מחלקה למדעי המחשב

15/10/24 י"ג בתשרי תשפ"ד
13 : 30 – 16 : 30

קריפטוגרפיה

מועד ג'

מרצה: 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)

יהי n מספר טבעי. ריבוע לטיני של סדר n הוא מטריצה L מסדר $n \times n$ של מספרים שלמים $1, 2, \ldots, n$ כך שכל אחד של ה- n שלמים מופיע בדיוק פעם אחת בכל שורה ובכל עמודה של L.
למשל המטריצה הבאה היא דוגמה של ריבוע לטיני מסדר 4:

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

נסמן את הרכיב בשורה ה- i ובעמודה ה- j של L ב- $L(i,j)$.
בהינתן ריבוע לטיני L של סדר n, ניתן להגדיר קריפטו-מערכת בצורה הבאה:
יהי P הטקסט גלוי, יהי C הטקסט מוצפן, ויהי K הקבוצת מפתחות של הקריפטו-מערכת.
יהיו

$$P = C = K = \{1, 2, \ldots, n\} \ .$$

לכל מפתח i ולכל טקסט גלוי j ($1 \leq i \leq n, 1 \leq j \leq n$) יהי הכלל מצפין מוגדר להיות

$$e_i(j) = L(i,j) \ .$$

לכל מפתח יש הסתברות שווה.
הוכיחו: לקריפטו-מערכת זו יש סודיות מושלמת.

שאלה 2 (25 נקודות)

יהי p מספר ראשוני ויהי n מספר שלם חיובי.
תהי $\phi(a)$ הפונקצית אוילר לכל a מספר שלם חיובי.

א) (12 נקודות) הוכיחו כי $\phi(pn) = (p-1)\phi(n)$ אם p לא מחלק את n.

ב) (13 נקודות) הוכיחו כי $\phi(pn) = p\phi(n)$ אם p מחלק את n.

שאלה 3 (25 נקודות)

תהי $X = \{\mathtt{s}, \mathtt{t}, \mathtt{u}\}$ קבוצת טקסט גלוי בעלת פונקצית הסתברות

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

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

$$P_K(k_1) = \frac{1}{16} \ , \qquad P_K(k_2) = \frac{1}{8} \ , \qquad P_K(k_3) = \frac{1}{4} \ , \qquad P_K(k_4) = \frac{9}{16} \ .$$

תהי $Y = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}\}$ קבוצת טקסט מוצפן. יהי

$$e_{k_i}(x) = 2x + i \mod 4$$

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

א) (20 נקודות)
מצאו את הפונקצית הסתברות של הטקסט מוצפן.

ב) (5 נקודות)
הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.

שאלה 4 (25 נקודות)

נתון צופן פייסטאל בעל פונקצית ליבה

$$f\left(x_1x_2x_3x_4x_4\ ,\ \pi\right) = x_{\pi(1)}x_{\pi(2)}x_{\pi(3)}x_{\pi(4)}x_{\pi(5)}\ .$$

יהי המפתח ההתחלתי התמורה

$$\pi_0 = (135)(24)$$

ויהי כל תת-מפתח k_i $(i = 1, 2, 3)$ התמורה המתקבלת על ידי לבצע i פעמים את התמורה π_0.
חשבו את הטקסט מוצפן של הטקסט גלוי 0010111001.

שאלה 5 (25 נקודות)

בשאלה הזאת אין קשר בין הסעיפים.

א) (15 נקודות)
אליס שולחת את הטקסט גלוי הבא לבוב:

$$\texttt{coffee}\ .$$

אליס הצפינה את ההודעה באמצעות צופן היל. הטקסט מוצפן המתקבל הוא

$$\texttt{GOMDUS}\ .$$

מצאו את המפתח של הצופן.

