מחלקה למדעי המחשב

17/09/24 י"ד באלול תשפ"ד
09 : 00 – 12 : 00

קריפטוגרפיה

מועד ב'

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)

הוכיחו כי פונקצית ההצפנה ופונקצית הפענוח של צופן ה-RSA הן פונקציות הופכיות.

שאלה 2 (25 נקודות)

יהיו p,q מספרים ראשוניים וכן $n=pq$.
תהי $\lambda:\mathbb{N}\to\mathbb{N}$ פונקציה שמוגדרת

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

נגדיר צופן חדש שהוא כמעט זהה לצופן ה-RSA. ההבדל היחיד בין צופן ה-RSA לבין הצופן החדש הוא ש- $\phi(n)$ הוחלפה עם $\lambda(n)$ כך ש-

$$ab\equiv 1 \mod \lambda(n)$$

כאשר a ו- b הם אותם מספרים שלמים שמופיעים בההגדרה של צופן ה-RSA.
הוכיחו כי הכלל מצפין והכלל מפענח של הצופן החדש הם פונקציות הופכיות.

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

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

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)**

אליס רוצה לשלוח הודעה לבוב. היא מבקשת להצפין את ההודעה באמצעות צופן אל-גמאל. למטרה הזאת בוב בוחר במפתח הציבורי הבא : $(p = 47, \alpha = 12, a = 10)$.
בוב צריך מפתח הסודי המתאים למפתח הציבורי הזה, כדי לפענח את הטקסט מוצפן אשר אליס שולחת.

א) (10 נקודות) חשבו את המפתח הסודי.

ב) (15 נקודות)
הטקסט המוצפן של ההודעה אשר בוב מקבל הוא $(3, 42)$.
מצאו את הטקסט הגלוי של ההודעה.

שאלה 5 **(25 נקודות)**

בשאלה הזאת אין קשר בין הסעיפים.

א) (15 נקודות)
אליס שולחת לבוב הודעה.
אליס הצפינה את ההודעה באמצעות צופן תמורה עם המפתח $k = \begin{pmatrix} 4 & 2 & 3 & 1 \end{pmatrix}$.
הטקסט המוצפן של ההודעה אשר בוב מקבל הוא $y = \texttt{DOOGKUCL}$.
מצאו את הטקסט גלוי של ההודעה אשר אליס שלחה.

ב) (10 נקודות)
יהי $k = (5, 21)$ מפתח של צופן אפיני מעל $\mathbb{Z}_{29}$. יהי

$$d_k(y) = ay + b$$

הכלל מפענח של צופן האפיני הזה לכל $y \in \mathbb{Z}_{29}$ ו- $a, b \in \mathbb{Z}_{29}$.
חשבו את a ו- b.

פתרונות

שאלה 1 (25 נקודות)

א) (20 נקודות)
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

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

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

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

שלב 5)

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

כאשר $z = x^{t(p-1)}$.
q ראשוני לכן

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

שלב 6) מכיוון ש- p, q ראשוניים אז

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

לפיכך

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

כנדרש.

שאלה 2 (25 נקודות)

שלב 1) רושמים את הצופן:

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

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

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

באותה מידה קיים q' שלם כך ש-

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

שלב 3)

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

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

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

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

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

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

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

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

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

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

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

שלב 6) מכיוון ש- p,q ראשוניים אז

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

לפיכך

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

כנדרש.

שאלה 3 (25 נקודות)

א)

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

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

ב)

