

שיעור 4

הצפנים הבסיסיים (המשך)

4.1 צפני זרם

עד כה דיברנו על צפנים המבוססים על מפתח k אילו הטקסט מוצפן y מתקבל על ידי הכלל מצפין

$$y = y_1 y_2 \cdots = e_k(x_1) e_k(x_2) \cdots .$$

צפנים מסוג זה נקראים צפני בלוק.

כעת נדבר על צפני זרם. להתחיל נגדיר **צופן זרם סינכרוני**.

הגדרה 4.1 צופן זרם סינכרוני

צופן זרם סינכרוני (synchronized stream cipher) מוצג באמצעות קבוצה (P, C, K, L, E, D) יחד עם פונקציה כאשר:

(1) E מסמן קבוצה של טקסטים גלויים (plaintexts),

(2) C מסמן קבוצה של טקסטים מוצפנים (ciphertexts),

(3) K מסמן קבוצה של המפתחות אפשריים (keyspace),

(4) L מסמן את האלפיבית של המפתח הפנימי (key-stream alphabet).

(5) g מסמן את ה **מחולל הפנימי** (keystream generator). g מקבלת מפתח k ומחזירה רצף אותיות אינסופי $z_1 z_2 \cdots$ כאשר $z_i \in L$ לכל $i \geq 1$.

(6) לכל $z \in L$ יש כלל מצפין $e_z \in E$ וכלל מפענח $d_z \in D$:

$$e_z : P \rightarrow C, \quad d_z : C \rightarrow P,$$

כך ש-

$$d_z(e_z(x)) = x$$

לכל איבר של מרחב הטקסט גלוי $x \in P$.

הגדרה 4.2 צופן אוטו מפתח (Autokey cipher)

נניח כי $P = C = K = L = \mathbb{Z}_{26}$. נגדיר מפתח הפנימי

$$g : \quad z_1 = k, \quad z_i = x_{i-1} \quad \forall i \geq 2.$$

לכל $z \in \mathbb{Z}_{26}$ נגדיר כלל מצפין

$$e_z(x) = (x + z) \mod 26$$

לכל $x \in \mathbb{Z}_{26}$ ונגדיר כלל מפענח

$$d_z(y) = (y - z) \mod 26$$

לכל $y \in \mathbb{Z}_{26}$.

דוגמה 4.1 (צופן אוטו-מפתח)

נתון צופן אוטו-מפתח עם מפתח $k = 8$.

(1) מצאו את הטקסט מוצפן של המילה

rendezvous .

(2) פענחו את הטקסט מוצפן המתקבל וודאו שקיבלתם את הטקסט הגלוי.

פתרון:

סעיף 1) נרשום את האותיות של הטקסט גלוי ב- \mathbb{Z}_{26} :

$x \in P$	r	e	n	d	e	z	v	o	u	s
$x \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18

המפתח הפנימי הוא

$x_i \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18
$z_i \in \mathbb{Z}_{26}$	8	17	4	13	3	4	25	21	14	20

על פי המפתח הפנימי נפעיל את הכלל מצפין

$$e_z(x_i) = x_i + z_i \mod 26$$

על הטקסט גלוי ונחשב את ה- x_i של הטקסט מצפון באמצעות הכלל מצפין:

$$\begin{aligned} y_1 = e_8(17) &= (8 + 17) \mod 26 = 25, \\ y_2 = e_{17}(4) &= (17 + 4) \mod 26 = 21, \\ y_3 = e_4(13) &= (4 + 13) \mod 26 = 17, \\ y_4 = e_{13}(3) &= (13 + 3) \mod 26 = 16, \\ y_5 = e_3(4) &= (3 + 4) \mod 26 = 7, \\ y_6 = e_4(25) &= (4 + 25) \mod 26 = 3, \\ y_7 = e_{25}(21) &= (25 + 21) \mod 26 = 20, \\ y_8 = e_{21}(14) &= (21 + 14) \mod 26 = 9, \\ y_9 = e_{14}(20) &= (14 + 20) \mod 26 = 8, \\ y_{10} = e_{20}(18) &= (20 + 18) \mod 26 = 12. \end{aligned}$$

$x \in P$	r	e	n	d	e	z	v	o	u	s
$x_i \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18
$z_i \in \mathbb{Z}_{26}$	8	17	4	13	3	4	25	21	14	20
$y_i = e_{z_i}(x_i)$	25	21	17	16	7	3	20	9	8	12

