

אופן כתיבת תשובות לשאלות

- (1) יש להראות פתרון מלא. הסבירו היטב את מהלך הפתרון.
- (2) יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר וללא נימוק, אפילו נכונה, לא תתקבל.
- (3) יש לרשום ליד כל תשובה את מספר של השאלה שעליה אתם עונים.

מועד הגשה

- (1) ההגשה היא עד סוף יום ההגשה, כלומר עד השעה 23:59 באותו היום. אל תחכו לרגע האחרון. תכננו את זמנכם בהתאם. הגישו לפני.
- (2) איחור במועד ההגשה יגרור הורדה של ציון, 5 נק' לכל יום איחור או חלק ממנו. בכל מקרה לא יהיה ניתן להגיש מעבר ל-2 ימי איחור ממועד ההגשה דלעיל.

אופן הגשה

- (1) קראו היטב את השאלות. עליכם לענות על כל השאלות בעבודה זו.
 - (2) הגשת העבודה תהיה דרך אתר הקורס במודל בלבד. הגשת העבודה היא **ביחידים או בזוגות**.
 - (3) כיצד להגיש?
- א)** יש לסרוק או להמיר את העבודה לקובץ pdf ולהגיש אותו (סריקה לא ברורה או מטושטשת לא תיבדק).
- ב)**
- במידה שאתם מגישים פתרונות לבד אז בשם הקובץ שיוגש למערכת ההגשה יהיה מספר ת"ז ושם של המגיש ושם של העבודה. לדוגמה: עבודה2-ירמיהו-תז-123456789.pdf.
 - במידה שאתם מגישים פתרונות כזוג אז בשם הקובץ שיוגש למערכת ההגשה יהיו מספרי ת"ז ושמות של המגישים ושם של העבודה. לדוגמה: עבודה2-ירמיהו-תז-123456789-גל-113114115.pdf.
- (4) בקובץ המוגש יש להוסיף את התיעוד הבא בעמוד הראשון (בעברית או באנגלית, לבחירתכם). יש לשנות את השם לשם שלכם ואת תעודת הזהות לתעודת שלכם. ובמקום סולמית יש לכתוב את מספר העבודה.

Assignment: #

Author1: Israel Israeli, ID: 01234567

Author2: Dave David, ID: 8910111213

- (5) לאחר שהעליתם את הקבצים שלכם למודל, הורידו אותם מהמודל למחשב שלכם וודאו כי הקבצים תקינים וכי העליתם את הקבצים הנכונים והמלאים. לאחר תום מועד ההגשה לא יתקבלו ערעורים על כך שהעליתם קבצים לא תקינים או שהעליתם בטעות קבצים אחרים / לא נכונים.

שאלות

- (1) שאלות בנוגע העבודה יש לשאול בפורום באתר המודל של הקורס או בשעות קבלה של המתרגל/ת האחראי/ת בלבד. אין לשלוח שאלות במייל לא למתרגל האחראי ולא למתרגלים/מרצים אחרים.

(2) ניתן לשאול שאלות הבהרה ומיקוד על המשימות שבעבודה במידה ומשימה מסוימת לא ברורה. לא ניתן לשאול על הפתרונות שלכם. לדוגמא, לא ניתן לשאול האם הפתרון שלי נכון, לא ניתן לשאול למה הפתרון לא עובד, וכדומה.

שונות

- (1) השאלות בעבודה זו הינן שוות משקל. כלומר, משקל כל שאלה הוא 100 חלקי מספר השאלות בעבודה.
 - (2) בשאלה מרובת סעיפים, הסעיפים הם שווי משקל. כלומר משקל כל סעיף הוא משקל השאלה כולה חלקי מספר הסעיפים השאלה.
 - (3) בעדוה זו יש 5 שאלות.
- בהצלחה!

עבודת 3.

