# שיעור 7
# צופן אל-גמאל

**הגדרה 7.1 צופן אל-גמאל**

יהי $p$ מספר ראשוני (גדול), $\alpha$ יוצר של $\left(\mathbb{Z}_p^*, \times_p\right)$ ויהי $a \in \{2, 3, \ldots, p-2\}$.
יהי הקבוצת טקסט גלוי $P = \mathbb{Z}_p^*$ והקבוצת טקסט מוצפן $C = \mathbb{Z}_p^* \times Z_p^*$. נגדיר קבוצת מפתחות

$$K = \left\{(p, \alpha, a, \beta) \;\middle|\; \beta = \alpha^a \mod p\right\} .$$

לכל $k = (p, \alpha, a, \beta) \in K$, $x \in P$, $(y_1, y_2) \in P$ ו- $d = \{2, 3, \ldots, p-2\}$ נגדיר

$$e_k(x, d) = (y_1, y_2)$$

כאשר $y_1 = \alpha^d \mod p$, ו- $y_2 = \beta^d x \mod p$

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \mod p .$$

$(p, \alpha, \beta)$ מפתח ציבורי ו- $a$ מפתח סודי.

**משפט 7.1 צופן אל-גמאל צופן חוקי**

אם $p$ מספר ראשוני ו- $\alpha$ יוצר של $\left(\mathbb{Z}_p^*, \times_p\right)$, $a \in \{2, 3, \ldots, p-2\}$, $\beta = \alpha^a \mod p$ ו- $x \in \mathbb{Z}_p^*$ אז לכל $d \in \{2, 3, \ldots, p-2\}$

$$\left(\left(\alpha^d\right)^a\right)^{-1} \beta^d x = x \mod p .$$

**הוכחה:** תרגיל בית. ■

**כלל 7.1 אלגורים הצפנת אל-גמאל**

נניח שאליס $(A)$ שולחת הודעה לבוב $(B)$.

**שלב הרכבת המפתח**

1. $B$ יוצר מספר ראשוני גדול $p$, ויוצר $\alpha$ של החבורה $\left(\mathbb{Z}_p^*, \times_p\right)$.
2. $B$ בוחר באקראי שלם $a \in \{2, 3, \ldots, p-2\}$,
3. $B$ מחשב $\beta$ כך ש- $\beta = \alpha^a \mod p$.
4. $B$ שומר את המפתח ציבורי $(p, \alpha, \beta)$ בכתובת ציבורית ושמור על $a$ כמפתח סודי.

**שלב הצפנה**

5. אליס $(A)$ קוראת את המפתח ציבורי $(p, \alpha, \beta)$ מהכתובת ציבורית.
6. $A$ בוחרת באקראי שלם $d \in \{2, 3, \ldots, p-2\}$.
7. כדי להצפין הודעה $x$ כאשר $0 \le x < p$, אליס $(A)$ מחשבת $y_1 = \alpha^d \mod p$ ו- $y_2 = \beta^d x \mod p$.

8 $A$ שולחת הטקסט מוצפן $(y_1, y_2)$ ל- $B$.

9 כדי לפענח את הטקסט מוצפן $(y_1, y_2)$, $B$ משמש המפתח הסודי $a$ כדי לחשב את $x = ((y_1)^a)^{-1} y_2 \mod p$.

### דוגמה 7.1 הצפנת אל-גמאל

נניח כי אליס שולחת הטקסט גלוי $x = 123$. בוב בוחר במספר ראשוני $p = 727$, יוצר $\alpha = 80$ ומפתח סודי $a = 6$. אליס בוחרת ב- $d = 7$. מצאו את הטקסט מוצפן.

**פתרון:**

$$\beta = \alpha^a \mod p = 80^6 \mod 727 = 514 .$$

$$y_1 = \alpha^d \mod p = 80^7 \mod 727 = 408 , \qquad y_2 = \beta^d x \mod p = 514^7 \cdot 123 \mod 727 = 390 .$$

■

### דוגמה 7.2 הצפנת אל-גמאל

נניח כי בוב מקבל את הטקסט מוצפן $(y_1, y_2) = (408, 390)$. בוב בחר במספר ראשוני $p = 727$, יוצר $\alpha = 80$ ומפתח סודי $a = 6$. ואליס בחרה ב- $d = 7$. פענחו את הקטסט מוצפן.

**פתרון:**

$$\beta = \alpha^a \mod p = 80^6 \mod 727 = 514 .$$

$$x = \left((y_1^a)^{-1}\right) y_2 \mod p = \left(\left(480^6\right)^{-1}\right) \cdot 390 \mod 727$$

בעזרת משפט פרמה,

$$\left(408^6\right)^{-1} \mod 727 = 408^{727-1-6} \mod 727 = 408^{720} \mod 727 = 375 .$$

■