מחלקה למדעי המחשב

29/08/2024 כ"ה באב תשפ"ד
09 : 00 – 12 : 00

קריפטוגרפיה

מועד א'

מרצים: ד"ר ירמיהו מילר,

תשפ"ד סמסטר ב'

השאלון מכיל 11 **עמודים (כולל עמוד זה וכולל דף נוסחאות).**

בהצלחה!

==========

הנחיות למדור בחינות שאלוני בחינה

- לשאלון הבחינה יש לצרף מחברת.
- ניתן להשתמש במחשבון מדעי לא גרפי עם צג קטן.

חומר עזר

- דפי נוסחאות של הקורס (8 עמודים בפורמט $A4$), מצורפים לשאלון.

אחר / הערות יש לענות על השאלות באופן הבא:

- יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר וללא נימוק, אפילו נכונה, לא תתקבל.
- יש לפתור 4 מתוך 5 השאלות הבאות. משקל כל שאלה 25 נקודות.
- סדר התשובות אינו משנה, אך יש לרשום ליד כל תשובה את מספרה.
- הסבירו היטב את מהלך הפתרון.

==========

שאלה 1 **(25 נקודות)** נתונה המטריצה $k \in \mathbb{Z}_{26}^{2\times 2}$ שמוגדרת $k = \begin{pmatrix} 3 & 4 \\ 7 & 11 \end{pmatrix}$.

א) **(5 נקודות)** הוכיחו כי k מפתח חוקי של צופן היל.

ב) **(15 נקודות)** נתון הטקסט מוצפן GIBO אשר מוצפן באמצעות צופן היל עם המפתח k. פענחו את הטקסט מוצפן כדי למצוא את הטקסט גלוי.

ג) **(5 נקודות)** נתון כלל מצפין $e_k(x) = xk$ של צופן היל כאשר $x \in \mathbb{Z}_{26}^{n}$ ו- $k \in \mathbb{Z}_{26}^{n\times n}$. הוכיחו שאם $\gcd(\det k, 26) = 1$ אז קיים כלל מפענח.

שאלה 2 **(25 נקודות)**

נתונה קריפטו-מערכת בעלת קבוצת טקסט גלוי $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, קבוצת מפתחות $K = \{k_1, k_2, k_3\}$, וקבוצת טקסט מוצפן $Y = \{\mathtt{A}, \mathtt{B}, \mathtt{C}\}$. הפונקצית הסתברות של X הינה

$$P_X(\mathtt{a}) = \frac{5}{8}\ , \qquad P_X(\mathtt{b}) = \frac{1}{4}\ , \qquad P_X(\mathtt{c}) = \frac{1}{8}\ .$$

הפונקצית הסתברות של המפתחות K הינה

$$P_K(k_1) = \frac{1}{3}\ , \qquad P_K(k_2) = \frac{1}{3}\ , \qquad P_K(k_3) = \frac{1}{3}\ .$$

המטריצת הצפנה היא

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

א) **(15 נקודות)** מצאו את הפונקצית הסתברות של הטקסט מוצפן $P_Y(y)$.

ב) **(10 נקודות)** הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.

שאלה 3 **(25 נקודות)**

א) **(20 נקודות)** אליס מצפינה טקסט גלוי 10 ביטים באמצעות צופן פייסטל בעל 3 מחזורים. המפתח ההתחלתי k נתון על ידי התמורה

$$\pi = (142)(35)\ .$$

התזמון מפתחות הוא כך: כל תת-מפתח k_i $(1 \le i \le 3)$ מתקבל על ידי ההרכבה i- פעמים של התמורה π. פענחו את הטקסט מוצפן 1100100011.

ב) **(5 נקודות)** כמה מפתחות קיימים של צופן אפיני מעל $\mathbb{Z}_m$ כאשר $m = 900$.

שאלה 4 (25 נקודות)

א) (15 נקודות) נתונה קבוצת טקסט גלוי $\{\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d},\mathtt{e}\}$ בעלת פונקצית הסתברות

$$P_X(\mathtt{a})=\frac{1}{10}\ ,\qquad P_X(\mathtt{b})=\frac{1}{2}\ ,\qquad P_X(\mathtt{c})=\frac{3}{20}\ ,\qquad P_X(\mathtt{d})=\frac{1}{20}\ ,\qquad P_X(\mathtt{e})=\frac{1}{5}\ .$$

בעזרת האלגוריתם של האפמן מצאו ההצפנה של X.

ב) (5 נקודות) חשבו את האנטרופיה $H[X]$ של X.

ג) (5 נקודות) בדקו אם אי-שוויון האפמן מתקיים עבור ההצפנה שמצאתם בסעיף א'.

