Κρυπτογραφία

Εργαστηριακό μάθημα 2-3-4

Ασκήσεις επανάληψης – Αλγόριθμοι μετατόπισης

- Προσπαθήστε, χωρίς να γνωρίζετε το κλειδί, να αποκρυπτογραφήσετε το ακόλουθο κρυπτόγραμμα που έχει προκύψει από κάποιον αλγόριθμο μετατόπισης:

  ΥΧΕΩΓΤΙΦΙΤΛΓ

  απάντηση*: εξετάζουμε όλες τις πιθανές ολισθήσεις (1,2,3…) των γραμμάτων του κρυπτογράμματος προς τα αριστερά, μέχρις ώτου εμφανιστεί το μήνυμα. Βρίσκουμε λοιπόν το αρχικό μήνυμα για ολίσθηση d=2 :*

  ΣΥΓΧΑΡΗΤΗΡΙΑ

- ***Άρα: οι αλγόριθμοι μετατόπισης δεν είναι ασφαλείς, γιατί το πλήθος των δυνατών κλειδιών είναι πολύ μικρό.***
- Πειραματική δοκιμή: κατεβάστε το αρχείο *caesar.zip* και εκτελέστε τις συναρτήσεις *encrypt_caesar* και *cryptanalyse_caesar*.

Ασκήσεις επανάληψης – αλγόριθμοι μονοαλφαβητικής αντικατάστασης

- Προσπαθήστε, χωρίς να γνωρίζετε το κλειδί, να αποκρυπτογραφήστε το ακόλουθο μήνυμα, που έχει προκύψει από κάποιον αλγόριθμο απλής (μονοαλφαβητικής) αντικατάστασης:

  ΩΣΠΧΣΧΒΚΑΚΡΚΧΑΚΡΚΚΑΧΠΡΚΓΡΣΟΧ

  αν οι πιθανότητες εμφάνισης των γραμμάτων της ελληνικής γλώσσας ήταν:

  Ο: 0,12, Α:0,11, Μ:0,10, Τ: 0,09, Ι:0,09,

  Ν: 0,08, Π:0,07, Λ:0,07, Ε:0,07, Υ:0,06 …..
- *Εδώ δεν μπορούμε να εξετάσουμε όλα τα πιθανά κλειδιά γιατί είναι πάρα πολλά (24! για το ελληνικό αλφάβητο – όσες οι πιθανές αντιστοιχίσεις των 24 γραμμάτων)*

Ασκήσεις επανάληψης – αλγόριθμοι μονοαλφαβητικής αντικατάστασης (ΙΙ)

- **Απάντηση**: με βάση τις συχνότητες εμφάνισης των γραμμάτων στο κρυπτόγραμμα, κάνουμε την παρακάτω αντιστοίχιση:

  Κ -> Ο, Χ -> Α, Ρ -> Μ, Σ -> Τ, Α->Ι,

  Π -> Ν, Ω -> Π, Β -> Λ, Ο->Ε, Γ -> Υ

  (τυχαία ανάθεση στα Σ,Α αφού εμφανίζονται τον ίδιο αριθμό φορών (3). Ομοίως τυχαία ανάθεση στα Ω,Β,Ο,Γ (που εμφανίζονται 1 φορά). Αποκρυπτογραφούμε τότε το ακόλουθο μήνυμα:

  ΠΤΝΑΤΑΛΟΙΟΜΟΑΙΟΜΟΟΙΑΝΜΟΥΜΤΕΑ

  που προφανώς δεν είναι το μήνυμα που μας έστειλαν.

  Αλλάζουμε την ανάθεση των Σ,Α σε Ι,Τ αντίστοιχα. Τότε, αποκρυπτογραφούμε σε:

  ΠΙΝΑΙΑΛΟΤΟΜΟΑΤΟΜΟΟΤΑΝΜΟΥΜΙΕΑ

  όπου αρχίζει και διαφαίνεται το μήνυμα. Μπορούμε να δούμε, αλλάζοντας τις αναθέσεις στα Ω,Β,Ο,Γ σε Ε,Π,Λ,Υ αντίστοιχα ότι το μήνυμα είναι

