עבודת 2: קריפטו-אנליזה וצופן RSA.

שאלה 1 **(10 נקודות)** פתרו את המערכת משוואות הבאה בעזרת המשפט השאריות הסיני:

$$\begin{aligned} x \equiv & 12 \mod 25 \\ x \equiv & 9 \mod 26 \\ x \equiv & 23 \mod 27 \ . \end{aligned}$$

שאלה 2 **(10 נקודות)** פתרו את המערכת משוואות הבאה:

$$\begin{aligned} 13x \equiv & 4 \mod 99 \\ 15x \equiv & 56 \mod 101 \ . \end{aligned}$$

רמז: השתמשו באלגוריתם המוכלל של אוקליד ואחר כך המשפט השאירות הסיני.

שאלה 3 **(10 נקודות)** בוב הרכיב סכימת RSA עם הפרמטרים $p = 37, q = 41$ ו- $b = 31$.

א) חשבו את n, $\phi(n)$ ו- a.

ב) אליס קיבלה את המפתח ציבורי (b, n) מבוב ובאמצעותה היא מצפינה את ההודעה `1228`. מהי הטקסט מוצפן שהיא שולחת לבוב?

ג) הוכיחו שהפענוח של הטקסט מוצפן שמצאתם בסעיף ב' נותן `1228`.

שאלה 4 **(10 נקודות)** נתון הטקסט גלוי

```
thefutureisgood
```

והטקסט מוצפן שלו

```
FOPBVFWDFCCGMAT
```

הטקסט הוצפן עם צופן היל. מצאו את המפתח.

שאלה 5 **(10 נקודות)** נתון הטקסט הבא אשר הוצפן באמצעות צופן אפיני:

```
EYDDGBHFXSDQNDBXNEVXLPPDDWMLXEADBQODSDQNEYFOREZFPD .
```

מצאו את המפתח של הצופן והטקסט גלוי.

שאלה 6 **(10 נקודות)** נתונה האלפיבית הבאה של טקסט גלוי $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}, \mathtt{x}, \mathtt{y}, \mathtt{z}\}$ ונתונה פונקצית ההסתברות

$$P_X(\mathtt{a}) = 0.13\ , \quad P_X(\mathtt{b}) = 0.01\ , \quad P_X(\mathtt{c}) = 0.26\ , \quad P_X(\mathtt{d}) = 0.10\ , \quad P_X(\mathtt{e}) = 0.15\ .$$
$$P_X(\mathtt{f}) = 0.22\ , \quad P_X(\mathtt{x}) = 0.02\ , \quad P_X(\mathtt{y}) = 0.04\ , \quad P_X(\mathtt{z}) = 0.07\ .$$

א) מצאו הצפנת האפמן של X.

ב) חשבו את האנטרופיה של ההצפנה.

ג) מצאו את $l(f)$.

שאלה 7 **(10 נקודות)** יהי $X = \{\mathtt{q}, \mathtt{r}, \mathtt{s}\}$ קבוצת טקסט גלוי עם פונקצית הסתברות

$$P_X(\mathtt{q}) = \frac{1}{3}\ , \qquad P_X(\mathtt{r}) = \frac{1}{4}\ , \qquad P_X(\mathtt{s}) = \frac{5}{12}\ .$$

יהי $K = \{k_1, k_2, k_3, k_4\}$ קבוצת מפתחות בעלת פונקצית הסתברות

$$P_K(k_i) = \frac{1}{4}$$

לכל $k_i \in K$. יהי $Y = \{\mathtt{A}, \mathtt{B}, \mathtt{C}\}$ קבוצת טקטסט מוצפן. נגדיר הכלל מצפין

$$e_{k_i}(x) = 2x + i \mod 3$$

לכל $x \in \mathbb{Z}_{26}$ ולכל $i \in \{1, 2, 3, 4\}$. לדגומה

א) מצאו את $P_Y(y)$ לכל $y \in Y$.

ב) מצאו את $P(X = \mathtt{q} | Y = \mathtt{B})$.

ג) מצאו את $P(X = \mathtt{r} | Y = \mathtt{C})$.

ד) הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.

שאלה 8 **(10 נקודות)** נתונה הקריפטו-מערכת בעלת הקבוצת טקסט גלוי $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, קבוצת מפתחות $K = \{k_1, k_2, k_3\}$ וקבוצת טקסט מוצפן $Y = \{\mathtt{A}, \mathtt{B}, \mathtt{C}\}$. הפונקציות הסתברויות הן

$$P_X(\mathtt{a}) = \frac{1}{6}, \quad P_X(\mathtt{b}) = \frac{1}{3}, \quad P_X(\mathtt{c}) = \frac{1}{2}, \quad P_K(k_1) = \frac{1}{2}, \quad P_K(k_2) = \frac{1}{4}, \quad P_K(k_3) = \frac{1}{4}\ .$$

המטריצת ההצפנה היא

	a	b	c
k_1	B	A	C
k_2	A	C	B
k_3	C	A	B

א) מצאו את הפונקצית הסתברות של הטקסט מוצפן Y.

