שם: שחר אשר
ת.ז. 209305408

מבוא להצפנה – תרגיל 1

.1

.a

$$81X \equiv 125 \; mod \; 39200$$
$$\underline{\Rightarrow gcd(81, 39200) = 1}$$
$$\Leftrightarrow X \equiv 81^{-1} \times 125 \; mod \; 39200$$
$$\underline{\Rightarrow 81^{-1} \; mod \; 39200 \; \equiv \; 29521 \; mod \; 39200}$$
$$\Leftrightarrow \; X \equiv 29521 \times 125 \; \equiv 3690125 \; mod \; 39200 \; \equiv 5325$$
$$\Leftrightarrow X \equiv 5325$$

.b

$$30X \equiv 100 \; mod \; 39200$$
$$\underline{\Rightarrow gcd(30, 39200) = 10}$$

<u>כל המשוואה מתחלקת ב – 10, לכן נחלק ב – 10. ⇒</u>

$$\Leftrightarrow 3X \equiv 10 \; mod \; 3920$$
$$\underline{\Rightarrow gcd(3, 3920) = 1}$$
$$\Leftrightarrow X \equiv 3^{-1} \times 10 \; mod \; 3920$$
$$\underline{\Rightarrow 3^{-1} \; mod \; 3920 \; \equiv \; 1307 \; mod \; 3920}$$
$$\Leftrightarrow \; X \equiv 1307 \times 10 \; \equiv 13070 \; mod \; 3920 \; \equiv 1310$$
$$\Leftrightarrow X \equiv 1310$$

.c

$$30X \equiv 55 \; mod \; 39200$$
$$\underline{\Rightarrow gcd(30, 39200) = 10}$$

<u>55 לא מתחלק ב – 10 ⇒</u>

<u>לכן אין פתרון למשוואה.</u>

שם: שחר אשר
ת.ז. 209305408

.2

- *GE ----> IS*

ז"א: *e(6) = 8; e(4) = 18*

$$6a + b \equiv 8 \; mod \; 26$$
$$-$$
$$4a + b \equiv 18 \; mod \; 26$$
$$- - - - - - - - - - -$$
$$2a \equiv -10 \equiv 16 \; mod \; 26$$

$$\underline{\Rightarrow gcd(2, 26) = 2}$$
$$\underline{\Rightarrow gcd(2, 16) = 2}$$

<u>כל המשוואה מתחלקת ב – 2, לכן נחלק ב – 2. ⇒</u>

$$a \equiv 8 \; mod \; 13$$
$$\underline{\Longrightarrow a \equiv 8}$$

$$\Longrightarrow 4 \cdot 6 + b \equiv 18 \; mod 26$$
$$24 + b \equiv 18 \; mod 26$$
$$b \equiv 18 - 24 \; mod 26$$
$$b \equiv 20 \; mod 26$$
$$\underline{\Longrightarrow b \equiv 20}$$

- *EG ----> IS*

ז"א: *e(4) = 8; e(6) = 18*

$$6a + b \equiv 18 \; mod \; 26$$
$$-$$
$$4a + b \equiv 8 \; mod \; 26$$
$$- - - - - - - - - - -$$
$$2a \equiv 10 \; mod \; 26$$

$$\underline{\Rightarrow gcd(2, 26) = 2}$$
$$\underline{\Rightarrow gcd(2, 10) = 2}$$

<u>כל המשוואה מתחלקת ב – 2, לכן נחלק ב – 2. ⇒</u>

$$a \equiv 5 \; mod \; 13$$
$$\Longrightarrow a \equiv 5$$

שם: שחר אשר
ת.ז. 209305408

$$\Longrightarrow 4 \cdot 5 + b \equiv 8 \; mod 26$$
$$20 + b \equiv 8 \; mod 26$$
$$b \equiv 8 - 20 \; mod 26$$
$$b \equiv 14 \; mod 26$$
$$\underline{\Longrightarrow b \equiv 14}$$