ב) (10 נקודות)
מצאו מספרים שלמים s, t, u כך ש-

$$57s + 93t = u\ .$$

פתרונות

שאלה 1 (25 נקודות)

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 2 (25 נקודות)

א) (12 נקודות)

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

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

ב) (13 נקודות)

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 $1 \leq i \leq k$, i 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 3 (25 נקודות)

א)

$$\begin{aligned}
e_{k_1}(\mathtt{s}) &= e_{k_1}(18) = (2 \cdot 18 + 1) \mod 4 = 37 \mod 4 = 1 \to \mathtt{B} \ , \\
e_{k_2}(\mathtt{s}) &= e_{k_2}(18) = (2 \cdot 18 + 2) \mod 4 = 38 \mod 4 = 2 \to \mathtt{C} \ , \\
e_{k_3}(\mathtt{s}) &= e_{k_3}(18) = (2 \cdot 18 + 3) \mod 4 = 39 \mod 4 = 3 \to \mathtt{D} \ , \\
e_{k_4}(\mathtt{s}) &= e_{k_4}(18) = (2 \cdot 18 + 4) \mod 4 = 40 \mod 4 = 0 \to \mathtt{A} \ , \\
e_{k_1}(\mathtt{t}) &= e_{k_1}(19) = (2 \cdot 19 + 1) \mod 4 = 39 \mod 4 = 3 \to \mathtt{D} \ , \\
e_{k_2}(\mathtt{t}) &= e_{k_2}(19) = (2 \cdot 19 + 2) \mod 4 = 40 \mod 4 = 0 \to \mathtt{A} \ , \\
e_{k_3}(\mathtt{t}) &= e_{k_3}(19) = (2 \cdot 19 + 3) \mod 4 = 41 \mod 4 = 1 \to \mathtt{B} \ , \\
e_{k_4}(\mathtt{t}) &= e_{k_4}(19) = (2 \cdot 19 + 4) \mod 4 = 42 \mod 4 = 2 \to \mathtt{C} \ , \\
e_{k_1}(\mathtt{u}) &= e_{k_1}(20) = (2 \cdot 20 + 1) \mod 4 = 41 \mod 4 = 1 \to \mathtt{B} \ , \\
e_{k_2}(\mathtt{u}) &= e_{k_2}(20) = (2 \cdot 20 + 2) \mod 4 = 42 \mod 4 = 2 \to \mathtt{C} \ , \\
e_{k_3}(\mathtt{u}) &= e_{k_3}(20) = (2 \cdot 20 + 3) \mod 4 = 43 \mod 4 = 3 \to \mathtt{D} \ , \\
e_{k_4}(\mathtt{u}) &= e_{k_4}(20) = (2 \cdot 20 + 4) \mod 4 = 44 \mod 4 = 0 \to \mathtt{A} \ .
\end{aligned}$$

	s	t	u
k_1	B	D	B
k_2	C	A	C
k_3	D	B	D
k_4	A	C	A

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

$$\begin{aligned}
&P_Y\left(\mathtt{A}\right)=\sum_{k\in k_1,k_2,k_3,k_4}P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{A})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{A})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{A})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{A})\right)+P\left(K=k_4\right)P\left(X=d_{k_4}(\mathtt{A})\right)\\
=&P\left(K=k_1\right)P\left(\emptyset\right)+P\left(K=k_2\right)P\left(X=\mathtt{t}\right)+P\left(K=k_3\right)P\left(X=\emptyset\right)\\
&+P\left(K=k_4\right)P\left(X=\mathtt{s}\right)+P\left(K=k_4\right)P\left(X=\mathtt{u}\right)\\
=&\frac{1}{8}\cdot\frac{1}{4}+\frac{9}{16}\cdot\frac{1}{6}+\frac{9}{16}\cdot\frac{7}{12}\\
=&\frac{29}{64}\ .
\end{aligned}$$