ב) הוכיחו כי לקריפטו-מערכת זו אין סודיות מושלמת.

שאלה 9 (10 נקודות)

א) הוכיחו כי

$$H(X,Y) = H(Y) + H(X|Y) \ .$$

ב) הוכיחו כי

$$H(X|Y) \leq H(X) \ .$$

ו- $H(X|Y) = H(X)$ אם ורק אם X ו- Y בלתי תלויים.

שאלה 10 (10 נקודות)

הוכיחו שלקריפטו-מערכת יש סודיות מושלמת אם ורק אם

$$H(P|C) = H(P) \ .$$

פתרונות

שאלה 1 נפתור מערכת זו באמצעות משפט השאריות הסיני. נסמן

$$\begin{aligned} x \equiv & a_1 \mod m_1 \\ x \equiv & a_2 \mod m_2 \\ x \equiv & a_3 \mod m_3 \ . \end{aligned}$$

כאשר

$$a_1 = 12 \ , \quad a_2 = 9 \ , \quad a_3 = 23 \ , \quad m_1 = 25 \ , \quad m_2 = 26 \ , \quad m_3 = 27 \ .$$

נחשב

$$M = m_1 m_2 m_3 = 17550 \ , \quad M_1 = \frac{M}{m_1} = 702 \ , \quad M_2 = \frac{M}{m_2} = 675 \ , \quad M_3 = \frac{M}{m_3} = 650 \ .$$

באמצעות הקוד פייתון שנמצא באתר המודל נחשב את ההופכיים

$$\begin{aligned} y_1 = & M_1^{-1} \mod m_1 = 702^{-1} \mod 25 = 13 \ , \\ y_2 = & M_2^{-1} \mod m_2 = 675^{-1} \mod 26 = 25 \ , \\ y_3 = & M_3^{-1} \mod m_3 = 650^{-1} \mod 27 = 14 \ . \end{aligned}$$

הפתרון (מודולר M) הוא

$$\begin{aligned} x = & a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \mod M \\ = & (12)(702)(13) + (9)(675)(25) + (23)(650)(14) \mod 17550 \\ = & 470687 \mod 17550 \\ = & 14387 \ . \end{aligned}$$

שאלה 2 נמצא את ההופכי המודולרי של 13 ביחס ל- 99:

$a = 99, b = 13$.

$$\begin{aligned} r_0 = & a = 99 \ , & r_1 = & b = 13 \ , \\ s_0 = & 1 \ , & s_1 = & 0 \ , \\ t_0 = & 0 \ , & t_1 = & 1 \ . \end{aligned}$$

שלב $k=1$:	$r_2 = 99 - 7 \cdot 13 = 8$	$s_2 = 1 - 7 \cdot 0 = 1$	$t_2 = 0 - 7 \cdot 1 = -7$	$q_1 = 7$
שלב $k=2$:	$r_3 = 13 - 1 \cdot 8 = 5$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-7) = 8$	$q_2 = 1$
שלב $k=3$:	$r_4 = 8 - 1 \cdot 5 = 3$	$s_4 = 1 - 1 \cdot (-1) = 2$	$t_4 = -7 - 1 \cdot (8) = -15$	$q_3 = 1$
שלב $k=4$:	$r_5 = 5 - 1 \cdot 3 = 2$	$s_5 = -1 - 1 \cdot 2 = -3$	$t_5 = 8 - 1 \cdot (-15) = 23$	$q_4 = 1$
שלב $k=5$:	$r_6 = 3 - 1 \cdot 2 = 1$	$s_6 = 2 - 1 \cdot (-3) = 5$	$t_6 = -15 - 1 \cdot (23) = -38$	$q_5 = 1$
שלב $k=6$:	$r_7 = 2 - 2 \cdot 1 = 0$	$s_7 = -3 - 2 \cdot (5) = -13$	$t_7 = 23 - 2 \cdot (-38) = 99$	$q_6 = 2$

$$\gcd(a,b) = r_6 = 1 \ , \qquad s = s_6 = 5 \ , \qquad t = t_6 = -38 \ .$$

$$sa + tb = 5(99) - 38(13) = 1 \ .$$

לכן

$$13^{-1} \equiv -38 \mod 99 = 61 \mod 99 \ .$$

■נמצא את ההופכי המודולרי של 15 ביחס ל- 101:

$a = 101, b = 15$.