שאלה 5 (25 נקודות)

אליס שולחת הודעה $x=22$ לבוב. בוב משתמש בצופן RSA עם המפתח ציבורי $(p=11,q=17,b=29)$.

א) (15 נקודות)
הוכיחו כי המפתח הסודי $a=149$.

ב) (10 נקודות)
הוכיחו כי ההודעה המוצפנת אשר בוב מקבל היא $y=88$.

פתרונות

שאלה 1 (25 נקודות)

א) k מפתח חוקי אם k הפיך ב- $\mathbb{Z}_{26}$, ז"א אם קיים k^{-1} כך ש- $kk^{-1}=I$ כאשר $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ מטריצה יחידה של $\mathbb{Z}_{26}$.

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

כאשר C המטריצה של קופקטורים של k ו- $|k|$ הדטרמיננטה של k ב- $\mathbb{Z}_{26}$. מכאן $\exists\ k^{-1} \Leftrightarrow \exists\ |k|^{-1}\in\mathbb{Z}_{26} \Leftrightarrow \exists\ \gcd(|k|,26)=1$.

$$\begin{vmatrix}3&4\\7&11\end{vmatrix} \mod 26 = 33-28 \mod 26 = 5 \mod 26 = 5\ .$$

לכן $\gcd(|k|,26)=\gcd(5,26)=1$ ולכן k הפיך ולכן k מפתח חוקי.

ב)

y $\in C$	G	I	B	O
$y\in\mathbb{Z}_{26}$	6	8	1	14

$$k=\begin{pmatrix}3&4\\7&11\end{pmatrix} \quad\Rightarrow\quad C=\begin{pmatrix}11&-7\\-4&3\end{pmatrix} \mod 26=\begin{pmatrix}11&19\\22&3\end{pmatrix}\ .$$

מסעיף הקודם $|k|=5$ לכן

$$|k|^{-1} \mod 26 = 5^{-1} \mod 26 \overset{\text{דף הנוסחאות}}{=} 21$$

$$k^{-1}=|k|^{-1}C^t \mod 26 = 21\begin{pmatrix}11&22\\19&3\end{pmatrix} \mod 26=\begin{pmatrix}231&462\\399&63\end{pmatrix} \mod 26=\begin{pmatrix}23&20\\9&11\end{pmatrix}$$

$$\begin{pmatrix}6&8\end{pmatrix}k^{-1}=\begin{pmatrix}6&8\end{pmatrix}\begin{pmatrix}23&20\\9&11\end{pmatrix}=\begin{pmatrix}210&208\end{pmatrix} \mod 26=\begin{pmatrix}2&0\end{pmatrix}\ .$$

$$\begin{pmatrix}1&14\end{pmatrix}k^{-1}=\begin{pmatrix}1&14\end{pmatrix}\begin{pmatrix}23&20\\9&11\end{pmatrix}=\begin{pmatrix}149&174\end{pmatrix} \mod 26=\begin{pmatrix}19&18\end{pmatrix}\ .$$

y $\in C$	G	I	B	O
$y\in\mathbb{Z}_{26}$	6	8	1	13
$x\in\mathbb{Z}_{26}$	2	0	19	18
x $\in P$	c	a	t	s

ג) $\gcd(|k|,26)=1 \Leftarrow \exists\ |k|^{-1} \Leftarrow$ לפי נוסחת קריימר קיימת מטריצה הופכית $k^{-1}=|k|^{-1}C^t$. מכאן ניתן להפוך את הכלל מצפין:

$$y=xk \quad \Rightarrow \quad x=yk^{-1} \quad \Rightarrow \quad d_k(y)=yk^{-1} \ . \ .$$

נבדוק כי $d_k(e_k(x))=x$:

$$d_k(e_k(x))=d_k(xk)=xkk^{-1}=xI=x \ .$$

שאלה 2 (25 נקודות)

א)

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

לפיכך

$$\begin{aligned}
P_Y\left(\mathtt{A}\right)=&\sum_{k\in k_1,k_2,k_2} P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{A})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{A})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{A})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{A})\right)\\
=&P\left(K=k_1\right)P\left(X=\mathtt{b}\right)+P\left(K=k_2\right)P\left(X=\mathtt{a}\right)+P\left(K=k_3\right)P\left(X=\mathtt{b}\right)\\
=&\frac{1}{3}\cdot\frac{1}{4}+\frac{1}{3}\cdot\frac{5}{8}+\frac{1}{3}\cdot\cdot\frac{1}{4}\\
=&\frac{3}{8} \ .
\end{aligned}$$

