תרגילים שונים: קריפטוגרפיה

שאלה 1 מצאו את

א) $7503 \,\%\, 81$

ב) $(-7503) \,\%\, 81$

ג) $81 \,\%\, 7503$

ד) $(-81) \,\%\, 7503$

שאלה 2 נניח כי $a, m > 0$ ו- $a \not\equiv 0 \mod m$. הוכיחו כי

$$(-a) \,\%\, m = m - (a \,\%\, m) \ .$$

שאלה 3 הוכיחו כי $a \,\%\, m = b \,\%\, m$ אם ורק אם $a \equiv b \mod m$.

שאלה 4

א) מצאו את $d = \gcd(12327, 2409)$.
רמז: 587 מספר ראשוני ו- 73 מספר ראשוני.

ב) **(העשרה בלבד)** מצאו מספרים שלמים t ו- s כך ש- $d = 12327s + 2409t$.

שאלה 5 הוכיחו כי 7563 ו- 526 מספרים זרים.

רמז: 2521 מספר ראשוני ו- 263 מספר ראשוני.

שאלה 6 בחוגים הבאים מצאו את איברים יש עבורם קיים איבר הופכי:

א) $\mathbb{Z}_{200}$

ב) $\mathbb{Z}_{400}$

ג) $\mathbb{Z}_{1000}$

ד) $\mathbb{Z}_{263}$

ה) $\mathbb{Z}_{2521}$

שאלה 7 מצאו את ההופכית של

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

שאלה 8 מצאו את ההופכית של

$$A = \begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

שאלה 9 הטקסט מוצפן הבא מוצפן על ידי צופן הזזה (צופן קיסר).

VWDUZDUV

מצאו את המפתח של הצופן ומצאו את הטקסט גלוי (רמז: חיפוש ממצה).

שאלה 10 מצאו את מספר המפתחות של צופן האפיני מעל החוגים הבאים:

א) $\mathbb{Z}_{30}$

ב) $\mathbb{Z}_{100}$

ג) $\mathbb{Z}_{1225}$

שאלה 11

שאלה 12 נתונה התמורה הבאה:

i	1	2	3	4	5	6	7	8
$\pi(i)$	4	1	6	2	7	3	8	5

א) מצאו את התמורה ההופכית.

ב) פענחו את הטקסט מוצפן הבא

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

שאלה 13 נתון המפתח

$$k = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix}$$

של הצופן היל. לכל טקסט מוצפן למטה מתון את הטקסט גלוי

א) VAZMJR

ב) NDIMZZEMV

שאלה 14 נתון הטקטסט מוצפן הבא:

MALVVMAFBHBUQPTSOXALTGVWWRG

אשר היה מוצפן על ידי צופפן אוטו-מפתח עם מפתח התחלתי $k = 19$. מצאו את הטקטס גלוי.

שאלה 15 נתון הטקטסט מוצפן

FOHTXTZVVCDIQCZWWUYIQTNEUEOLHSHEUTZWW

המתקבל באמצעות צופן ויז'נר עם המפתח

$k = \text{DAVE}$.

מצאו את הטקטט גלוי.

שאלה 16 נתון הטקטס גלוי

mynameisbond

והטקסט מוצפן

KAANAEMKWVVC

המתקבל באמצעות צופן היל. מצאו את המפתח של הצופן.

שאלה 17 נתון הטקטסט מוצפן

SKVVOVIFVSPLSVVONSVNSVQSKVPIOVHVEVLSITOPLFBQFVSNVMLPSVQSTVMYETIVVCVIRA

VBSXIVBOQQVSBPESTFVSKVI

נניח כי הטקסט היה מוצפן על ידי צפון אפיני. מצאו את המפתח ואת הטקטס גלוי.

שאלה 18 נניח כי לקבוצה של טקטסט גלוי $X = \{a, b, c, d, e\}$ יש את הפונקצית הסתברות

$$P_X(a) = 0.32 \ , \quad P_X(b) = 0.23 \ , \quad P_X(c) = 0.2 \ , \quad P_X(d) = 0.15 \ , \quad P_X(e) = 0.10 \ .$$

א) בעזרת האלגוריתם של האפמן מצאו את ההצפנה של X.

ב) מצאו את $H(X)$.

ג) מצאו את $l(f)$.

שאלה 19 יהי $X=\{0,1,2\}$ עם פונקצית הסתברות

$$P_X(0)=\frac{1}{3}\ ,\qquad P_X(1)=\frac{1}{4}\ ,\qquad P_X(2)=\frac{5}{12}\ .$$

יהי $K=\{k_1,k_2,k_3,k_4\}$ עם פונקצית הסתברות $P_K(k_i)=\frac{1}{4}$ לכל $i=1,2,3,4$. יהי $Y=\{0,1,2\}$. נגדיר כלל מצפין

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

לכל $x\in\{0,1,2\}$ ולכל $i\in\{1,2,3,4\}$.

א) מצאו את $P_Y(y)$ לכל $y=0,1,2$.

ב) מצאו את $P(X=0|Y=1)$ ו- $P(X=1|Y=2)$.

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

שאלה 20 נתונה קריפטו-מערכת $X=\{\mathtt{a},\mathtt{b},\mathtt{c}\}$, $K=\{k_1,k_2,k_3,k_4\}$, $Y=\{1,2,3,4\}$ עם המטריצה הצפנה הבאה:

	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

לכל מפתח יש הסתברות שווה. הפונקצית הסתברות של X היא

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

א) חשבו $H[X]$.

ב) חשבו $H[K]$.

ג) חשבו $H[Y]$.

ד) חשבו $H[K|Y]$.

ה) חשבו $H[X|Y]$.

שאלה 21 הוכיחו: אם לכל מפתח של צופן אפיני יש הסתברות שווה $P_K(k_i)=\frac{1}{312}$ אז לצופן אפיני יש סודיות מושלמת.

שאלה 22 יהי n מספר שלם. ריבוע לטיני של אורך n הוא מטריצה L מסדר $n \times n$ של n מספרים שלמים $1, 2, \ldots, n$ כך שכל אחד מהמספרים שלמים מופיע בדיוק פעם אחת בכל שורה, מופיע בדיוק פעם אחת בכל עמודה של L. נסמן המספר בשורה ה- i ובשורה ה- j של הריבוע הלטיני L ב- L_{ij}. דוגמה של ריבוע לטיני של סדר 4 היא

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

נתון כל ריבוע לטיני L של סדר n, אפשר להגדיר קריפטו-מערכת. נתון $X = Y = K = \{1, 2, \ldots, n\}$. עבור המפתח i וטקסט גלוי j (כאשר $1 \leq i \leq n$ ו- $1 \leq j \leq n$), הכלל מצפין e_i מוגדר

$$e_i(j) = L_{ij} \ .$$

לכל מפתח יש הסתברות שווה. הוכיחו כי לקריפטו-מערכת זו המוגדרת על ידי הריבוע לטיני הזה יש סודיות מודלמת.

שאלה 23 אם a ו- b רצפים של סיביות:

$$a = 0011010111010101$$
$$b = 1110011100011101$$

א) מצאו את $a \wedge b$.

ב) מצאו את $a \oplus b$.

שאלה 24 נתון צופן פייסטל בעל 3 שלבים. הפונקצית ליבה מוגדרת

$$f\left((x_1, x_2, x_3, x_4, x_5), \pi\right) = x_{\pi(1)}\ x_{\pi(2)}\ x_{\pi(3)}\ x_{\pi(4)}\ x_{\pi(5)}\ .$$

יהי המפתח ההתחלתי התמורה

$$k = \pi\ , \qquad \pi = (1234)$$

ויהי כל תת-מפתח k_i התמורה המתקבלת על ידי ההרכבה i פעמים של התמורה π. חשבו את הטקסט מוצפן המתקבל מהטקסט גלוי

x=00011011 .

שאלה 25 נתון טקסט מוצפן המתקבל שלב ראשון של הצפנת פייסטל

$$L_1 R_1 = 010110\ .$$

התת-מפתח הראשון הוא $k_1 = (123)$ והפונקציה היא $f\left((x_1 x_2 x_3), \pi\right) = x_{\pi(1)} x_{\pi(2)} x_{\pi(3)}$. מצאו את הטקסט גלוי.

שאלה 26 מחזור הראשון של הצפנת פייסטל עם מפתח התחלתי (132) והפונקצית ליבה

$$f((x_1,x_2,x_3),\pi)=x_{\pi(1)}x_{\pi(2)}x_{\pi(3)}$$

נותן $L_1R_1=110010$. מצאו את הטקסט גלוי.

שאלה 27 מצאו את המפתוח פענוח למחזור ראשון של פענוח IDEA בעזרת המפתח ההתחלתי

`00221166993366778899aabbccddffee` .

שאלה 28 בוב הרכיב צופן אל-גמאל עם המפתח $(p=347,\alpha=62,a=20)$.

א) חשבו את β.

ב) אליס קוראת את המפתח ציבורי (p,α,β), והיא בוחרת ב- $d=4$ ומשתמשת במפתח כדי להצפין ההודעה 204. מהו הטקסט מוצפן?

ג) אחר כך אליס שולחת הודעה אחרת לבוב. הטקסט מוצפן הוא $(88,176)$. מהו הטקסט גלוי.

שאלה 29

נתון הטקסט מוצפן

FPHOEMJSUPSZZYJ

אשר מוצפן על ידי צופן היל עם המפתח

$$k=\begin{pmatrix}1&2&3\\4&5&6\\11&9&8\end{pmatrix}.$$

מצאו את הטקסט גלוי.

שאלה 30

נתונה התמורה

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

א) מצאו את $\pi^{-1}(x)$.

ב) פענחו את הטקסט מצפון

SQIUOENTMFHREOFTLIXNAAME

שאלה 31

נתון את הטקסט מוצפן

YGSOYNGSUUTOYZNKHKYZIURRKMKOTOYXGKR

אשר מוצפן על ידי צופן קיסר. מצאו את המפתח ואת הטקסט גלוי.

שאלה 32 נניח כי $K=(5,21)$ הוא מפתח של צופן האפיני מעל החוג $\mathbb{Z}_{29}$.

א) מצאו את האיברים a',b' בכלל מפענח

$$d_K(y)=a'y+b'$$

כאשר $a',b'\in\mathbb{Z}_{29}$.

ב) הוכיחו כי $d_K\left(e_K(x)\right)=x$ לכל $x\in\mathbb{Z}_{29}$.

שאלה 33 הטקסט מוצפן `FLAKIYIMWQ` מתקבל באמצעות צופן ויז'נר עם המפתח $MESSAGE$. מצאו את הטקסט גלוי.

שאלה 34 נניח כי לקבוצה של טקסט גלוי $X=\{\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d},\mathtt{e},\mathtt{f},\mathtt{x},\mathtt{y},\mathtt{z}\}$ יש את הפונקצית הסתברות

$$P_X(\mathtt{a})=0.12\ ,\quad P_X(\mathtt{b})=0.10\ ,\quad P_X(\mathtt{c})=0.06\ ,\quad P_X(\mathtt{d})=0.09\ ,\quad P_X(\mathtt{e})=0.45\ .$$

$$P_X(\mathtt{f})=0.12\ ,\quad P_X(\mathtt{x})=0.02\ ,\quad P_X(\mathtt{y})=0.02\ ,\quad P_X(\mathtt{z})=0.02\ .$$

א) בעזרת האלגוריתם של האפמן מצאו את ההצפנה של X.