$$\begin{aligned} r_0 &= a = 101 \ , & r_1 &= b = 15 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $k=1$:	$r_2 = 101 - 6 \cdot 15 = 11$	$s_2 = 1 - 6 \cdot 0 = 1$	$t_2 = 0 - 6 \cdot 1 = -6$	$q_1 = 6$
שלב $k=2$:	$r_3 = 15 - 1 \cdot 11 = 4$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-6) = 7$	$q_2 = 1$
שלב $k=3$:	$r_4 = 11 - 2 \cdot 4 = 3$	$s_4 = 1 - 2 \cdot (-1) = 3$	$t_4 = -6 - 2 \cdot (7) = -20$	$q_3 = 2$
שלב $k=4$:	$r_5 = 4 - 1 \cdot 3 = 1$	$s_5 = -1 - 1 \cdot 3 = -4$	$t_5 = 7 - 1 \cdot (-20) = 27$	$q_4 = 1$
שלב $k=5$:	$r_6 = 3 - 3 \cdot 1 = 0$	$s_6 = 3 - 3 \cdot (-4) = 15$	$t_6 = -20 - 3 \cdot (27) = -101$	$q_5 = 3$

$$\gcd(a,b) = r_6 = 1 \ , \qquad s = s_5 = -4 \ , \qquad t = t_5 = 27 \ .$$

$$sa + tb = -4(101) + 27(15) = 1 \ .$$

לכן

$$15^{-1} \equiv 27 \mod 101 \ .$$

$$13^{-1} \cdot 13x \equiv 61 \cdot 4 \mod 99 \quad \Rightarrow \quad x \equiv 244 \mod 99 = 46 \mod 99$$

$$15^{-1} \cdot 15x \equiv 27 \cdot 56 \mod 101 \quad \Rightarrow \quad x \equiv 1512 \mod 101 = 98 \mod 101$$

כעת נפתור את המערכת

$$\begin{aligned} x \equiv & 46 \mod 99 \\ x \equiv & 98 \mod 101 \ . \end{aligned}$$

בעזרת המשפט השאריות הסיני.
נסמן

$$a_1 = 46 \ , \quad m_1 = 99 \ , \quad a_2 = 98 \ , \quad m_2 = 101 \ , \quad M = m_1 m_2 = 9999 \ , \quad M_1 = \frac{M}{m_1} = 101 \ , \quad M_2 = \frac{M}{m_2} = 99 \ .$$

$$y_1 = M_1^{-1} \mod m_1 = 101^{-1} \mod 99 = 50 \ , \qquad y_2 = M_2^{-1} \mod m_2 = 99^{-1} \mod 101 = 50 \ .$$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 \mod M = 717400 \mod 9999 = 7471 \ .$$

שאלה 3

א)

$$n = pq = 37 \times 41 = 1517$$
$$\phi(n) = \phi(pq) = (p-1)(q-1) = 36 \times 40 = 1440 \ .$$

$a = 31^{-1} \mod 1440$. נשתמש באלגוריתם של אוקליד:

שיטה 1

$$\begin{aligned} r_0 = & \phi(n) = 1440 \ , & r_1 = & b = 31 \ , \\ s_0 = & 1 \ , & s_1 = & 0 \ , \\ t_0 = & 0 \ , & t_1 = & 1 \ . \end{aligned}$$

שלב $i = 1$:	$r_2 = 1440 - 46 \cdot 31 = 14$	$s_2 = 1 - 46 \cdot 0 = 1$	$t_2 = 0 - 46 \cdot 1 = -46$	$q_1 = 46$
שלב $i = 2$:	$r_3 = 31 - 2 \cdot 14 = 3$	$s_3 = 0 - 2 \cdot 1 = -2$	$t_3 = 1 - 2 \cdot (-46) = 93$	$q_2 = 2$
שלב $i = 3$:	$r_4 = 14 - 4 \cdot 3 = 2$	$s_4 = 1 - 4 \cdot (-2) = 9$	$t_4 = -46 - 4 \cdot (93) = -418$	$q_3 = 4$
שלב $i = 4$:	$r_5 = 3 - 1 \cdot 2 = 1$	$s_5 = -2 - 1 \cdot (9) = -11$	$t_5 = 93 - 1 \cdot (-418) = 511$	$q_4 = 1$
שלב $i = 5$:	$r_6 = 2 - 2 \cdot 1 = 0$	$s_6 = 9 - 2 \cdot (-11) = 31$	$t_6 = -418 - 2 \cdot (511) = -1440$	$q_5 = 2$

$$\gcd(a,b) = r_5 = 1\ , \qquad s = s_5 = -11\ , \qquad y = t_5 = 511\ .$$

$$(-11)(1440) + (511)(31) = 1\ .$$

מכאן

$$31^{-1} = 511 \mod 1440\ .$$

לכן $a = b^{-1} \mod \phi(n) = 31^{-1} \mod 1440 = 511$.

