρυπτοσύστημα $S_3 = \{\mathcal{F}_3, \mathcal{G}_3, \boldsymbol{E}_3, \boldsymbol{D}_3, \boldsymbol{K}_3\}$ ορίζεται ως το κρυπτογραφικό γινόμενο των S_1 και S_2, με:

$\mathcal{F}_3 = \mathcal{G}_3 (= \mathcal{F}_1 = \ldots)$
$e_3(p) = e_2(e_1(p))$,
$d_3(c) = d_1(d_2(c))$,
$\boldsymbol{K_3} = \boldsymbol{K_1} \times \boldsymbol{K_2}$.

Το κρυπτογραφικό γινόμενο ονομάζεται και ***κρυπτογραφική σύνθεση***.

Το κρυπτογραφικό γινόμενο ορίζει μια ομάδα κρυπταλγόριθμων οι οποίοι είναι ενδεχομένως κρυπτογραφικά δυνατοί. Στην πράξη οι περισσότεροι κρυπταλγόριθμοι συμμετρικών συστημάτων προκύπτουν από κρυπτογραφικό γινόμενο απλών κρυπτογραφικών πράξεων. Το κρυπτογραφικό γινόμενο μπορεί να έχει ως αποτέλεσμα την αποτελεσματική ενίσχυση των χαρακτηριστικών της σύγχυσης και της διάχυσης.

Κρυπτογραφικό γινόμενο μπορεί να προκύψει και από ένα μόνο κρυπτοσύστημα, όταν το απλό κείμενο κρυπτογραφείται και το αποτέλεσμα (κρυπτοκείμε-

νο) επανακρυπτογραφείται με την ίδια πράξη. Αναγκαία συνθήκη για την αύξηση της κρυπτογραφικής δύναμης του γινομένου σε αυτήν την περίπτωση είναι το κρυπτοσύστημα να μην αποτελεί ομάδα.

ΟΡΙΣΜΟΣ 3.15 – Ένα κρυπτοσύστημα $\{\boldsymbol{\mathcal{P}}, \boldsymbol{\mathcal{C}}, \boldsymbol{E}, \boldsymbol{D}, \boldsymbol{K}\}$ αποτελεί ***ομάδα*** όταν:

$$\exists k \in K : e_k(p) = e_{k_1}(e_{k_2}(p)), \forall k_1, k_2 \in K .$$

Με άλλα λόγια, ένα κρυπτοσύστημα αποτελεί ομάδα όταν υπάρχει ένα κλειδί k για το οποίο η διαδοχική κρυπτογράφηση ενός απλού κειμένου με οποιαδήποτε σειρά κλειδιών, δίνει το ίδιο αποτέλεσμα με την κρυπτογράφηση υπό του κλειδιού k.

ΠΑΡΑΔΕΙΓΜΑ 3.16 – Έλεγχος ύπαρξης ομάδας. Έστω το κρυπτοσύστημα $\{\boldsymbol{\mathcal{P}}, \boldsymbol{\mathcal{C}}, \boldsymbol{E}, \boldsymbol{D}, \boldsymbol{K}\}$ με:

$$e_k(p) = kp \mod n,$$

$$d_k(c) = k^{-1}c \mod n$$

και

$$K = \{k \in \boldsymbol{Z_n} : \gcd(k, n) = 1\} .$$

Για να αποτελεί το κρυπτοσύστημα ομάδα, θα πρέπει να υπάρχει κλειδί $k \in \boldsymbol{K}$, τέτοιο ώστε:

$$e_k(p) = kp = e_{k_1}(e_{k_2}(p)) = e_{k_1}(k_2 p) = k_1 k_2 p \mod n .$$

Δηλαδή, θα πρέπει το γινόμενο k_1k_2 να ανήκει στο σύνολο κλειδιών $\boldsymbol{K}$. Για να ισχύει αυτό, θα πρέπει $\gcd(k_1k_2, n) = 1$, για κάθε k_1, k_2. Η συνθήκη αυτή ισχύει μόνον αν ο n είναι πρώτος αριθμός. Συνεπώς μπορούμε να ισχυριστούμε ότι το κρυπτοσύστημα του παραδείγματος αποτελεί ομάδα εάν ο n είναι πρώτος αριθμός.

Κρυπτοσυστήματα τα οποία προκύπτουν από το κρυπτογραφικό γινόμενο ενός κρυπτοσυστήματος με τον εαυτό του είναι ευρέως διαδεδομένα. Ένα κρυπτοσύστημα γινομένου όπου η πράξη κρυπτογράφησης επαναλαμβάνεται στη σειρά t φορές, λέμε ότι αποτελείται από t ***γύρους κρυπτογράφησης***. Σε κάθε γύρο κρυπτογράφησης το κλειδί είναι διαφορετικό. Η ακολουθία των κλειδιών $\{k_1, k_2, \ldots, k_t\}$ ονομάζεται ***πρόγραμμα κλειδιού*** (key schedule).

