שאלה 1 **(25 נקודות)**

נתון קבוצת טקסט גלוי $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, קבוצת טקסט מוצפן $Y = \{\mathtt{S}, \mathtt{T}, \mathtt{U}, \mathtt{V}\}$, $K = \{k_1, k_2, k_3\}$. נתונה מטריצת הצפנה

	a	b	c
k_1	S	T	U
k_2	T	U	V
k_3	U	V	S

כל מפתח נבחר בהסתברות שווה. הפונקצית הסתברות של הטקסט גלוי היא

$$P_X(\mathtt{a}) = \frac{1}{2}\ , \qquad P_X(\mathtt{b}) = \frac{1}{3}\ , \qquad P_X(\mathtt{c}) = \frac{1}{6}\ .$$

חשבו את $H(X)$, $H(Y)$, ו- $H(K)$.

שאלה 2 **(25 נקודות)**

א) אליס שולחת לבוב הטקסט מוצפן הבא

IEEHFZYA .

אליס הצפינה את ההודעה באמצעות צופן תמורה עם המפתח $\begin{pmatrix} 5 & 11 \\ 4 & 3 \end{pmatrix}$. מצאו את הטקסט גלוי.

ב) הוכיחו: פונקצית הצפנה ופונקצית פענוח של צופן RSA הן פונקציות הופיכות.

שאלה 3 **(25 נקודות)**

בטבלה למטה רשום הפונקצית הסתברות של אותיות בטקסט גלוי:

$\frac{3}{10}$	$\frac{1}{9}$	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{18}$
ה	ד	ג	ב	א

א) מצאו הצפנת האפמן של כל אחד של האותיות.

ב) מצאו את האנטרופיה של ההצפנה.

ג) נתונה אלפיבית בעל 100 אותיות. יהי $e_a(x) = ax$ לכל $x \in \mathbb{Z}_{100}$. כמה ערכים של a קיימים כך ש- $e(x)$ ניתן לפענח.

שאלה 4 **(25 נקודות)**

יהיו p, q מספרים ראשוניים ויהי $n = pq$. יהי

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} \ .$$

נגדיר צופן חדש אשר זהה ל- RSA אלא $\phi(n)$ הוחלף עם $\lambda(n)$ כך ש- $ab \equiv 1 \mod \lambda(n)$. הוכיחו כי הכלל מצפין והכלל מפענח המתקבלים מהווים צופן שניתן לפענח.

שאלה 5 **(25 נקודות)** אליס שולחת הודעה $x = 222$ לבוב. בוב משתמש בצופן RSA עם המפתח ציבורי $(p = 37, q = 79, b = 7)$.

א) (15 נקודות)
מצאו את המפתח הסודי.

ב) (10 נקודות)
מצאו את הטקסט מוצפן.

פתרונות

שאלה 1 (25 נקודות)

$$
\begin{aligned}
H[X] =& -P_X(\mathtt{a})\log_2 P_X(\mathtt{a}) - P_X(\mathtt{b})\log_2 P_X(\mathtt{b}) - P_X(\mathtt{c})\log_2 P_X(\mathtt{c})\\
=& -\frac{1}{2}\ln_2\left(\frac{1}{2}\right) - \frac{1}{3}\ln_2\left(\frac{1}{3}\right) - \frac{1}{6}\ln_2\left(\frac{1}{6}\right)\\
=& 1.45915\ .
\end{aligned}
$$