ב) אליס שולחת את ההודעה $x^b \mod n = 1228^{31} \mod 1517$. כדי לחשב זה נשתמש בשיטת ריבועים: $31 = 16 + 8 + 4 + 2 + 1$.

$$\begin{aligned}
(1228)^2 \mod 1517 &= 86 \mod 1517\\
(1228)^4 \mod 1517 &= (86)^2 \mod 1517 = 1328 \mod 1517\\
(1228)^8 \mod 1517 &= (1328)^2 \mod 1517 = 830 \mod 1517\\
(1228)^{16} \mod 1517 &= (830)^2 \mod 1517 = 182 \mod 1517
\end{aligned}$$

לכן

$$\begin{aligned}
1228^{31} \mod 1517 &= (1228)^{16} \times (1228)^8 \times (1228)^4 \times (1228)^2 \times 1228 \mod 1517\\
&= 182 \times 830 \times 1328 \times 86 \times 1228 \mod 1517\\
&= 699 \mod 1517\ .
\end{aligned}$$

לכן הטקסט מוצפן הינו $y = 699$.

ג) $y = 699$.

$$y \mod p = 699 \mod 37 = 33\ , \qquad a \mod (p-1) = 511 \mod 36 = 7\ .$$

לכן

$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p = 33^7 \mod 37 = 7\ .$$

(ניתן לחשב זה לפי $33^7 \times 33^4 \times 33^2 \times 33^1$.)

בנוסף

$$y \mod q = 699 \mod 41 = 2\ , \qquad a \mod (q-1) = 511 \mod 40 = 31\ .$$

לכן

$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q = 2^{31} \mod 41 = 39$$

(ניתן לחשב זה לפי $2 \times 2^2 \times 2^4 \times 2^8 \times 2^{16} \times 2^{31}$.)

לכן עלינו לפתור את המערכת

$$\begin{aligned} x =& x_1 \mod p = 7 \mod 37 \\ x =& x_2 \mod q = 39 \mod 41 \end{aligned}$$

בעזרת המשפט השאריות הסיני. נסמן $a_1 = 7$, $m_1 = 37$, $a_2 = 39$, $m_2 = 41$.

$$M = m_1 m_2 = (37)(41) = 1517 \ , \qquad M_1 = \frac{M}{m_1} = 41 \ , \qquad M_2 = \frac{M}{m_2} = 37 \ .$$

כעת נחשב $y_1 = M_1^{-1} \mod m_1 = 41^{-1} \mod 37 = 28$ ו- $y_2 = M_2^{-1} \mod m_2 = 37^{-1} \mod 41 = 10$.

לכן

$$\begin{aligned} x =& a_1 M_1 y_1 + a_2 M_2 y_2 \mod M \\ =& 7(41)(28) + 39(37)(10) \mod 1517 \\ =& 22466 \mod 1517 \\ =& 1228 \ . \end{aligned}$$

<u>שאלה 4</u> יש 15 תווים בטקסט מוצפן ובטקסט גלוי. לכן הסדר הכי קטן של המטריצה של המפתח הוא 3. נבדוק אם קיים מפתח $k \in \mathbb{Z}_{26}^{3\times 3}$ אשר באמצעותו הטקסט מוצפן מתקבל מהטקסט גלוי.

$x \in P$	t	h	e	f	u	t	u	r	e	i	s	g	o	o	d
$x \in \mathbb{Z}_{26}$	19	7	4	5	20	19	20	17	4	8	18	6	14	14	4
$y \in C$	F	O	P	B	V	F	W	D	F	C	C	G	M	A	T
$y \in \mathbb{Z}_{26}$	5	14	15	1	21	5	22	3	5	2	2	6	12	0	19

אם k מטריצה 2×2 אז הכלל מצפין יהיה

$$e_k(x_1, x_2, x_3) = (x_1 \ x_2 \ x_3)k \mod 26$$

לכן השתי אותיות הראשונות של הטקסט מוצפן $(y_1 \ y_2 \ y_3)$ מתקבלים באמצעות הסעלה של הכלל מצפין על השתי אותיות הראשונות של טקסט גלוי לפי

$$(y_1 \ y_2 \ y_3) = (x_1 \ x_2 \ x_3)k$$

באותה מידה הצמד השני של אותיות של טקסט מוצפן $(y_4 \ y_5 \ y_6)$ מתקבלים על ידי הפעלת הכלל מצפין על הצמד השני של אותיות של טקסט גלוי:

$$(y_3 \ y_4 \ y_5) = (x_3 \ x_4 \ x_5)k$$

באותה מידה הצמד השני של אותיות של טקסט מוצפן $(y_7 \ y_8 \ y_9)$ מתקבלים על ידי הפעלת הכלל מצפין על הצמד השני של אותיות של טקסט גלוי:

$$(y_7 \ y_8 \ y_9) = (x_7 \ x_8 \ x_9)k$$

כעת אפשר לרשום את השתי משוואות האלו כמשוואה מטריציאלית:

$$\begin{pmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} k \ .$$

כדי לבדד את k נכפיל בהמטריצה ההופכית של $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}$ מצד שמאל ונקבל את הביטוי

