תוכנית

1. El-gammal
2. דוגמה – הצפנה ופענוח ב-EG
3. הוכחה: EG ניתן / לפענוח
4. צופן / פ"סול.
5. DES
6. דיפי – הלמן / Diffie Hellman

הגדרה: צופן / **El-Gammal**

- יהי p ראשוני.
- יהי $a \in \{2,3,\dots,p-2\}$ (מספר שלם בין 2 עד $p-2$)
- יהי α שלם ב-קבוצת היוצרת של $\mathbb{Z}_p$
  (α כל מספר שלם).

נגדיר מפתח ציבורי:

נתונים

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

תהליך המצפין של צופן El-gamal מוגדר כ:

$$e_K(x) = (y_1, y_2)$$

כאשר x מספר שלם זה הטקסט הגלוי,

$$\left.\begin{aligned} y_1 &= \alpha^{d} \mod p \\ y_2 &= x\,\beta^{d} \mod p \end{aligned}\right\}$$

כאשר d כל מספר שלם $d \in \{2, \dots, p-2\}$

שנבחר באקראי.

<u>כלל מפענח</u>: בהינתן טקסטים מוצפנים y_1 ו-y_2 והמפתח k:

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

<u>דוגמה</u>: אליס שולחת הודעה לבוב שמוצפנת באמצעות צופן EG.

. אליס בוחרת במפתח: $p = 47$, $\alpha = 12$, $a = 10$,

תיקון: $d = 2$

. אליס שולחת את הטקסט הגלוי $x = 8$.