ב) מצאו את $H(X)$.

ג) מצאו את $l(f)$.

שאלה 35 יהי $X=\{\mathtt{s},\mathtt{t},\mathtt{u}\}$ קבוצת טקסט גלוי עם פונקצית הסתברות

$$P_X\left(\mathtt{s}\right)=\frac{1}{6}\ ,\qquad P_X\left(\mathtt{t}\right)=\frac{1}{4}\ ,\qquad P_X\left(\mathtt{u}\right)=\frac{7}{12}\ .$$

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

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

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

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

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

א) מצאו את $P_Y(y)$ לכל $y\in Y$.

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

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

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

שאלה 36 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

$$P_X(\mathtt{a}) = \frac{3}{8}, \quad P_X(\mathtt{b}) = \frac{1}{8}, \quad P_X(\mathtt{c}) = \frac{1}{2}, \quad P_K(k_1) = \frac{1}{3}, \quad P_K(k_2) = \frac{1}{3}, \quad P_K(k_3) = \frac{1}{3} .$$

המטריצת הצפנה 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 37 טקסט גלוי של 10 bit היה מוצפן באמצעות צופן פייסטל עם מפתח התחלתי $k = (124)(35)$. כל תת מפתח k_i מתקבל על ידי לבצע התמורה ההתחלתית i פעמים. הטקסט מוצפן הוא 1010111100. מצאו את הטקסט גלוי.

שאלה 38 נתון המפתח ההתחלתי 202078785353abcd התת-מפתח הראשון של DES הוא

1100 1001 0001 1110 0000 0011 1011 1111 0010 1000 1001 1101 .

נתון הטקסט גלוי 364e6ead76fabc59, מצאו את הרצף המתקבל לאחר מחזור הראשון של DES.

שאלה 39 חשבו את המפתחות פענוח של IDEA בעזרת המפתח ההתחלתי

997766553322ff11aa00bb44ccdd88ee .

שאלה 40 הוכיו שאם p מספר ראשוני ו- n מספר שלם חיובי אז

$$\phi(pn) = \begin{cases} (p-1)\phi(n) \ , & \text{אם } p \nmid n \\ p\phi(n) \ , & \text{אם } p \mid n \end{cases} .$$

שאלה 41 בוב הרכיב סכימת RSA עם הפרמטרים $p = 191$, $q = 127$ ו- $b = 47$.

א) חשבו את n, $\phi(n)$ ו- a.

ב) אליס מוצאת את המפתח ציבורי (b, n) ומשתמשת בה להצפין את המסר 2468. מהי הטקסט מוצפן שהיא שולחת לבוב?

ג) אליס שולחת הודעה שנייה לבוב. הטקסט מוצפן שהיא שולחת הוא 9625. בעזרת המשפט השארית הציני פענחו את ההודעה.

פתרונות

שאלה 1

א) לכל $a>0$ השארית בחלוקה ב- m נתונה ע"י $a \,\%\, m = a - \left\lfloor \frac{a}{m} \right\rfloor m$.

$$7503 \,\%\, 81 = 7503 - \left\lfloor \frac{7503}{81} \right\rfloor \cdot 81 = 7503 - 92 \cdot 81 = 7503 - 7452 = 51 \ .$$

ב) לכל $a>0$ השארית של $-a$ בחלוקה ב- m נתונה ע"י $(-a) \,\%\, m = m - (a \,\%\, m)$

$$(-7503) \,\%\, 81 = 81 - 51 = 30 \ .$$

ג) $a \,\%\, m = a - \left\lfloor \frac{a}{m} \right\rfloor m$.

$$a \,\%\, m = 81 - \left\lfloor \frac{81}{7503} \right\rfloor \cdot 7503 = 81 - 0 \cdot 81 = 81 \ .$$

ד) $(-a) \,\%\, m = m - a \,\%\, m$.

$$(-81) \,\%\, 7503 = 7503 - (81 \,\%\, 7503) = 7503 - 81 = 7422 \ .$$

שאלה 2

א) $a \not\equiv 0 \mod m$ ז"א $m \nmid a$ לכן

$$a = qm + r \ , \qquad 1 \leq r \leq m-1 \ ,$$

כאשר $r = a \,\%\, m$. לכן

$$-a = -q, -r = -(q+1)m + m - r \ .$$

$1 \leq r \leq m-1 \Leftarrow 1 \leq m-r \leq m-1$. לפיכך

$$-a \,\%\, m = m - r = m - (a \,\%\, m) \ .$$

שאלה 3 נניח כי $a \,\%\, m = b \,\%\, m$.

נסמן $r = a \,\%\, m = b \,\%\, m$. אז

$$a = mq_1 + r \ , \qquad b = mq_2 + r$$

כאשר q_1, q_2 מספרים שלמים. ז"א

$$a - b = mq_1 - mq_2 = m(q_1 - q_2) \ .$$

$q_1 - q_2$ מספר שלם לכן $m \mid a - b$ לכן $a \equiv b \mod m$ כנדרש.

כעת נניח כי $a \equiv b \mod m$.
ז"א $m \mid a-b$ ⇐ קיים q שלם כך ש-

$$a-b=mq$$

נסמן $r=a \% m$. קיים מספר שלם q_1 כך ש-

$$a=q_1 m+r\ .$$

מכאן

$$b=a-qm=q_1m+r-qm=(q_1-q)m+r\ .$$

ז"א $b \% m=r$.
כנדרש.

שאלה 4

א) נמצא את הפירוק לראשונים של 12327.

- 12327 אי זוגי לכן הוא לא מתחלק ב-2.
- נבדוק אם השלם 12327 מתחלק ב- 3.

$$\frac{12327}{3}=4109 \quad \Rightarrow \quad 12327=3\cdot 4109\ .$$

4109 לא מתחלק ב- 3.

- נבדוק אם השלם 4109 מתחלק ב- 5:

$$\frac{4109}{5}\neq \text{שלם}\ .$$

- נבדוק אם השלם 4109 מתחלק ב- 7:

$$\frac{4109}{7}=587 \quad \Rightarrow \quad 4109=7\cdot 587\ .$$

587 מספר ראשוני לכן התהליך מסתיים.

$$12327=3^1 7^1 587^1\ .$$

נמצא את הפירוק לראשונים של 2409.

- 2409 אי זוגי לכן הוא לא מתחלק ב-2.
- נבדוק אם השלם 2409 מתחלק ב- 3.

$$\frac{2409}{3}=803 \quad \Rightarrow \quad 2409=3\cdot 803.$$

803 לא מתחלק ב- 3.

- נבדוק אם השלם 803 מתחלק ב- 5:

$$\frac{803}{5}\neq \text{שלם}\ .$$

- נבדוק אם השלם 803 מתחלק ב- 7:

$$\frac{803}{7} \neq \text{שלם} .$$

- נבדוק אם השלם 803 מתחלק ב- 11:

$$\frac{803}{1}1 = 73 \quad \Rightarrow \quad 803 = 11 \cdot 73 .$$

73 מספר ראשוני לכן התהליך מסתיים.

$$2409 = 3^1 11^1 73^1 = 3^1 7^0 11^1 73^1 587^0 .$$

נמצא את ה gcd:

$$12327 = 3^1 7^1 587^1 = 3^1 7^1 11^0 73^0 587^1 , \qquad 2409 = 3^1 11^1 73^1 = 3^1 7^0 11^1 73^1 587^0$$

$$\gcd(12327, 2409) = 3^{\min(1,1)} 7^{\min(1,0)} 11^{\min(0,1)} 73^{\min(0,1)} 587^{\min(1,0)} = 3^1 5^0 7^0 11^0 73^0 587^0 = 3 .$$

ב) (העשרה בלבד)

נתונים השלמים a, m. אם $d = \gcd(a, m)$ אז לפי משפט בזו קיימים שלמים x, y כך ש-

$$d = ax + my .$$

האלגוריתם הבא נותן את ה המקדמים x, y.

$$r_0 = a , \quad r_1 = m , \quad s_0 = 1 , \quad t_0 = 0 , \quad s_1 = 0 , \quad t_1 = 1 , \quad q_0 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{a}{m} \right\rfloor .$$

$$r_{i+1} = r_{i-1} - q_i r_i , \quad s_{i+1} = s_{i-1} - q_1 s_i , \quad t_{i+1} = t_{i-1} - q_1 t_i , \quad q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor .$$

האלגוריתם מסתיים כאשר $r_k = 0$. המקדמים נתונים על ידי $x = s_{k-1}$, $y = t_{k-1}$.
נצאו את המקדמי בזו של $a = 12327$, $m = 2409$.

0	$q(-1)$	12327	1	0
1	5	2409	0	1
2	5	282	1	−5
3	8	153	−8	41
4	1	129	9	−46
5	1	24	−17	87
6	5	9	94	−481
7	2	6	−205	1049
8	1	3	299	−1530
9	2	0	−803	4109

$x = s_8 = 299$,$y = t_8 = -1530$. לכן

$$ax + my = 299(12327) - 1530(2409) = 3 .$$

ז"א $\gcd(12327, 2409) = 3$.

שאלה 5

נמצא את הפירוק לראשונים של 7563.

- 7563 אי זוגי לכן הוא לא מתחלק ב-2.
- נבדוק אם השלם 7563 מתחלק ב- 3.

$$\frac{7563}{3} = 2521 \quad \Rightarrow \quad 7563 = 3 \cdot 2521 \ .$$

2521 לכן התהליך מסתיים.

$$7563 = 3^1 2521^1 \ .$$

נמצא את הפירוק לראשונים של 526.
$526 = 2 \cdot 263$. המספר 263 מספר ראשוני לכן הפירוק לראשוניים שלו הוא

$$526 = 2^1 t 263^1 \ .$$

נמצא את ה gcd:

$$7563 = 3^1 2521^1 = 2^0 3^1 263^0 2521^1 \ , \qquad 526 = 2^1 263^1 = 2^1 3^0 263^1 2521^0 \ .$$

$$\gcd(7563, 526) = 2^{\min(1,0)} 3^{\min(1,0)} 263^{\min(1,0)} 2521^{\min(0,1)} = 3^0 263^0 2521^0 = 1 \ .$$

לכן 7563 ו- 526 מספרים זרים.

שאלה 6 לכל a בחוג $\mathbb{Z}_m$ קיים איבר הופכי a^{-1} אם ורק אם $\gcd(a,m) = 1$. נניח כי הפירוק לראשוניים של a הוא $\prod_{i=1}^{n} p_i^{e_i}$. אז מספר האיברים עבורם $\gcd(a,m) = 1$ ניתן ע"י הנסוחה

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i - 1} \right) \ .$$

א) $\mathbb{Z}_{200}$

$$200 = 2^3 5^2$$

לכן

$$\phi(200) = \left(2^3 - 2^2\right)\left(5^2 - 5^1\right) = 80 \ .$$

ב) $\mathbb{Z}_{400}$

$$400 = 2^4 5^2$$

לכן

$$\phi(400) = \left(2^4 - 2^3\right)\left(5^2 - 5^1\right) = 160 \ .$$

ג) $\mathbb{Z}_{1000}$

$$1000 = 2^3 5^3$$

לכן

$$\phi(1000) = \left(2^3 - 2^2\right)\left(5^3 - 5^2\right) = 400 \ .$$

ד) $\mathbb{Z}_{263}$.