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}^{-1} \begin{pmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 \end{pmatrix} = k \ .$$

נציב $x_1 = 19, x_2 = 7, x_3 = 4, x_4 = 5, x_5 = 20, x_6 = 19, x_7 = 20, x_8 = 17, x_9 = 4$
ונציב $y_1 = 5, y_2 = 14, y_3 = 15, y_4 = 1, y_5 = 21, y_6 = 5, y_7 = 22, y_8 = 3, y_9 = 5$:

$$k = \begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 5 & 14 & 15 \\ 1 & 21 & 5 \\ 22 & 3 & 5 \end{pmatrix} \ .$$

נחשב את המטריצה ההופכית של $X = \begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix}$ בעזרת נוסחת קריימר:

$$X^{-1} = |X|^{-1} C^t$$

כאשר C המטריצה של קופקטורים. תחילה נמצא את הדטרמיננטה:

$$|X| = -3357 \mod 26 = 23 \ , \qquad |X|^{-1} \mod 26 = 23^{-1} \mod 26 = 17 \ .$$

$$\begin{pmatrix} \cancel{19} & \cancel{7} & \cancel{4} \\ \cancel{5} & 20 & 19 \\ \cancel{20} & 17 & 4 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 20 & 19 \\ 17 & 4 \end{vmatrix} \mod 26 = -243 \mod 26 = 17 \ .$$

$$\begin{pmatrix} \cancel{19} & \cancel{7} & \cancel{4} \\ \cancel{5} & \cancel{20} & 19 \\ \cancel{20} & \cancel{17} & 4 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 5 & 19 \\ 20 & 4 \end{vmatrix} \mod 26 = 360 \mod 26 = 22 \ .$$

$$\begin{pmatrix} \cancel{19} & \cancel{7} & \cancel{4} \\ \cancel{5} & 20 & \cancel{19} \\ \cancel{20} & 17 & \cancel{4} \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 5 & 20 \\ 20 & 17 \end{vmatrix} \mod 26 = -315 \mod 26 = 23 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1} \begin{vmatrix} 7 & 4 \\ 17 & 4 \end{vmatrix} \mod 26 = 40 \mod 26 = 14 .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2} \begin{vmatrix} 19 & 4 \\ 20 & 4 \end{vmatrix} \mod 26 = -4 \mod 26 = 22 .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \Rightarrow C_{23} = (-1)^{2+3} \begin{vmatrix} 19 & 7 \\ 20 & 17 \end{vmatrix} \mod 26 = -183 \mod 26 = 25 .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \Rightarrow C_{31} = (-1)^{3+1} \begin{vmatrix} 7 & 4 \\ 20 & 19 \end{vmatrix} \mod 26 = 53 \mod 26 = 1 .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \Rightarrow C_{32} = (-1)^{3+2} \begin{vmatrix} 19 & 4 \\ 5 & 19 \end{vmatrix} \mod 26 = -341 \mod 26 = 23 .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \Rightarrow C_{33} = (-1)^{3+3} \begin{vmatrix} 19 & 7 \\ 5 & 20 \end{vmatrix} \mod 26 = 345 \mod 26 = 7 .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 17 & 22 & 23 \\ 14 & 22 & 25 \\ 1 & 23 & 7 \end{pmatrix} .$$

$$\text{adj}(X) = C^t = \begin{pmatrix} 17 & 14 & 1 \\ 22 & 22 & 23 \\ 23 & 25 & 7 \end{pmatrix} .$$

$$X^{-1} = |X|^{-1}\text{adj}(X) = 17 \begin{pmatrix} 17 & 14 & 1 \\ 22 & 22 & 23 \\ 23 & 25 & 7 \end{pmatrix} \mod 26 = \begin{pmatrix} 289 & 238 & 17 \\ 374 & 374 & 391 \\ 391 & 425 & 119 \end{pmatrix} \mod 26 = \begin{pmatrix} 3 & 4 & 17 \\ 10 & 10 & 1 \\ 1 & 9 & 15 \end{pmatrix}$$

$$
\begin{aligned}
k =& X^{-1}Y \mod 26 \\
=& \begin{pmatrix} 3 & 4 & 17 \\ 10 & 10 & 1 \\ 1 & 9 & 15 \end{pmatrix} \begin{pmatrix} 5 & 14 & 15 \\ 1 & 21 & 5 \\ 22 & 3 & 5 \end{pmatrix} \mod 26 \\
=& \begin{pmatrix} 393 & 177 & 150 \\ 82 & 353 & 205 \\ 344 & 248 & 135 \end{pmatrix} \mod 26 \\
=& \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix} .
\end{aligned}
$$

