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 $x=2468$ לבוב. בוב משתמש בצופן RSA עם המפתח ציבורי $(p=191,q=127,b=47)$.

א) (15 נקודות)
הוכיחו כי המפתח הסודי $a=5603$.

ב) (10 נקודות)
הוכיחו כי ההודעה המוצפנת אשר בוב מקבל היא $y=10642$.