  ΕΙΝΑΙ ΑΠΟΤΟΜΟ ΑΤΟΜΟ ΟΤΑΝ ΜΟΥ ΜΙΛΑ

  Άσκηση: κρυπτογραφήστε το μήνυμα αυτό με τον αλγόριθμο Vigenere, έχοντας ως κλειδί τη λέξη ΑΤΟΜΟ (Α-> ολίσθηση 0 θέσεων, Τ -> ολίσθηση 18 θέσεων, Ο -> ολίσθηση 14 θέσεων, Μ -> ολίσθηση 11 θέσεων)

Πολυαλφαβητικοί αλγόριθμοι αντικατάστασης – Αλγόριθμος Vigenere

- Έστω η φράση «TO BE OR NOT TO BE THAT IS THE QUESTION» και σαν κλειδί έχουμε τη φράση RELATIONS. Τότε, έχουμε το εξής κρυπτόγραμμα:

R E L A T I O N S R E L A T I O N S R E L A T I O N S R E L
T O B E O R N O T T O B E T H A T I S T H E Q U E S T I O N

K S M E H Z B B L K S M E M P O G A J X S E J C S F L Z S Y

Το R (πρώτο γράμμα της λέξης RELATIONS) είναι το 18ο γράμμα του αλφαβήτου, άρα όπου συμπίπτει με κάποιο γράμμα του μηνύματος αυτό ολισθαίνει κατά 17 θέσεις κ.ο.κ.

Κρυπτανάλυση Vigenere

- Είναι πιο ασφαλής από κάποιον πολυαλφαβητικό αλγόριθμο, γιατί δεν μπορούμε να εφαρμόσουμε την τεχνική που βασίζεται στις πιθανότητες εμφάνισης των γραμμάτων, όπως κάναμε στο προηγούμενο παράδειγμα
- Ωστόσο, αν ανακαλύψει κάποιος το μήκος του κλειδιού, μπορεί να «σπάσει» τον αλγόριθμο.
- **Μέθοδος Kasiski**: Αναζητούμε στο κρυπτόγραμμα τμήματα επαναλαμβανόμενα. Κάνουμε την υπόθεση ότι κάτι τέτοιο σημαίνει ότι το ίδιο τμήμα μηνύματος συνέπεσε με το ίδιο τμήμα του κλειδιού. Έτσι μπορούμε να βρούμε το μήκος του κλειδιού (για την ακρίβεια βρίσκουμε πιθανά μήκη κλειδιού).

Κρυπτανάλυση Vigenere (II)

- Στο προηγούμενο παράδειγμα: έχουμε τα κομμάτια KS, SM και ΜΕ που εμφανίζονται δύο φορές (για το κάθε ζευγάρι, η απόσταση μεταξύ τους είναι 9 γράμματα). Άρα, τα πιθανά μήκη κλειδιού είναι 3 ή 9, τα οποία είναι οι διαιρέτες του 9. (δεν πειράζει που δεν καταλήξαμε σε ένα συγκεκριμένο μήκος κλειδιού αλλά σε δύο πιθανά μήκη: και μόνο το γεγονός ότι βρήκαμε δύο πιθανά μήκη μειώνει σημαντικά τους υπολογισμούς που έχουμε να κάνουμε).
- Έχοντας εκτιμήσει το μήκος του κλειδιού, σπάμε το κρυπτόγραμμα σε τμήματα μήκους όσο το μήκος του κλειδιού και δουλεύουμε αντίστοιχα όπως στους απλούς αλγόριθμους αντικατάστασης (με έλεγχο συχνότητας γραμμάτων).

Μονοαλφαβητικοί αλγόριθμοι αντικατάστασης (συνέχεια)

- Γραμμικός κρυπταλγόριθμος
  - Το κρυπτόγραμμα καθορίζεται από τη σχέση c=am + b mod n, όπου το ζευγάρι (a,b) είναι το κλειδί. Το μήνυμα m ανακτάται τότε από τη σχέση

    $$m=a^{-1}(c-b) \bmod n.$$

  - Προσοχή: για να είναι αντιστρεπτός ο αλγόριθμος, πρέπει τα a, n να είναι πρώτα μεταξύ τους.
    - Παράδειγμα: έστω c=4m + 5 mod 24.