שימו לב 263 מספר ראשוני לכן הפירוק לראשוניים שלו הוא $263 = 263^1$ ו-

$$\phi(263) = 263^1 - 263^0 = 263 - 1 = 262 \ .$$

(בכללי, אם p מספר ראשוני אז $\phi(p) = p - 1$.

ה) $\mathbb{Z}_{2521}$.

$\mathbb{Z}_{2521}$. שימו לב 2521 מספר ראשוני לכן הפירוק לראשוניים שלו הוא $2521 = 2521^1$ ו-

$$\phi(2521) = 2521^1 - 2521^0 = 2521 - 1 = 2520.$$

(בכללי, אם p מספר ראשוני אז $\phi(p) = p - 1$.

שאלה 7

$$|A| = 1 \cdot \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} + 1 \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = 1 \cdot 15 + 1 \cdot (-10) = 5 \ .$$

$\gcd(15, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{11} = (-1)^{1+1} \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} = 15 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = -10 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 1 \\ 0 & 3 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 1 \ .$$

$$\begin{pmatrix}1&0&1\\0&5&0\\2&0&3\end{pmatrix} \qquad \Rightarrow \qquad C_{23}=(-1)^{2+3}\begin{vmatrix}1&0\\2&0\end{vmatrix}=0\ .$$

$$\begin{pmatrix}1&0&1\\0&5&0\\2&0&3\end{pmatrix} \qquad \Rightarrow \qquad C_{31}=(-1)^{3+1}\begin{vmatrix}0&1\\5&0\end{vmatrix}=-5\ .$$

$$\begin{pmatrix}1&0&1\\0&5&0\\2&0&3\end{pmatrix} \qquad \Rightarrow \qquad C_{32}=(-1)^{3+2}\begin{vmatrix}1&1\\0&0\end{vmatrix}=0\ .$$

$$\begin{pmatrix}1&0&1\\0&5&0\\2&0&3\end{pmatrix} \qquad \Rightarrow \qquad C_{33}=(-1)^{3+3}\begin{vmatrix}1&0\\0&5\end{vmatrix}=5\ .$$

$$C=\begin{pmatrix}C_{11}&C_{12}&C_{13}\\C_{21}&C_{22}&C_{23}\\C_{31}&C_{32}&C_{33}\end{pmatrix}=\begin{pmatrix}15&0&-10\\0&1&0\\-5&0&5\end{pmatrix}$$

$$\text{adj}(A)=C^t=\begin{pmatrix}15&0&-5\\0&1&0\\-10&0&5\end{pmatrix}=\begin{pmatrix}15&0&21\\0&1&0\\16&0&5\end{pmatrix}\in\mathbb{Z}_{26}^{3\times3}\ .$$

$$A^{-1}=|A|^{-1}\text{adj}(A)\ .$$

$$|A|^{-1}=5^{-1}=21\in\mathbb{Z}_{26}$$

לפיכך

$$A^{-1}=|A|^{-1}\text{adj}(A)=21\cdot\begin{pmatrix}15&0&21\\0&1&0\\16&0&5\end{pmatrix}=\begin{pmatrix}315&0&441\\0&21&0\\336&0&105\end{pmatrix}\in\mathbb{Z}_{26}^{3\times3}\ .$$

$$315\ \%\ 26=315-26\cdot\left\lfloor\frac{315}{26}\right\rfloor=-23\equiv 3\mod 26\quad\Rightarrow\quad 315\equiv 3\mod 26\ .$$

$$441\ \%\ 26=441-26\cdot\left\lfloor\frac{441}{26}\right\rfloor=25\quad\Rightarrow\quad 441\equiv 25\mod 26\ .$$

$$336\ \%\ 26=336-26\cdot\left\lfloor\frac{336}{26}\right\rfloor=24\quad\Rightarrow\quad 336\equiv 24\mod 26\ .$$

$$105\ \%\ 26=105-26\cdot\left\lfloor\frac{105}{26}\right\rfloor=1\quad\Rightarrow\quad 105\equiv 1\mod 26\ .$$

לפיכך

$$A^{-1}=\begin{pmatrix}3&0&25\\0&21&0\\24&0&1\end{pmatrix}\in\mathbb{Z}_{26}^{3\times3}\ .$$

בדיקה:

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 27 & 0 & 26 \\ 0 & 105 & 0 \\ 78 & 0 & 53 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod 26 \ .$$

<u>שאלה 8</u> נחשב את הדטרמיננטה לפי השורה האחרונה:

$$|A| = 0 \cdot \begin{vmatrix} 0 & 3 \\ 1 & 5 \end{vmatrix} - 0 \begin{vmatrix} 1 & 3 \\ 3 & 5 \end{vmatrix} + 7 \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 7 \cdot 1 = 7 \ .$$

$\gcd(7, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 1 & 5 \\ 0 & 7 \end{vmatrix} = 7 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 3 & 5 \\ 0 & 7 \end{vmatrix} = -21 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 3 & 1 \\ 0 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 3 \\ 0 & 7 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 0 & 7 \end{vmatrix} = 7 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 0 & 3 \\ 1 & 5 \end{vmatrix} = -3 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 3 \\ 3 & 5 \end{vmatrix} = 4 \ .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 1 \ .$$

$$C=\begin{pmatrix}C_{11}&C_{12}&C_{13}\\C_{21}&C_{22}&C_{23}\\C_{31}&C_{32}&C_{33}\end{pmatrix}=\begin{pmatrix}7&-21&0\\0&7&0\\-3&4&1\end{pmatrix}$$

$$\text{adj}(A)=C^t=\begin{pmatrix}7&0&-3\\-21&7&4\\0&0&1\end{pmatrix}=\begin{pmatrix}7&0&23\\5&7&4\\0&0&1\end{pmatrix}\in\mathbb{Z}_{26}^{3\times3}\ .$$

$$A^{-1}=|A|^{-1}\text{adj}(A)\ .$$

$$|A|^{-1}=7^{-1}=15\in\mathbb{Z}_{26}$$

לפיכך

$$A^{-1}=|A|^{-1}\text{adj}(A)=15\cdot\begin{pmatrix}7&0&23\\5&7&4\\0&0&1\end{pmatrix}=\begin{pmatrix}105&0&345\\75&105&60\\0&0&15\end{pmatrix}\ .$$

$$105\ \%\ 26=105-26\cdot\left\lfloor\frac{105}{26}\right\rfloor=1\ .$$

$$345\ \%\ 26=345-26\cdot\left\lfloor\frac{345}{26}\right\rfloor=7\ .$$

$$75\ \%\ 26=75-26\cdot\left\lfloor\frac{75}{26}\right\rfloor=23\ .$$

$$60\ \%\ 26=60-26\cdot\left\lfloor\frac{60}{26}\right\rfloor=8\ .$$

לפיכך

$$A^{-1}=\begin{pmatrix}1&0&7\\23&1&8\\0&0&15\end{pmatrix}\in\mathbb{Z}_{26}^{3\times3}\ .$$

בדיקה:

$$A\cdot A^{-1}=\begin{pmatrix}1&0&3\\3&1&5\\0&0&7\end{pmatrix}\begin{pmatrix}1&0&7\\23&1&8\\0&0&15\end{pmatrix}=\begin{pmatrix}1&0&52\\26&1&104\\0&0&105\end{pmatrix}\equiv\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\mod 26\ .$$

שאלה 9

$\mathtt{y} \in C$	V	W	D	U	Z	D	U	V
$y \in C$	21	22	3	20	25	3	20	21
$x = y - 0 \in P$	21	22	3	20	25	3	20	21
$\mathtt{x} \in P$	v	w	d	u	z	d	u	v
$x = y - 1 \in P$	20	21	2	19	24	2	19	20
$\mathtt{x} \in P$	u	v	c	t	y	c	t	u
$x = y - 2 \in P$	19	20	1	18	23	1	18	19
$\mathtt{x} \in P$	t	u	b	s	x	b	s	t
$x = y - 3 \in P$	18	19	0	17	22	0	17	18
$\mathtt{x} \in P$	s	t	a	r	w	a	r	s

המפתח הוא 3 והטקסט גלוי הוא

starwars

שאלה 10 הצופן האפיני מעל $\mathbb{Z}_m$ מכיל כלל מצפין

$$e_k(x) = ax + b \mod m$$

וכלל המפענח

$$d_k(y) = a^{-1}(y - b) \mod m \ .$$

הכלל מצפין $e_k(x)$ הפיך, כלומר קיים כלל מפענח $d_k(y) = a^{-1}(y-b) \mod m$ אם קיים איבר הופכי $a^{-1} \in \mathbb{Z}_m$.
קיים איבר הופכי a^{-1} רק אם $\gcd(a, m) = 1$.
אם הפירוק למספרים ראשוניים של m הוא $m = \prod_{i=1}^{n} p_i^{e_i}$ אז מספר האברים ב- $\mathbb{Z}_m$ עבורם $\gcd(a, m) = 1$ נתון על ידי הפונקציית אוילר

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i - 1}\right) \ .$$

לכן, יש $\phi(m)$ אפשריות ל- a ו- m אפשריות ל- b. בסך הכל קיימים $m\ \phi(m)$ מפתחות של צופן אפיני מעל $\mathbb{Z}_m$.

א) $30 = 2^1 \times 3^1 \times 5^1$ לכן

$$\phi(30) = \left(2^1 - 2^0\right)\left(3^1 - 3^0\right)\left(5^1 - 5^0\right) = (1)(2)(4) = 8 \ .$$

לכן לצופן האפיני מעל $\mathbb{Z}_{30}$ יש $30 \times 8 = 240$ מפתחות.

ב) $100 = 2^2 \times 5^2$ לכן

$$\phi(100) = \left(2^2 - 2^1\right)\left(5^2 - 5^1\right) = (2)(20) = 40 \ .$$

לכן לצופן האפיני מעל $\mathbb{Z}_{100}$ יש $100 \times 40 = 4000$ מפתחות.

ג) $1225 = 5 \times 245 = 5^2 \times 49 = 5^2 \times 7^2$ לכן

$$\phi(1225) = \left(5^2 - 5^1\right)\left(7^2 - 7^1\right) = (20)(42) = 840 \ .$$

לכן לצופן האפיני מעל $\mathbb{Z}_{1225}$ יש $1225 \times 840 = 1,029,000$ מפתחות.

