

מבוא להצפנה – תרגיל 1

1.

a.

$$\begin{aligned}81X &\equiv 125 \pmod{39200} \\ \Rightarrow \gcd(81, 39200) &= 1 \\ \Leftrightarrow X &\equiv 81^{-1} \times 125 \pmod{39200} \\ \Rightarrow 81^{-1} \pmod{39200} &\equiv 29521 \pmod{39200} \\ \Leftrightarrow X &\equiv 29521 \times 125 \equiv 3690125 \pmod{39200} \equiv 5325 \\ \Leftrightarrow X &\equiv 5325\end{aligned}$$

b.

$$\begin{aligned}30X &\equiv 100 \pmod{39200} \\ \Rightarrow \gcd(30, 39200) &= 10 \\ \Rightarrow \text{כל המשוואה מתחלקת ב-10, לכן נחלק ב-10.} \\ \Leftrightarrow 3X &\equiv 10 \pmod{3920} \\ \Rightarrow \gcd(3, 3920) &= 1 \\ \Leftrightarrow X &\equiv 3^{-1} \times 10 \pmod{3920} \\ \Rightarrow 3^{-1} \pmod{3920} &\equiv 1307 \pmod{3920} \\ \Leftrightarrow X &\equiv 1307 \times 10 \equiv 13070 \pmod{3920} \equiv 1310 \\ \Leftrightarrow X &\equiv 1310\end{aligned}$$

c.

$$\begin{aligned}30X &\equiv 55 \pmod{39200} \\ \Rightarrow \gcd(30, 39200) &= 10 \\ \Rightarrow 55 \text{ לא מתחלק ב-10} \\ \text{לכן אין פתרון למשוואה.}\end{aligned}$$

2.

• $GE \rightarrow IS$

ז"א: $e(6) = 8; e(4) = 18$

$$6a + b \equiv 8 \pmod{26}$$

—

$$4a + b \equiv 18 \pmod{26}$$

$$2a \equiv -10 \equiv 16 \pmod{26}$$

$$\Rightarrow \gcd(2, 26) = 2$$

$$\Rightarrow \gcd(2, 16) = 2$$

כל המשוואה מתחלקת ב-2, לכן נחלק ב-2.

$$a \equiv 8 \pmod{13}$$

$$\Rightarrow a \equiv 8$$

$$\Rightarrow 4 \cdot 6 + b \equiv 18 \pmod{26}$$

$$24 + b \equiv 18 \pmod{26}$$

$$b \equiv 18 - 24 \pmod{26}$$

$$b \equiv 20 \pmod{26}$$

$$\Rightarrow b \equiv 20$$

• $EG \rightarrow IS$

ז"א: $e(4) = 8; e(6) = 18$

$$6a + b \equiv 18 \pmod{26}$$

—

$$4a + b \equiv 8 \pmod{26}$$

$$2a \equiv 10 \pmod{26}$$

$$\Rightarrow \gcd(2, 26) = 2$$

$$\Rightarrow \gcd(2, 10) = 2$$

כל המשוואה מתחלקת ב-2, לכן נחלק ב-2.

$$a \equiv 5 \pmod{13}$$

$$\Rightarrow a \equiv 5$$

$$\Rightarrow 4 \cdot 5 + b \equiv 8 \pmod{26}$$

$$20 + b \equiv 8 \pmod{26}$$

$$b \equiv 8 - 20 \pmod{26}$$

$$b \equiv 14 \pmod{26}$$

$$\Rightarrow \underline{b \equiv 14}$$

3.

האות הנפוצה ביותר בצופן הראשון ($1M$) היא: k
האות הנפוצה ביותר בצופן השני ($2M$) היא: a

נניח כי האות הנפוצה ביותר במקור היא: s

• $1M$: אם s מוצפן ל- k אז זאת הזזה של $22 \bmod 26 = 14 - 10$ והפענוח נותן:
 $b o b s u h x q x o q y h k u f o g d e t q o h k x o u t y i w$
ולהודעה זאת אין משמעות.

• $2M$: אם s מוצפן ל- a אז זאת הזזה של $12 \bmod 26 = 14 - 0$ והפענוח נותן:
 $b o b w a n t s t o s i n g a j o y f u l s o n g t o a l i c e$
קיבלנו הודעה עם משמעות:
 $b o b w a n t s t o s i n g a j o y f u l s o n g t o a l i c e$

מצאנו כי ההודעה $2M$ מוצפנת עם צופן הזזה: $e(x) = x + 12 \bmod 26$
והעתקת הפענוח היא: $d(y) = d - 12 = d + 14 \bmod 26$

ההודעה $1M$ מוצפנת על ידי צופן אפיני. נשתמש בשתי אותיות של הצופן וטקסט מקור כדי למצוא את העתקת ההצפנה וההעתקת הפענוח.