      Επειδή gcd(4,24) = 4 (≠ 1), κάθε μήνυμα m κρυπτογραφείται στο ίδιο με το m + k · 24/4 (k=1,2,3…). Παράδειγμα, για m=2, c=8+5 mod 24 = 13, ενώ και για m=8 (8=2+24/4), c=32 + 5 mod 24 = 37 mod 24 = 13.
  - Για a=1, ο γραμμικός αλγόριθμος μετατρέπεται σε αλγόριθμο μετατόπισης (ειδικά για a=1 και b=3, ο γραμμικός αλγόριθμος γίνεται ο αλγόριθμος του Καίσαρα).

Παράδειγμα κρυπτογράφησης με τον γραμμικό αλγόριθμο

- Έστω a=5, b=1 και η λέξη ΑΝΤΙΟ (ελληνικό αλφάβητο, άρα n=24).
- Για το Α (1ο γράμμα της αλφαβήτου):

$$c= 5 \cdot 0 + 1 \bmod 24 = 1$$

  - Άρα Α -> Β (το 2ο γράμμα της αλφαβήτου)
- Για το Ν (13ο γράμμα):

$$c=5 \cdot 12 + 1 \bmod 24 = 61 \bmod 24 = 13$$

  - Άρα Ν - > Ξ (το 14ο γράμμα)

Συνεχίζοντας αντίστοιχα, θα έχουμε:

- Για το Τ: $c=5 \cdot 18 + 1 \bmod 24 = 91 \bmod 24 = 19$
- Για το Ι: $c= 5 \cdot 8 + 1 \bmod 24 = 41 \bmod 24 = 17$
- Για το Ο: $c= 5 \cdot 14 + 1 \bmod 24 = 71 \bmod 24 = 23$

- Άρα ΑΝΤΙΟ -> ΒΞΥΣΩ

Κρυπτανάλυση του γραμμικού αλγορίθμου

1. Είναι ένας απλός (μονοαλφαβητικός) αλγόριθμος αντικατάστασης, συνεπώς σε μεγάλα κείμενα μπορεί να εφαρμοστεί η αποκρυπτογράφηση με βάση τις συχνότητες εμφάνισης των γραμμάτων.
2. Καλύτερος τρόπος να κάνουμε κρυπτανάλυση: Εξαντλητική αναζήτηση για την εύρεση των a,b (το b μπορεί να πάρει 24 τιμές – συγκεκριμένα, από 0 μέχρι 23, ενώ το a μπορεί να πάρει τόσες τιμές όσοι οι αριθμοί που είναι πρώτοι ως προς το n. Για παράδειγμα, για n=24 (ελληνικό αλφάβητο) το a μπορεί να είναι μόνο ένα από τα 1,5,7,11,13,17,19,23). Με άλλα λόγια, ο αριθμός των κλειδιών είναι πολύ μικρός!!
3. **Εργαστηριακή άσκηση**: εκτελέστε τα αρχεία *encrypt_affine* και *cryptanalyse_affine*

Πολυαλφαβητικοί αλγόριθμοι αντικατάστασης (συνέχεια)

- Αλγόριθμος του Hill (Lester S. Hill – 1929)
  - Αποτελεί επέκταση του γραμμικού αλγορίθμου. Το μήνυμα κωδικοποιείται ανά block L στοιχείων (L τυχαίος ακέραιος) με βάση L γραμμικές εξισώσεις (αντί για μία που είναι στο γραμμικό κρυπταλγόριθμο). Συγκεκριμένα:

$$c = Km \mod n$$

όπου K πίνακας διαστάσεων L × L (το κλειδί)

Παράδειγμα αλγορίθμου Hill

Χωρίζουμε το μήνυμά μας (που είναι αγγλικό κείμενο) σε μπλοκ μήκους 3. Αn (p1 p2 p3) είναι ένα τέτοιο μπλοκ, τότε αυτό κρυπτογραφείται ως εξής:

$$C1 = 9*p1 + 18*p2 + 10*p3 \pmod{26}$$

$$C2 = 16*p1 + 21*p2 + 1*p3 \pmod{26}$$

$$C3 = 5*p1 + 12*p2 + 23*p3 \pmod{26}$$

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \pmod{26}$$

Παράδειγμα αλγορίθμου Hill (2)