$$\begin{aligned}
P_Y\left(\mathtt{B}\right)=&\sum_{k\in k_1,k_2,k_2} P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{B})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{B})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{B})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{B})\right)\\
=&P\left(K=k_1\right)P\left(X=\mathtt{a}\right)+P\left(K=k_2\right)P\left(\mathtt{c}\right)+P\left(K=k_3\right)P\left(X=\mathtt{c}\right)\\
=&\frac{1}{3}\cdot\frac{5}{8}+\frac{1}{3}\cdot\frac{1}{8}+\frac{1}{3}\cdot\frac{1}{8}\\
=&\frac{7}{24} \ .
\end{aligned}$$

$$\begin{aligned}
P_Y\left(\mathtt{C}\right)=&\sum_{k\in k_1,k_2,k_2} P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{C})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{C})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{C})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{C})\right)\\
=&P\left(K=k_1\right)P\left(X=\mathtt{c}\right)+P\left(K=k_2\right)P\left(\mathtt{b}\right)+P\left(K=k_3\right)P\left(X=\mathtt{a}\right)\\
=&\frac{1}{3}\cdot\frac{1}{8}+\frac{1}{3}\cdot\frac{1}{4}+\frac{1}{3}\cdot\frac{5}{8}\\
=&\frac{8}{24} \ .
\end{aligned}$$

ב)

לקריפטו-מערכת יש סודיות מושלמת אם התנאי $P(Y=y|X=x)=P(Y=y)$ מתקיים. תנאי השקול לזה הוא $P(X=x|Y=y)=P(X=x)$.

בדף נוסחאות: $P(K=k_i)$. $\sum_{\substack{k\in K \\ x=d_k(y)}}$

לכן

$$P\left(Y=\mathtt{A}|X=\mathtt{a}\right)=\sum_{\substack{k\in\{k_1,k_2,k_3\} \\ \mathtt{a}=d_{k_i}(\mathtt{A})}} P(K=k_i)=P(K=k_2)=\frac{1}{3}\ .$$

$$P\left(Y=\mathtt{A}\right)=\frac{3}{8}\ .$$

הרי $\frac{1}{3}=P\left(Y=\mathtt{A}|X=\mathtt{a}\right)\neq P\left(Y=\mathtt{A}\right)=\frac{3}{8}$ לכן לקריפטו-מערכת אין סודיות מושלמת.

שאלה 3 (25 נקודות)

א)

$$k_1=\begin{pmatrix}1&2&3&4&5\\4&1&5&2&3\end{pmatrix}$$
$$k_2=\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}$$
$$k_3=\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix}$$

הטקסט מוצפן התקבל על ידי להפוך את השני חצאים, $L_3=00011$, $R_3=11001$. לכן, השלב 1 הוא:

$$R_2=L_3=00011$$

ו-

$$L_2=R_3\oplus f(R_2,k_3)=11001\oplus 00110=11111\ .$$

שלב 2:

$$R_1=L_2=11111\ .$$

$$L_1=R_2\oplus f(R_1,k_2)=00011\oplus 11111=11100$$

שלב 3:

$$R_0 = L_1 = 11100 \ .$$

$$L_0 = R_1 \oplus f(R_0, k_1) = 11111 \oplus 01011 = 10100$$

לכן הטקס גלוי הוא

$$X = L_0 R_0 = 1010011100 \ .$$

ב)

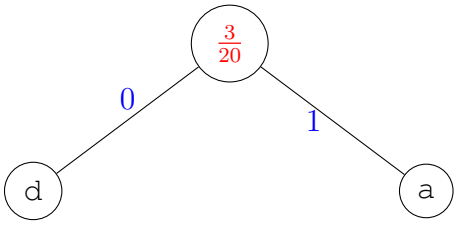
$$900 = 2^2 3^2 5^2 \ .$$

$$\phi(900) = \left(2^2 - 2^1\right)\left(3^2 - 3^1\right)\left(5^2 - 5^1\right) = (2)(6)(20) = 240 \ .$$

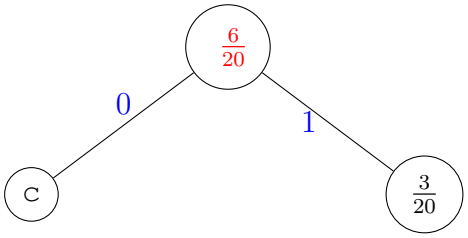
לכן קיימים $240 \cdot 900 = 216000$ מפתחות.

