.

מחלקה למדעי המחשב

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

# קריפטוגרפיה

## מועד ב' מותאם למתווה המילואים

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.
- הסבר היטב את מהלך הפתרון.

==========

## שאלה 1 (25 נקודות)

**א) (15 נק')**

תהי $X = \{\mathrm{q}, \mathrm{r}, \mathrm{s}\}$ קבוצת טקסט גלוי בעלת פונקצית ההסתברות

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

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 $Y = \{\mathrm{A}, \mathrm{B}, \mathrm{C}\}$ 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) (10 נק')**

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

## 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) (10 נק')**

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

**ב) (15 נק')**

הוכיחו את הטענה הבאה: צופן אל-גמאל ניתן לפענוח.

## שאלה 4

**א) (15 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')**
יהיו $a, b, c, m$ שלמים. הוכיחו את הטענה הבאה:
אם $a \equiv b \mod m$ אזי $a + c \equiv (b + c) \mod m$.

**ג) (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) (12 נק')** יהיו $a, m$ מספרים זרים. הוכיחו כי $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod m$.