Έστω το ακόλουθο μήνυμα (με την αντίστοιχη θέση των γραμμάτων στο αλφάβητο (a ->0, b->1 κ.ο.κ.):

I can't do it

8 2 0 13 19 3 14 8 19

Χωρίζουμε το μήνυμα σε μπλοκ των 3 γραμμάτων κι έχουμε:

$$\begin{pmatrix} 4 \\ 14 \\ 12 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 8 \\ 2 \\ 0 \end{pmatrix} \pmod{26}$$

Παράδειγμα αλγορίθμου Hill (3)

$$\begin{pmatrix} 19 \\ 12 \\ 24 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 13 \\ 19 \\ 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 18 \\ 21 \\ 9 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 14 \\ 8 \\ 19 \end{pmatrix} \pmod{26}$$

Το κρυπτόγραμμα είναι: EOM TMY SVJ

Αλγόριθμος Hill - συνέχεια

Η αποκρυπτογράφηση γίνεται πολλαπλασιάζοντας κάθε ένα μπλοκ του κρυπτογράμματος, όπως αυτά προέκυψαν με την προηγούμενη διαδικασία, με τον αντίστροφο του Κ. Συνεπώς, **ο πίνακας Κ πρέπει να είναι αντιστρέψιμος (mod n).**

Ο Κ είναι αντιστρέψιμος αν και μόνο αν ισχύει gcd(det(K),n)=1

Αν ο Κ δεν είναι αντιστρέψιμος, τότε υπάρχουν ζευγάρια μπλοκ του μηνύματος, τα οποία κρυπτογραφούνται στο ίδιο κρυπτόγραμμα – το οποίο βέβαια απαγορεύεται να συμβαίνει.

Το ακόλουθο παράδειγμα εμπίπτει σε αυτήν την περίπτωση:

bcd → XJR

hfa → XJR

$$\begin{pmatrix} 23 \\ 9 \\ 17 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 22 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 23 \\ 9 \\ 17 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 22 \end{pmatrix} \begin{pmatrix} 7 \\ 5 \\ 0 \end{pmatrix} \pmod{26}$$

Κρυπτανάλυση αλγορίθμου Hill

- Επίθεση τύπου known plaintext attack: αν κάποιος γνωρίζει L^2 στοιχεία του μηνύματος καθώς και τα αντίστοιχα στοιχεία του κρυπτογράμματος, τότε μπορεί να φτιάξει ένα γραμμικό σύστημα της μορφής:

$$\begin{pmatrix} c_1 & c_{L+1} & \cdots & c_{L^2-L} \\ c_2 & c_{L+2} & \cdots & \vdots \\ \vdots & \vdots & \cdots & c_{L^2-1} \\ c_L & c_{2L} & \cdots & c_L \end{pmatrix} = K \begin{pmatrix} m_1 & m_{L+1} & \cdots & m_{L^2-L} \\ m_2 & m_{L+2} & \cdots & \vdots \\ \vdots & \vdots & \cdots & m_{L^2-1} \\ m_L & m_{2L} & \cdots & m_L \end{pmatrix} \bmod(n)$$

Κρυπτανάλυση αλγορίθμου Hill (2)

- Παρατηρείστε ότι δεν χρειάζεται τα L^2 στοιχεία του μηνύματος να είναι διαδοχικά – αρκεί ανά μπλοκ των L να είναι διαδοχικά.
- Αν την προηγούμενη σχέση τη γράψουμε σαν C=KM mod (n), τότε αν ο πίνακας M αντιστρέφεται, μπορούμε να υπολογίσουμε τον K (βλέπε επόμενο παραδειγμα).
- Άρα, και στον αλγόριθμο του Hill επαληθεύεται η γενική αρχή πως το κλειδί πρέπει να είναι όσο γίνεται πιο μεγάλο.