שאלה 5

שלב 1) נרשום את התדירויות של האותיות המופיעות בטקסט מוצפן:

A	1	N	3
B	3	O	2
C	0	P	3
D	10	Q	3
E	5	R	1
F	3	S	2
G	1	T	0
H	1	U	0
I	0	V	1
J	0	W	1
K	0	X	4
L	2	Y	2
M	1	Z	1

שלב 2) נרשום את האותיות הנפוצות ביותר:

- D מופיעה 10 פעמים.
- E מופיעה 5 פעמים.

שלב 3) ננסה למצוא את המפתח $k = (a, b)$ ($a, b \in \mathbb{Z}_{26}$) של הכלל מצפין של הצופן אפיני

$$e_k(x) = ax + b \ ,$$

לכל $x \in \mathbb{Z}_{26}$ על ידי **התאמת אותיות הכי נפוצים.**

- נניח כי

$$\texttt{e} \xrightarrow{e_k} \texttt{D}\ , \qquad \texttt{t} \xrightarrow{e_k} \texttt{E}\ .$$

- ז"א

$$\begin{aligned} e_k(4) =& 3 \\ e_k(19) =& 4\ . \end{aligned}$$

- נציב $e_k = ax + b$ ונקבל

$$\begin{aligned} 4a + b &= 3\ , \\ 19a + b &= 4\ . \end{aligned}$$

כעת נפתור את המערת מעל $\mathbb{Z}_{26}$:

$$\left(\begin{array}{cc|c} 4 & 1 & 3 \\ 19 & 1 & 4 \end{array}\right) \xrightarrow{R_2 \to R_2 - R_1} \left(\begin{array}{cc|c} 4 & 1 & 3 \\ 15 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_2 \to 15^{-1} R_2 = 7R_2} \left(\begin{array}{cc|c} 4 & 1 & 3 \\ 1 & 0 & 7 \end{array}\right)$$

$$\xrightarrow{R_1 \to R_1 - 4R_2} \left(\begin{array}{cc|c} 0 & 1 & -25 \\ 1 & 0 & 7 \end{array}\right) = \left(\begin{array}{cc|c} 0 & 1 & 1 \\ 1 & 0 & 7 \end{array}\right)$$

$a = 7, b = 1$.

$\gcd(a, 26) = 1$ אז המפתח $k = (7, 1)$ תקין.

- נבנה את הכלל מפענח עם המפתח המתקבל:

$$\begin{aligned} d_k(y) =& a^{-1}(y - b) \mod 26 \\ =& 7^{-1}(y - 1) \\ =& 15(y - 1) \mod 26 \\ =& 15y - 15 \mod 26 \\ =& 15y + 11\ . \end{aligned}$$

שלב 4) ננסה לפענח את הטקטסט מצפון עם הכלל מפענח

$\mathrm{y} \in C$	E	Y	D	D	G	B	H	F	X	S	D	Q	N	D	B	X	N
$y \in \mathbb{Z}_{26}$	4	24	3	3	6	1	7	5	23	18	3	16	13	3	1	23	13
$x = d_k(y) \in \mathbb{Z}_{26}$	19	7	4	4	23	0	12	8	18	21	4	17	24	4	0	18	24
$\mathrm{x} \in P$	t	h	e	e	x	a	m	i	s	v	e	r	y	e	a	s	y

$y \in C$	E	V	X	L	P	P	D	D	W	M	L	X	E	A	D	B	Q	O
$y \in \mathbb{Z}_{26}$	4	21	23	11	15	15	3	3	22	12	11	23	4	0	3	1	16	14
$x = d_k(y) \in \mathbb{Z}_{26}$	19	14	18	20	2	2	4	4	3	9	20	18	19	11	4	0	17	13
$x \in P$	t	o	s	u	c	c	e	e	d	j	u	s	t	l	e	a	r	n

$y \in C$	D	S	D	Q	N	E	Y	F	O	R	E	Z	F	P	D
$y \in \mathbb{Z}_{26}$	3	18	3	16	13	4	24	5	14	17	4	25	5	15	3
$x = d_k(y) \in \mathbb{Z}_{26}$	4	21	4	17	24	19	7	8	13	6	19	22	8	2	4
$x \in P$	e	v	e	r	y	t	h	i	n	g	t	w	i	c	e

שאלה 6

א) ראו קובץ נפרד.