האות $a=0$ מוצפנת כ- $q=16$. ולכן $b \equiv 16 \bmod 26$
האות $b=1$ מוצפנת כ- $x=23$. ולכן $a + b \equiv 23 \bmod 26$

$$\Leftrightarrow a \equiv 7 \bmod 26$$

$$\Rightarrow 7 + b \equiv 23 \bmod 26$$

$$b \equiv 16 \bmod 26$$

פונקציית ההצפנה היא:

$$\Rightarrow e(x) = 7x + 16 \bmod 26$$

פונקציית הפענוח היא:

האות $a=0$ מוצפנת כ- $q=16$. ולכן $16a + b \equiv 0 \bmod 26$

האות $b=1$ מוצפנת כ- $x=23$. ולכן $23a + b \equiv 1 \bmod 26$

$$\Leftrightarrow 7a \equiv 1 \bmod 26$$

$$a \equiv 7^{-1} \equiv 15 \bmod 26$$

$$\Rightarrow a \equiv 15$$

$$\Rightarrow 23 \cdot 15 + b \equiv 1 \pmod{26}$$

$$7 + b \equiv 1 \pmod{26}$$

$$b \equiv 20 \pmod{26}$$

$$b \equiv 16 \pmod{26}$$

פונקציית הפענוח היא:

$$\Rightarrow \underline{d(x) = 15x + 16 \pmod{26}}$$

.4

•

$$2021 = 43 \times 47$$

⇐ מספר הצפנים טריוויאליים שניתן להגדיר הוא :

$$\begin{aligned}\mathbb{Z}_{2021} &= \varphi(2021) \times 2021 - 1 = \\ &= (43 - 1)(47 - 1) \times 2021 - 1 = \\ &= 3904571\end{aligned}$$

•

$$2023 = 7 \times 17^2$$

⇐ מספר הצפנים טריוויאליים שניתן להגדיר הוא :

$$\begin{aligned}\mathbb{Z}_{2023} &= \varphi(2023) \times 2023 - 1 = \\ &= (7 - 1)(289 - 17) \times 2023 - 1 = \\ &= \underline{3301535}\end{aligned}$$

•

$$2024 = 2^3 \times 11 \times 23$$

⇐ מספר הצפנים טריוויאליים שניתן להגדיר הוא :

$$\begin{aligned}\mathbb{Z}_{2024} &= \varphi(2024) \times 2024 - 1 = \\ &= (8 - 4)(11 - 1)(23 - 1) \times 2024 - 1 = \\ &= \underline{1781119}\end{aligned}$$

5.

$$\begin{aligned}e(x) \equiv x &\Leftrightarrow ax + b \equiv \text{mod}30 \\&\Leftrightarrow ax - x \equiv -b \text{mod}30 \\&\Leftrightarrow x(a - 1) \equiv -b \text{mod}30\end{aligned}$$

מספר הפתרונות של המשוואה הזו הוא 0 או $\gcd(a-1, 30)$.

a . $7 \nmid 30$, לכן לכל a לא מתקיים ש- $\gcd(a-1, 30) = 7$.
לכן לא קיימים a ו- b כך שמספר הפתרונות ל- $e(x) \equiv x$ הוא 7.

b . $6 \mid 30$, קיים a כך ש- $\gcd(a-1, 30) = 6$ צריך להיות שווה ל-6).
נבחר- $a = 7 \Leftrightarrow a - 1 = 6$, $\gcd(6, 30) = 6$.

ניתן דוגמא:

יהיו לנו 6 פתרונות כאשר: $\gcd(a-1, 30) = 6$ ו- $6 \mid (-b)$.
למשל - $e(x) = 7x + 6 \text{mod}30$.

.6

$$\begin{aligned}e_k(e_k(x)) &\equiv x \pmod{28} \\a(ax + b) + b &\equiv x \pmod{28} \\aax + ab + b &\equiv x \pmod{28} \\x(aa - 1) &\equiv -b(a + 1) \pmod{28} \\x(a^2 - 1) &\equiv -b(a + 1) \pmod{28}\end{aligned}$$

קיים צופן אפיוני לכל x אם $(a+1)$ הוא מספר הפיך. ואז מתקבל:

$$\begin{aligned}x(a + 1)^{-1}(a^2 - 1) &\equiv -b(a + 1)^{-1}(a + 1) \pmod{28} \\x(a - 1) &\equiv -b \pmod{28}\end{aligned}$$

למשוואה יש 28 פתרונות לכל X אם מתקיים ש- $\gcd(a-1, 28) = 28$ וגם מתקיים:
b-28 .