Παράδειγμα κρυπτανάλυσης σε Hill

- Έστω ότι το κρυπτόγραμμα είναι:
  JQSNOMHHDNNBDSTE
  και ξέρουμε ότι τα πρώτα 4 γράμματα αντιστοιχούν στη λέξη TELL.
  Αφού TELL->JQSN, ισχύει

$$K\begin{pmatrix}19 & 11\\ 4 & 11\end{pmatrix} \equiv \begin{pmatrix}9 & 18\\ 16 & 13\end{pmatrix} \bmod 26$$

Έχουμε $\det\begin{pmatrix}19 & 11\\ 4 & 11\end{pmatrix} \equiv (19\cdot 11 - 4\cdot 11) \bmod 26 \equiv 165 \equiv 9 \bmod 26$

Παράδειγμα κρυπτανάλυσης σε Hill (2)

Επειδή gcd(9,26)=1, υπάρχει ο αντίστροφος του K.
Έχουμε $9^{-1}=3 \pmod{26}$, συνεπώς:

$$\begin{pmatrix} 19 & 11 \\ 4 & 11 \end{pmatrix}^{-1} \equiv 3 \begin{pmatrix} 11 & -11 \\ -4 & 19 \end{pmatrix} \bmod 26 \equiv$$

$$\equiv \begin{pmatrix} 33 & -33 \\ -12 & 57 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 7 & 19 \\ 14 & 5 \end{pmatrix} \bmod 26$$

Συνεπώς: $$K \equiv \begin{pmatrix} 9 & 18 \\ 16 & 13 \end{pmatrix} \begin{pmatrix} 7 & 19 \\ 14 & 5 \end{pmatrix} \equiv \begin{pmatrix} 315 & 261 \\ 294 & 369 \end{pmatrix} \equiv \begin{pmatrix} 3 & 1 \\ 8 & 5 \end{pmatrix} \bmod 26$$

Παράδειγμα κρυπτανάλυσης σε Hill (3)

Για την αποκρυπτογράφηση, χρειαζόμαστε τον αντίστροφο του K.

$$K^{-1} \equiv 7^{-1} \begin{pmatrix} 5 & -1 \\ -8 & 3 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \bmod 26$$

(το $7^{-1} \bmod 26$ ισούται με 15)

Για την αποκρυπτογράφηση λοιπόν έχουμε τα ακόλουθα γινόμενα:

$$\begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 9 \\ 16 \end{pmatrix}, \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 18 \\ 13 \end{pmatrix}, \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 14 \\ 12 \end{pmatrix}, \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 7 \\ 7 \end{pmatrix}$$

$$\begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 3 \\ 13 \end{pmatrix}, \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 13 \\ 1 \end{pmatrix}, \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 3 \\ 18 \end{pmatrix}, \begin{pmatrix} 23 & 11 \\ 10 & 19 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

Παράδειγμα κρυπτανάλυσης σε Hill (4)

Τα αποτελέσματα των γινομένων είναι:

$$\begin{pmatrix}19\\4\end{pmatrix},\begin{pmatrix}11\\11\end{pmatrix},\begin{pmatrix}12\\4\end{pmatrix},\begin{pmatrix}4\\21\end{pmatrix},\begin{pmatrix}4\\17\end{pmatrix},\begin{pmatrix}24\\19\end{pmatrix},\begin{pmatrix}7\\8\end{pmatrix},\begin{pmatrix}13\\6\end{pmatrix}$$

Κάνοντας τις αντιστοιχίες των παραπάνω με τα τα γράμματα του αλφαβήτου, προκύπτει το αρχικό μήνυμα: TELL ME EVERYTHING

Κρυπτανάλυση γραμμικού αλγορίθμου με επίθεση γνωστού κειμένου

- Όπως και στον αλγόριθμο του Hill, και ο γραμμικός αλγόριθμος μπορεί να σπάσει εύκολα με επίθεση γνωστού κειμένου (Known plaintext attack).
- Παράδειγμα: έστω ότι το κρυπτόγραμμα είναι

JAKNHOZXQUQPPSOGAVOGONNOU

και κάνουμε την υπόθεση ότι το μήνυμα ξεκινάει με τη λέξη DEAR.

Μπορούμε να βρούμε το κλειδί?? Αν ναι, πώς??