שאלה 1 (20 נקודות)

נתונה האלפיבית הבאה של טקסט גלוי $X = \{a, b, c, d, e, f, g, h, i\}$ ונתונה פונקצית ההסתברות

$$P_X(a) = 0.11, \quad P_X(b) = 0.005, \quad P_X(c) = 0.15, \quad P_X(d) = 0.3, \quad P_X(e) = 0.085.$$

$$P_X(f) = 0.22, \quad P_X(x) = 0.02, \quad P_X(y) = 0.04, \quad P_X(z) = 0.07.$$

(א) מצאו הצפנת האפמן של X .

(ב) חשבו את האנטרופיה של ההצפנה.

(ג) מצאו את $l(f)$.

שאלה 2 (20 נקודות)

יהי $X = \{p, q, r\}$ קבוצת טקסט גלוי עם פונקצית ההסתברות

$$P_X(p) = \frac{1}{7}, \quad P_X(q) = \frac{2}{7}, \quad P_X(r) = \frac{4}{7}.$$

יהי $K = \{k_1, k_2, k_3, k_4\}$ קבוצת מפתחות בעלת פונקצית ההסתברות

$$P_K(k_i) = \frac{1}{4}$$

לכל $k_i \in K$ יהי $Y = \{A, B, C\}$ קבוצת טקסט מוצפן. נגדיר הכלל מצפין

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

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

(א) מצאו את $P_Y(y)$ לכל $y \in Y$.

(ב) מצאו את $P(X = q|Y = B)$.

(ג) מצאו את $P(X = r|Y = C)$.

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

שאלה 3 (20 נקודות)

נתונה הקריפטו-מערכת בעלת הקבוצת טקסט גלוי $X = \{a, b, c\}$, קבוצת מפתחות $K = \{k_1, k_2, k_3\}$ וקבוצת טקסט מוצפן $Y = \{A, B, C\}$. הפונקציות הסתברויות הן

$$P_X(a) = \frac{1}{12}, \quad P_X(b) = \frac{1}{6}, \quad P_X(c) = \frac{3}{4}, \quad P_K(k_1) = \frac{1}{5}, \quad P_K(k_2) = \frac{2}{5}, \quad P_K(k_3) = \frac{2}{5}.$$

המטריצת ההצפנה היא

	a	b	c
k_1	B	A	C
k_2	A	C	B
k_3	C	B	A

(א) מצאו את הפונקציית הסתברות של הטקסט מוצפן Y .

(ב) הוכיחו כי לקריפטו-מערכת זו אין סודיות מושלמת.

שאלה 4 (20 נקודות)

(א) אליס שולחת לבוב את הטקסט הגלוי

$$x = BA.$$

היא מצפינה את הטקסט ע"י הצופן ElGamal עם המפתח הבא:

$$(p, \alpha, a, d) = (37, 16, 12, 20).$$

הוכיחו כי הטקסט מוצפן הוא

$$y_1 = DE, \quad y_2 = CG.$$

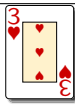
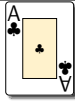




יש להתעלם מספרות הפרדה בין אותיות.

(ב) בוב מקבל את הטקסטים

$$y_1 = DE, \quad y_2 = CG$$

שהוצפנו ע"י צופן ElGamal והמפתח מאליס שמוגדר בסעיף א'. הוכיחו שכאשר בוב מפענח את הטקסט המוצפן הוא יקבל את אותו טקסט הגלוי המקורי שאליס שלחה.

שאלה 5 (20 נקודות)

מספר	קלף
42	
5	
13	
21	
9	
10	

(א) מצאו הצפנת בינארית של הקלפים בעלת תוחלת אורך ההצפנה מקסימלית.

(ב) מצאו הצפנת בינארית של הקלפים בעלת תוחלת אורך ההצפנה מינימלית.