לכן $P_K(k_1) = P_K(k_2) = P_K(k_3) = \frac{1}{3}$

$$
H[K] = -3\cdot\frac{1}{3}\ln_2\left(\frac{1}{3}\right) = 1.58496\ .
$$

מדף הנוסחאות

$$
P\left(Y = y\right) = \sum_{k\in K} P(K = k)P(X = d_k(y))\ .
$$

לפיכך

$$
\begin{aligned}
P_Y\left(\mathtt{S}\right) =& \sum_{k\in k_1,k_2,k_2} P\left(K = k_i\right)P\left(X = d_{k_i}(\mathtt{S})\right)\\
=& P\left(K = k_1\right)P\left(X = d_{k_1}(\mathtt{S})\right) + P\left(K = k_2\right)P\left(X = d_{k_2}(\mathtt{S})\right) + P\left(K = k_3\right)P\left(X = d_{k_3}(\mathtt{S})\right)\\
=& P\left(K = k_1\right)P\left(X = \mathtt{a}\right) + P\left(K = k_2\right)P\left(\emptyset\right) + P\left(K = k_3\right)P\left(X = \mathtt{c}\right)\\
=& \frac{1}{3}\cdot\frac{1}{2} + \frac{1}{3}\cdot 0 + \frac{1}{3}\cdot\frac{1}{6}\\
=& \frac{4}{18}\ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y\left(\mathtt{T}\right) =& \sum_{k\in k_1,k_2,k_2} P\left(K = k_i\right)P\left(X = d_{k_i}(\mathtt{T})\right)\\
=& P\left(K = k_1\right)P\left(X = d_{k_1}(\mathtt{T})\right) + P\left(K = k_2\right)P\left(X = d_{k_2}(\mathtt{T})\right) + P\left(K = k_3\right)P\left(X = d_{k_3}(\mathtt{T})\right)\\
=& P\left(K = k_1\right)P\left(X = \mathtt{b}\right) + P\left(K = k_2\right)P\left(\mathtt{a}\right) + P\left(K = k_3\right)P\left(X = \emptyset\right)\\
=& \frac{1}{3}\cdot\frac{1}{3} + \frac{1}{3}\cdot\frac{1}{2} + \frac{1}{3}\cdot 0\\
=& \frac{5}{18}\ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\texttt{U}) =& \sum_{k\in k_1,k_2,k_2} P(K=k_i)\,P(X=d_{k_i}(\texttt{U}))\\
=&P(K=k_1)\,P(X=d_{k_1}(\texttt{U}))+P(K=k_2)\,P(X=d_{k_2}(\texttt{U}))+P(K=k_3)\,P(X=d_{k_3}(\texttt{U}))\\
=&P(K=k_1)\,P(X=\texttt{c})+P(K=k_2)\,P(\texttt{b})+P(K=k_3)\,P(X=\texttt{a})\\
=&\frac{1}{3}\cdot\frac{1}{6}+\frac{1}{3}\cdot\frac{1}{3}+\frac{1}{3}\cdot\frac{1}{2}\\
=&\frac{6}{18}\ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\texttt{V}) =& \sum_{k\in k_1,k_2,k_2} P(K=k_i)\,P(X=d_{k_i}(\texttt{V}))\\
=&P(K=k_1)\,P(X=d_{k_1}(\texttt{V}))+P(K=k_2)\,P(X=d_{k_2}(\texttt{V}))+P(K=k_3)\,P(X=d_{k_3}(\texttt{V}))\\
=&P(K=k_1)\,P(X=\emptyset)+P(K=k_2)\,P(\texttt{c})+P(K=k_3)\,P(X=\texttt{b})\\
=&\frac{1}{3}\cdot 0+\frac{1}{3}\cdot\frac{1}{6}+\frac{1}{3}\cdot\frac{1}{3}\\
=&\frac{3}{18}\ .
\end{aligned}
$$

$$
\begin{aligned}
H[Y] =& -P_Y(\texttt{S})\log_2 P_Y(\texttt{S})-P_Y(\texttt{T})\log_2 P_Y(\texttt{T})-P_Y(\texttt{U})\log_2 P_Y(\texttt{U})-P_Y(\texttt{V})\log_2 P_Y(\texttt{V})\\
=&-\frac{4}{18}\ln_2\left(\frac{4}{18}\right)-\frac{5}{18}\ln_2\left(\frac{5}{18}\right)-\frac{6}{18}\ln_2\left(\frac{6}{18}\right)-\frac{3}{18}\ln_2\left(\frac{3}{18}\right)\\
=&\frac{\log(3)}{3\log(2)}+\frac{\log(6)}{6\log(2)}+\frac{2\log\left(\frac{9}{2}\right)}{9\log(2)}+\frac{5\log\left(\frac{18}{5}\right)}{18\log(2)}\\
=&1.95469\ .
\end{aligned}
$$

