

Το Αφινικό Κρυπτοσύστημα

$$P = C = Z_{26}$$

$$K = \{(a,b) \in (Z_{26} \times Z_{26})\}. \quad \text{Αν } K = (a,b) \text{ τότε } e_k(x) = ax+b$$

Έστω $ax+b = y \pmod{26} \Rightarrow ax=y-b \pmod{26} \Rightarrow (a,26)$:σχετικοί πρώτοι.

Θα πρέπει να μπορώ να λύσω ως προς x και μάλιστα να έχω μοναδική λύση.

Αυτό συμβαίνει αν και μόνο αν $\text{ΜΚΔ}(a,26) = 1$.

Αν θεωρήσουμε την ισοδυναμία $a \cdot x = 1 \pmod{26}$ και συμβολίσουμε τη λύση της με $x = a^{-1}$ τότε $d_k(y) = a^{-1}(y-b) \pmod{26}$.

ΠΑΡΑΔΕΙΓΜΑ

Έστω το κλειδί $K=(7,3)$ και ο $\text{ΜΚΔ}(7,26)=1$ ισχύει $e_k(x) = 7x+3 \pmod{26}$.

Για τη συνάρτηση αποκωδικοποίησης πρέπει $7^{-1} = 15$ αφού $7x = 1 \pmod{26}$. Επομένως $d_k(y) = 15(y-3) = 15y - 19 \pmod{26}$

➤ *Κωδικοποίηση*

[Textplain = hot](#)

$$h \rightarrow 7 \Rightarrow e_k(7) = 7 \cdot 7 + 3 = 52 = 0 \pmod{26}$$

$$o \rightarrow 14 \Rightarrow e_k(14) = 7 \cdot 14 + 3 = 101 = 23 \pmod{26}$$

$$t \rightarrow 19 \Rightarrow e_k(19) = 7 \cdot 19 + 3 = 136 = 6 \pmod{26}$$

[Άρα Ciphertext = AXG](#)

➤ *Αποκωδικοποίηση*

$$0 \rightarrow A \Rightarrow d_k(0) = 15 \cdot 0 - 19 = 7 \pmod{26}$$

$$23 \rightarrow X \Rightarrow d_k(23) = 15 \cdot 23 - 19 = 14 \pmod{26}$$

$$6 \rightarrow G \Rightarrow d_k(6) = 15 \cdot 6 - 19 = 19 \pmod{26}$$

[Άρα Textplain = hot](#)

Σημείωση

Για να λύσουμε την $7x = 1 \pmod{26}$:

Γνωρίζουμε ότι αν $\text{ΜΚΔ}(a,b) = d$ τότε $\exists x_0, y_0 \in Z : d = a x_0 + y_0$ και πρέπει να βρούμε τα x_0, y_0, d .

Π.χ $26 = 7 \cdot 3 + 5$ και $7 = 5 \cdot 1 + 2$ και $5 = 2 \cdot 2 + 1$.

Προχωράμε ανάποδα: $1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5) = -2 \cdot 7 + 3 \cdot 5 = -2 \cdot 7 + 3(26 - 3 \cdot 7) = 3 \cdot 26 - 11 \cdot 7$

Άρα $26 \cdot 3 + 7(-11)$ όπου $x_0 = 3$ και $y_0 = -11$. Είναι $7(-11) = 1 \pmod{26}$ και $-11 = 15$ στο Z_{26}

Δηλαδή $a^{-1} = 15$.

Το Κρυπτοσύστημα Vigenere

$$P = C = (\mathbb{Z}_{26})^m = K$$

$$m \in \mathbb{N} (m \neq 0)$$

$$k \in K = (\mathbb{Z}_{26})^m \Rightarrow K = (k_1, k_2, \dots, k_m) \text{ με } k_i \in \mathbb{Z}_{26}$$

$$e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

$$d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$$

Παρατηρήσεις

- ✓ Το σύστημα είναι πολυαλφαβητικό άρα η κρυπτοανάλυση είναι πιο δύσκολη από ότι στα προηγούμενα μονοαλφαβητικά συστήματα.
- ✓ Το πλήθος των κλειδιών είναι 26^m . Επειδή το m αυθαίρετο μπορούμε να φτιάξουμε κρυπτοσύστημα με όσο αριθμό κλειδιών επιθυμώ.
- ✓ Δεν χρειάζεται το κείμενο να έχει πλήθος γραμμάτων πολλαπλάσιο του m .