פתרונות

שאלה 1

(א) ראו קובץ נפרד.

a	001
b	100000
c	101
d	11
e	000
f	01
x	100001
y	10001
z	1001

(ב)

$$\begin{aligned}
 H[X] &= -P_X(a) \log_2 P_X(a) - P_X(b) \log_2 P_X(b) - P_X(c) \log_2 P_X(c) \\
 &\quad - P_X(d) \log_2 P_X(d) - P_X(e) \log_2 P_X(e) - P_X(f) \log_2 P_X(f) \\
 &\quad - P_X(x) \log_2 P_X(x) - P_X(y) \log_2 P_X(y) - P_X(z) \log_2 P_X(z) \\
 &= - (0.11)(-3.18442) - (0.005)(-7.64386) - 0.15(-2.73697) - 0.3(-1.73697) \\
 &\quad - 0.085(-3.55639) - 0.22(-2.18442) - 0.02(-5.64386) - 0.04(-4.64386) - 0.07(-3.8365) \\
 &= 2.67019 .
 \end{aligned}$$

(ג)

$$\begin{aligned}
 l[f] &= P_X(a)l(a) + P_X(b)l(b) + P_X(c)l(c) + P_X(d)l(d) + P_X(e)l(e) \\
 &\quad + P_X(f)l(f) + P_X(x)l(x) + P_X(y)l(y) + P_X(z)l(z) \\
 &= 0.11 \cdot (3) + 0.005 \cdot (6) + 0.15 \cdot (3) + 0.3 \cdot (2) + 0.085 \cdot (3) + 0.22(2) + 0.02(6) + 0.04(5) + 0.07(4) \\
 &= 0.33 + 0.03 + 0.45 + 0.3 + 0.45 + 0.6 + 0.295 + 0.44 + 0.12 + 0.28 \\
 &= 2.705 .
 \end{aligned}$$

מתקיים

$$H[X] < l[f] < H[X] + 1 .$$

שאלה 2

(א)

$$2(15) + 1 \mod 3 = 31 \mod 3 = 1$$

$$2(15) + 2 \mod 3 = 32 \mod 3 = 2$$

$$2(15) + 3 \mod 3 = 33 \mod 3 = 0$$

$$2(15) + 4 \mod 3 = 34 \mod 3 = 1$$

$$2(16) + 1 \mod 3 = 33 \mod 3 = 0$$

$$2(16) + 2 \mod 3 = 34 \mod 3 = 1$$

$$2(16) + 3 \mod 3 = 35 \mod 3 = 2$$

$$2(16) + 4 \mod 3 = 36 \mod 3 = 0$$

$$2(17) + 1 \mod 3 = 35 \mod 3 = 2$$

$$2(17) + 2 \mod 3 = 36 \mod 3 = 0$$

$$2(17) + 3 \mod 3 = 37 \mod 3 = 1$$

$$2(17) + 4 \mod 3 = 38 \mod 3 = 2$$

$K \backslash X$	p	q	r
k_1	B	A	C
k_2	C	B	A
k_3	A	C	B
k_4	B	A	C

$$\begin{aligned}
P_Y(A) &= P_K(k_1)P_X(X = d_{k_1}(A)) + P_K(k_2)P_X(X = d_{k_2}(A)) \\
&\quad + P_K(k_3)P_X(X = d_{k_3}(A)) + P_K(k_4)P_X(X = d_{k_4}(A)) \\
&= P_K(k_1)P_X(q) + P_K(k_2)P_X(r) + P_K(k_3)P_X(p) + P_K(k_4)P_X(q) \\
&= \left(\frac{1}{4}\right)\left(\frac{2}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{4}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{2}{7}\right) \\
&= \frac{9}{28} .
\end{aligned}$$

$$\begin{aligned}
P_Y(B) &= P_K(k_1)P_X(X = d_{k_1}(B)) + P_K(k_2)P_X(X = d_{k_2}(B)) \\
&\quad + P_K(k_3)P_X(X = d_{k_3}(B)) + P_K(k_4)P_X(X = d_{k_4}(B)) \\
&= P_K(k_1)P_X(p) + P_K(k_2)P_X(q) + P_K(k_3)P_X(r) + P_K(k_4)P_X(p) \\
&= \left(\frac{1}{4}\right)\left(\frac{1}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{2}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{4}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{7}\right) \\
&= \frac{8}{28} .
\end{aligned}$$