שאלה 4 (25 נקודות)

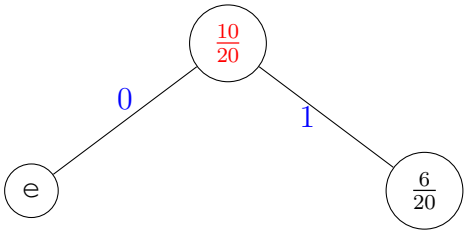
א)



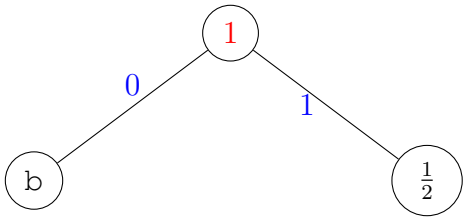
$\frac{1}{20}$	$\frac{1}{10}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{2}$
d	a	c	e	b



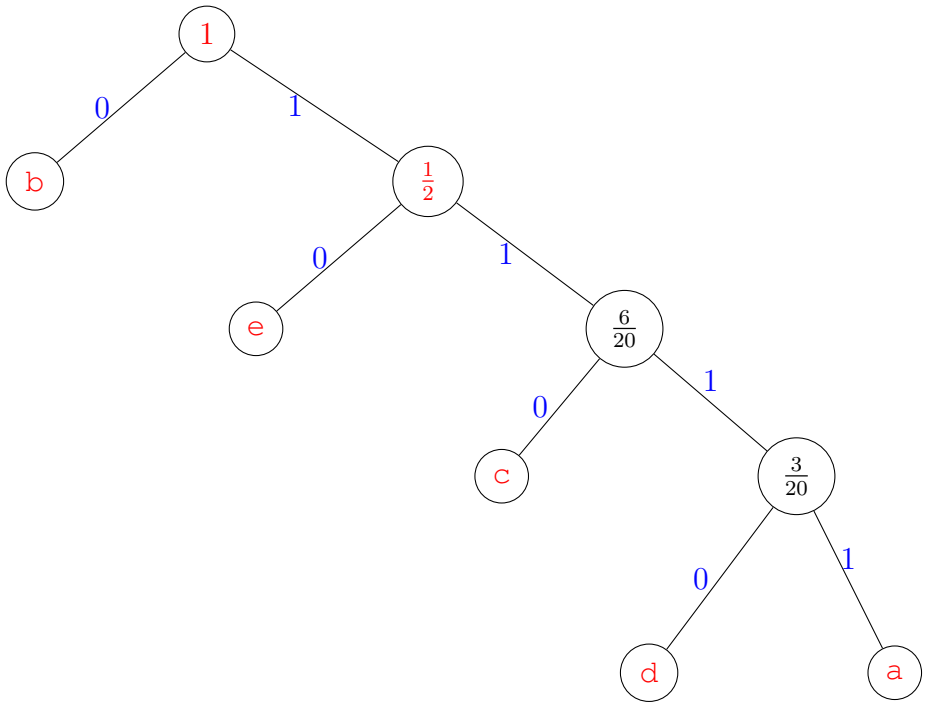
$\frac{3}{20}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{2}$
	c	e	b



$\frac{1}{5}$	$\frac{6}{20}$	$\frac{1}{2}$
e		b



$\frac{1}{2}$	$\frac{1}{2}$
	b



a	1111
b	0
c	110
d	1110
e	10

ב)

$$
\begin{aligned}
H[X] =& -P_X(\mathtt{a})\log_2 P_X(\mathtt{a}) - -P_X(\mathtt{b})\log_2 P_X(\mathtt{b}) - P_X(\mathtt{c})\log_2 P_X(\mathtt{c}) - P_X(\mathtt{d})\log_2 P_X(\mathtt{d}) - P_X(\mathtt{e})\log_2 P_X(\mathtt{e}) \\
=& -\frac{1}{10}\log_2\frac{1}{10} - \frac{1}{2}\log_2\frac{1}{2} - \frac{3}{20}\log_2\frac{3}{20} - \frac{1}{20}\log_2\frac{1}{20} - \frac{1}{5}\log_2\frac{1}{5} \\
=& \frac{\log(10)}{10\log(2)} + \frac{1}{2} + \frac{3\log\left(\frac{20}{3}\right)}{20\log(2)} + \frac{\log(20)}{20\log(2)} + \frac{\log(5)}{5\log(2)} \\
=& \frac{1}{2} + \frac{\log(5)}{5\log(2)} + \frac{\log(10)}{10\log(2)} + \frac{\log(20)}{20\log(2)} + \frac{3\log\left(\frac{20}{3}\right)}{20\log(2)} \\
=& 1.92322\ .
\end{aligned}
$$