שאלה 11

שאלה 12

$\mathrm{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14

$\mathrm{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12

נפרק את האותיות לתת-קבוצות מאורך $m=8$ (לפי האורך של התמורה).
נפעיל את התמורה ההופכית:

$\mathrm{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14

$\mathrm{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12

i	1	2	3	4	5	6	7	8
$\pi^{-1}(i)$	2	4	6	1	8	3	5	7

$\mathrm{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14
$x=\pi^{-1}(y)$	6	4	13	19	11	4	12	4	13	3	14	13	14	19	17	4

$\mathrm{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12
$x=\pi^{-1}(y)$	0	3	4	0	2	7	14	19	7	4	17	18	12	0	8	11

$\mathrm{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14
$x=\pi^{-1}(y)$	6	4	13	19	11	4	12	4	13	3	14	13	14	19	17	4
$\mathrm{x} \in P$	g	e	n	t	l	e	m	e	n	d	o	n	o	t	r	e

$\mathrm{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12
$x=\pi^{-1}(y)$	0	3	4	0	2	7	14	19	7	4	17	18	12	0	8	11
$\mathrm{x} \in P$	a	d	e	a	c	h	o	t	h	e	r	s	m	a	i	l

```
gentlemandonotreadeachothersmail
```

שאלה 13

$$|k| = 1 \cdot \begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} - 3 \begin{vmatrix} 0 & 1 \\ 3 & 1 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 3 & 0 \end{vmatrix} = 9 \ .$$

$\gcd(9,26)=1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 1 \\ 3 & 1 \end{vmatrix} = 3 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 0 \\ 3 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 3 & 0 \\ 0 & 1 \end{vmatrix} = -3 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 1 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 3 \\ 3 & 0 \end{vmatrix} = 9 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 3 & 0 \\ 0 & 1 \end{vmatrix} = 3 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = -1 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 3 \\ 0 & 0 \end{vmatrix} = 0 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 0 & 3 & 0 \\ -3 & 1 & 9 \\ 3 & -1 & 0 \end{pmatrix}$$

$$\mathrm{adj}(A)=C^t=\begin{pmatrix}0&-3&3\\3&1&-1\\0&9&0\end{pmatrix}\mod 26=\begin{pmatrix}0&23&3\\3&1&25\\0&9&0\end{pmatrix}\in\mathbb{Z}_{26}^{3\times 3}\ .$$

$$A^{-1}=|A|^{-1}\mathrm{adj}(A)\ .$$

$$|A|^{-1}=9^{-1}=3\in\mathbb{Z}_{26}$$

לפיכך

$$\begin{aligned}A^{-1}=&|A|^{-1}\mathrm{adj}(A)\\=&3\cdot\begin{pmatrix}0&23&3\\3&1&25\\0&9&0\end{pmatrix}\mod 26\\=&\begin{pmatrix}0&69&9\\9&3&75\\0&27&0\end{pmatrix}\mod 26\\=&\begin{pmatrix}0&17&9\\9&3&23\\0&1&0\end{pmatrix}\end{aligned}$$

א) <u>שלב 1:</u>

נעביר את האותיות של הטקסט גלוי לערכים של $\mathbb{Z}_{26}$:

$\mathrm{y}\in C$	V	A	Z	M	J	R
$y\in\mathbb{Z}_{26}$	21	0	25	12	9	17

<u>שלב 2:</u>

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m=3$ תווים:

$\mathrm{y}\in C$	V	A	Z	M	J	R
$y\in\mathbb{Z}_{26}$	21	0	25	12	9	17

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned}\begin{pmatrix}x_1&x_2&x_3\end{pmatrix}&=\begin{pmatrix}y_1&y_2&y_3\end{pmatrix}k^{-1}\mod 26\\&=\begin{pmatrix}y_1&y_2&y_3\end{pmatrix}\begin{pmatrix}0&17&9\\9&3&23\\0&1&0\end{pmatrix}\mod 26\end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned}\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 21 & 0 & 25 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 0 & 382 & 189 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 0 & 18 & 7 \end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned}\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 12 & 9 & 17 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 81 & 248 & 315 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 3 & 14 & 3 \end{pmatrix}\end{aligned}$$

$\mathrm{y} \in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17
$x \in \mathbb{Z}_{26}$	0	18	7	3	14	3

שלב 5:

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט מוצפן:

$\mathrm{y} \in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17
$x \in \mathbb{Z}_{26}$	0	18	7	3	14	3
$\mathrm{x} \in \mathbb{Z}_{26}$	a	s	h	d	o	d

הטקסט גלוי המתקבל הוא

ashdod

ב) שלב 1:

נעביר את האותיות של הטקסט גלוי לערכים של $\mathbb{Z}_{26}$:

$\mathrm{y} \in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21

שלב 2:

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 3$ תווים:

$\mathrm{y} \in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned}\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix} k^{-1} \mod 26 \\ &= \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26\end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned}\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 13 & 3 & 8 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 27 & 238 & 186 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 1 & 4 & 4 \end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned}\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 12 & 25 & 25 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 225 & 304 & 683 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 17 & 18 & 7 \end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השלישית נקבל

$$\begin{aligned}\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 4 & 12 & 21 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 108 & 125 & 312 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 4 & 21 & 0 \end{pmatrix}\end{aligned}$$

y $\in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21
$x \in \mathbb{Z}_{26}$	1	4	4	17	18	7	4	21	0

<u>שלב 5:</u>

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט מוצפן:

y $\in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21
$x \in \mathbb{Z}_{26}$	1	4	4	17	18	7	4	21	0
x $\in P$	b	e	e	r	s	h	e	v	a

הטקסט גלוי המתקבל הוא

beersheva

שאלה 14

there is no time like the present

שאלה 15

computersciencestudentsarethesmartest

שאלה 16 יש 12 תווים בטקסט מוצפן ובטקסט גלוי, כלומר מספר זוגי של אותיות. לכן הסדר הכי קטן של המטריצה של המפתח הוא 2. נבדוק אם קיים מפתח $k \in \mathbb{Z}_{26}^{2\times 2}$ אשר באמצעותו הטקסט מוצפן מתקבל מהטקסט גלוי.

x $\in P$	m	y	n	a	m	e	i	s	b	o	n	d
$x \in \mathbb{Z}_{26}$	12	24	13	0	12	4	8	18	1	14	13	3
y $\in C$	K	A	A	N	A	E	M	K	W	V	V	C
$y \in \mathbb{Z}_{26}$	10	0	0	13	0	4	12	10	22	21	21	2

אם k מטריצה 2×2 אז הכלל מצפין יהיה

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

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

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

באותה מידה הצמד השני של אותיות של טקסט מוצפן $(y_3 \ y_4)$ מתקבלים על ידי הפעלת הכלל מצפין על הצמד השני של אותיות של טקסט גלוי:

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

כעת אפשר לרשום את השתי משוואות האלו כמשוואה מטריציאלית:

$$\begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} k \ .$$

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

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}^{-1} \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} = k \ .$$

נציב $x_1 = 12, x_2 = 24, x_3 = 13, x_4 = 0$ ונציב $y_1 = 10, y_2 = 0, y_3 = 0, y_4 = 13$:

$$k = \begin{pmatrix} 12 & 24 \\ 13 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 10 & 0 \\ 0 & 13 \end{pmatrix} \ .$$

נחשב את המטריצה ההופכית של $X = \begin{pmatrix} 12 & 24 \\ 13 & 0 \end{pmatrix}$ בעזרת נוסחת קריימר:

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

כאשר C המטריצה של קופקטורים. תחילה נמצא את הדטרמיננטה:

$$|X| = 12 \cdot 0 - 24 \cdot 13 = -312 \mod 26$$

$.k = \begin{pmatrix} 2 & 3 \\ 7 & 5 \end{pmatrix}$

שאלה 17

The energetic teens tested their new electronic gadgets, excited to explore every feature and detail together.

מפתח $.a = 5, b = 1$

שאלה 18

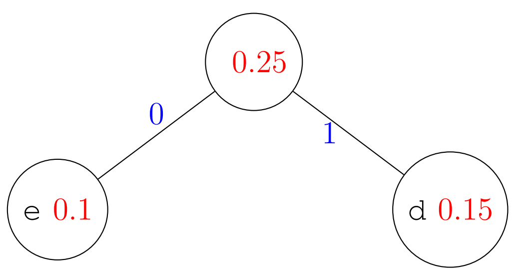
א)

שלב 1)

e	d	c	b	a
0.1	0.15	0.20	0.23	0.32

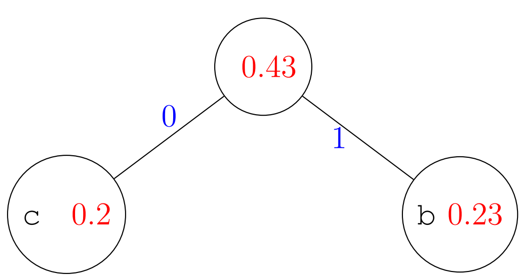
שלב 2)

e	d	c	b	a
0.1	0.15	0.20	0.23	0.32
0	1			
0.25		0.20	0.23	0.32



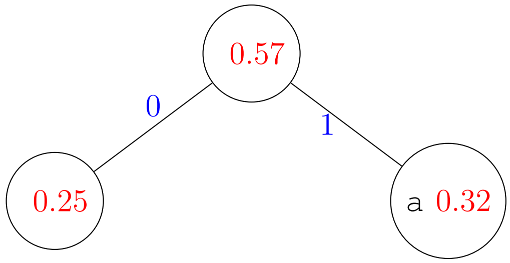
שלב 3)

c	b	0.25	a
0.20	0.23	0.25	0.32
0	1		



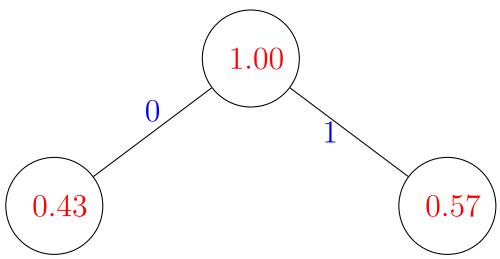
שלב 4)

0.25	a	0.43
0.25	0.32	0.43
0	1	

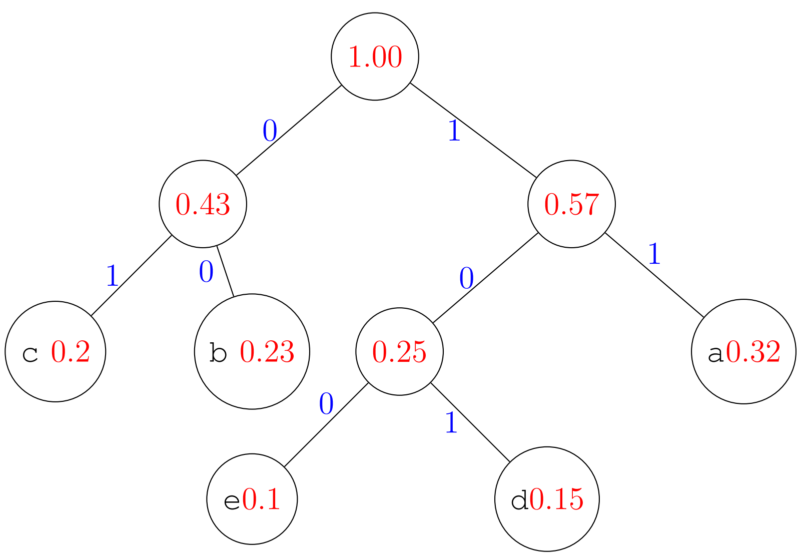


שלב 5)

0.43	0.57
0.43	0.57
0	1



שלב 6)



שלב 7)

a	11
b	00
c	01
d	101
e	100

ב)

$$\begin{aligned} H[X] =& - P_X(\mathtt{a}) \log_2 P_X(\mathtt{a}) - P_X(\mathtt{b}) \log_2 P_X(\mathtt{b}) - P_X(\mathtt{c}) \log_2 P_X(\mathtt{c}) \\ & - P_X(\mathtt{d}) \log_2 P_X(\mathtt{d}) - P_X(\mathtt{e}) \log_2 P_X(\mathtt{e}) \\ =& 0.526034 + 0.487668 + 0.464386 + 0.410545 + 0.332193 \\ =& 2.22082 \ . \end{aligned}$$