$$\begin{aligned}
P_Y(C) &= P_K(k_1)P_X(X = d_{k_1}(C)) + P_K(k_2)P_X(X = d_{k_2}(C)) \\
&\quad + P_K(k_3)P_X(X = d_{k_3}(C)) + P_K(k_4)P_X(X = d_{k_4}(C)) \\
&= P_K(k_1)P_X(r) + P_K(k_2)P_X(p) + P_K(k_3)P_X(q) + P_K(k_4)P_X(r) \\
&= \left(\frac{1}{4}\right)\left(\frac{4}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{2}{7}\right) + \left(\frac{1}{4}\right)\left(\frac{4}{7}\right) \\
&= \frac{11}{28} .
\end{aligned}$$

(ב)

$$\begin{aligned}
P(X = q | Y = B) &= \frac{P(Y = B | X = q) P(X = q)}{P(Y = B)} \\
&= \frac{[P(K = k_2) + P(K = k_4)] P(X = q)}{P(Y = B)} \\
&= \frac{\left(\frac{1}{2}\right)\left(\frac{2}{7}\right)}{\left(\frac{8}{28}\right)} \\
&= \frac{1}{2} .
\end{aligned}$$

(ג)

$$\begin{aligned}
 P(X = r | Y = c) &= \frac{P(Y = c | X = r) P(X = r)}{P(Y = c)} \\
 &= \frac{[P(K = k_1) + P(K = k_4)] P(X = r)}{P(Y = c)} \\
 &= \frac{\left(\frac{1}{2}\right) \left(\frac{4}{7}\right)}{\left(\frac{11}{28}\right)} \\
 &= \frac{8}{11} .
 \end{aligned}$$

(ד) דוגמה נגדית:

$$P(Y = a | X = p) = P(K = k_3) = \frac{1}{4} \neq P(Y = p) = \frac{9}{28} .$$

לכן לקריפטו-מערכת אין סודיות מושלמת.

שאלה 3

(א)

$$P_Y(A) = P_X(a)P_K(k_2) + P_X(b)P_K(k_1) + P_X(c)P_K(k_3) = \left(\frac{1}{12}\right) \left(\frac{2}{5}\right) + \left(\frac{1}{5}\right) \left(\frac{1}{6}\right) + \left(\frac{3}{4}\right) \left(\frac{2}{5}\right) = \frac{11}{30} .$$

$$P_Y(B) = P_X(a)P_K(k_1) + P_X(b)P_K(k_3) + P_X(c)P_K(k_2) = \left(\frac{1}{12}\right) \left(\frac{1}{5}\right) + \left(\frac{1}{6}\right) \left(\frac{2}{5}\right) + \left(\frac{3}{4}\right) \left(\frac{2}{5}\right) = \frac{23}{60} .$$

$$P_Y(C) = P_X(a)P_K(k_3) + P_X(b)P_K(k_2) + P_X(c)P_K(k_1) = \left(\frac{1}{12}\right) \left(\frac{2}{5}\right) + \left(\frac{1}{6}\right) \left(\frac{2}{5}\right) + \left(\frac{3}{4}\right) \left(\frac{1}{5}\right) = \frac{1}{4} .$$

(ב)

$$P(X = a | Y = B) = \frac{P(Y = B | X = a)P(X = a)}{P(Y = B)} = \frac{P_K(k_1)P(X = a)}{P(Y = B)} = \frac{\left(\frac{1}{5}\right) \left(\frac{1}{12}\right)}{\left(\frac{2}{5}\right)} = \frac{1}{24} .$$

$$\frac{1}{12} = P(X = a) \neq P(X = a | Y = B) = \frac{1}{24}$$

לכן למערכת זו אין שודיות מושלמת.