(απάντηση: κλειδί (a,b)=(17,10) και $a^{-1}=23$ – υπολογίζεται με επίλυση γραμμικού συστήματος – Άσκηση εργαστηριακή)

Αλγόριθμος Playfair (1854)

- Ένας 5 x 5 πίνακας συμπληρώνεται με τη λέξη-κλειδί (δύο ίδια γράμματα δεν εμφανίζονται δύο φορές) και οι υπόλοιπες θέσεις του πίνακα συμπληρώνονται από τα εναπομείναντα γράμματα του αλφαβήτου.
- Στο διπλανό πίνακα, κλειδί είναι η λέξη “query”
- Τα I/J πηγαίνουν μαζί, στο ίδιο τετράγωνο (εναλλακτικά, αν κάποιο από αυτά ανήκει στη λέξη κλειδί, τότε παραλείπουμε το Q από τον πίνακα – **συνηθέστερη περίπτωση**).
- Κρυπτογράφηση: χωρίζουμε το μήνυμα σε ζεύγη γραμμάτων. Κάθε ένα ζεύγος το κρυπτογραφούμε με βάση τους ακόλουθους κανόνες:

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

Κανόνες κρυπτογράφησης του Playfair

- Αν υπάρχει ζευγάρι με δύο ίδια γράμματα, τότε ανάμεσά τους προστίθεται ένα Χ. Στην αποκρυπτογράφηση, τα πλεονάζοντα αυτά Χ εύκολα αναγνωρίζονται και απομακρύνονται.
- Αν τα δύο γράμματα του ζεύγους εμφανίζονται στην ίδια γραμμή στον πίνακα, τότε το καθένα αντικαθίσταται από το δεξιότερό του (αν κάποιο από αυτά είναι το τελευταίο στη γραμμή, τότε αντικαθίσταται από το πρώτο της γραμμής).
- Αν τα δύο γράμματα του ζεύγους εμφανίζονται στην ίδια στήλη στον πίνακα, τότε το καθένα αντικαθίσταται από αυτό που βρίσκεται αμέσως κάτω του (αν κάποιο από αυτά είναι το τελευταίο στη στήλη, τότε αντικαθίσταται από το πρώτο της στήλης).
- Αν δεν βρίσκονται ούτε στην ίδια γραμμή ούτε στην ίδια στήλη, τότε φανταζόμαστε το νοητό ορθογώνιο που ορίζουν τα δύο γράμματα και τα αντικαθιστούμε από τα άλλα δύο γράμματα που αντιστοιχούν στις γωνίες του ορθογωνίου (έχει σημασία η σειρά – κάθε γράμμα (γωνία του ορθογωνίου) θα αντικατασταθεί από εκείνο το γράμμα (γωνία) που βρίσκεται στην ίδια γραμμή.

Εξήγηση των κανόνων του Playfair

- “br” -> “DU”
  “vk” -> “XH”
  “mo” -> “NP”

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

Παράδειγμα Playfair (1)

- Έχοντας ως κλειδί τη φράση «Playfair example”, προκύπτει ο πίνακας (όπου απουσιάζει το Q)

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

Παράδειγμα Playfair (2)

Έστω η φράση:

Hide the gold in the tree stump

- Τη «σπάμε» σε ζευγάρια γραμμάτων:

HI DE TH EG OL DI NT HE TR EX ES TU MP

Εισήχθη για να μην υπάρξει το ζεύγος EE

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

Παράδειγμα Playfair (3)

- Το ζευγάρι HI σχηματίζει ορθογώνιο, κρυπτογραφείται σε BM
- Το ζευγάρι DE βρίσκεται στην ίδια στήλη, κρυπτογραφείται σε ND
- Το ζευγάρι TH σχηματίζει ορθογώνιο, κρυπτογραφείται σε ZB
- Το ζευγάρι EG σχηματίζει ορθογώνιο, κρυπτογραφείται σε XD
- Το ζευγάρι OL σχηματίζει ορθογώνιο, κρυπτογραφείται σε KY
- Το ζευγάρι DI σχηματίζει ορθογώνιο, κρυπτογραφείται σε BE
- Το ζευγάρι NT σχηματίζει ορθογώνιο, κρυπτογραφείται σε JV
- Το ζευγάρι HE σχηματίζει ορθογώνιο, κρυπτογραφείται σε DM
- Το ζευγάρι TR σχηματίζει ορθογώνιο, κρυπτογραφείται σε UI
- Το ζευγάρι EX βρίσκεται στην ίδια γραμμή, κρυπτογραφείται σε XM
- Το ζευγάρι ES σχηματίζει ορθογώνιο, κρυπτογραφείται σε MN
- Το ζευγάρι TU βρίσκεται στην ίδια γραμμή, κρυπτογραφείται σε UV
- Το ζευγάρι MP σχηματίζει ορθογώνιο, κρυπτογραφείται σε IF