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

$$
\begin{aligned}
P_Y(\texttt{A}) =& \sum_{k\in k_1,k_2,k_3,k_4} P(K=k_i)\,P(X=d_{k_i}(\texttt{A}))\\
=& P(K=k_1)P(X=d_{k_1}(\texttt{A})) + P(K=k_2)P(X=d_{k_2}(\texttt{A})) + P(K=k_3)P(X=d_{k_3}(\texttt{A})) + P(K=k_4)P(X=d_{k_4}(\texttt{A}))\\
=& P(K=k_1)P(X=\texttt{t}) + P(K=k_2)P(X=\texttt{u}) + P(K=k_3)P(X=\texttt{s}) + P(K=k_4)P(X=\texttt{t})\\
=& \frac{1}{4}\cdot\frac{1}{4} + \frac{1}{4}\cdot\frac{7}{12} + \frac{1}{4}\cdot\frac{1}{6} + \frac{1}{4}\cdot\frac{1}{4}\\
=& \frac{5}{16}\ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\texttt{B}) =& \sum_{k\in k_1,k_2,k_3,k_4} P(K=k_i)\,P(X=d_{k_i}(\texttt{B}))\\
=& P(K=k_1)P(X=d_{k_1}(\texttt{B})) + P(K=k_2)P(X=d_{k_2}(\texttt{B})) + P(K=k_3)P(X=d_{k_3}(\texttt{B})) + P(K=k_4)P(X=d_{k_4}(\texttt{B}))\\
=& P(K=k_1)P(X=\texttt{s}) + P(K=k_2)P(X=\texttt{t}) + P(K=k_3)P(X=\texttt{u}) + P(K=k_4)P(X=\texttt{s})\\
=& \frac{1}{4}\cdot\frac{1}{6} + \frac{1}{4}\cdot\frac{1}{4} + \frac{1}{4}\cdot\frac{7}{12} + \frac{1}{4}\cdot\frac{1}{6}\\
=& \frac{7}{24}\ .
\end{aligned}
$$

$$P_Y(\texttt{C}) = \sum_{k\in k_1,k_2,k_3,k_4} P(K=k_i)\,P(X=d_{k_i}(\texttt{C}))$$
$$=P(K=k_1)P(X=d_{k_1}(\texttt{C}))+P(K=k_2)P(X=d_{k_2}(\texttt{C}))+P(K=k_3)P(X=d_{k_3}(\texttt{C}))+P(K=k_4)P(X=d_{k_4}(\texttt{C}))$$
$$=P(K=k_1)P(X=\texttt{u})+P(K=k_2)P(X=\texttt{s})+P(K=k_3)P(X=\texttt{t})+P(K=k_4)P(X=\texttt{u})$$
$$=\frac{1}{4}\cdot\frac{7}{12}+\frac{1}{4}\cdot\frac{1}{6}+\frac{1}{4}\cdot\frac{1}{4}+\frac{1}{4}\cdot\frac{7}{12}$$
$$=\frac{19}{48}\ .$$

בדיקה: $P_Y(\texttt{A})+P_Y(\texttt{B})+P_Y(\texttt{C})=\frac{5}{16}+\frac{7}{24}+\frac{19}{48}=1$.

ג) 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

$$P(Y=\texttt{A}|X=\texttt{s}) = \sum_{\substack{k\in\{k_1,k_2,k_3,k)4\}\\ \texttt{s}=d_{k_i}(\texttt{A})}} P(K=k_i)=P(K=k_3)=\frac{1}{4}\ .$$

$$P(Y=\texttt{A})=\frac{5}{16}\ .$$

הרי $\frac{5}{16}=P(Y=\texttt{A})\neq P(Y=\texttt{A}|X=\texttt{s})=\frac{1}{4}$ לכן לקריפטו-מערכת אין סודיות מושלמת.

שאלה 4

א)

$$\beta=\alpha^a \mod p = 12^{10} \mod 47\ .$$

מכיוון ש- $10=8+2$ ניתן להשתמש בשיטית הריבועים:

$$12^2 \mod 47 = 3\ .$$
$$12^4 \mod 47 = 3^2 \mod 47 = 9 \mod 47 = 9\ .$$
$$12^8 \mod 47 = 9^2 \mod 47 = 81 \mod 47 = 34\ .$$

לכן

$$12^{10} \mod 47 = (3)(34) \mod 47 = 102 \mod 47 = 8.$$

ז"א $\beta=8$.