$$\begin{aligned}
&P_Y\left(\mathtt{B}\right)=\sum_{k\in k_1,k_2,k_3,k_4}P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{B})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{B})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{B})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{B})\right)+P\left(K=k_4\right)P\left(X=d_{k_4}(\mathtt{B})\right)\\
=&P\left(K=k_1\right)P\left(X=\mathtt{s}\right)+P\left(K=k_1\right)P\left(X=\mathtt{u}\right)+P\left(K=k_2\right)P\left(\emptyset\right)\\
&+P\left(K=k_3\right)P\left(X=\mathtt{t}\right)+P\left(K=k_4\right)P\left(\emptyset\right)\\
=&\frac{1}{16}\cdot\frac{1}{6}+\frac{1}{16}\cdot\frac{7}{12}+\frac{1}{4}\cdot\frac{1}{4}\\
=&\frac{7}{64}\ .
\end{aligned}$$

$$\begin{aligned}
&P_Y\left(\mathtt{C}\right)=\sum_{k\in k_1,k_2,k_3,k_4}P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{C})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{C})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{C})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{C})\right)+P\left(K=k_4\right)P\left(X=d_{k_4}(\mathtt{C})\right)\\
=&P\left(K=k_1\right)P\left(\emptyset\right)+P\left(K=k_2\right)P\left(X=\mathtt{s}\right)+P\left(K=k_2\right)P\left(X=\mathtt{u}\right)\\
&+P\left(K=k_3\right)P\left(\emptyset\right)+P\left(K=k_4\right)P\left(X=\mathtt{t}\right)\\
=&\frac{1}{8}\cdot\frac{1}{6}+\frac{1}{8}\cdot\frac{7}{12}+\frac{9}{16}\cdot\frac{1}{4}\\
=&\frac{15}{64}\ .
\end{aligned}$$

$$\begin{aligned}
&P_Y\left(\mathtt{D}\right)=\sum_{k\in k_1,k_2,k_3,k_4}P\left(K=k_i\right)P\left(X=d_{k_i}(\mathtt{C})\right)\\
=&P\left(K=k_1\right)P\left(X=d_{k_1}(\mathtt{D})\right)+P\left(K=k_2\right)P\left(X=d_{k_2}(\mathtt{D})\right)+P\left(K=k_3\right)P\left(X=d_{k_3}(\mathtt{D})\right)+P\left(K=k_4\right)P\left(X=d_{k_4}(\mathtt{D})\right)\\
=&P\left(K=k_1\right)P\left(X=\mathtt{t}\right)+P\left(K=k_2\right)P\left(\emptyset\right)+P\left(K=k_3\right)P\left(X=\mathtt{s}\right)+P\left(K=k_3\right)P\left(X=\mathtt{u}\right)\\
&+P\left(K=k_3\right)P\left(\emptyset\right)\\
=&\frac{1}{16}\cdot\frac{1}{4}+\frac{1}{4}\cdot\frac{1}{6}+\frac{1}{4}\cdot\frac{7}{12}\\
=&\frac{13}{64}\ .
\end{aligned}$$

בדיקה: $P_Y(\mathtt{A})+P_Y(\mathtt{B})+P_Y(\mathtt{C})+P_Y(\mathtt{D})=\frac{29}{64}+\frac{7}{64}+\frac{15}{64}+\frac{13}{64}=1$.

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: $P(Y=y|X=x)=\sum_{\substack{k\in K\\ x=d_k(y)}}P(K=k_i)$.

לכן

$$P\left(Y=\mathtt{A}|X=\mathtt{s}\right)=\sum_{\substack{k\in\{k_1,k_2,k_3,k)4\}\\ \mathtt{s}=d_{k_i}(\mathtt{A})}}P(K=k_i)=P(K=k_4)=\frac{9}{16}\ .$$

$$P\left(Y=\mathtt{A}\right)=\frac{29}{64}\ .$$

הרי $\frac{9}{16}=P\left(Y=\mathtt{A}|X=\mathtt{s}\right)\neq P\left(Y=\mathtt{A}\right)=\frac{29}{16}$ לכן לקריפטו-מערכת אין סודיות מושלמת.