ג)

$$\begin{aligned} l[f] =& P_X(\mathtt{a})l(\mathtt{a}) + P_X(\mathtt{b})l(\mathtt{b}) + P_X(\mathtt{c})l(\mathtt{c}) + P_X(\mathtt{d})l(\mathtt{d}) + P_X(\mathtt{e})l(\mathtt{e}) \\ =& 0.32 \cdot (2) + 0.23 \cdot (2) + 0.2 \cdot (2) + 0.15 \cdot (3) + 0.1 \cdot (3) \\ =& 0.64 + 0.46 + 0.4 + 0.45 + 0.3 \\ =& 2.25 \ . \end{aligned}$$

מתקיים

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

שאלה 19

א)

$K \backslash X$	0	1	2
k_1	1	0	2
k_2	2	1	0
k_3	0	2	1
k_4	1	0	2

$$\begin{aligned}P_Y(0) =&P_K(k_1)P_X(1)+P_K(k_2)P_X(2)+P_K(k_3)P_X(0)+P_K(k_4)P_X(1)\\ =&\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{4}\right)\left(\frac{5}{12}\right)+\left(\frac{1}{4}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)\\ =&\frac{5}{16}\ .\end{aligned}$$

$$\begin{aligned}P_Y(1) =&P_K(k_1)P_X(0)+P_K(k_2)P_X(1)+P_K(k_3)P_X(2)+P_K(k_4)P_X(0)\\ =&\left(\frac{1}{4}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{4}\right)\left(\frac{5}{12}\right)+\left(\frac{1}{4}\right)\left(\frac{1}{3}\right)\\ =&\frac{1}{3}\ .\end{aligned}$$

$$\begin{aligned}P_Y(2) =&P_K(k_1)P_X(2)+P_K(k_2)P_X(0)+P_K(k_3)P_X(1)+P_K(k_4)P_X(2)\\ =&\left(\frac{1}{4}\right)\left(\frac{5}{12}\right)+\left(\frac{1}{4}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)+\left(\frac{1}{4}\right)\left(\frac{5}{12}\right)\\ =&\frac{17}{48}\ .\end{aligned}$$

ב)

$$P(X=0|Y=1)=\frac{P(Y=1|X=0)P(X=0)}{P(Y=1)}=\frac{P_X(0)\left(P_K(k_1)+P_K(k_4)\right)}{P_Y(1)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{4}+\frac{1}{4}\right)}{\left(\frac{1}{3}\right)}=\frac{1}{2}$$

$$P(X=1|Y=2)=\frac{P(Y=2|X=1)P(X=1)}{P(Y=2)}=\frac{P_X(1)P_K(k_3)}{P_Y(2)}=\frac{\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)}{\left(\frac{17}{48}\right)}=\frac{3}{17}$$

ג) דוגמה נגדית:

$$\frac{1}{2}=P(X=0|Y=1)\neq P(X=0)=\frac{1}{3}\ .$$

לכן לקריפטו-מערכת אין סודיות מושלמת

שאלה 20

א)

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

ב)

$$\begin{aligned}H[K]=&-P_K(k_1)\log_2 P_K(k_1)-P_K(k_2)\log_2 P_K(k_2)-P_K(k_3)\log_2 P_K(k_3)\\ =&-\frac{1}{3}\log_2\frac{1}{3}-\frac{1}{3}\log_2\frac{1}{3}-\frac{1}{3}\log_2\frac{1}{3}\\ =&\log_2 3=1.58496\,\text{bit}\ .\end{aligned}$$

ג)

$$P_Y(1)=P_K(k_1)P_X(\mathtt{a})+P_K(k_3)P_X(\mathtt{c})=\frac{1}{3}\cdot\frac{1}{2}+\frac{1}{3}\cdot\frac{1}{6}=\frac{4}{18}\ ,$$

$$P_Y(2)=P_K(k_1)P_X(\mathtt{b})+P_K(k_2)P_X(\mathtt{a})=\frac{1}{3}\cdot\frac{1}{3}+\frac{1}{3}\cdot\frac{1}{2}=\frac{5}{18}\ ,$$

$$P_Y(3)=P_K(k_1)P_X(\mathtt{c})+P_K(k_2)P_X(\mathtt{b})+P_K(k_2)P_X(\mathtt{a})=\frac{1}{3}\cdot\frac{1}{6}+\frac{1}{3}\cdot\frac{1}{3}+\frac{1}{3}\cdot\frac{1}{2}=\frac{6}{18}\ ,$$

$$P_Y(4)=P_K(k_2)P_X(\mathtt{c})+P_K(k_2)P_X(\mathtt{b})=\frac{1}{3}\cdot\frac{1}{6}+\frac{1}{3}\cdot\frac{1}{3}=\frac{3}{18}\ .$$

$$\begin{aligned}H[Y]=&-P_Y(1)\log_2 P_Y(1)-P_Y(2)\log_2 P_X(2)-P_Y(3)\log_2 P_Y(3)-P_Y(4)\log_2 P_Y(4)\\&-\frac{4}{18}\log_2\frac{4}{18}-\frac{5}{18}\log_2\frac{5}{18}-\frac{6}{18}\log_2\frac{6}{18}-\frac{3}{18}\log_2\frac{3}{18}\\=&1.95469\,\text{bit}\ .\end{aligned}$$

ד) לפי משפט אנטרופיה לקריפטו-מערכת:

$$H[K|Y]=H[K]+H[X]-H[Y]=1.089\ .$$

ה) בכדי לחשב את $H[X|Y]$, ראשית מחשבים את ההסתברות מותנית $P(X=x|Y=y)$ לכל $y\in$, $x\in X$:Y

$$P(X=\mathtt{a}|Y=1)=\frac{P(Y=1|X=\mathtt{a})P(X=\mathtt{a})}{P(Y=1)}=\frac{P(K=k_1)P(X=\mathtt{a})}{P(Y=1)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{2}\right)}{\left(\frac{4}{18}\right)}=\frac{3}{4}$$

$$P(X=\mathtt{b}|Y=1)=\frac{P(Y=1|X=\mathtt{b})P(X=\mathtt{b})}{P(Y=1)}=\frac{P(K=\emptyset)P(X=\mathtt{b})}{P(Y=1)}=0\ .$$

$$P(X=\mathtt{c}|Y=1)=\frac{P(Y=1|X=\mathtt{c})P(X=\mathtt{c})}{P(Y=1)}=\frac{P(K=k_3)P(X=\mathtt{c})}{P(Y=1)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{6}\right)}{\left(\frac{4}{18}\right)}=\frac{1}{4}$$

$$P(X=\mathtt{a}|Y=2)=\frac{P(Y=2|X=\mathtt{a})P(X=\mathtt{a})}{P(Y=2)}=\frac{P(K=k_2)P(X=\mathtt{a})}{P(Y=2)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{2}\right)}{\left(\frac{5}{18}\right)}=\frac{3}{5}$$

$$P(X=\mathtt{b}|Y=2)=\frac{P(Y=2|X=\mathtt{b})P(X=\mathtt{b})}{P(Y=2)}=\frac{P(K=k_1)P(X=\mathtt{b})}{P(Y=2)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{3}\right)}{\left(\frac{5}{18}\right)}=\frac{2}{5}\ .$$

$$P(X=\texttt{c}|Y=2)=\frac{P(Y=2|X=\texttt{c})P(X=\texttt{c})}{P(Y=\ \ 2)}=\frac{P(K=\emptyset)P(X=\texttt{c})}{P(Y=2)}=0\ .$$

$$P(X=\texttt{a}|Y=3)=\frac{P(Y=3|X=\texttt{a})P(X=\texttt{a})}{P(Y=3)}=\frac{P(K=k_3)P(X=\texttt{a})}{P(Y=3)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{2}\right)}{\left(\frac{6}{18}\right)}=\frac{1}{2}$$

$$P(X=\texttt{b}|Y=3)=\frac{P(Y=3|X=\texttt{b})P(X=\texttt{b})}{P(Y=3)}=\frac{P(K=k_2)P(X=\texttt{b})}{P(Y=3)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{3}\right)}{\left(\frac{6}{18}\right)}=\frac{1}{3}\ .$$

$$P(X=\texttt{c}|Y=3)=\frac{P(Y=3|X=\texttt{c})P(X=\texttt{c})}{P(Y=3)}=\frac{P(K=k_1)P(X=\texttt{c})}{P(Y=3)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{6}\right)}{\left(\frac{6}{18}\right)}=\frac{1}{6}$$

$$P(X=\texttt{a}|Y=4)=\frac{P(Y=4|X=\texttt{a})P(X=\texttt{a})}{P(Y=4)}=\frac{P(K=\emptyset)P(X=\texttt{a})}{P(Y=4)}=0$$

$$P(X=\texttt{b}|Y=4)=\frac{P(Y=4|X=\texttt{b})P(X=\texttt{b})}{P(Y=4)}=\frac{P(K=k_3)P(X=\texttt{b})}{P(Y=4)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{3}\right)}{\left(\frac{3}{18}\right)}=\frac{2}{3}\ .$$

$$P(X=\texttt{c}|Y=4)=\frac{P(Y=4|X=\texttt{c})P(X=\texttt{c})}{P(Y=4)}=\frac{P(K=k_2)P(X=\texttt{c})}{P(Y=4)}=\frac{\left(\frac{1}{3}\right)\left(\frac{1}{6}\right)}{\left(\frac{3}{18}\right)}=\frac{1}{3}$$

	a	b	c
1	$\frac{3}{4}$	0	$\frac{1}{4}$
2	$\frac{3}{5}$	$\frac{2}{5}$	0
3	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{6}$
4	0	$\frac{2}{3}$	$\frac{1}{3}$

$$\begin{aligned}H[X|Y=1] =& -P(X=\texttt{a}|Y=1)\log_2 P(X=\texttt{a}|Y=1)+P(X=\texttt{b}|Y=1)\log_2 P(X=\texttt{b}|Y=1)\\ &+P(X=\texttt{c}|Y=1)\log_2 P(X=\texttt{c}|Y=1)\\ =&0.811278\end{aligned}$$

$$\begin{aligned}H[X|Y=2] =& -P(X=\texttt{a}|Y=2)\log_2 P(X=\texttt{a}|Y=2)+P(X=\texttt{b}|Y=2)\log_2 P(X=\texttt{b}|Y=2)\\ &+P(X=\texttt{c}|Y=2)\log_2 P(X=\texttt{c}|Y=2)\\ =&0.970951\end{aligned}$$

$$\begin{aligned}H[X|Y=3] =& -P(X=\texttt{a}|Y=3)\log_2 P(X=\texttt{a}|Y=3)+P(X=\texttt{b}|Y=3)\log_2 P(X=\texttt{b}|Y=3)\\ &+P(X=\texttt{c}|Y=3)\log_2 P(X=\texttt{c}|Y=3)\\ =&1.45915\end{aligned}$$

$$\begin{aligned}H[X|Y=4] =& -P(X=\texttt{a}|Y=4)\log_2 P(X=\texttt{a}|Y=4)+P(X=\texttt{b}|Y=4)\log_2 P(X=\texttt{b}|Y=4)\\ &+P(X=\texttt{c}|Y=4)\log_2 P(X=\texttt{c}|Y=4)\\ =&0.918296\ .\end{aligned}$$

$$H[X|Y]=\left(\frac{4}{18},\frac{5}{18},\frac{6}{18},\frac{3}{18}\right)\cdot(0.811278,0.970951,1.45915,0.918296)=1.08942\ .$$

שאלה 21

לכל $x,y\in\mathbb{Z}_{26}$ הכלל מצפין של צופן אפיני והכלל מפענח הם

$$e_k(x)=ax+b\ ,\qquad d_k(y)=a^{-1}(y-b)\ .$$

כאשר $b\in\mathbb{Z}_{26}$ ו- $a\in\mathbb{Z}_{26}^*$ (כאשר $\mathbb{Z}_{26}^*$ מסמן את הקבוצת איברים $a\in\mathbb{Z}_{26}$ עבורם $\gcd(a,26)=1$).
קיימים 12 איברים עבורם $\gcd(a,26)=1$ לכן בסה"כ קיימים $12\times 26=312$ מפתחות $k=(a,b)$.

