.

מחלקה למדעי המחשב

19/03/2025 י"ט באדר תשפ"ד
09 : 00 – 12 : 00

קריפטוגרפיה

מועד ב'

מרצה: ד"ר ירמיהו מילר.

תשפ"ה סמסטר א'

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)

א) (15 נק')
תהי $X = \{\mathtt{q}, \mathtt{r}, \mathtt{s}\}$ קבוצת טקסט גלוי בעלת פונקצית ההסתברות

$$P_X(\mathtt{q}) = \frac{1}{3}\ , \qquad P_X(\mathtt{r}) = \frac{1}{4}\ , \qquad P_X(\mathtt{s}) = \frac{5}{12}\ .$$

תהי $K = \{k_1, k_2, k_3, k_4\}$ קבוצת מפתחות בעלת פונקצית הסתברות $P_K(k_i) = \frac{1}{4}$ לכל $k_i \in K$. תהי $Y = \{\mathtt{A}, \mathtt{B}, \mathtt{C}\}$ קבוצת טקטסט מוצפן. נגדיר כלל המצפין

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

לכל $x \in \mathbb{Z}_{26}$ ולכל $i \in \{1, 2, 3, 4\}$.
הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.

ב) (5 נק')
יהיו a, m שלמים לא זרים. הוכיחו כי $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod \left(\frac{m}{\gcd(a,m)}\right)$.

ג) (5 נק')
יהיו a, b, c שלמים. הוכיחו: $\gcd(a, b) = \gcd(a + cb, b)$.

שאלה 2 (25 נקודות)

א) (18 נק')
הוכיחו את הטענה הבאה: צפון RSA ניתן לפענוח.

ב) (7 נק')
מצאו שלמים s, t, d עבורם $285s + 89t = d$.

שאלה 3 (25 נקודות)

א) (5 נק')
יהיו a, b, m שלמים. הוכיחו את הטענה הבאה: $(a \mod m)(b \mod m) \mod m \equiv ab \mod m$.

ב) (5 נק')
יהיו a, m שלמים. הוכיחו את הטענה הבאה: $(a \mod m)^{-1} \mod m \equiv a^{-1} \mod m$.

ג) (15 נק')
הוכיחו את הטענה הבאה: צופן אל-גמאל ניתן לפענוח.

שאלה 4

א) (10 נק')
אליס שלחה את הטקסט המוצפן הבא לבוב: `HIFUWNJITUQF`. אליס הצפינה את הטקסט באמצעות צופן אפיני עם המפתח $(7, 19)$. חשבו את הטקסט הגלוי.

ב) (5 נק')
יהי p מספר ראשוני. הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה: לכל שלם a מתקיים

$$a^p \equiv a \mod p \ .$$

ג) (5 נק')
יהיו a, b, c, m שלמים. הוכיחו את הטענה הבאה:
אם $a \equiv b \mod m$ אזי $a + c \equiv (b + c) \mod m$.

ד) (5 נק')
יהיו $a, m > 0$ שלמים. הוכיחו את הטענה הבאה:

$$(-a) \mod m = m - (a \mod m) \ .$$

שאלה 5 (25 נקודות)

א) (13 נק')
אליס הצפינה את הטקסט הגלוי `dear` על ידי צופן היל ושולחת אותו לבוב.
הטקסט המוצפן אשר בוב מקבל הוא `BVGF`.
מצאו את המפתח שבאמצעותו אליס הצפינה את הטקסט הגלוי.

ב) (6 נק') הוכיחו את הטענה הבאה: אם $c|ab$ ו- $\gcd(b, c) = 1$ אז $c|a$.

ג) (6 נק') יהיו a, m מספרים זרים. הוכיחו כי $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod m$.

