# עבודת 3: צופן פייסטל

## שאלה 1 (30 נקודות)

נתון צופן פייסטל שמוגדר עם הפונקציית ליבה

$$f\left(x_1x_2x_3x_4x_5,\pi\right)=x_{\pi(1)}x_{\pi(2)}x_{\pi(3)}x_{\pi(4)}x_{\pi(5)}$$

המפתח ההתחלתי הוא התמורה $(124)(35)$. כל תת-מפתח $k_i$ הוא התמורה המתקבלת על ידי לבצע $i$ פעמים את התמורה $\pi$. מצאו את טקסט מוצפן של הטקסט גלוי

$$x=\texttt{0110111010}\ .$$

## שאלה 2 (30 נקודות)

טקסט גלוי של $10$ bit היה מוצפן באמצעות צופן פייסטל עם מפתח התחלתי

$$k=(145)(23)\ .$$

כל תת מפתח $k_i$ מתקבל על ידי לבצע התמורה ההתחלתית $i$ פעמים.
הטקסט מוצפן הוא

$$y=\texttt{1101101010}\ .$$

מצאו את הטקסט גלוי.

## שאלה 3 (60 נקודות) בוב בונה צופן אל-גמאל עם המפתח $(p=317,\alpha=32,a=16)$.

**א)** חשבו את $\beta$.

**ב)** אליס מקבלת את מפתח הציבורי $(p,\alpha,\beta)$ מבוב, היא בוחרת בשלם $d=4$, ובאמצעות המפתח הזה היא מצפינה את ההודעה $x=224$. מהו הטקסט מוצפן?

**ג)** אחר כך אליס שולחת הודעה אחרת לבוב. הטקסט מוצפן של הודעה הזו הוא $(82,174)$. מהו הטקסט גלוי.

# פתרונות

**<u>שאלה 1</u>** $L_0 = 00101$ ו- $R_0 = 11001$. התת מפתחות הם

$$k_1 = (124)(35)\ , \qquad k_2 = (142)(3)(5)\ , \qquad k_3 = (1)(2)(4)(53)\ .$$

מכאן

$$L_1 = R_0 = 11010\ .$$
$$R_1 = L_0 \oplus f\left(R_0, k_1\right) = 01101 \oplus 11010 = 10111\ .$$

$$L_2 = R_1 = 10111\ .$$
$$R_2 = L_1 \oplus f\left(R_1, k_2\right) = 11010 \oplus 11101 = 00111\ .$$

$$L_3 = R_2 = 00111\ .$$
$$R_3 = L_2 \oplus f\left(R_2, k_3\right) = 10111 \oplus 11110 = 10000\ .$$
$$y = R_3 L_3 = 100000111$$

**<u>שאלה 2</u>** התת מפתחות הם:

$$k_1 = (145)(23)\ , \qquad k_2 = (154)(2)(3)\ , \qquad k_3 = (1)(4)(5)(23)\ .$$

הטקסט מוצפן התקבל על ידי להפוך את השני חצאים, $L_3 = 01010$, $R_3 = 11011$. לכן, השלב 1 הוא:

$$R_2 = L_3 = 01010$$

ו-

$$L_2 = R_3 \oplus f(R_2, k_3) = 11011 \oplus 00110 = 11101\ .$$

שלב 2:

$$R_1 = L_2 = 11101\ .$$

$$L_1 = R_2 \oplus f(R_1, k_2) = 01010 \oplus 11110 = 10100$$

שלב 3:

$$R_0 = L_1 = 10100\ .$$

$$L_0 = R_1 \oplus f(R_0, k_1) = 11101 \oplus 01001 = 10100$$

לכן הטקס גלוי הוא

$$X = L_0 R_0 = 1010010100\ .$$

## שאלה 3

**א)**

$$\beta = \alpha^a \mod p = 32^{16} \mod 317 .$$

ניתן להשתמש בשיטת הריבועים:

$$\begin{aligned}
32^2 \mod 317 &= 1024 \mod 317 = 73 .\\
32^4 \mod 317 &= = 73^2 \mod 317 = 257 .\\
32^8 \mod 317 &= 257^2 \mod 317 = 113 .\\
32^{16} \mod 317 &= 113^2 \mod 317 = 89 .
\end{aligned}$$

לכן

$$32^{16} \mod 317 = 89 .$$

ז"א $\beta = 89$.

**ב)** הטקסט מוצפן הוא $(y_1, y_2)$ כאשר

$$y_1 = \alpha^d \mod p = 32^4 \mod 317 = 1048576 \mod 317 = 257 .$$

$$y_2 = \beta^d x \mod p = (89^4)(224) \mod 317 = 97 .$$

לכן הטקסט מוצפן הוא $(y_1, y_2) = (257, 97)$.

**ג)** $(y_1, y_2) = (257, 97)$.

$$M = (y_1^a)^{-1} \cdot y_2 \mod p = \left(257^{16}\right)^{-1} (97) \mod 317$$

$$257^{-16} \mod 317 = 257^{317-1-16} \mod 317 = 257^{300} \mod 317$$

$300 = 256 + 32 + 8 + 4$.

$$\begin{aligned}
257^2 \mod 317 &= 113 ,\\
257^4 \mod 317 &= 113^2 \mod 317 = 89 ,\\
257^8 \mod 317 &= 89^2 \mod 317 = 313 ,\\
257^{16} \mod 317 &= 313^2 \mod 317 = 16 ,\\
257^{32} \mod 317 &= 16^2 \mod 317 = 256 ,\\
257^{64} \mod 317 &= 256^2 \mod 317 = 234 ,\\
257^{128} \mod 317 &= 234^2 \mod 317 = 232 ,\\
257^{256} \mod 317 &= 232^2 \mod 317 = 251 .
\end{aligned}$$

$$257^{300} \mod 317 = (251)(256)(313)(89) \mod 317 = 218$$

$$x = (y_1^a)^{-1} y_2 \mod p = (218)(97) \mod 317 = 224 .$$