נניח כי ל-312 מפתחות של צופן אפיני יש הסתברות שווה $P_K(k)=\dfrac{1}{312}$ לכל $k\in K$.
$26=|X|\neq|K|=312$ לכן אי אפשר להשתמש במשפט שאנון.

תחילה נראה שלכל צמד אותיות של טקסט-גלוי וטקסט מוצפן (x,y) יש בדיוק 12 מפתחות אפשריים שבאמצעותם ניתן להצפין x ל- y. הרי לכל $a\in\mathbb{Z}_{26}^*$,

$$b=y-ad_k(y)=y-ax\ .$$

ז"א לכל $x\in X$, $y\in Y$ ולכל $a\in\mathbb{Z}_{26}^*$ הערך של b נקבע על ידי האילוץ למעלה.
במילים אחרות לכל בחירה של a המפתח $(a,b)=(a,y-ax)$ מצפין את התו טקסט גלוי x ל-
$e_k(x)\overset{k=(a,y-ax)}{=}ax+y-ax=y$.
מכיוון שיש 12 אפשרויות ל- a אז יש 12 מפתחות אשר מצפינים תו טקסט גלוי x לתו טקסט מוצפן y.

לפי הנוסחה מהדף נוסחאות,

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

לכל תו של טקסט גלוי קיימים 12 מפתחות שבאמצעותם ניתן להצפין x ל- y. לדוגמה, עבור $X = \mathrm{a}$, $y \in Y$, קיימים $k_1, \ldots, k_{12} \in K$ עבורם

$$\mathrm{a} = d_{k_1}(y) \ , \quad \mathrm{a} = d_{k_2}(y) \ , \qquad \cdots \qquad , \ \mathrm{a} = d_{k_{12}}(y) \ .$$

החלק של הסכום בצד ימין עבור $X = \mathrm{a}$ הוא

$$\begin{aligned} & P(K = k_1)P(X = \mathrm{a}) + P(K = k_2)P(X = \mathrm{a}) + \ldots + P(K = k_{12})P(X = \mathrm{a}) \\ =& \frac{1}{312}P(X = \mathrm{a}) \qquad + \frac{1}{312}P(X = \mathrm{a}) \qquad + \ldots + \frac{1}{312}P(X = \mathrm{a}) \\ =& \frac{12}{312}P(X = \mathrm{a}) \ . \end{aligned}$$

לפיכך הסכום מעל כל ה- 312 מפתחות נותן

$$P(Y = y) = \frac{12}{312}P_X(\mathrm{a}) + \frac{12}{312}P_X(\mathrm{b}) + \ldots + \frac{12}{312}P_X(\mathrm{z}) = \frac{12}{312}\sum_{x=\mathrm{a}\cdots\mathrm{z}} P_X(x) = \frac{12}{312} \cdot 1 = \frac{1}{26} \ .$$

מצד שני,

$$P(Y = y|X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) = \frac{12}{312} = \frac{1}{26}$$

בגלל שכל מפתח מתקבל בהסתברות $\frac{1}{312}$ ויש 12 מפתחות k עבורם $x = d_k(y)$, ז"א יש 12 מפתחות שמצפינים x ל- y. לכן

$$P(X = x|Y = y) = \frac{P(Y = y|X = x)P(X = x)}{P(Y = y)} = \frac{\left(\frac{1}{26}\right)P(X = x)}{\left(\frac{1}{26}\right)} = P(X = x)$$

לכן לצופן אפיני יש סודיות מושלמת.

<u>שאלה 22</u> הכלל מצפין מוגדר

$$e_i(j) = L_{ij} = y$$

לכל $j \in [1, n]$, כלומר לכל עמודה ה- j של הריבוע לטיני, i מופיע בדיוק פעם אחת בשורה ה- i.

$\Leftarrow$ לכל $x = j$ ולכל $y = L_{ij}$ קיים מפתח i יחיד עבורו $y = e_i(x)$.

לפי משפט שאנון (משפט 6.2 בדפים) לצופן יש סודיות מושלמת אם"ם

1) לכל $x \in X$ ולכל $y \in U$ קיים מפתח יחיד k עבורו $y = e_k(x)$,

2) ולכל מפתח יש הסתברות שווה.

תנאי (1) הוכחנו ותנאי (2) נתון בשאלה, לכן לצופן יש סודיות מושלמת.

שאלה 23

$$a = 0011010111010101$$

$$b = 1110011100011101$$

$$a \wedge b = 0010010100010101$$

$$a \oplus b = 1101001011101000$$

שאלה 24 $L_0 = 0001$ ו- $R_0 = 1011$. התת מפתחות הם

$$k_1 = (1234)\ , \qquad k_2 = (31)(42)\ , \qquad k_3 = (4321)\ .$$

מכאן

$$L_1 = R_0 = 1011\ .$$
$$R_1 = L_0 \oplus f(R_0, k_1) = 0001 \oplus 0111 = 0110\ .$$

$$L_2 = R_1 = 0110\ .$$
$$R_2 = L_1 \oplus f(R_1, k_2) = 1011 \oplus 1001 = 0010\ .$$

$$L_3 = R_2 = 0010\ .$$
$$R_3 = L_2 \oplus f(R_2, k_3) = 0110 \oplus 0001 = 0111\ .$$
$$y = R_3 L_3 = 01110010$$

שאלה 25

$$L_1 = 010\ , \qquad R_1 = 110\ .$$

ממשוואות פייסטל נקבל

$$R_0 = L_1 = 010\ ,$$
$$L_0 = R_1 \oplus f(R_0, k_1) = 110 \oplus 100 = 010$$

לכן הטקסט גלוי הוא 010010.

שאלה 26 $L_1 = 110$, $R_1 = 101$. לפי משוואות פייסטל לפענוח ($R_{i-1} = L_i$ ו- $L_{i-1} = R_i \oplus f(R_{i-1}, k_i$) נקבל $R_0 = L_1 = 110$ ו-

$$L_0 = R_1 \oplus f(R_0, k_1)$$

$$f(R_0, k_1) = \pi(R_0) = \pi(101) = 110$$

לכן

$$L_0 = R_1 \oplus f(R_0, k_1) = 101 \oplus 110 = 011\ .$$

לפיכך הטקסט גלוי היה

$$L_0 R_0 = 011110\ .$$

שאלה 27 המפתחות לפענוח:

$$DK_1^{(1)} = \left(K_1^{(9)}\right)^{-1} \ , \quad DK_2^{(1)} = -\left(K_2^{(9)}\right)^{-1} \ , \quad DK_3^{(1)} = -\left(K_3^{(9)}\right)^{-1} \ , \quad DK_4^{(1)} = \left(K_4^{(9)}\right)^{-1} \ ,$$

$$DK_5^{(1)} = K_5^{(8)} \ , \quad DK_6^{(1)} = K_6^{(8)} \ ,$$

ממירים את המפתי ההתחלתי לסיביות:

hex	0	0	2	2	1	1	6	6
binary	0000	0000	0010	0010	0001	0001	0110	0110
hex	9	9	3	3	6	6	7	7
binary	1001	1001	0011	0011	0110	0110	0111	0111
hex	8	8	9	9	a	a	b	b
binary	1000	1000	1001	1001	1010	1010	1011	1011
hex	c	c	d	d	f	f	e	e
binary	1100	1100	1101	1101	1111	1111	1110	1110

$$\begin{array}{lll}
\text{Bits } 22-37 & K_1^{(9)} = 0010110011010011 & = 11475 \\
\text{Bits } 38-53 & K_2^{(9)} = 0010011001101100 & = 9836 \\
\text{Bits } 54-69 & K_3^{(9)} = 1100111011110001 & = 52977 \\
\text{Bits } 70-85 & K_4^{(9)} = 0001001100110101 & = 4917 \\
\text{Bits } 93-108 & K_5^{(8)} = 1011110011001101 & = 48333 \\
\text{Bits } 109-124 & K_6^{(8)} = 1101111111111110 & = 57342
\end{array}$$

$$DK_1^{(1)} = \left(K_1^{(9)}\right)^{-1} = (11475)^{-1} \quad \text{mod } 65537 = 22571$$
$$=0101100000101011$$

$$DK_2^{(1)} = -\left(K_2^{(9)}\right) = -9836 \quad \text{mod } 65536 = 55700$$
$$=1101100110010100$$

$$DK_3^{(1)} = \left(K_3^{(9)}\right) = -52977 \quad \text{mod } 65536 = 12559$$
$$=0011000100001111$$

$$DK_4^{(1)} = \left(K_4^{(9)}\right)^{-1} = (4917)^{-1} \quad \text{mod } 65537 = 18047$$
$$=0100011001111111$$

$$DK_5^{(1)} = K_5^{(8)} = 1011110011001101$$

$$DK_6^{(1)} = K_6^{(8)} = 1101111111111110$$

שאלה 28

א)

$$\beta = \alpha^a \mod p = 62^{20} \mod 347 \ .$$

מכיוון ש- $20 = 16 + 4$ ניתן להשתמש בשיטית הריבועים:

$$\begin{aligned}
62^4 &\mod 347 = 35 \ . \\
62^8 &\mod 347 = 35^2 \mod 347 = 1225 \mod 347 = 184 \ . \\
62^{16} &\mod 347 = 184^2 \mod 347 = 33856 \mod 347 = 197 \ .
\end{aligned}$$

לכן

$$62^{20} \mod 347 = (35)(197) \mod 347 = 6895 \mod 347 = 302.$$

ז"א $\beta = 302$.

ב) הטקסט מוצפן הוא (y_1, y_2) כאשר

$$y_1 = \alpha^d \mod p = 62^4 \mod 347 = 35 \mod 347 \ .$$

$$y_2 = \beta^d x \mod p = (302^4)(205) \mod 347 = 26 \mod 347 \ .$$

לכן הטקסט מוצפן הוא $(y_1, y_2) = (35, 26)$.