<u>שאלה 2</u> (25 נקודות)

א)

$$
k=\begin{pmatrix} 5 & 11\\ 4 & 3\end{pmatrix} \qquad \Rightarrow \qquad |k| \mod 26 = -29 \mod 26 = 23\ .
$$

ההופכית של $|k|$ ב- $\mathbb{Z}_{26}$ היא (דף הנוסחאות):

$$
|k|^{-1} \mod 26 = 23^{-1} \mod 26 = 17
$$

הקופקטורים של k:

$$
C_{11}=3\ ,\qquad C_{12}=-4\ ,\qquad C_{21}=-11\ ,\qquad C_{22}=5\ .
$$

מטריצת הקופקטורים:

$$C = \begin{pmatrix} 3 & -4 \\ -11 & 3 \end{pmatrix} \mod 26 = \begin{pmatrix} 3 & 22 \\ 15 & 5 \end{pmatrix} .$$

המטריצה ההופכית של k:

$$k^{-1} = |k|^{-1} C^t = 17 \cdot \begin{pmatrix} 3 & 15 \\ 22 & 5 \end{pmatrix} \mod 26 = \begin{pmatrix} 51 & 255 \\ 374 & 85 \end{pmatrix} \mod 26 = \begin{pmatrix} 25 & 21 \\ 10 & 7 \end{pmatrix} .$$

$\mathrm{x} \in P$	I	E	E	H	F	Z	Y	A
$x \in \mathbb{Z}_{26}$	8	4	4	7	5	25	24	0

$$(8\ 4)k^{-1} \mod 26 = (8\ 4) \begin{pmatrix} 25 & 21 \\ 10 & 7 \end{pmatrix} = (240\ 196) \mod 26 = (6\ 14) .$$

$$(4\ 7)k^{-1} \mod 26 = (4\ 7) \begin{pmatrix} 25 & 21 \\ 10 & 7 \end{pmatrix} = (170\ 133) \mod 26 = (14\ 3) .$$

$$(5\ 25)k^{-1} \mod 26 = (5\ 25) \begin{pmatrix} 25 & 21 \\ 10 & 7 \end{pmatrix} = (375\ 280) \mod 26 = (11\ 20) .$$

$$(24\ 0)k^{-1} \mod 26 = (24\ 0) \begin{pmatrix} 25 & 21 \\ 10 & 7 \end{pmatrix} = (600\ 504) \mod 26 = (2\ 10) .$$

$\mathrm{x} \in P$	I	E	E	H	F	Z	Y	A
$x \in \mathbb{Z}_{26}$	8	4	4	7	5	25	24	0
$y \in \mathbb{Z}_{26}$	6	14	14	3	11	20	2	10
$\mathrm{y} \in C$	g	o	o	d	l	u	c	k

ב) צופן RSA ניתן לפענח אומר ש-

$$d_k\left(e_k(x)\right) = x \qquad \Leftrightarrow \qquad \text{פענוח}\left(\text{הצפנה}(x)\right) = x .$$

שלב 1) רושמים את כלל המצפין וכלל הפענוח של RSA (דף הנוסחאות). לכל מפתח $k = (p, q, a, b)$ כאשר p, q ראשוניים, a, b שלמים נגדיר

$$\left.\begin{aligned} e_k(x) &= x^b \mod n \\ d_k(y) &= y^a \mod n \end{aligned}\right\} \qquad n = pq , \qquad ab \equiv 1 \mod \phi(n) .$$

שלב 2) צריך להוכיח כי

$$d_k\left(e_k(x)\right) = x \qquad \Leftrightarrow \qquad d_k\left(x^b \mod n\right) = x \qquad \Rightarrow \qquad \left(x^b\right)^a \equiv x \mod n ,$$

ז"א הטענה שאנחנו רוצים להוכיח היא ש- $\left(x^b\right)^a \equiv x \mod n$.

