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*

$$6a + b \equiv 8 \bmod 26$$

-

$$4a + b \equiv 18 \bmod 26$$

$$- - - - - - - - - - -$$

$$2a \equiv -10 \equiv 16 \; mod \; 26$$

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

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

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

$$a \equiv 8 \; mod \; 13$$

$$\Longrightarrow a \equiv 8$$

- *EG ----> IS*

ז"א: *e(4) = 8; e(6) = 18*

$$6a + b \equiv 18 \bmod 26$$

-

$$4a + b \equiv 8 \bmod 26$$

$$- - - - - - - - - - -$$

$$2a \equiv 10 \; mod \; 26$$

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

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

<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

.3