פתרונות

שאלה 1

א)

K \ X	q	r	s
k_1	A	C	B
k_2	B	A	C
k_3	C	B	A
k_4	A	C	B

$$\begin{aligned}P_Y(\mathtt{A}) =& P_K(k_1)P_X(\mathtt{q}) + P_K(k_2)P_X(\mathtt{r}) + P_K(k_3)P_X(\mathtt{s}) + P_K(k_4)P_X(\mathtt{q}) \\ =& \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) \\ =& \frac{16}{48} \ .\end{aligned}$$

$$\begin{aligned}P_Y(\mathtt{C}) =& P_K(k_1)P_X(\mathtt{r}) + P_K(k_2)P_X(\mathtt{s}) + P_K(k_3)P_X(\mathtt{q}) + P_K(k_4)P_X(\mathtt{r}) \\ =& \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) \\ =& \frac{15}{48} \ .\end{aligned}$$

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

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

דוגמה נגדית:

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

לכן לקריפטו-מערכת אין סודיות מושלמת

ב) נניח כי $ab \equiv ac \mod m$. אז

$$ab = ac + qm \quad \Rightarrow \quad ab - ac = qm \quad \Rightarrow \quad m \mid a(b-c) \quad \Rightarrow \quad \frac{m}{\gcd(a,m)} \mid \frac{a}{\gcd(a,m)}(b-c) \ .$$

מכיוון ש- $\frac{m}{\gcd(a,m)}$ ו- $\frac{a}{\gcd(a,m)}$ זרים, אז

$$\frac{m}{\gcd(a,m)} \mid (b-c) \ .$$

לכן

$$b \equiv c \mod \left(\frac{m}{\gcd(a,m)}\right) \ .$$

ג) אם a, b שלמים אז קיימים שלמים s ו- t עבורם $sa + tb = d$ כאשר $d = \gcd(a,b)$. מכאן

$$\begin{aligned} sa + tb &= d \\ s(a + cb) + tb &= d + scb \\ s(a + cb) + tb - scb &= d \\ s(a + cb) + (t - sc)b &= d \end{aligned}$$

לכן קיימים שלמים $x = s$ ו- $y = t - cb$ עבורם

$$x(a + cb) + yb = d$$

ולכן $\gcd(a + cb, b) = d = \gcd(a,b)$.

שאלה 2

א) נתון כי $ab = 1 \mod \phi(n)$.
$\phi(n) = \phi(pq) = (p-1)(q-1)$.
ז"א

$$ab = 1 \mod \phi(n) = 1 \mod (p-1)(q-1)$$

לכן קיים $t \in \mathbb{Z}$ כך ש-

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

לכל $z \neq 0 \in \mathbb{Z}$ לפי משפט **??**, $z^{p-1} = 1 \mod p$. בפרט

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

כאשר $y = x^{t(q-1)}$. מכאן $x^{ab-1} = 1 \mod p$.

משיקולות של סיימטריה באותה מידה $x^{ab-1} = 1 \mod q$.

לכן $x^{ab-1}-1=0 \mod p$ ו- $x^{ab-1}-1=0 \mod q$.

מכיוון ש- p ו- q זרים אז

$$x^{ab-1}-1=0 \mod (pq) .$$

לפיכך

$$x^{ab-1}=1 \mod (pq) .$$

נכפיל ב- x ונקבל

$$(x^a)^b=x \mod (pq) .$$

ז"א הוכחנו כי לכל טקסט גלוי x, אם נצפין אותו ואז אחר כך נפענח את הטקסט מוצפן המתקבל מאלגוריתם RSA, נקבל אותו טקסט גלוי המקורי בחזרה.

ב) $a=285, b=89$.

$$\begin{aligned} r_0 &= a = 285 , & r_1 &= b = 89 , \\ s_0 &= 1 , & s_1 &= 0 , \\ t_0 &= 0 , & t_1 &= 1 . \end{aligned}$$

שלב $k=1$:	$r_2 = 285 - 3 \cdot 89 = 18$	$s_2 = 1 - 3 \cdot 0 = 1$	$t_2 = 0 - 3 \cdot 1 = -3$	$q_1 = 3$
שלב $k=2$:	$r_3 = 89 - 4 \cdot 18 = 17$	$s_3 = 0 - 4 \cdot 1 = -4$	$t_3 = 1 - 4 \cdot (-3) = 13$	$q_2 = 4$
שלב $k=3$:	$r_4 = 18 - 1 \cdot 17 = 1$	$s_4 = 1 - 1 \cdot (-4) = 5$	$t_4 = -3 - 1 \cdot (13) = -16$	$q_3 = 1$
שלב $k=4$:	$r_5 = 17 - 17 \cdot 1 = 0$	$s_5 = -4 - 17 \cdot 5 = -89$	$t_5 = 13 - 17 \cdot (-16) = 285$	$q_4 = 17$

$$\gcd(a,b) = r_4 = 1 , \qquad s = s_4 = 5 , \qquad t = t_4 = -16 .$$

$$ta + sb = 5(289) - 16(85) = 1 .$$

■

שאלה 3 (25 נקודות)