ג) אי-שוויון האפמן: $H[X] \leq l[f] \leq H[X]+1$. כאשר $l[f]$ התוחלת אורך ההצפנה. נחשב את $l[f]$:

$$\begin{aligned} l[f] =& P_X(\mathtt{a})l\big(f(\mathtt{a})\big) + P_X(\mathtt{b})l\big(f(\mathtt{b})\big) + P_X(\mathtt{c})l\big(f(\mathtt{c})\big) + P_X(\mathtt{d})l\big(f(\mathtt{d})\big) + P_X(\mathtt{e})l\big(f(\mathtt{e})\big) \\ =& 4\left(\frac{1}{10}\right) + 1\left(\frac{1}{2}\right) + 3\left(\frac{3}{20}\right) + 4\left(\frac{1}{20}\right) + 2\left(\frac{1}{5}\right) \\ =& \frac{2}{5} + \frac{1}{2} + \frac{9}{20} + \frac{1}{5} + \frac{2}{5} \\ =& \frac{39}{20} = 1.95 \ . \end{aligned}$$

$H[X] = 1.9322 < 1.95 = l[f]$ ו- $l[f] = 1.95 < 2.9322 = H[X]+1$ לפיכך אי-שוויון האפמן $H[X] \leq l[f] \leq H[X]+1$ מתקיים.

שאלה 5 (25 נקודות)

א)

$$n = pq = 11 \times 17 = 187$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 10 \times 16 = 160 \ .$$

$a = 29^{-1} \mod 160$. נשתמש באלגוריתם של אוקליד:

שיטה 1

$a = 160, b = 29$.

$$\begin{aligned} r_0 =& a = 160, & r_1 =& b = 29 \ , \\ s_0 =& 1 \ , & s_1 =& 0 \ , \\ t_0 =& 0 \ , & t_1 =& 1 \ . \end{aligned}$$

שלב $i=1$:	$r_2 = 160 - 5 \cdot 29 = 15$	$s_2 = 1 - 5 \cdot 0 = 1$	$t_2 = 0 - 5 \cdot 1 = -5$	$q_1 = 5$
שלב $i=2$:	$r_3 = 29 - 1 \cdot 15 = 14$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-5) = 6$	$q_2 = 1$
שלב $i=3$:	$r_4 = 15 - 1 \cdot 14 = 1$	$s_4 = 1 - 1 \cdot (-1) = 2$	$t_4 = -5 - 1 \cdot (6) = -11$	$q_3 = 1$
שלב $i=4$:	$r_5 = 14 - 14 \cdot 1 = 0$	$s_5 = -1 - 14 \cdot 2 = -29$	$t_5 = 6 - 14 \cdot (-11) = 160$	$q_4 = 14$

$$\gcd(a,b) = r_4 = 1 \ , \qquad x = s_4 = 2 \ , \qquad y = t_4 = -11 \ .$$

$$ax + by = 2(160) - 11(29) = 1 \ .$$

מכאן

$$-11(29) = 1 - 2(160) \quad \Rightarrow \quad -11(29) = 1 \mod 160 \quad \Rightarrow \quad 29^{-1} = -11 \mod 160 = 149 \ .$$

<u>שיטה 2</u>

$$\begin{aligned} 160 &= 5(29) + 15 \\ 29 &= 1(15) + 14 \\ 15 &= 1(14) + 1 \\ 14 &= 14(1) + 0 \ . \end{aligned}$$

$$\begin{aligned} 1 &= 15 - 1(14) \\ &= 15 - 1(29 - 1(15)) \\ &= 2(15) - 1(29) \\ &= 2(160 - 5(29)) - 1(29) \\ &= 2(160) - 11(29) \end{aligned}$$

לכן

$$a = b^{-1} \mod \phi(n) = 29^{-1} \mod 160 = -11 \mod 160 = 149 \ .$$

ב)

$$y = x^b \mod n = 22^{29} \mod 187 \ .$$

$$22^{29} = 22^{16+8+4+1}$$

$$\begin{aligned} 22 \mod 187 &= && = 22 \ , \\ 22^2 \mod 187 &= 484 \mod 187 && = 110 \ . \\ 22^4 \mod 187 &= 484^2 \mod 187 = 234256 \mod 187 && = 132 \ . \\ 22^8 \mod 187 &= 132^2 \mod 187 = 17424 \mod 187 && = 33 \ . \\ 22^{16} \mod 187 &= 33^2 \mod 187 = 1089 \mod 187 && = 154 \ . \end{aligned}$$

$$22^{29} \mod 187 = (22^{16})(22^8)(22^4)(22^1) \mod 187 = (154)(33)(132)(22) \mod 187 = 88 \ .$$

לכן הטקסט מוצפן $y = 88$.