נמיר את האיברים y_i של \mathbb{Z}_{26} לתווים של הטקסט מוצפן:

$x \in P$	r	e	n	d	e	z	v	o	u	s
$x_i \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18
$z_i \in \mathbb{Z}_{26}$	8	17	4	13	3	4	25	21	14	20
$y_i = e_{z_i}(x_i)$	25	21	17	16	7	3	20	9	8	12
$y \in C$	Z	V	R	Q	H	D	U	J	I	M

סעיף 2) נתחיל עם הטקסט מוצפן:

ZVRQHDUJIM

$y \in C$	Z	V	R	Q	H	D	U	J	I	M
$y_i = \mathbb{Z}_{26}$	25	21	17	16	7	3	20	9	8	12

נחשב את ה- x_i של הטקסט גלוי באמצעות הכלל מפענח:

$$\begin{aligned}
 x_1 = d_8(25) &= (25 - 8) \bmod 26 = 17, \\
 x_2 = d_{17}(21) &= (21 - 17) \bmod 26 = 4, \\
 x_3 = d_4(17) &= (17 - 4) \bmod 26 = 13, \\
 x_4 = d_{13}(16) &= (16 - 13) \bmod 26 = 3, \\
 x_5 = d_3(7) &= (7 - 3) \bmod 26 = 4, \\
 x_6 = d_4(3) &= (3 - 4) \bmod 26 = 25, \\
 x_7 = d_{25}(20) &= (20 - 25) \bmod 26 = 21, \\
 x_8 = d_{21}(9) &= (9 - 21) \bmod 26 = 14, \\
 x_9 = d_{14}(8) &= (8 - 14) \bmod 26 = 20, \\
 x_{10} = d_{20}(12) &= (12 - 20) \bmod 26 = 18.
 \end{aligned}$$

$y \in C$	Z	V	R	Q	H	D	U	J	I	M
$y_i = \mathbb{Z}_{26}$	25	21	17	16	7	3	20	9	8	12
$x_i = d_{z_i}(y_i)$	17	4	13	3	4	25	21	14	20	18

לבסוף נעבור מאיברים של \mathbb{Z}_{26} דתווים של טקסט גלוי:

$y \in C$	Z	V	R	Q	H	D	U	J	I	M
$y_i = \mathbb{Z}_{26}$	25	21	17	16	7	3	20	9	8	12
$x_i = d_{z_i}(y_i)$	17	4	13	3	4	25	21	14	20	18
x	r	e	n	d	e	z	v	o	u	s

■

4.2 צופן חד פעמי

הגדרה 4.3 צופן חד פעמי

יהי n שלם ויהי $X = Y = K = (\mathbb{Z}_2)^n$. לכל $k \in (\mathbb{Z}_2)^n$ נגדיר כלל מצפין

$$e_k(x) = (x_1 + k_1, \dots, x_n + k_n) \bmod 2,$$

ונגדיר כלל מפענח

$$\begin{aligned} d_k(y) &= (y_1 - k_1, \dots, y_n - k_n) \mod 2 \\ &= (y_1 + k_1, \dots, y_n + k_n) \mod 2. \end{aligned}$$

דוגמה 4.2

נתון הקבוצת מפתחות $K = \{0, 1, 1, 0, 0\}$ של צופן חד-פעמי ונתון הטקסט גלוי $x = 1110100010$.

(1) מצאו את הטקסט מוצפן.

(2) וודאו כי הכלל מפענח מחזירה הטקסט גלוי המקורי.

פתרון:

(1)

$$\begin{aligned} e_k(x) &= \{1+0, 1+1, 1+1, 0+0, 1+1, 0+0, 0+1, 0+1, 1+0, 0+1\} \mod 2 \\ &= \{1, 0, 0, 0, 0, 0, 1, 1, 1, 1\}. \end{aligned}$$

(2)

$$\begin{aligned} d_k(y) &= \{1+0, 0+1, 0+1, 0+0, 0+1, 0+0, 1+1, 1+1, 1+0, 1+1\} \mod 2 \\ &= \{1, 1, 1, 0, 1, 0, 0, 0, 1, 0\}. \end{aligned}$$

■

נשים לב כי בצופן חד-פעמי

$$|X| = |Y| = |K| = \mathbb{Z}_2^n$$

לפיכך לפי משפט שאנון לצופן חד-פעמי יש סודיות מושלמת.