

Κρυπτοσυστήματα Ροής

Ιδέα: Χρησιμοποιούμε κλειδί ροής $z=z_1 z_2 \dots$ και κρυπτογραφούμε το μήνυμα $x=x_1 x_2 \dots$ ως $y=y_1 y_2 \dots = e_{z_1}(x_1) e_{z_2}(x_2) \dots$

Η συνάρτηση f_i (εξαρτάται από το κλειδί K και από τους $i-1$ χαρακτήρες του μηνύματος) χρησιμοποιείται για να μας δώσει το z_i (i -οστό στοιχείο του κλειδιού ροής). Δηλαδή:
 $Z_i = f_i(K, x_1, x_2, \dots, x_{i-1})$. Το Z_i χρησιμοποιείται και δίνει το $y_i = e_{z_i}(x_i)$. Επομένως κρυπτογραφούμε το μήνυμα $x_1 x_2 \dots x_{i-1}$ υπολογίζοντας διαδοχικά τα $z_1, y_1, z_2, y_2, \dots$

Ορισμός:

Διατεταγμένη 7-αδα (P, C, K, L, F, E, D) όπου

P : πεπερασμένο σύνολο όλων των δυνατών plaintext

C : πεπερασμένο σύνολο όλων των δυνατών cipher text

K : πεπερασμένο σύνολο όλων των δυνατών κλειδιών

L : πεπερασμένο σύνολο που λέγεται αλφάβητο κλειδιών ροής

F = (f_1, f_2, \dots) σύνολο-γεννήτορας κλειδιών ροής. Για κάθε $i \geq 1$ είναι $f_i : K \times P^{i-1} \rightarrow L$

Για κάθε $z \in L$ υπάρχει $e_z \in E$ και $d_z(e_z(x)) = x, \forall x \in P$. Δηλαδή $e_z : P \rightarrow C$ και $d_z : C \rightarrow P$

Συγχρονισμένο: λέγεται το σύστημα όταν το κλειδί ροής εξαρτάται μόνο από το κλειδί K

Περιοδικό: με περίοδο d λέγεται όταν $Z_{i+d} = Z_i, \forall i \geq 1$.

Παρατήρηση:

1. Όλα τα προηγούμενα κρυπτοσυστήματα μπορούν να θεωρηθούν ως ειδική περίπτωση του κρυπτοσυστήματος ροής όταν $Z_i = K, \forall i \geq 1$

2. Το Vigenere με κλειδί μήκους m μπορεί να θεωρηθεί σαν κρυπτοσύστημα ροής, περιοδικό με περίοδο m .

Το Vigenere μοιάζει με το μεταφοράς $e_z(x) = x+z$ και $d_z(y) = y-z$. Συνήθως $P=C=L=Z_2$

και $e_z(x) = x+z \pmod{2}$ και $d_z(y) = y-z \pmod{2}$

3. Άλλη μέθοδος (συγχρονισμένου) κλειδιού ροής :

Αν ξεκινήσουμε από (K_1, K_2, \dots, K_m) και θέσουμε $z_i = K_i (1 \leq i \leq m)$ συνεχίζουμε να παράγουμε το κλειδί ροής χρησιμοποιώντας την αναδρομική σχέση βαθμού m

$$Z_{i+m} = \sum_{j=0}^{m-1} c_j Z_{i+j} \pmod{2}, \quad \begin{array}{l} \text{όπου } c_i \in Z_2 \text{ δοσμένα} \\ \text{και } c_0 = 1 \end{array}$$

Εδώ το K αποτελείται από 2^m τιμές, τις k_1, k_2, \dots, k_m και c_0, c_1, \dots, c_{m-1}

Κρυπτοανάλυση

Υπόθεση: Το κρυπτοσύστημα επικοινωνίας θεωρείται γνωστό.

Συχνότητα Εμφάνισης Γραμμάτων:

<u>Γράμμα</u>	<u>Συχνότητα</u>
E	0,120
T,A,O,I,N,S,H,R	0,06 έως 0,09 (σε φθίνουσα σειρά)
D,L	0,04
C,U,M,W,F,G,Y,P,B	0,015 έως 0,028
V,K,J, X,Q, Z	<0,01

Συχνότητα Εμφάνισης Διγραμμάτων:

Σε φθίνουσα σειρά της συχνότητας εμφάνισης των διγραμμάτων:

TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OE

Συχνότητα Εμφάνισης Τριγραμμάτων:

Σε φθίνουσα σειρά της συχνότητας εμφάνισης των τριγραμμάτων:

THE, ING, AND, HER, ERG, ENT, THA, NTH, WAS, ETH, FOR, DTH

ΠΑΡΑΔΕΙΓΜΑ

(ΚΡΥΠΤΟΑΝΑΛΥΣΗ ΑΦΙΝΙΚΟΥ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΟΣ)

Κρυπτομήνυμα:

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLR
HHRH

Πίνακας Συχνοτήτων εμφάνισης των γραμμάτων:

<u>Γράμμα</u>	<u>Συχνότητα</u>	<u>Γράμμα</u>	<u>Συχνότητα</u>	<u>Γράμμα</u>	<u>Συχνότητα</u>
A	2	J	0	S	3
B	1	K	5	T	0
C	0	L	2	U	2
D	7	M	2	V	4
E	5	N	1	W	0
F	4	O	1	X	2
G	0	P	2	Y	1
H	5	Q	0	Z	0
I	0	R	8		

Τα γράμματα με την μεγαλύτερη συχνότητα εμφάνισης στο κρυπτομήνυμα είναι:

Γράμμα	Συχνότητα
R	8
D	7
E, H, K	5
F, S, V	4

Βάσει των συχνοτήτων εμφάνισης κάνουμε τις εξής αντιστοιχίσεις:

- $R \rightarrow E \Leftrightarrow e_k(4)=17 \Leftrightarrow 4a+b=17 \pmod{26}$
 $D \rightarrow T \Leftrightarrow e_k(19)=3 \Leftrightarrow 19a+b=3 \pmod{26}$

Λύνουμε το παραπάνω σύστημα οπότε πιθανές λύσεις είναι:

$a=6$ και $b=19$. Επειδή όμως $\text{ΜΚΔ}(6, 26) = 2 \neq 1 \Leftrightarrow$ υπάρχει λάθος στην αρχική αντιστοίχηση.

- $R \rightarrow E$
 $E \rightarrow T$

Από εδώ βρίσκουμε $a=13 \Leftrightarrow$ **ΑΤΟΠΟ**

- $R \rightarrow E$
 $H \rightarrow T$

Από εδώ βρίσκουμε $a=8 \Leftrightarrow$ **ΑΤΟΠΟ**

- $R \rightarrow E$
 $K \rightarrow T$

Από εδώ βρίσκουμε $a=3$ και $b=5$. Είναι $\text{ΜΚΔ}(3,26) = 1$ και $\text{ΜΚΔ}(5,26) = 1$
Άρα τα a, b δίνουν τιμές αποδεκτές και πιθανό κλειδί το $K=(3,5)$

Υπολογίζουμε το $a^{-1} = 9$ και $d_k(y) = 9(4-5) = 9y-19$

Οπότε η αποκρυπτογράφηση δίνει:

*algorithms are quite general definitions of arithmetic processes.
που αποτελεί το μήνυμα (plaintext)*