שם: שחר אשר
ת.ז. 209305408

.3

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

נניח כי האות הנפוצה ביותר במקור היא: o

- $1M$: אם o מוצפן ל- k אז זאת הזזה של $10 - 14 = 22\ mod\ 26$ 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 o מוצפן ל- a אז זאת הזזה של $0 - 14 = 12\ mod\ 26$ 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:
bob wants to sing a joyful song to alice

מצאנו כי ההודעה $2M$ מוצפנת עם צופן הזזה: $e(x) = x + 12\ mod26$
והעתקת הפענוח היא: $d(y) = d - 12 = d + 14\ mod26$

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 $b \equiv 16\ mod26$
האות b=1 מוצפנת כ- x=23. ולכן $a + b \equiv 23\ mod26$

$$\Leftrightarrow a \equiv 7\ mod26$$

$$\Rightarrow 7 + b \equiv 23\ mod26$$
$$b \equiv 16\ mod26$$

פונקציית ההצפנה היא:
$$\underline{\Rightarrow e(x) = 7x + 16\ mod26}$$

פונקציית הפענוח היא:
האות a=0 מוצפנת כ- q=16. ולכן $16a + b \equiv 0\ mod26$
האות b=1 מוצפנת כ- x=23. ולכן $23a + b \equiv 1\ mod26$

$$\Leftrightarrow 7a \equiv 1\ mod26$$
$$a \equiv 7^{-1} \equiv 15\ mod26$$
$$\Rightarrow a \equiv 15$$

שם: שחר אשר
ת.ז. 209305408

$$\Longrightarrow 23 \cdot 15 + b \equiv 1 \, mod 26$$
$$7 + b \equiv 1 \, mod 26$$
$$b \equiv 20 \, mod 26$$
$$b \equiv 16 \, mod 26$$

פונקציית הפענוח היא:

$$\underline{\Longrightarrow d(x) = 15x + 16 \, mod 26}$$

שם: שחר אשר
ת.ז. 209305408

.4

- $$2021 = 43 \times 47$$

$\Leftarrow$ מספר הצפנים הלא טריוויאלים שניתן להגדיר הוא :

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

- $$2023 = 7 \times 17\text{^}2$$

$\Leftarrow$ מספר הצפנים הלא טריוויאלים שניתן להגדיר הוא :

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

- $$2024 = 2\text{^}3 \times 11 \times 23$$

$\Leftarrow$ מספר הצפנים הלא טריוויאלים שניתן להגדיר הוא :

$$\mathbb{Z}_{2023} = \varphi(2024) \times 2024 - 1 =$$
$$= (8-4)(11-1)(23-1) \times 2024 - 1 =$$
$$\underline{= 1781119}$$

שם: שחר אשר
ת.ז. 209305408

.5

$$e(x) \equiv x \Leftrightarrow ax + b \equiv mod30$$
$$\Leftrightarrow ax - x \equiv -b\ mod30$$
$$\Leftrightarrow x(a-1) \equiv -bmod30$$

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

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

<u>ניתן דוגמא</u>:
יהיו לנו 6 פתרונות כאשר: 6 = *gcd(a-1, 30)* ו- *(-b)*|6.
למשל - $e(x) = 7x + 6\ mod30$.

שם: שחר אשר
ת.ז. 209305408

.6

$$e_k\big(e_k(x)\big) \equiv x\ mod 28$$
$$a(ax+b)+b\ \equiv x\ mod 28$$
$$aax+ab+b\ \equiv x\ mod 28$$
$$x(aa-1) \equiv -b(a+1) mod 28$$
$$x(a^2-1) \equiv -b(a+1) mod 28$$

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

$$x(a+1)^{-1}(a^2-1) \equiv -b(a+1)^{-1}(a+1) mod 28$$
$$x(a-1) \equiv -b\ mod 28$$

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