Παράδειγμα

Έστω $m=6$ και κλειδί η λέξη *CIPHER*, δηλαδή $K=(2,8,15,7,4,17)$

- ✓ *Κωδικοποίηση*

Textplain = this cryptosystem is not secure

Μετατρέπουμε το μήνυμα σε αριθμούς, ομαδοποιούμε ανά 6 και προσθέτουμε το κλειδί στο \mathbb{Z}_{26}

Μήνυμα	19 7 8 18 2 17	24 15 19 14 18 24	18 19 4 12 8 18	13 14 19 18 4 2	20 17 4
Κλειδί	2 8 15 7 4 17	2 8 15 7 4 17	2 8 15 7 4 17	2 8 15 7 4 17	2 8 15
Άθροισμα	21 15 23 25 6 8	0 23 8 21 22 15	20 1 19 19 12 9	15 22 8 25 8 19	22 25 19
Κρυπτο/μα	V P X Z G I	A X I V W P	U B T T M J	P W I Z I T	W Z T

Το Κρυπτοσύστημα του Hill

$$P = C = (Z_{26})^m = K$$

$$m \in \mathbb{N} (m \neq 0)$$

$$K = M_{m \times m} (= Z_{26})$$

Αν $X = (x_1, x_2, \dots, x_m) \in P$ και $K = (k_{ij}) \mid 1 \leq i \leq m, 1 \leq j \leq m$

Τότε $y = e_k(x) = (y_1, y_2, \dots, y_m) = x \cdot K$

Πρέπει να ορίσουμε το K^{-1} οπότε ορίζουμε $d_k(y) = y \cdot K^{-1}$

Για να υπάρξει ο αντίστροφος πίνακας του K θα πρέπει $\text{MK}\Delta (\det K, 26) = 1$

Παράδειγμα

$$\text{Κλειδί } K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \text{ και } \det K = 53 = 1 \pmod{26}$$

Plaintext: july

✓ Κωδικοποίηση

Είναι $m=2$ άρα

$$ju \rightarrow (9,20) \Rightarrow (9,10) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99+60, 72+140) = (3,4) = \text{DE}$$

$$ly \rightarrow (11,24) \Rightarrow (11,24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121+72, 88+168) = (11,22) = \text{LW}$$

δηλαδή το κρυπτογραφημένο μήνυμα είναι DELW.

✓ Αποκωδικοποίηση

$$K^{-1} = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26}$$

$$\text{DE} \rightarrow (3,4) \Rightarrow (3,4) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9,20) = ju$$

$$\text{LW} \rightarrow (11,22) \Rightarrow (11,22) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (11,24) = ly$$

Παρατηρήσεις

Αν $\det K \neq 1$ τότε $(\det K)^{-1}$ συμβολίζει τον αντίστροφο της $\det K$ στον δακτύλιο Z_{26}

Δηλαδή θα πρέπει να λύσουμε την ισοδυναμία $(\det K) \cdot x = 1 \pmod{26}$

6. Το Κρυπτοσύστημα μεταθέσεων

{ Ειδική περίπτωση του κρυπτοσυστήματος του Hill }

Έστω π μετάθεση του συνόλου $S = \{1, 2, \dots, m\}$

Στη μετάθεση π αντιστοιχεί ένας πίνακας (πίνακας διαμεταθέσεων) K_π ο οποίος ορίζεται ως

$$\text{εξής: } K_\pi = k_{i,j} \text{ με } k_{i,j} = \begin{cases} 1, & \text{αν } i = \pi(j) \\ 0, & \text{αλλιώς} \end{cases}$$

$$P = C = (Z_{26})^m$$

$$e_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$$

$$d_\pi(y_1, y_2, \dots, y_m) = (y_{\pi(1)}^{-1}, y_{\pi(2)}^{-1}, \dots, y_{\pi(m)}^{-1})$$

ΠΑΡΑΔΕΙΓΜΑ

Κλειδί π

1	2	3	4	5	6
3	5	1	6	4	2

 και $m=6$

[Textplain : shesellsseashellsbytheseashore](#)

✓ Κωδικοποίηση

Παίρνουμε ανά 6 τα γράμματα της ακολουθίας του μηνύματος και τα αντιστοιχούμε σύμφωνα με τον πίνακα μεταθέσεων του κλειδιού

textplain	s h e s e l	l s s e a s	h e l l s b
μετάθεση	3 5 1 6 4 2	3 5 1 6 4 2	3 5 1 6 4 2
New textplain	e e s l s h	s a l s e s	l s h b l e

✓ Αποκωδικοποίηση

Για την αποκρυπτογράφηση πρέπει να ξέρουμε τον π^{-1}

Είναι π^{-1}

1	2	3	4	5	6
3	5	1	6	4	2