ב)

שיטה 1:

$(y_1,y_2)=(3,42)$.

$$x=(y_1^a)^{-1}\cdot y_2 \mod p=(3^{10})^{-1}\cdot 42 \mod 47$$

$$(3^{10})^{-1} \mod 47 \overset{\text{משפט פרמה}}{=} 3^{47-1-10} \mod 47 = 3^{36} \mod 47\ .$$

$36=32+4$.

$$\begin{aligned}
3^2 &\mod 47 &&= 9\ ,\\
3^4 &\mod 47 = 81 \mod 47 &&= 34\ ,\\
3^8 &\mod 47 = 81^2 \mod 47 = 6561 \mod 47 &&= 28\ ,\\
3^{16} &\mod 47 = 28^2 \mod 47 = 784 \mod 47 &&= 32\ ,\\
3^{32} &\mod 47 = 32^2 \mod 47 = 1024 \mod 47 &&= 37\ .
\end{aligned}$$

מכאן

$$3^{36} \mod 47=(37)(34) \mod 47 = 1258 \mod 47 = 36$$

ולכן

$$x=(y_1^a)^{-1}\cdot y_2 \mod p=(3^{10})^{-1}\cdot 42 \mod 47=(36)(42) \mod 47=1512 \mod 47=8$$

שיטה 2:

$A=3^{10}=59049,\ B=47$.

$$\begin{aligned}
r_0 &= A=3^{10}=59049\ , & r_1 &= B=47\ ,\\
s_0 &= 1\ , & s_1 &= 0\ ,\\
t_0 &= 0\ , & t_1 &= 1\ .
\end{aligned}$$

שלב $i=1$:	$r_2=59049-1256\cdot 47=17$	$s_2=1-1256\cdot 0=1$	$t_2=0-1256\cdot 1=-1256$	$q_1=1256$
שלב $i=2$:	$r_3=47-2\cdot 17=13$	$s_3=0-2\cdot 1=-2$	$t_3=1-2\cdot(-1256)=2513$	$q_2=2$
שלב $i=3$:	$r_4=17-1\cdot 13=4$	$s_4=1-1\cdot(-2)=3$	$t_4=-1256-1\cdot(2513)=-3769$	$q_3=1$
שלב $i=4$:	$r_5=13-3\cdot 4=1$	$s_5=-2-3\cdot(3)=-11$	$t_5=2513-3\cdot(-3769)=13820$	$q_4=3$
שלב $i=5$:	$r_6=4-4\cdot 1=0$	$s_6=3-4\cdot(-11)=47$	$t_6=-3769-4\cdot(13820)=-59049$	$q_5=4$

$$\gcd(A,B)=r_5=1\ ,\qquad x=s_5=-11\ ,\qquad y=t_5=13820\ .$$

$$Ax+By=3^{10}(-11)+47(13820)=1\ .$$

מכאן

$$-11(3^{10})=1-47(13820)\quad\Rightarrow\quad -11(3^{10})\equiv 1\mod 47\quad\Rightarrow\quad \left(3^{10}\right)^{-1}=-11\mod 47=36\mod 47\ .$$

לכן

$$x=\left(3^{10}\right)^{-1}\cdot 42\mod 47=(36)(42)\mod 47=1512\mod 47=8\ .$$

<u>שאלה 5</u> (25 נקודות)

א) $\pi=(4231)$, ז"א

$$\pi=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$$

ומכאן

$$\pi^{-1}=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}\ .$$

$x\in P$	D	O	O	G	K	U	C	L
$x\in\mathbb{Z}_{26}$	3	14	14	6	10	20	2	11
$y=d_k(x)$	6	14	14	3	11	20	2	10
$y\in C$	g	o	o	d	l	u	c	k

ב) $e_k(x)=5x+21\mod 29$. מכאן

$$x=5^{-1}(y-21)$$

נחשב את האיבר ההופכי של 5 ב- $\mathbb{Z}_{29}$ באמצעות האלגוריתם של אוקליד:

$$\begin{aligned}29&=5(5)+4\\5&=1(4)+1\end{aligned}$$

$$4=4(1)+0$$

$$\begin{aligned}1&=5-4\\&=5-(29-5(5))\\&=6(5)-29\\&=6(5)+(-1)(29)\ .\end{aligned}$$

מכאן $5^{-1}\mod 29=6$.

לכן

$$x = 5^{-1}y - 5^{-1}(21) \mod 29 = 6y - 6(21) \mod 29 = 6y - 126 \mod 29 = 6y + 19 \mod 29$$

לפיכך

$$d_k(y) = 6y + 19 \mod 29 \ ,$$

ז"א $a = 6$, $b = 19$.