שלב 3) p,q ראשוניים לכן

$$\phi(n) \overset{\text{דף נוסחאות}}{=} (p-1)(q-1) \ .$$

מכאן

$$ab \equiv 1 \mod \phi(n) \quad \Rightarrow \quad ab \equiv 1 \mod (p-1)(q-1)$$

לכן קיים שלם

$$ab-1 = t(p-1)(q-1) \ .$$

שלב 4)

$$x^{ab-1} = x^{t(p-1)(q-1)} = y^{p-1}$$

כאשר $y = x^{t(q-1)}$. לפי משפט פרמה (דף נוסחאות) לכל y שלם ולכל p ראשוני $y^{p-1} \equiv 1 \mod p$.

לפיכך

$$y^{p-1} \equiv 1 \mod p \quad \Rightarrow \quad x^{ab-1} \equiv 1 \mod p \ .$$

שלב 5)

$$x^{ab-1} = x^{t(p-1)(q-1)} = z^{q-1}$$

כאשר $z = x^{t(p-1)}$.

q ראשוני לכן

$$z^{q-1} \equiv 1 \mod q \quad \Rightarrow \quad x^{ab-1} \equiv 1 \mod q \ .$$

שלב 6) מכיוון ש- p,q ראשוניים אז

$$\left.\begin{array}{ll} x^{ab-1} & \equiv 1 \mod q \\ x^{ab-1} & \equiv 1 \mod q \end{array}\right\} \quad \Rightarrow \quad x^{ab-1} \equiv 1 \mod pq$$

לפיכך

$$x^{ab-1} \equiv 1 \mod n \quad \Rightarrow \quad \left(x^b\right)^a \equiv x \mod n$$

כנדרש.

שאלה 3 (25 נקודות)

א)

ב)

שאלה 4 (25 נקודות)

שלב 1) רושמים את הצופן:

$$\left.\begin{array}{ll} e_k(x) & = x^b \mod n \\ d_k(y) & = y^a \mod n \end{array}\right\} \qquad n = pq \ , \qquad ab \equiv 1 \mod \lambda(n) \ .$$

שלב 2) נתון כי $d = \gcd(p-1, q-1)$. ז"א שקיים p' שלם כך ש-

(#1)
$$p - 1 = p'd \quad \Leftrightarrow \quad \frac{p-1}{d} = p' \quad \Leftrightarrow \quad d = \frac{p-1}{p'} \ .$$

באותה מידה קיים q' שלם כך ש-

(#2)
$$q - 1 = q'd \quad \Leftrightarrow \quad \frac{q-1}{d} = q' \quad \Leftrightarrow \quad d = \frac{q-1}{q'} \ .$$

שלב 3)

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} = \frac{(p-1)(q-1)}{d} \ .$$

(1*)
$$\lambda(n) \overset{(\#1)}{=} \frac{(p-1)(q-1)}{\left(\frac{p-1}{p'}\right)} = p'(q-1) \ . \quad \Leftrightarrow \quad d = \frac{p-1}{p'} \ .$$

(2*)
$$\lambda(n) \overset{(\#2)}{=} \frac{(p-1)(q-1)}{\left(\frac{q-1}{q'}\right)} = q'(p-1) \ . \quad \Leftrightarrow \quad d = \frac{p-1}{p'} \ .$$