Για μια ακόμα φορά βρισκόμαστε αντιμέτωποι με το πρόβλημα του (μεγάλου) κλειδιού. Ας ανακαλέσουμε ότι η κρυπτογραφία δεν μας λύνει το πρόβλημα, αλλά το μετασχηματίζει σε μια «καλύτερη» μορφή. Ο συμβιβασμός που κάναμε με την εισαγωγή της ιδέας του κλειδιού, φαίνεται να μην ισχύει πλέον. Ο συμβιβασμός αυτός ήταν να χρησιμοποιήσουμε μια αρκετά μικρότερη ποσότητα πληροφορίας η οποία θα ήταν μυστική μεταξύ της Αλίκης και του Βύρωνα, και θα ήταν αρκετή για να προστατέψει την επικοινωνία μεταξύ των δύο. Ας φανταστούμε ένα κρυπτοσύστημα γινομένου με 16 γύρους κρυπτογράφησης, όπου ο κάθε γύρος χρησι-

μοποιεί ένα κλειδί μήκους 64-bit. Επιπλέον, το κρυπτοσύστημα αυτό αποτελείται από κρυπταλγόριθμο τμήματος, όπου το τμήμα του απλού κειμένου έχει μήκος 64-bit. Τότε για κάθε κρυπτογράφηση τμήματος απλού κειμένου των 64-bit, θα απαιτείται κλειδί μήκους $64 \cdot 16 = 1024$ bits. Οι τιμές που δώσαμε στο παράδειγμα είναι αντιπροσωπευτικές για πραγματικά κρυπτοσυστήματα.

Το παραπάνω πρόβλημα αντιμετωπίζεται με τη χρήση μιας συνάρτησης s_k η οποία μπορεί να παράγει το πρόγραμμα κλειδιού από το αρχικό κλειδί. Μια τέτοια συνάρτηση ονομάζεται ***γεννήτρια προγράμματος κλειδιού*** (key schedule generator) η οποία αντιστοιχίζει ένα κλειδί $k \in \boldsymbol{K}$ στο σύνολο των κλειδιών του γινομένου:

$$s_k : \boldsymbol{K} \rightarrow \boldsymbol{K'}.$$

Με αυτόν τον τρόπο πετυχαίνουμε ένα κρυπτοσύστημα το οποίο είναι κρυπτογραφικά δυνατό, εφόσον έχει τα πλεονεκτήματα της κρυπτογράφησης γινομένου, αλλά και η ασφάλειά του εξαρτάται μόνο από το μήκος του κλειδιού $k \in \boldsymbol{K}$ και όχι των επιμέρους κλειδιών που ορίζονται στο πρόγραμμα του κλειδιού. Ο στόχος της χρήσης του κρυπτογραφικού γινομένου είναι να επιτύχουμε την απόκρυψη κάθε υπολείμματος πληροφορίας του απλού κειμένου στο κρυπτοκείμενο, ώστε η μόνη επίθεση που θα μπορούσε να εκτελέσει ο αντίπαλος να είναι αυτή της εξαντλητικής αναζήτησης του κλειδιού. Εάν καταλήξουμε σε κρυπτοσύστημα στο οποίο η μόνη επίθεση είναι η εξαντλητική αναζήτηση, τότε θα είμαστε και σε θέση να μεγαλώσουμε αρκετά το κλειδί ώστε μια τέτοια επίθεση να είναι πρακτικώς αδύνατη.

Όροι-κλειδιά του κεφαλαίου

- αβεβαιότητα πηγής
- αμοιβαία πληροφορία
- από κοινού και υπό συνθήκη αβεβαιότητα
- τέλεια μυστικότητα
- περίσσεια γλώσσας
- σύγχυση και διάχυση
- κρυπταλγόριθμος ροής και κρυπταλγόριθμος τμήματος
- αναδιάταξη και αντικατάσταση
- μονοαλφαβητική και πολυαλφαβητική αντικατάσταση
- γραμμικός κρυπταλγόριθμος
- κρυπταλγόριθμος του Hill
- κρυπταλγόριθμος του Vernam και άνευ όρων ασφάλεια
- έλεγχος του Kasiski και δείκτης σύμπτωσης
- έλεγχος Κάπα και έλεγχος Χι
- κρυπτογραφική σύνθεση (κρυπτογραφικό γινόμενο)
- πρόγραμμα κλειδιού και γεννήτρια προγράμματος κλειδιού

