

## שיעור 8

### צופן אל-גמאל

#### הגדלה 8.1 צופן אל-גמאל

יהי  $p$  מספר ראשוני (גדול),  $\alpha$  יוצר של  $(\mathbb{Z}_p^*, \times_p)$  ויהי  $a \in \{2, 3, \dots, p-2\}$ .  
יהי הקבוצה טקסט גלי  $P = \mathbb{Z}_p^*$  והקבוצה טקסט מוצפן  $C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ . נגידיר קבוצת מפתחות

$$K = \{(p, \alpha, a, \beta) \mid \beta = \alpha^a \pmod{p}\}.$$

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

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

כאשר  $y_1 = \beta^d x \pmod{p}$ ,  $y_2 = \alpha^d \pmod{p}$

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

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

#### משפט 8.1 צופן אל-גמאל צופן חוקי

אם  $p$  מספר ראשוני ו-  $\alpha$  יוצר של  $(\mathbb{Z}_p^*, \times_p)$ ,  $x \in \mathbb{Z}_p^*$  ו-  $\beta = \alpha^a \pmod{p}$ ,  $a \in \{2, 3, \dots, p-2\}$ ,  
 $d \in \{2, 3, \dots, p-2\}$

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

הוכחה: תרגיל בית.

#### כל 1.8 אלגורים הצפנה אל-גמאל

נניח שאليس ( $A$ ) שולחת הودעה לבוב ( $B$ ).

##### שלב הרכבת המפתח

- 1  $B$  יוצר מספר ראשוני גדול  $p$ , ויווצר  $\alpha$  של החבורה  $(\mathbb{Z}_p^*, \times_p)$ .
- 2  $B$  בוחר באקראי שלם  $a \in \{2, 3, \dots, p-2\}$ .
- 3  $B$  מחשב  $\beta = \alpha^a \pmod{p}$ .
- 4  $B$  שומר את המפתח ציבורי  $(p, \alpha, \beta)$  בכתב ציבורי ושמור על  $a$  כמפתח סודי.

##### שלב הצפנה

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

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  $x = ((y_1)^a)^{-1} y_2 \pmod{p}$ .

### דוגמה 8.1 הצפנה אל-גמאל

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

**פתרון:**

$$\beta = \alpha^a \pmod{p} = 80^6 \pmod{727} = 514 .$$

$$y_1 = \alpha^d \pmod{p} = 80^7 \pmod{727} = 408 , \quad y_2 = \beta^d x \pmod{p} = 514^7 \cdot 123 \pmod{727} = 390 .$$

### דוגמה 8.2 הצפנה אל-גמאל

נניח כי בוב מקבל את הטקסט מוצפן  $(y_1, y_2) = (408, 390)$ . בוב בוחר במספר ראשון  $p = 727$ ,  $\alpha = 80$  ומפתח סודי  $a = 6$ . אליס בחרה ב- $d = 7$ . פענחו את הקטע מוצפן.

**פתרון:**

$$\beta = \alpha^a \pmod{p} = 80^6 \pmod{727} = 514 .$$

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

בעזרת משפט פרמה,

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