שלב 4) $ab \equiv 1 \mod \lambda(n)$ (נתון) לכן קיים t שלם כך ש-

$$ab = 1 + t\lambda(n) \overset{(2*)}{=} 1 + t(p-1)q' \ .$$

לכן

$$ab - 1 = t(p-1)q' \ .$$

מכאן

$$x^{ab-1}x^{tq'(p-1)} = y^{p-1} \overset{\text{פרמה}}{\equiv} 1 \mod p$$

כאשר $y = x^{tq'}$ והשוויון השני מתקיים בגלל ש- p מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \mod p \ .$$

שלב 5) $ab \equiv 1 \mod \lambda(n)$ (נתון) לכן קיים t שלם כך ש-

$$ab = 1 + t\lambda(n) \overset{(1*)}{=} 1 + t(q-1)p' \ .$$

לכן

$$ab - 1 = t(q-1)p' \ .$$

מכאן

$$x^{ab-1}x^{tp'(q-1)} = z^{q-1} \overset{\text{פרמה}}{\equiv} 1 \mod q$$

כאשר $z = x^{tp'}$ והשוויון השני מתקיים בגלל ש- q מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \mod q \ .$$

שלב 6) מכיוון ש- p,q ראשוניים אז

$$\left.\begin{array}{lll} x^{ab-1} & \equiv 1 & \mod q \\ x^{ab-1} & \equiv 1 & \mod q \end{array}\right\} \quad \Rightarrow \quad x^{ab-1} \equiv 1 \mod pq$$

לפיכך

$$x^{ab-1} \equiv 1 \mod n \quad \Rightarrow \quad \left(x^b\right)^a \equiv x \mod n$$

כנדרש.

<u>שאלה 5</u> (25 נקודות)

א)

$$n = pq = 37 \times 79 = 2923$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 36 \times 78 = 2028 \ .$$

$a = 7^{-1} \mod 2028$. נשתמש באלגוריתם של אוקליד:

<u>שיטה 1</u>

$a = 2808, b = 7$.

$$\begin{aligned} r_0 = & a = 2808, & r_1 &= b = 7 \ , \\ s_0 = & 1 \ , & s_1 &= 0 \ , \\ t_0 = & 0 \ , & t_1 &= 1 \ . \end{aligned}$$

$q_1 = 401$	$t_2 = 0 - 401 \cdot 1 = -401$	$s_2 = 1 - 401 \cdot 0 = 1$	$r_2 = 2808 - 401 \cdot 7 = 1$	שלב $i = 1$:
$q_2 = 7$	$t_3 = 1 - 7 \cdot (-401) = 2808$	$s_3 = 0 - 7 \cdot 1 = -7$	$r_3 = 7 - 7 \cdot 1 = 0$	שלב $i = 2$:

$$\gcd(a,b) = r_2 = 1 \ , \qquad x = s_2 = 1 \ , \qquad y = t_2 = -401 \ .$$

$$ax + by = 1(2808) - 7(401) = 1 \ .$$

מכאן

$$-401(7) = 1 - 1(2808) \quad \Rightarrow \quad -401(7) = 1 \mod 2808 \quad \Rightarrow \quad 7^{-1} = -401 \mod 2808 = 2407 \ .$$

<u>שיטה 2</u>

$$\begin{aligned} 2808 =& 401(7) + 1 \\ 7 =& 7(1) + 0 \ . \end{aligned}$$

$$1 = 2808 - 401(7) \ .$$

לכן

$$a = b^{-1} \mod \phi(n) =^{-1} \mod 2808 = -401 \mod 2808 = 2407 \ .$$

ב)

$$y = x^b \mod n = 222^7 \mod 2133 \ .$$

$$\begin{aligned} 222 \mod 2923 =& & = 222 \ , \\ 222^2 \mod 2923 =& 49284 \mod 2923 & = 2516 \ . \\ 222^4 \mod 2133 =& 2516^2 \mod 2133 & = 1961 \ . \end{aligned}$$

$$222^7 \mod 2133 = (222^4)(222^2)(222) \mod 2133 = (1961)(2516)(222) = 2220 \ .$$

לכן הטקסט מוצפן $y = 2220$.