3.4. Ασκήσεις

1. Χρησιμοποιήστε εξαντλητική αναζήτηση για να αποκρυπτογραφήσετε το παρακάτω κείμενο:
   [ΔΩΚΡΒΩΣΓΦΚΔΙΧΜΣΧΣΙΧΞΧΩΓΔΒΣΜΙΧΩΕΞΣΧΚΣΞΤΚΔΩΧΩ-
   ΜΝΩΧΔΚΦΩΣΒΞΓ]
2. Εντοπίστε με τον έλεγχο του Kasiski πιθανά μήκη του κλειδιού για το παρακάτω κρυπτοκείμενο:
   [ΤΜΞΜΦΖΜΠΖΒΘΙΥΒΧΞΣΒΥΦΛΧΡΤΞΧΜΗΒΣΡΙΝΩΨΓΠΚΠΩΠΛΨΤΤ
   ΜΠΔΠΤΞΖΒΞΘΗΥΣΑΝΘΓΜΖΚΣΤΑΨΣΥΑΥΩΑΙΡΘΠΤΤΘΠΨΤΡΒΨΣΒΡ
   ΨΤΛΓΗΕΧΑΨΚΛΟΤΥΚΧΚΠΙΧΓΠΝΥΝΒΖΜΝΤΒΗΜΥΧΥΤΝΙΧΛΖΒΥΤ
   ΖΓΒΨΜΧΠΙΜΧΑΝΚΛΣΨΚΜΧΞΣΥΠΨΤΘΣΣΞΜΗΗΕΝΥΤΥΡΥΖΘΟΘΗ
   ΑΖΒΓΠΝΩΓΞΥΡΙΚΜΩΙΡΘΨΙΚΩΑΨΚΛΟΤΔΒΥΙΞΜΘΗΝΧΒΑΞΧΠΜΒΥ
   ΗΦΘΙΩΙΤΧΡΝΚΓΘΨΡΒΣΨΔΕΜΗΑΖΒΤΚΖΠΣΞΙΧΞΙΣΤΨΥΧΒΛΖΙΘΗΥΩ
   ΤΓΒΙΧΕΦΦΓΗΒΕΞΖΘΟΘΗΘΛΜΖΘΟΘΗΘΦΠΤΚΚΜΜΘΛΨΙΜΔΘΚΜΣ
   ΑΓΒΛΤΙΦΩΧΚΠΒΧΞΕΩΨΙΥΧΘΕΜΘΓΝΦΙΧΞ]
3. Κρυπτογραφήστε το απλό κείμενο:
   [αυριοαπεργουμε]
   με το κρυπτοσύστημα του Hill, και το κλειδί:
   $$\begin{pmatrix} 11 & 7 \\ 4 & 15 \end{pmatrix}$$
4. Ποια από τα παρακάτω κλειδιά είναι έγκυρα για το κρυπτοσύστημα του Hill; Θεωρείστε ότι χρησιμοποιούνται για να κρυπτογραφηθούν μηνύματα από το ελληνικό αλφάβητο (n=24).
   $$\begin{pmatrix} 2 & 5 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 16 \\ 6 & 8 \end{pmatrix}, \begin{pmatrix} 11 & 12 & 1 \\ 4 & 2 & 23 \\ 17 & 9 & 15 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 5 \\ 21 & 7 & 6 \\ 2 & 12 & 2 \end{pmatrix}$$
5. Υπολογίστε την πράξη αποκρυπτογράφησης για τα έγκυρα κλειδιά της προηγούμενης άσκησης.
6. Δείξτε ότι το κρυπτοσύστημα του Hill με κλειδί:
   $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
   είναι αναδιάταξη.
7. Η πράξη της αναδιάταξης έχει στόχο την αύξηση της σύγχυσης, της διάχυσης ή και των δύο;
8. Εξηγήστε γιατί το κρυπτογραφικό γινόμενο δύο αναδιατάξεων δεν έχει ως αποτέλεσμα την αύξηση της κρυπτογραφικής δύναμης.

9. Θεωρώντας ότι όλα κλειδιά έχουν την ίδια πιθανότητα εμφάνισης και ότι τα σύμβολα του απλού κειμένου έχουν την ίδια πιθανότητα εμφάνισης, υπολογίστε τις αβεβαιότητες $H(K|C)$ και $H(K|P,C)$, για τον γραμμικό κρυπταλγόριθμο.
10. Υπολογίστε την αβεβαιότητα $H(P|C)$ σε ένα κρυπτοσύστημα τέλειας μυστικότητας.
11. Υπολογίστε τη unicity distance του κρυπταλγόριθμου μετατόπισης, όπου το απλό κείμενο προέρχεται από σύμβολα του ελληνικού αλφάβητου (είναι δηλαδή, $|\boldsymbol{F}|=24$).