Πολυαλφαβητικά Συστήματα Αντικατάστασης

Αλγόριθμος Κώδικα Αντικατάστασης 2-γραμμάτων PLAYFAIR

Το κρυπτοσύστημα Playfair βασίζεται στο Αγγλικό αλφάβητο.

**Λειτουργεί ως εξής:**

Διατάσσουμε τα γράμματα του Αγγλικού αλφαβήτου, παραλείποντας το J (το J και το I θεωρούνται σαν το ίδιο γράμμα) σε έναν πίνακα 5 × 5 (που λέγεται τετράγωνοPlayfair),με κάποιο τυχαίο τρόπο.

Συνήθως το τετράγωνοPlayfair δημιουργείται βασισμένο σε μια λέξη-κλειδί (ή φράση):

Τα γράμματα της λέξης κλειδί (οι επαναλήψεις διαγράφονται) τοποθετούνται κατά σειρές, ακολουθούμενα από τα υπόλοιπα γράμματα σε αλφαβητική σειρά.

(Οι λέξεις-κλειδιά χρησιμοποιούνται προκειμένου να γίνει η διαχείριση του κλειδιού ευκολότερη). Για παράδειγμα, η λέξη-κλειδί PLAYFAIR δίνει τον παρακάτω πίνακα:

P L A Y F

I R B C D

E G H K M

N O Q S T

U V W X Z

Χωρίζουμε το αρχικό κείμενο σε ομάδες που αποτελούνται από δύο γράμματα το καθένα (2-γράμματα).

Δεν πρέπει κανένα block να περιέχει δύο φορές το ίδιο γράμμα:

Οποτεδήποτε συμβαίνει αυτό, παρεμβάλλουμε (μεταξύ των δύο γραμμάτων στο αρχικό κείμενο) ένα μηδενικό χαρακτήρα (συνήθως τοQ).

Επίσης το απλό κείμενο πρέπει να περιέχει άρτιο αριθμό γραμμάτων (διαφορετικά βάζουμε ένα μηδενικό χαρακτήρα στο τέλος του).

Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης λειτουργούν στα 2-γράμματα όπως φαίνεται παρακάτω:

**Κρυπτογράφηση:**

Αν τα δύο γράμματα του block δεν είναι στην ίδια γραμμή ή στήλη του τετραγώνου Playfair, τότε κωδικοποιούμε χρησιμοποιώντας τις άλλες δύο γωνίες του ορθογωνίου που ορίζεται από τα δύο γράμματα του block. Για παράδειγμα, χρησιμοποιώντας το παραπάνω τετράγωνο Playfair, το2-γραμμα AD ορίζει το ορθογώνιο AFBD και κρυπτογραφείται ως FB.

Αν τα δύο γράμματα του block είναι στην ίδια γραμμή (στήλη), επιλέγουμε (κυκλικά) τα γειτονικά γράμματα δεξιά (κάτω) για κάθε γράμμα τουblock.Έτσι, το RC κωδικοποιείται με το BD, τοAW με το BA, το UVμε το VW. Με αυτή τη μέθοδο το αρχικό κείμενο MATHEMATICS χωρίζεται σε διγράμματα ως MATHEMATICSQ και κρυπτογραφείται: HFQMGEFQRDTS.