ג) $(y_1, y_2) = (88, 176)$.

$$M = (y_1^a)^{-1} \cdot y_2 \mod p = (88^{20})^{-1} \mod 34788^{347-1-20} \mod 347 = 88^{326} \mod 347 \ .$$

<u>שלב 1: שיטת הריבועים</u>

$$88^{20} \mod 347 = 88^{16} 88^4 \mod 347$$

$$\begin{aligned}
88 &\mod 347 = 88 \ . \\
88^2 &\mod 347 = 110 \ . \\
88^4 &\mod 347 = 110^2 \mod 347 = 12100 \mod 347 = 302 \ . \\
88^8 &\mod 347 = 302^2 \mod 347 = 91204 \mod 347 = 290. \\
88^{16} &\mod 347 = 290^2 \mod 347 = 84100 \mod 347 = 126.
\end{aligned}$$

$$88^{20} \mod 347 = 88^{16} 88^4 \mod 347 = (302)(126) \mod 347 = 229$$

<u>שלב 2: שיטת אלגוריתם של אוקליד:</u>

$a = 347, b = 229$.

$$\begin{aligned}
r_0 &= a = 347 \ , & r_1 &= b = 229 \ , \\
s_0 &= 1 \ , & s_1 &= 0 \ , \\
t_0 &= 0 \ , & t_1 &= 1 \ .
\end{aligned}$$

שלב $i=1$:	$r_2 = 347 - 1 \cdot 229 = 118$	$s_2 = 1 - 1 \cdot 0 = 1$	$t_2 = 0 - 1 \cdot 1 = -1$	$q_1 = 1$
שלב $i=2$:	$r_3 = 229 - 1 \cdot 118 = 111$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-1) = 2$	$q_2 = 1$
שלב $i=3$:	$r_4 = 118 - 1 \cdot 111 = 7$	$s_4 = 1 - 1 \cdot (-1) = 2$	$t_4 = -1 - 1 \cdot (2) = -3$	$q_3 = 1$
שלב $i=4$:	$r_5 = 111 - 15 \cdot 7 = 6$	$s_5 = -1 - 15 \cdot (2) = -31$	$t_5 = 2 - 15 \cdot (-3) = 47$	$q_4 = 15$
שלב $i=5$:	$r_6 = 7 - 1 \cdot 6 = 1$	$s_6 = 2 - 1 \cdot (-31) = 33$	$t_6 = -3 - 1 \cdot (47) = -50$	$q_5 = 1$
שלב $i=6$:	$r_7 = 6 - 6 \cdot 1 = 0$	$s_7 = -31 - 6 \cdot 33 = -229$	$t_7 = 47 - 6 \cdot (-50) = 347$	$q_6 = 6$

$$\gcd(a,b) = r_6 = 1 \ , \qquad x = s_6 = 33 \ , \qquad y = t_6 = -50 \ .$$

$$ax + by = 347(33) - 229(50) = 1 \ .$$

מכאן

$$-50(229) = 1 - 33(347) \quad \Rightarrow \quad -50(229) = 1 \mod 347 \quad \Rightarrow \quad 297(229) = 1 \mod 347 \quad \Rightarrow \quad 229^{-1} = 297 \quad \text{m}$$

לכן

$$M = \left(88^{20}\right)^{-1} \cdot 176 \mod 347 = (297)(176) \mod 347 = 222 \mod 347 \ .$$

שאלה 29

$y \in C$	F	P	H	O	E	M	J	S	U	P	S	Z	Z	Y	J
$y \in \mathbb{Z}_{26}$	5	15	7	14	4	12	9	18	20	15	18	25	25	24	9

דטרמיננטה של k היא $|k| = -3 \mod 26 = 23$.
$\gcd(23,26)=1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \qquad \Rightarrow \qquad C_{11} = (-1)^{1+1} \begin{vmatrix} 5 & 6 \\ 9 & 8 \end{vmatrix} \mod 26 = -14 \mod 26 = 12 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \qquad \Rightarrow \qquad C_{12} = (-1)^{1+2} \begin{vmatrix} 4 & 6 \\ 11 & 8 \end{vmatrix} \mod 26 = 24 \mod 26 = 8 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \qquad \Rightarrow \qquad C_{13} = (-1)^{1+3} \begin{vmatrix} 4 & 5 \\ 11 & 9 \end{vmatrix} \mod 26 = -19 \mod 26 = 7 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \qquad \Rightarrow \qquad C_{21} = (-1)^{2+1} \begin{vmatrix} 2 & 3 \\ 9 & 8 \end{vmatrix} = 11 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 11 & 8 \end{vmatrix} \mod 26 = -25 \mod 26 = 1 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 11 & 9 \end{vmatrix} = 13 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} \mod 26 = -3 \mod 26 = 23 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} = 6 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} \mod 26 = -3 \mod 26 = 23 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} -14 & 34 & -19 \\ 11 & -25 & 13 \\ -3 & 6 & -3 \end{pmatrix} \mod 26 = \begin{pmatrix} 12 & 8 & 7 \\ 11 & 1 & 13 \\ 23 & 6 & 23 \end{pmatrix} \ .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$k^{-1} = |k|^{-1}\text{adj}(k) \ .$$

$$|k|^{-1} = 23^{-1} = 17 \in \mathbb{Z}_{26}$$

$$k^{-1} = 17 \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} = \begin{pmatrix} 204 & 187 & 391 \\ 136 & 17 & 102 \\ 119 & 221 & 391 \end{pmatrix} = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}$$

$$(5,15,7)\cdot k^{-1} = (19,7,8) \ , \qquad (14,4,12)\cdot k^{-1} = (18,8,18) \ , \qquad (9,18,20)\cdot k^{-1} = (8,13,19) \ ,$$

$$(15,18,25)\cdot k^{-1} = (7,4,4) \ , \qquad (25,24,9)\cdot k^{-1} = (23,0,12) \ .$$

y $\in C$	F	P	H	O	E	M	J	S	U	P	S	Z	Z	Y	J
$y \in \mathbb{Z}_{26}$	5	15	7	14	4	12	9	18	20	15	18	25	25	24	9
$x \in \mathbb{Z}_{26}$	19	7	8	18	8	18	8	13	19	7	4	4	23	0	12
x $\in P$	t	h	i	s	i	s	i	n	t	h	e	e	x	a	m

שאלה 30

א)

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

y $\in C$	S	Q	I	U	O	E	N	T	M	F	H	R	E	O	F	T
$y \in \mathbb{Z}_{26}$	18	16	8	20	14	4	13	19	12	5	7	17	4	14	5	19

y $\in C$	L	I	X	N	A	A	M	E
$y \in \mathbb{Z}_{26}$	11	8	23	13	0	0	12	4

y $\in C$	S	Q	I	U	O	E	N	T	M	F	H	R	E	O	F	T
$y \in \mathbb{Z}_{26}$	18	16	8	20	14	4	13	19	12	5	7	17	4	14	5	19
$x \in \mathbb{Z}_{26}$	16	20	4	18	19	8	14	13	5	17	14	12	19	7	4	5
x $\in P$	q	u	e	s	t	i	o	n	f	r	o	m	t	h	e	f

y $\in C$	L	I	X	N	A	A	M	E
$y \in \mathbb{Z}_{26}$	11	8	23	13	0	0	12	4
$x \in \mathbb{Z}_{26}$	8	13	0	11	4	23	0	12
x $\in P$	i	n	a	l	e	x	a	m

שאלה 31

y $\in C$	Y	G	S	O	Y	N	G	S	U	U	T	O	Y	Z	N	K	H	K	Y	Z
$y \in \mathbb{Z}_{26}$	24	6	18	14	24	13	6	18	20	20	19	14	24	25	13	10	7	10	24	25
$d_6(y)$	18	0	12	8	18	7	0	12	14	14	13	8	18	19	7	4	1	4	18	19
x $\in P$	s	a	m	i	s	h	a	m	o	o	n	i	s	t	h	e	b	e	s	t

y $\in C$	I	U	R	R	K	M	K	O	T	O	Y	X	G	K	R
$y \in \mathbb{Z}_{26}$	8	20	17	17	10	12	10	14	19	14	24	23	6	10	17
$d_6(y)$	2	14	11	11	4	6	4	8	13	8	18	17	0	4	11
x $\in P$	c	o	l	l	e	g	e	i	n	i	s	r	a	e	l

שאלה 32

א) נתון המפתח $a=5, b=21$ בכלל מצפין $e_k(x)=ax+b$. אז הכלל מפענח הינו

$$d_k(y)=a^{-1}(y-b)=5^{-1}(y-21)\ .$$

ב- $\mathbb{Z}_{29}$, $5^{-1}=6$ מכיוון ש- $5\cdot 6 \mod 29 = 30 \mod 29 = 1$. לפיכך

$$d_k(y)=6(y-21)=6y-126 \mod 29 = 6y-4\cdot 29-10 \mod 29 = 6y-10 \mod 29 = 6y+19\ .$$

לפיכך $a'=6, b'=19$.

ב)

$$d_k\left(e_k(x)\right) = 6\left(5x+21\right)+19 \mod 29 = 30x+126+19 \mod 29 = 1\cdot x+145 \mod 29 = x+5\cdot 29 \mod 29 = x\ .$$

שאלה 33

y $\in C$	F	L	A	K	I	Y	I	M	W	Q
$x \in \mathbb{Z}_{26}$	5	11	0	10	8	24	8	12	22	16
$k \in \mathbb{Z}_{26}$	12	4	18	18	0	6	4	12	4	18
$y \in \mathbb{Z}_{26}$	19	7	8	18	8	18	4	0	18	24
y $\in C$	t	h	i	s	i	s	e	a	s	y

שאלה 34 ראו קובץ נפרד.

שאלה 35

שאלה 36

א)

$$P_Y(A) = P_X(a)P_K(k_2)+P_X(b)P_K(k_1)+P_X(b)P_K(k_3) \quad = \left(\frac{3}{8}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{8}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{8}\right)\left(\frac{1}{3}\right) \quad = \frac{5}{24}\ .$$

$$P_Y(B) = P_X(a)P_K(k_1)+P_X(b)P_K(k_2)+P_X(b)P_K(k_3) \quad = \left(\frac{3}{8}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{2}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{2}\right)\left(\frac{1}{3}\right) \quad = \frac{11}{24}\ .$$

$$P_Y(C) = P_X(a)P_K(k_3)+P_X(b)P_K(k_2)+P_X(b)P_K(k_1) \quad = \left(\frac{3}{8}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{8}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{2}\right)\left(\frac{1}{3}\right) \quad = \frac{1}{3}\ .$$

ב) מכיוון ש- $|K|=|X|=|Y|$ אפשר להשתמש במשפט שאנון. למערכת זו אין סודיות מושלמת בגלל שמקתיים כי לכל $x \in X$ ולכל $y \in Y$ יש מפתח יחיד $k \in K$ עבורו $e_k(x)=y$. לדוגמה,

אין מפתח שמצפין b ל- B.

אין מפתח שמצפין c ל- A.

יש יותר ממפתח אחד אשר מצפין b ל- A.

יש יותר ממפתח אחד אשר מצפין c ל- B.

חילופי אפשר להוכיח כי

$$P_X(x|y) \neq P_X(x)$$

עבור אחד מ- $x \in \{a,b,c\}$ ואחד מ- $y \in \{A.B,C\}$.