Συνεπώς, το κρυπτόγραμμα είναι:
BMNDZBXDKYBEJVDMUIXMMNUVIF

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

Ασφάλεια του Playfair αλγορίθμου

- Περισσότερη ασφάλεια από τους μονοαλφαβητικούς αλγόριθμους αντικατάστασης. Συνεπώς, ένας έλεγχος συχνότητας εμφάνισης ζευγών γίνεται πιο σύνθετος.
- Χρησιμοποιήθηκε στον πρώτο παγκόσμιο πόλεμο (από τον αμερικάνικο και τον αγγλικό στρατό).
- Σήμερα, με αρκετό δοθέν κρυπτόγραμμα, μπορεί να σπάσει με ελέγχους συχνότητας εμφάνισης διγραμμάτων

Σειριακός Playfair (Seriated Playfair)

- Έστω η φράση «COME QUICKLY WE NEED HELP IMMEDIATELY TOM”. Τη γράφουμε σε μπλοκ γραμμάτων, όπου το κάθε μπλοκ αποτελείται από 2 γραμμές. Αν το μήκος του μπλοκ (που καλείται περίοδος του μπλοκ) είναι για παράδειγμα 6, τότε το παραπάνω μήνυμα γράφεται ως εξής:
- C O M E Q U E N E E D H M E D I A T
  I C K L Y W (X)E L P I M E L Y T O M

Σειριακός Playfair (Seriated Playfair) (II)

- Κάθε ζευγάρι γραμμάτων που εμφανίζεται σε κάθε στήλη κρυπτογραφείται με τον κλασικό αλγόριθμο Playfair. Έτσι, αν έχουμε ως κλειδί τη φράση LOGARITHM, ο πίνακας που προκύπτει φαίνεται δίπλα:

  (όπου χρησιμοποιούμε την εκδοχή όπου τα I,J υπάρχουν στο ίδιο τετράγωνο)
- Άρα, το κρυπτόγραμμα προκύπτει ως εξής:

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

N L B C S P Q Q C D C M H C F T R H

C D F G X Z G C G Q T B F G W H G B

Σειριακός Playfair (Seriated Playfair) (III)

- Το κρυπτόγραμμα μεταδίδεται κατά τον προφανή τρόπο (τα γράμματα διευθετούνται όπως ακριβώς τα αντίστοιχά τους στο αρχικό μήνυμα) – συνεπώς:

  NLBCSP CDFG XZ QQCDCM GCGQTB HCFTRH FGWHGB

- Η αποκρυπτογράφηση γίνεται κατά τον προφανή τρόπο - ο παραλήπτης σχηματίζει τα ίδια γκρουπ μήκους 6 και τα αποκρυπτογραφεί κατά στήλη
- Ο Seriated Playfair είναι πιο ασφαλής από τον απλό Playfair (και αυτό γιατί είναι δύο πια τα άγνωστα στοιχεία για τον κρυπταναλυτή: η λέξη-κλειδί αφενός, αλλά αφετέρου και η περίοδος του μπλοκ (π.χ. 6 για το προηγούμενο παράδειγμα))
- Κρυπτανάλυση στον Σειριακό Playfair: κάποιος μπορεί να δοκιμάσει διάφορα μήκη μπλοκ και να αποκλείσει εκείνα που έχουν ως αποτέλεσμα σε μία στήλη να προκύπτουν δύο ίδια γράμματα.
  - Στο προηγούμενο παράδειγμα, όλες οι περίοδοι από 4 μέχρι 10 (πλην φυσικά της τιμής 6) έχουν ως αποτέλεσμα την εμφάνιση κάποιας στήλης με δύο ίδια γράμματα. Άρα ο κρυπταναλυτής βρίσκει αμέσως την περίοδο (6)).