א) לכל a, m שלמים $\exists\ q_1, r_1$ כך ש-

$$a = q_1 m + r_1 \quad \Rightarrow \quad r_1 \equiv a \mod m .$$

באותה מידה לכל b, m שלמים $\exists\ q_2, r_2$ כך ש-

$$b = q_2 m + r_2 \quad \Rightarrow \quad r_2 \equiv b \mod m .$$

לכן

$$ab = (q_1 m + r_1)(q_2 m + r_2) = (q_1 q_2 m + r_1 q_2 + r_2 q_1)m + r_1 r_2 = Qm + r_1 r_2$$

לכן $\exists$ שלם Q שך כ-

$$ab = Qm + r_1 r_2$$

ולכן

$$ab \equiv r_1 r_2 \mod m \quad \Rightarrow \quad r_1 r_2 \equiv ab \mod m \quad \Rightarrow \quad (a \mod m)(b \mod m) \equiv ab \mod m$$

ב) נסמן $x = (a \mod m)^{-1} \mod m$. ז"א, מכיוון ש- x הוא האיבר ההופכי של $a \mod m$ מודולר m אזי

$$(a \mod m)\, x \equiv 1 \mod m\ .$$

מכאן מנובע

$$ax \equiv 1 \mod m$$

ולכן

$$x = a^{-1} \mod m \quad \Rightarrow \quad (a \mod m)^{-1} \mod m \equiv a^{-1} \mod m\ .$$

ג) לפי ההגדרה של צופן El-Gamal, הכלל מצפיון הוא

$$e_k(x) = (y_1, y_2) \quad y_1 \alpha^d \mod p\ , \quad y_2 = \beta^d x \mod p\ ,$$

כאשר p ראשוני ו- d שלם, והכלל מעפנח הוא

$$d_k(y_1, y_2) = (y_1{}^a)^{-1} y_2 \mod p\ .$$

לפיכך:

$$\begin{aligned}
d_k\left(e_k(x)\right) =& d_k\left(y_1, y_2\right) \\
=& \left(y_1{}^a\right)^{-1} y_2 \mod p \\
=& \left[\left(\alpha^d \mod p\right)^a\right]^{-1} \left(x\beta^d \mod p\right) \mod p \\
=& \left(\alpha^{da} \mod p\right)^{-1} \left(x\beta^d \mod p\right) \mod p && \text{(כלל הכפל של יחסי מודולרים)} \\
=& \left(\left(\alpha^{da}\right)^{-1} \mod p\right) \left(x\beta^d \mod p\right) \mod p && \text{(סעיף ב')} \\
=& \left(\alpha^{da}\right)^{-1} \left(x\beta^d\right) \mod p && \text{(סעיף א')} \\
=& \left(\alpha^{da}\right)^{-1} \left(x\left(\alpha^a\right)^d\right) \mod p && \text{(הגדרה של צופן El-Gamal)} \\
=& \left(\alpha^{da}\right)^{-1} \left(x\alpha^{ad}\right) \mod p \\
=& \left(\alpha^{da}\right)^{-1} \alpha^{ad} x \mod p \\
=& x \mod p\ .
\end{aligned}$$

שאלה 4 (25 נקודות)

א) (11 נק')

ב) (10 נק') נוכיח באינדוקציה.

<u>בסיס:</u>

עבור $a = 0$ הטענה $0^p \equiv 0 \mod p$ מתקיימת.

<u>מעבר:</u>

נניח כי הטענה מתקיימת עבור a.

$$(a+1)^p = a^p + pa^{p-1} + \frac{p(p-1)}{2}a^{p-2} + \cdots + pa + 1 \equiv a^p + 1 \mod p$$

ההנחת האינדוקציה אומרת ש- $a^p \equiv a \mod p$ לכן

$$(a+1)^p \mod p \equiv a^p + 1 \mod p \equiv (a+1) \mod p$$

כנדרש.