ב)

$$\begin{aligned}H[X] = &- P_X(\mathtt{a})\log_2 P_X(\mathtt{a}) - P_X(\mathtt{b})\log_2 P_X(\mathtt{b}) - P_X(\mathtt{c})\log_2 P_X(\mathtt{c})\\ &- P_X(\mathtt{d})\log_2 P_X(\mathtt{d}) - P_X(\mathtt{e})\log_2 P_X(\mathtt{e}) - P_X(\mathtt{f})\log_2 P_X(\mathtt{f})\\ &- P_X(\mathtt{x})\log_2 P_X(\mathtt{x}) - P_X(\mathtt{y})\log_2 P_X(\mathtt{y}) - P_X(\mathtt{z})\log_2 P_X(\mathtt{z})\end{aligned}$$

$$=0.382644 + 0.0664386 + 0.505288 + 0.332193 + 0.410545 + 0.480573 + 0.112877 + 0.185754 + 0.268555$$

$$=2.74487\ .$$

ג)

$$\begin{aligned}l[f] =&P_X(\mathtt{a})l(\mathtt{a}) + P_X(\mathtt{b})l(\mathtt{b}) + P_X(\mathtt{c})l(\mathtt{c}) + P_X(\mathtt{d})l(\mathtt{d}) + P_X(\mathtt{e})l(\mathtt{e})\\ &+ P_X(\mathtt{f})l(\mathtt{f}) + P_X(\mathtt{x})l(\mathtt{x}) + P_X(\mathtt{y})l(\mathtt{y}) + P_X(\mathtt{z})l(\mathtt{z})\end{aligned}$$

$$=0.13\cdot(3) + 0.01\cdot(6) + 0.26\cdot(2) + 0.1\cdot(3) + 0.15\cdot(3) + 0.22(2) + 0.02(6) + 0.04(5) + 0.07(4)$$

$$=0.39 + 0.06 + 0.52 + 0.3 + 0.45 + 0.44 + 0.12 + 0.2 + 0.28$$
$$=2.76\ .$$

מתקיים

$$H[X] < l[f] < H[X] + 1\ .$$

שאלה 7

א)

$$
\begin{aligned}
2(16)+1 \mod 3 &= 33 \mod 3 = 0\\
2(16)+2 \mod 3 &= 34 \mod 3 = 1\\
2(16)+3 \mod 3 &= 35 \mod 3 = 2\\
2(16)+4 \mod 3 &= 36 \mod 3 = 0
\end{aligned}
$$

$$
\begin{aligned}
2(17)+1 \mod 3 &= 35 \mod 3 = 2\\
2(17)+2 \mod 3 &= 36 \mod 3 = 0\\
2(17)+3 \mod 3 &= 37 \mod 3 = 1\\
2(17)+4 \mod 3 &= 38 \mod 3 = 2
\end{aligned}
$$

$$
\begin{aligned}
2(18)+1 \mod 3 &= 37 \mod 3 = 1\\
2(18)+2 \mod 3 &= 38 \mod 3 = 2\\
2(18)+3 \mod 3 &= 39 \mod 3 = 0\\
2(18)+4 \mod 3 &= 40 \mod 3 = 1
\end{aligned}
$$

K \ X	q	r	s
k_1	a	c	b
k_2	b	a	c
k_3	c	b	a
k_4	a	c	b

$$
\begin{aligned}
P_Y(\mathtt{a}) =& P_K(k_1)P_X(\mathtt{q}) + P_K(k_2)P_X(\mathtt{r}) + P_K(k_3)P_X(\mathtt{s}) + P_K(k_4)P_X(\mathtt{q})\\
=& \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right)\\
=& \frac{1}{3} \ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\mathtt{b}) =& P_K(k_1)P_X(\mathtt{s}) + P_K(k_2)P_X(\mathtt{q}) + P_K(k_3)P_X(\mathtt{r}) + P_K(k_4)P_X(\mathtt{s})\\
=& \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right)\\
=& \frac{17}{48} \ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\mathtt{c}) =& P_K(k_1)P_X(\mathtt{r}) + P_K(k_2)P_X(\mathtt{s}) + P_K(k_3)P_X(\mathtt{q}) + P_K(k_4)P_X(\mathtt{r})\\
=& \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right)\\
=& \frac{5}{16} \ .
\end{aligned}
$$

ב)

$$P(X=\mathtt{q}|Y=\mathtt{b})=\frac{P(Y=\mathtt{b}|X=\mathtt{q})P(X=\mathtt{q})}{P(Y=\mathtt{b})}=\frac{P_X(\mathtt{q})P_K(k_2)}{P_Y(\mathtt{b})}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{4}\right)}{\left(\frac{17}{48}\right)}=\frac{4}{17}$$