שאלה 4

$L_0=\mathtt{00101}$ ו- $R_0=\mathtt{11001}$. התת מפתחות הם

$$k_1=(135)(24)\ ,\qquad k_2=(153)(2)(4)\ ,\qquad k_3=(1)(3)(5)(24)\ .$$

מכאן

$$L_1=R_0=\mathtt{11001}\ .$$
$$R_1=L_0\oplus f\left(R_0,k_1\right)=\mathtt{00101}\oplus\mathtt{00111}=\mathtt{00010}\ .$$

$$L_2=R_1=\mathtt{00010}\ .$$
$$R_2=L_1\oplus f\left(R_1,k_2\right)=\mathtt{11001}\oplus\mathtt{00010}=\mathtt{11011}\ .$$

$$L_3=R_2=\mathtt{11011}\ .$$
$$R_3=L_2\oplus f\left(R_2,k_3\right)=\mathtt{00010}\oplus\mathtt{11011}=\mathtt{11001}\ .$$
$$y=R_3L_3=\mathtt{1100111011}$$

שאלה 5 (25 נקודות)

א) (15 נקודות)

$x \in P$	c	o	f	f	e	e
$x \in \mathbb{Z}_{26}$	2	14	5	5	4	4
$y \in C$	G	O	M	D	U	S
$y \in \mathbb{Z}_{26}$	6	14	12	3	20	18

$$X_1 = \begin{pmatrix} 2 & 14 \end{pmatrix} \ , \quad X_2 = \begin{pmatrix} 5 & 5 \end{pmatrix} \ , \quad Y_1 = \begin{pmatrix} 6 & 14 \end{pmatrix} \ , \quad Y_2 = \begin{pmatrix} 12 & 3 \end{pmatrix} \ ,$$

$$k = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}^{-1} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 2 & 14 \\ 5 & 5 \end{pmatrix}^{-1} \begin{pmatrix} 6 & 14 \\ 12 & 3 \end{pmatrix} \ .$$

$$X = \begin{pmatrix} 2 & 14 \\ 5 & 5 \end{pmatrix} \ , \quad \Rightarrow \quad |X| = -60 \mod 26 = 18 \ .$$

$|X|^{-1}$ המטריצה של קופקטורים:

$$C = \begin{pmatrix} 5 & -5 \\ -14 & 2 \end{pmatrix} \mod 26 = \begin{pmatrix} 5 & 19 \\ 12 & 2 \end{pmatrix}$$

לכן

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

ב) $a = 93, b = 57$.

$$\begin{aligned} r_0 &= a = 93 \ , & r_1 &= b = 57 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $i = 1$:	$r_2 = 93 - 1 \cdot 57 = 36$	$s_2 = 1 - 1 \cdot 0 = 1$	$t_2 = 0 - 1 \cdot 1 = -1$	$q_1 = 1$
שלב $i = 2$:	$r_3 = 57 - 1 \cdot 36 = 21$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-1) = 2$	$q_2 = 1$
שלב $i = 3$:	$r_4 = 36 - 1 \cdot 21 = 15$	$s_4 = 1 - 1 \cdot (-1) = 2$	$t_4 = -1 - 1 \cdot (2) = -3$	$q_3 = 1$
שלב $i = 4$:	$r_5 = 21 - 1 \cdot 15 = 6$	$s_5 = -1 - 1 \cdot (2) = -3$	$t_5 = 2 - 1 \cdot (-3) = 5$	$q_4 = 1$
שלב $i = 5$:	$r_6 = 15 - 2 \cdot 6 = 3$	$s_6 = 2 - 2 \cdot (-3) = 8$	$t_6 = -3 - 2 \cdot (5) = -13$	$q_5 = 2$
שלב $i = 6$:	$r_7 = 6 - 2 \cdot 3 = 0$	$s_7 = -3 - 2 \cdot (8) = -19$	$t_7 = 5 - 2 \cdot (-13) = 31$	$q_6 = 2$

$$\gcd(a, b) = r_6 = 3 \ , \qquad x = s_6 = 8 \ , \qquad y = t_6 = -13 \ .$$

$$ax + by = 8(93) - 13(57) = 3 \ .$$