ג) (4 נק') לפי משפט החילוק של אוקליד קיימים שלמים $0 \leq q < a$ ו- $0 \leq r < m$:

$$a = qm + r$$

כאשר $r = a \mod m$. מכאן

$$(-a) = (-q)m - r = -(q+1)m + m - r = \bar{q}m + \bar{r}$$

כאשר $\bar{r} = m - r$, $\bar{q} = -(q+1)$. קיבלנו כי

$$(-a) = \bar{q}m + \bar{r}$$

כאשר $\bar{r} = (-a) \mod m$. לכן

$$(-a) \mod m = m - r = m - (a \mod m)\ .$$

שאלה 5 (25 נקודות)

א) (13 נק')

	d	e	a	r
	3	4	0	17
	B	V	G	F
	1	21	6	5

$$X=\begin{pmatrix}3 & 4\\ 0 & 17\end{pmatrix}\ , \qquad Y=\begin{pmatrix}1 & 21\\ 6 & 5\end{pmatrix}\ .$$

$$|X| \mod 26 = 51 \mod 26 = 25 \quad \Rightarrow \quad |X|^{-1} \mod 26 = 25^{-1} \mod 26 = 25\ .$$

המטירצה של קופקטורים של X היא $\begin{pmatrix}17 & 0\\ 22 & 3\end{pmatrix} \mod 26 = \begin{pmatrix}17 & 0\\ -4 & 3\end{pmatrix}$ לכן C

$$X^{-1}=|X|^{-1}C^t \mod 26 = 25\begin{pmatrix}17 & 22\\ 0 & 3\end{pmatrix} \mod 26 = \begin{pmatrix}425 & 550\\ 0 & 75\end{pmatrix} \mod 26 = \begin{pmatrix}9 & 4\\ 0 & 23\end{pmatrix}$$

לכן

$$k=X^{-1}Y=\begin{pmatrix}9 & 4\\ 0 & 23\end{pmatrix}\begin{pmatrix}1 & 21\\ 6 & 5\end{pmatrix}=\begin{pmatrix}33 & 209\\ 138 & 115\end{pmatrix} \mod 26 = \begin{pmatrix}7 & 1\\ 8 & 11\end{pmatrix}\ .$$

ב) (6 נק') ראשית נציין כי $\gcd(b,c)=1 \Leftarrow c \nmid b$.

(הסבר: לפי משפט איוקלידס קיימים שלמים s,t: $sb+tc=1$. נחלק ב- c: $s\frac{b}{c}+t=\frac{1}{c}$.

ז"א אם $c \mid b$ אז $\frac{b}{c}=q$ שלם ולכן $sq+t=\frac{1}{c}$. סתירה!)

$c \mid ab$ לכן קיים שלם q כך ש- $\frac{ab}{c}=q$.

הצד שמאל שלם, לכן $\frac{b}{c}$ שלם או $\frac{a}{c}$ שלם.

כיוון ש- $\frac{b}{c}$ לא שלם אז בהכרח $\frac{a}{c}$ שלם ולכן $a \mid c$.

ג) (6 נק')

נניח כי $ab \equiv ac \mod m$.

$$ab \equiv ac \mod m \quad \Rightarrow \quad ab=ac+qm \quad \Rightarrow \quad ab-ac=qm \quad \Rightarrow \quad a(b-c)=qm\ .$$

מכאן $a \mid qm$.

a,m זרים לכן $a \nmid m$ לכן $a \mid q$. ז"א $\exists\ k$ שלם עבורו $q=ak$.

לפיכך

$$a(b-c)=qm \quad \Rightarrow \quad a(b-c)=akm \quad \Rightarrow \quad b-c=km \quad \Rightarrow \quad b=c+km \quad \Rightarrow \quad b \equiv c \mod m\ .$$

נניח כי $b \equiv c \mod m$. אז

$$b=qm+c \quad \Rightarrow \quad ab=aqm+ac \quad \Rightarrow \quad ab \equiv ac \mod m\ .$$