<u>שאלה 37</u> התת מפתחות הם:

$$k_1 = (124)(35)\ , \qquad k_2 = (142)(3)(5)\ , \qquad k_3 = (1)(2)(4)(35)\ .$$

הטקסט מוצפן התקבל על ידי להפוך את השני חצאים, $L_3 = 11100$, $R_3 = 10101$. לכן

$$R_2 = L_3 = 11100$$

ו-

$$L_2 = R_3 \oplus f(R_2, k_3) = 10101 \oplus 11001 = 01100\ .$$

$$R_1 = L_2 = 01100\ .$$

$$L_1 = R_2 \oplus f(R_1, k_2) = 11100 \oplus 00110 = 11010$$

$$R_0 = L_1 = 11010\ .$$

$$L_0 = R_1 \oplus f(R_0, k_1) = 01100 \oplus 11010 = 10110$$

לכן הטקס גלוי הוא

$$X = L_0 R_0 = 1011011010\ .$$

<u>שאלה 38</u>

<u>שאלה 39</u>

$$\begin{aligned}
DK_1^{(1)} &= \left(K_1^{(9)}\right)^{-1}\ , \\
DK_2^{(1)} &= -\left(K_2^{(9)}\right)\ , \\
DK_3^{(1)} &= -\left(K_3^{(9)}\right)\ , \\
DK_4^{(1)} &= \left(K_4^{(9)}\right)^{-1}\ , \\
DK_5^{(1)} &= K_5^{(8)}\ , \\
DK_6^{(1)} &= K_6^{(8)}\ .
\end{aligned}$$

hex	9	9	7	7	6	6	5	5	3	3	2
binary	1001	1001	0111	0111	0110	0110	0101	0101	0011	0011	0010

hex	2	f	f	1	1	a	a	0	0	b	b
binary	0010	1111	1111	0001	0001	1010	1010	0000	0000	1011	1011

hex	4	4	c	c	d	d	8	8	e	e
binary	0100	0100	1100	1100	1101	1101	1000	1000	1110	1110

ביטים $37 - 22$: $k_1^{(9)} = 1100\ 1010\ 1010\ 0110 = 51878$.

ביטים $38 - 53$: $k_2^{(9)} = 0110\ 0100\ 0101\ 1111 = 25695$.

ביטים $54 - 69$: $k_3^{(9)} = 1110\ 0010\ 0011\ 0101 = 57909$.

ביטים $70 - 85$: $k_4^{(9)} = 0100\ 0000\ 0001\ 0111 = 16407$.

ביטים $93 - 108$: $k_5^{(8)} = 0100\ 1100\ 1100\ 1101$.

ביטים $109 - 124$: $k_6^{(8)} = 1101\ 1000\ 1000\ 1110$.

$$
\begin{aligned}
DK_1^{(1)} &= \left(K_1^{(9)}\right)^{-1} = (51878)^{-1} \mod 65537 &&= 37521 &&= 1001\ 0010\ 1001\ 0001 \ ,\\
DK_2^{(1)} &= -\left(K_2^{(9)}\right) = -25695 \mod 65536 &&= 39841 &&= 1001\ 1011\ 1010\ 0001 \ .\\
DK_3^{(1)} &= -\left(K_3^{(9)}\right) = -57909 \mod 65536 &&= 7627 &&= 0000\ 1110\ 1110\ 0101 \ .\\
DK_4^{(1)} &= \left(K_4^{(9)}\right)^{-1} = (16407)^{-1} \mod 65537 &&= 46092 &&= 1011\ 0100\ 0000\ 1100 \ .\\
DK_5^{(1)} &= K_5^{(8)} && &&= 0100\ 1100\ 1100\ 1101 \ .\\
DK_6^{(1)} &= K_6^{(8)} && &&= 1101\ 1000\ 1000\ 1110 \ .
\end{aligned}
$$

שאלה 40 אם $p \nmid n$ אז p לא מופיע לפירוק לראשוניים של n. ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}$$

אז $p \neq p_i$ לכל $1 \leq i \leq k$. לכן הפיקור לראשוניים של pn הוא

$$pn = p^1 p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k} \ .$$

מכאן הפונקציית אוילר עבור pn היא

$$\phi(pn) = \left(p^1 - p^0\right)\left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right) \ .$$

אבל הפונקציית אוילר של p היה $\phi(p) = p-1$ והפונקציית אוילר של n הוא $\phi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right)$ לכן

$$\phi(pn) = (p-1)\phi(n) \ .$$

אם $p \mid n$ אז p מופיע בפירוק לראשוניים של n. ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}$$

אז קיים i, $1 \leq i \leq k$ עבורו $p_i = p$. לכן

$$np = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p^{e_i+1} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k} \ .$$

מכאן הפונקציית אוילר של np היא

$$\begin{aligned}\phi(np) &= \left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_{i-1}^{e_{i-1}}-p_i^{e_{i-1}-1}\right)\left(p^{e_i+1}-p^{e_i}\right)\left(p_{i+1}^{e_{i+1}}-p_{i+1}^{e_{i+1}-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\\ &= \left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_{i-1}^{e_{i-1}}-p_i^{e_{i-1}-1}\right)p\left(p^{e_i}-p^{e_i-1}\right)\left(p_{i+1}^{e_{i+1}}-p_{i+1}^{e_{i+1}-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\\ &=p\left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_{i-1}^{e_{i-1}}-p_i^{e_{i-1}-1}\right)\left(p^{e_i}-p^{e_i-1}\right)\left(p_{i+1}^{e_{i+1}}-p_{i+1}^{e_{i+1}-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\\ &=p\phi(n)\ .\end{aligned}$$

שאלה 41

א)

$$n = pq = 191\times 127 = 24257$$
$$\phi(n)=\phi(pq)=(p-1)(q-1)=190\times 126=23940\ .$$

$a=47^{-1} \mod 23940$. נשתמש באלגוריתם של אוקליד:

שיטה 1

$a=23940, b=47$.

$$\begin{aligned} r_0 &=a=23940\ , & r_1&=b=47\ ,\\ s_0&=1\ , & s_1&=0\ ,\\ t_0&=0\ , & t_1&=1\ .\end{aligned}$$

שלב $i=1$:	$r_2=23940-509\cdot 47=17$	$s_2=1-509\cdot 0=1$	$t_2=0-509\cdot 1=-509$	$q_1=509$
שלב $i=2$:	$r_3=47-2\cdot 17=13$	$s_3=0-2\cdot 1=-2$	$t_3=1-2\cdot(-509)=1019$	$q_2=2$
שלב $i=3$:	$r_4=17-1\cdot 13=4$	$s_4=1-1\cdot(-2)=3$	$t_4=-509-1\cdot(1019)=-1528$	$q_3=1$
שלב $i=4$:	$r_5=13-3\cdot 4=1$	$s_5=-2-3\cdot(3)=-11$	$t_5=1019-3\cdot(-1528)=5603$	$q_4=3$
שלב $i=5$:	$r_6=4-4\cdot 1=0$	$s_6=3-4\cdot(-11)=47$	$t_6=-1528-4\cdot(5603)=-23940$	$q_5=4$

$$\gcd(a,b)=r_5=1\ ,\qquad x=s_5=-11\ ,\qquad y=t_5=5603\ .$$

$$ax+by=-11(23940)+5603(47)=1\ .$$

מכאן

$$5603(47)=1+11(23940)\quad\Rightarrow\quad 5603(47)=1\mod 23940\quad\Rightarrow\quad 47^{-1}=5603\mod 23940\ .$$

שיטה 2

$$\begin{aligned}
23940 =& 509(47) + 17\\
47 =& 2(17) + 13\\
17 =& 13 + 4\\
13 =& 3(4) + 1\\
4 =& 4(1) + 0\ .
\end{aligned}$$

$$\begin{aligned}
1 =& 13 - 3(4)\\
=& 13 - 3(17 - 13)\\
=& 4(13) - 3(17)\\
=& 4(47 - 2(17)) - 3(17)\\
=& 4(47) - 11(17)\\
=& 4(47) - 11(23940 - 509(47))\\
=& 5603(47) - 11(23940)
\end{aligned}$$

לכן $a^{-1} = 5603$.

ב) אליס שולחת את ההודעה $2468^{47} \mod 24257$. כדי לחשב זה נשתמש בשיטת ריבועים: $47 = 32 + 8 + 4 + 2 + 1$.

$$\begin{aligned}
(2468)^2 & &= 2517 \mod 24257\\
(2468)^4 =& (2517)^2 &= 4212 \mod 24257\\
(2468)^8 =& (4212)^2 &= 9077 \mod 24257\\
(2468)^{16} =& (9077)^2 &= 15157 \mod 24257\\
(2468)^{32} =& (15157)^2 &= 20859 \mod 24257
\end{aligned}$$

לכן

$$\begin{aligned}
246847 =& (2468)^{32} \times (2468)^8 \times (2468)^4 \times (2468)^2 \times 2468 \mod 24257\\
=& 20859 \times 9077 \times 4212 \times 2517 \times 2468 \mod 24257\\
=& 10642 \mod 24257\ .
\end{aligned}$$

ג) $y = 9625$.

$$y \mod p = 9625 \mod 191 = 75\ , \qquad a \mod (p-1) = 5603 \mod 190 = 93\ .$$

לכן

$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p = 75^{93} \mod 191 = 20$$

(ניתן לחשב זה לפי $75^{64} \times 75^{16} \times 75^8 \times 75^4 \times 75$).

בנוסף

$$y \mod q = 9625 \mod 127 = 100\ , \qquad a \mod (q-1) = 5603 \mod 126 = 59\ .$$

לכן

$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q = 100^{59} \mod 127 = 87$$

(ניתן לחשב זה לפי $100 \times 100^2 \times 100^8 \times 100^{16} \times 100^{32}$.)

לכן עלינו לפתור את המערכת

$$\begin{aligned} x =& 20 \mod 191 \\ x =& 87 \mod 127 \end{aligned}$$

בעזרת המשפט השאריות הסיני. נסמן $a_1 = 20$, $m_1 = 191$, $a_2 = 87$, $m_2 = 127$.

$$M = m_1 m_2 = (191)(127) = 24257 \ , \qquad M_1 = \frac{M}{m_1} = 127 \ , \qquad M_2 = \frac{M}{m_2} = 191 \ .$$

כעת נחשב $y_1 = M_1^{-1} \mod m_1 = 127^{-1} \mod 191$ ו- $y_2 = M_2^{-1} \mod m_2 = 191^{-1} \mod 127$.

<u>שיטה 1</u>

נחשב $y_1 = 127^{-1} \mod 191$ ו- $y_2 = 191^{-1} \mod 127$ בעזרת האלגוריתם של אוקליד:

$$\begin{aligned} 191 =& 127 \cdot 1 + 64 \\ 127 =& 64 \cdot 1 + 63 \\ 64 =& 63 \cdot 1 + 1 \\ 63 =& 1 \cdot 63 + 0 \ . \end{aligned}$$

לכן $\gcd(191, 127) = 1$.

$$\begin{aligned} 1 =& 64 - 63 \cdot 1 \\ =& 64 - (127 - 64 \cdot 1) \\ =& 64 \cdot 2 - 127 \cdot 1 \\ =& (191 - 127 \cdot 1) \cdot 2 - 127 \\ =& 191 \cdot 2 + 127 \cdot (-3) \ . \end{aligned}$$

לכן

$$127 \cdot (-3) \equiv 1 \mod 191 \quad \Rightarrow \quad 127 \cdot (188) \equiv 1 \mod 191 \quad \Rightarrow \quad 127^{-1} \mod 191 = 188 \ .$$

$$191 \cdot (2) \equiv 1 \mod 127 \quad \Rightarrow \quad 191^{-1} \mod 127 = 2 \ .$$

מכאן $y_1 = 127^{-1} \mod 191 = 188$ ו- $y_2 = 191^{-1} \mod 127 = 2$.

<u>שיטה 2</u>

בעזרת הקוד `mod_inverse.py` נחשב

$$y_1 = M_1^{-1} \mod m_1 = 127^{-1} \mod 191 = 188 \ , \qquad y_2 = M_2^{-1} \mod m_2 = 191^{-1} \mod 127 = 2 \ .$$

לכן

$$M = 20(127)(188) + 87(191)(2) \mod 24257 = 1357 \ .$$