ג)

$$P(X=\mathtt{r}|Y=\mathtt{c})=\frac{P(Y=\mathtt{c}|X=\mathtt{r})P(X=\mathtt{r})}{P(Y=\mathtt{c})}=\frac{P_X(\mathtt{r})\left(P_K(k_1)+P_K(k_4)\right)}{P_Y(\mathtt{c})}=\frac{\left(\frac{1}{4}\right)\left(\frac{1}{4}+\frac{1}{4}\right)}{\left(\frac{5}{16}\right)}=\frac{2}{5}$$

ד) דוגמה נגדית:

$$\frac{4}{17}=P(X=\mathtt{q}|Y=\mathtt{b})\neq P(X=\mathtt{q})=\frac{1}{3}\ .$$

לכן לקריפטו-מערכת אין סודיות מושלמת.

שאלה 8

א)

$$P_Y(A)=P_X(a)P_K(k_2)+P_X(b)P_K(k_1)+P_X(b)P_K(k_3)\quad=\left(\frac{1}{6}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{3}\right)\left(\frac{1}{2}\right)+\left(\frac{1}{3}\right)\left(\frac{1}{4}\right)\quad=\frac{7}{24}\ .$$

$$P_Y(B)=P_X(a)P_K(k_1)+P_X(c)P_K(k_2)+P_X(c)P_K(k_3)\quad=\left(\frac{1}{6}\right)\left(\frac{1}{2}\right)+\left(\frac{1}{2}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{2}\right)\left(\frac{1}{4}\right)\quad=\frac{8}{24}\ .$$

$$P_Y(C)=P_X(a)P_K(k_3)+P_X(b)P_K(k_2)+P_X(c)P_K(k_1)\quad=\left(\frac{1}{6}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{3}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{2}\right)\left(\frac{1}{2}\right)\quad=\frac{9}{24}\ .$$

ב)

$$P(X=a|Y=B)=\frac{P(Y=B|X=a)P(X=a)}{P(Y=B)}=\frac{P_K(k_1)P(X=a)}{P(Y=B)}=\frac{\left(\frac{1}{2}\right)\left(\frac{1}{6}\right)}{\left(\frac{8}{24}\right)}=\frac{1}{4}\ .$$

$$\frac{1}{6}=P(X=a)\neq P(X=a|Y=B)=\frac{1}{4}$$

לכן למערכת זו אין שודיות מושלמת.

שאלה 9

א)

$$P(Y=y)P(X=x|Y=y)=P(X=x\cap Y=y) \quad (*)$$

ו-

$$\log_2 P(X=x|Y=y)=\log_2\left(\frac{P(X=x\cap Y=y)}{P(Y=y)}\right)=\log_2 P(X=x\cap Y=y)-\log_2 P(Y=y)\ . \quad (\#)$$

לכן

$$\begin{aligned}
H[X|Y] =& -\sum_{y\in Y}\sum_{x\in X} P(Y=y)P(X=x|Y=y)\log_2 P(X=x|Y=y)\\
=& -\sum_{y\in Y}\sum_{x\in X} P(X=x\cap Y=y)\left(\log_2 P(X=x\cap Y=y)-\log_2 P(Y=y)\right)\\
=& H[X\cap Y]+\sum_{y\in Y}\sum_{x\in X} P(X=x\cap Y=y)\log_2 P(Y=y)\\
=& H[X\cap Y]+\sum_{y\in Y}\log_2 P(Y=y)\sum_{x\in X} P(X=x\cap Y=y)\\
=& H[X\cap Y]+\sum_{y\in Y}\log_2 P(Y=y)P(Y=y)\\
=& H[X\cap Y]-H[Y]\ .
\end{aligned}$$

ב) המשפט אומר כי $H[X\cap Y]\leq H[X]+H[Y]$ עם שוויון אם ורק אם X ו- Y בלתי תלויים. לכן

$$H[X]+H[Y]\geq H[X\cap Y]=H[Y]+H[X|Y]\ .$$

מכאן מנובע כי $H[X]\geq H[X|Y]$. השוויון מתקיים אם ורק אם X ו- Y בלתי תלויים.

שאלה 10

לפי השאלה הקודמת, $H[P|C]=H[P]$ אם ורק אם P ו- C בלתי תלויים.

P ו- C בלתי תלויים אם ורק אט $P(P=x\cap C=y)=P(P=x)P(C=y)$.

נציב $P(P=x\cap C=y)=P(P=x|C=y)P(C=y)$ בצד ימין ונקבל
$P(P=x|C=y)P(C=y)=P(P=x)P(C=y)$, ז"א $P(P=x|C=y)=P(P=x)$.

זוהי התנאי לסודיות מושלמת.