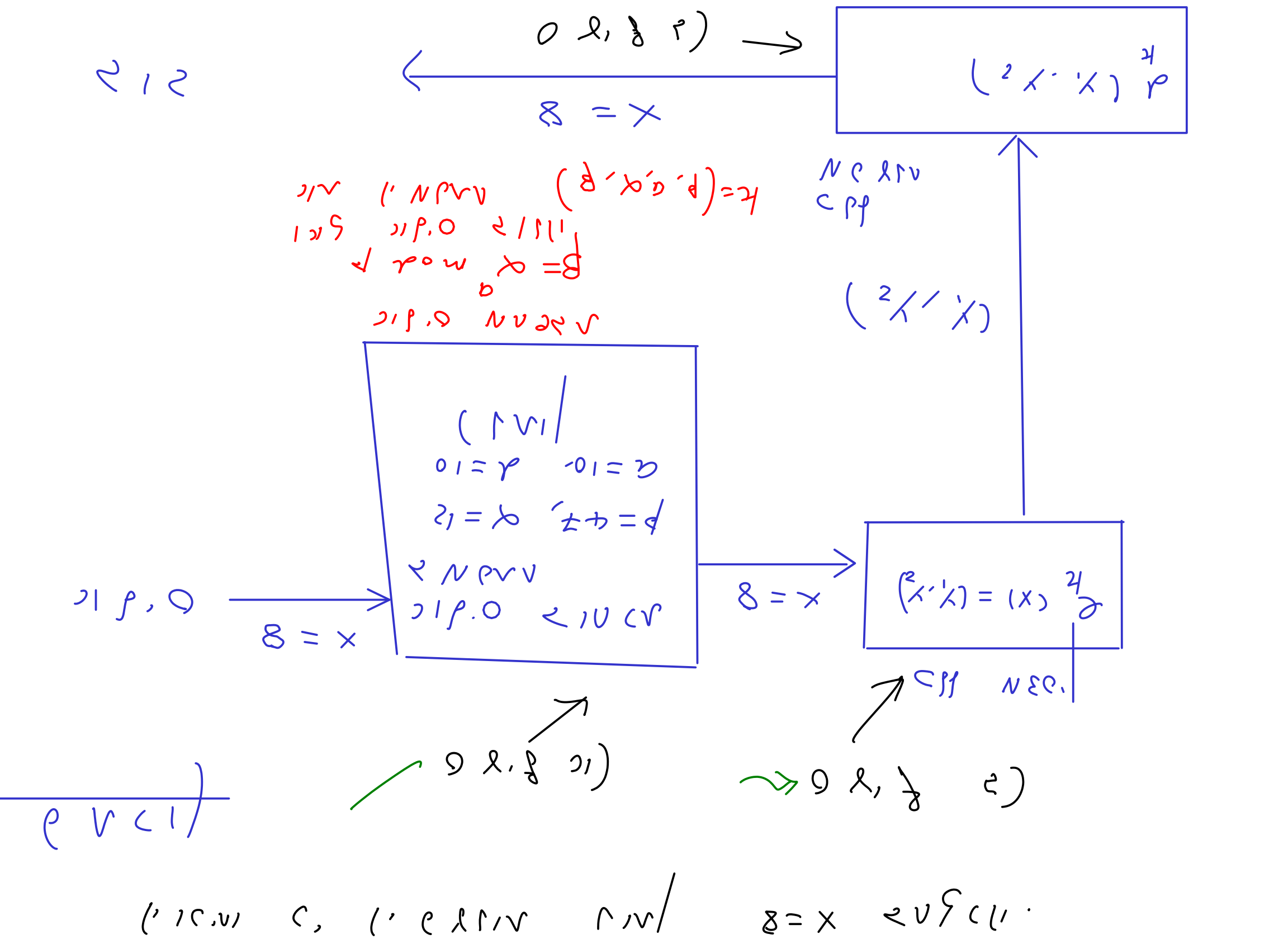
א) חשבו את המפתח הסודי β

ב) חשבו את הטקסט מוצפן (y_1, y_2).

ג) על פי הטקסט מוצפן שקיבלנו בסעיף ב (y_1, y_2)

$$12^{10} = 2^{8+2} = 2^{8} \cdot 12^{2} = 12$$

$$\beta = \alpha^{10} \bmod 29 = 12 \bmod 29$$



$$12^{10} \bmod 47 = 12^2 \, 12^8 \bmod 47$$

שיטת הריבועים

$$12^2 \bmod 47 = 144 \bmod 47 = 3$$

$$12^4 \bmod 47 = (12^2)^2 \bmod 47 = 3^2 \bmod 47 = 9$$

$$12^8 \bmod 47 = (12^4)^2 \bmod 47 = 9^2 \bmod 47 = 34$$

$$12^{10} \bmod 47 = 12^2 \cdot 12^8 \bmod 47 = (3)(34) \bmod 47$$

$$= 102 \bmod 47$$

$$= 8$$

לכן, $\boxed{\beta = 8}$

לכן, המפתח הוא: $(p = 47, \alpha = 12, a = 10, \beta = 8)$

סעיף ב)

$$Y_1 = \alpha^d \bmod p \qquad (d = 2)$$

$$Y_2 = x \cdot \beta^d \bmod p$$

$$Y_1 = 12^2 \bmod 47 = 3$$

$$Y_2 = 8 \cdot 8^2 \bmod 47 = 512 \bmod 47 = 42.$$

לכן הערכים מוצפנים: $(Y_1 = 3, Y_2 = 42)$

סעיף ב

בשלב הפענוח, אנחנו יודעים את הסודיים
מקבלים $y_1=3$ ו- $y_2=42$ יחד עם המפתח:

$$K=\{a=10,\ \alpha=12,\ p=47,\ \beta=8,\ d=2\}$$

ונחשב את הסוד כלו

$$x=d_K(y_1,y_2)=(y_1^{\,a})^{-1}\,y_2 \bmod p$$

שלב 1 נחשב קודם $(y_1^{\,a})^{-1} \bmod p$,

$$(y_1^{\,a})^{-1} \bmod p=(3^{10})^{-1} \bmod 47 \qquad = 3^{-10} \bmod 47$$

לפי המשפט ש $(a^k)^{-1} \bmod m \equiv a^{-k} \bmod m$.

משפט פרמה אומר כי לכל a שלם וזר ל p:

$$a^{p-1}\equiv 1 \bmod p \qquad a^p\equiv a \bmod p.$$

לכן,

$$3^{47-1} \overset{\text{פרמה}}{=} 1 \bmod 47$$

כלל הכפל של מודולים:

$$\begin{cases} a=c \bmod m \\ b=d \bmod m \end{cases} \Leftarrow ab=cd \bmod m.$$

$$1=3^{47-1} \bmod 47$$

$$3^{-10} \bmod 47 = 3^{-10}\cdot 1 \bmod 47 = 3^{-10}\cdot\left(3^{47-1}\right) \bmod 47$$

$$= 3^{-10+47-1} \bmod 47$$

$$= 3^{36} \bmod 47.$$

שלב 2 נחשב $3^{36} \bmod 47$ לפי שיטת הריבועים:

$$3^{36} = 3^4\cdot 3^{32}$$

$$3^2 \bmod 47 = 9$$
$$3^4 \bmod 47 = 81 \bmod 47 = 34$$
$$3^8 \bmod 47 = (34)^2 \bmod 47 = 28$$
$$3^{16} \bmod 47 = (28)^2 \bmod 47 = 32$$
$$3^{32} \bmod 47 = (32)^2 \bmod 47 = 37$$

$$3^{36} \bmod 47 = 3^4\cdot 3^{32} \bmod 47$$
$$= (34)(37) \bmod 47$$
$$= 36.$$

לכן,

$$(y_1^{\,a})^{-1} \bmod p = (3^{10})^{-1} \bmod 47 = 36$$

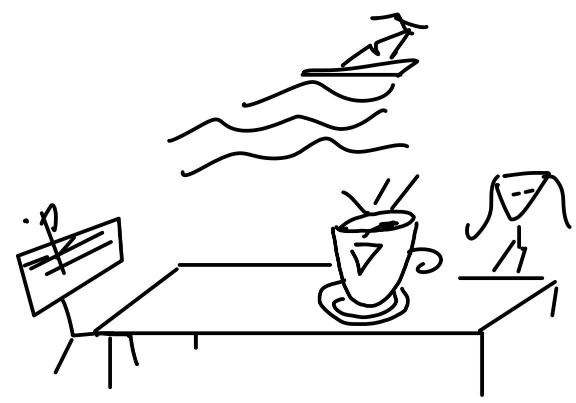
שלב 4

$$x = (y_1^a)^{-1} y_2 \bmod p = (3^{10})^{-1}(42) \bmod 47$$
$$= (36)(42) \bmod 47$$
$$= 8$$ ☺

משפט: צופן El-Gamal ניתן לפענוח.

ז"א, אם $e_k(x)$ הכלל מצפין של El-Gamal ו- $d_k(y_1, y_2)$ הכלל מפענח ז"א

$$e_k(\overbrace{d_k(y_1, y_2)}^{x}) = (y_1, y_2)$$
$$d_k(e_k(x)) = x$$



משפט ② כלל הכפל של מודולרים

$$(a \bmod m)(b \bmod m) = ab \bmod m$$

הוכחה:

לכל a, m שלמים $\exists\, q_1, r_1$ כך ש $a = q_1 m + r_1$ כאשר $r_1 = (a \bmod m)$

לכל b, m שלמים $\exists\, q_2, r_2$ כך ש $b = q_2 m + r_2$ כאשר $r_2 = b \bmod m$

לכן:

$$ab = (q_1 m + r_1)(q_2 m + r_2) = \overbrace{(q_1 m q_2 + r_1 q_2 + r_2 q_1)}^{Q} m + r_1 r_2$$

$$\Rightarrow \quad ab = Qm + r_1 r_2 \Rightarrow ab - r_1 r_2 = Qm \Rightarrow ab \equiv r_1 r_2 \bmod m$$

$r_1 r_2 \equiv ab \bmod m$

תזכורת: $x \equiv y \bmod m \iff m \mid x - y \iff x - y = Qm \iff y \equiv x \bmod m$

כאשר Q שלם. ז"א

$$ab \bmod m \equiv r_1 r_2 \bmod m$$

$$\Rightarrow \quad ab \bmod m = (a \bmod m)(b \bmod m) \bmod m$$

משפט ①

$$(a \bmod p)^{-1} \bmod p \equiv a^{-1} \bmod p$$

הוכחה:

$(a \bmod p)(x \bmod p) \bmod p = ax \bmod p$

נסמן: $x = (a \bmod p)^{-1} \bmod p$.

ז"א $x(a \bmod p) \equiv 1 \bmod p$

ז"א $x \cdot a \equiv 1 \bmod p$ (לפי משפט 11 [illegible])

לכן, $x \equiv a^{-1} \bmod p$

לכן, $(a \bmod p)^{-1} \bmod p \equiv a^{-1} \bmod p$.

מש"ל.

משפט El-Gamal תקין [illegible], כלומר $d_k(e_k(x)) = x$.

הוכחה: לפי ההגדרה, $e_k(x) = (y_1, y_2)$

$y_1 = \alpha^d \bmod p \qquad y_2 = x\beta^d \bmod p$

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

לכן,

$$d_k(e_k(x)) = d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \bmod p$$

$$= \left[(\alpha^d \bmod p)^a\right]^{-1} (x\beta^d \bmod p) \bmod p$$

$$= (\alpha^{da} \bmod p)^{-1} (x\beta^d \bmod p) \bmod p$$

$$\overset{\text{משפט 2}}{=} \left((\alpha^{da})^{-1} \bmod p\right)(x\beta^d \bmod p) \bmod p$$

$$\overset{\text{משפט 1}}{=} (\alpha^{da})^{-1}(x\beta^d) \bmod p$$

$$= x(\alpha^{da})^{-1}\beta^d \bmod p$$

לפי ההגדרה של El-Gamal: $\beta = \alpha^a \bmod p$

$$= x(\alpha^{da})^{-1}(\alpha^{ad} \bmod p) \bmod p$$

$$\overset{\text{משפט 1}}{=} x(\alpha^{da})^{-1}(\alpha^{ad}) \bmod p = x \bmod p$$

☺