שאלה 4

(א) ראשית נחשב את המפתח הסודי:

$$\beta = \alpha^a \bmod p = 16^{12} \bmod 37 .$$

נחשב את החזקה מודולרית בעזרת שיטת הריבועיים:

$$12 = 8 + 4 \Rightarrow [30]_2 = 1100 .$$

$$i \leftarrow 0, z_0 \leftarrow 16$$

$$z_1 = z_0^2 \bmod p = 16^2 \bmod 37 = 34 ,$$

$$z_2 = z_1^2 \bmod p = 34^2 \bmod 37 = 9 ,$$

$$z_3 = z_2^2 \bmod p = 9^2 \bmod 37 = 7 ,$$

$$i \leftarrow 0, y \leftarrow 1$$

$$y \leftarrow z_2 y \bmod p = (9)(1) \bmod 37 = 9 ,$$

$$y \leftarrow z_3 y \bmod p = (7)(9) \bmod 37 = 26 .$$

לכן:

$$\beta = \alpha^a \bmod p = 16^{12} \bmod 37 = 26 .$$

כעת נבצע את ההצפנה. הכלל מצפין הוא:

$$y_1 = \alpha^d \bmod p = 16^{20} \bmod 37$$

נחשב את החזקה מודולרית בעזרת שיטת הריבועיים:

$$20 = 16 + 4 \Rightarrow [20]_2 = 10100 .$$

$$i \leftarrow 0, z_0 \leftarrow 16$$

$$z_1 = z_0^2 \bmod p = 16^2 \bmod 37 = 34 ,$$

$$z_2 = z_1^2 \bmod p = 34^2 \bmod 37 = 9 ,$$

$$z_3 = z_2^2 \bmod p = 9^2 \bmod 37 = 7 ,$$

$$z_4 = z_3^2 \bmod p = 7^2 \bmod 37 = 12 .$$

$$i \leftarrow 0, y \leftarrow 1$$

$$y \leftarrow z_2 y \bmod p = (9)(1) \bmod 37 = 9 ,$$

$$y \leftarrow z_4 y \bmod p = (9)(12) \bmod 37 = 34 .$$

לכן

$$y_1 = \alpha^d \bmod p = 16^{20} \bmod 37 = 34 .$$

$$y_2 = x\beta^d \bmod p = (10)26^{20} \bmod 37 = (10 \bmod 37) (26^{20} \bmod 37) \bmod 37 .$$

נחשב את החזקה מודולרית בעזרת שיטת הריבועיים:

$$20 = 16 + 4 \Rightarrow [20]_2 = 10100 .$$

$$i \leftarrow 0, z_0 \leftarrow 26$$

$$\begin{aligned} z_1 &= z_0^2 \bmod p = 26^2 \bmod 37 = 10, \\ z_2 &= z_1^2 \bmod p = 10^2 \bmod 37 = 26, \\ z_3 &= z_2^2 \bmod p = 26^2 \bmod 37 = 10, \\ z_4 &= z_3^2 \bmod p = 10^2 \bmod 37 = 26. \end{aligned}$$

$$i \leftarrow 0, y \leftarrow 1$$

$$\begin{aligned} y &\leftarrow z_2 y \bmod p = (26)(1) \bmod 37 = 26, \\ y &\leftarrow z_4 y \bmod p = (26)(26) \bmod 37 = 10. \end{aligned}$$

לכן

$$y_2 = x\beta^d \bmod p = (10)26^{20} \bmod 37 = (10 \bmod 37)(10 \bmod 37) \bmod 37 = 100 \bmod 37 = 26.$$

לכן הטקסט מוצפן הוא: $(y_1, y_2) = (34, 26) \rightarrow (\text{DE}, \text{CG})$.

(ב) (8 נק')

$$x = (y_1^a)^{-1} (y_2) \bmod p = (34^{12})^{-1} (26) \bmod 37.$$

$$(34^{12})^{-1} \bmod 37 = 34^{-12} \bmod 37 \stackrel{\text{משפט פרמה}}{=} 34^{37-1-12} \bmod 37 = 34^{24} \bmod 37.$$

נפתור את החזקה מודולרית הזו בעזרת השיטת הריבועים באופן הבא:

$$24 = 16 + 8 \Rightarrow [24]_2 = 11000.$$

$$i \leftarrow 0, z_0 \leftarrow 25$$

$$\begin{aligned} z_1 &= z_0^2 \bmod p = 34^2 \bmod 37 = 26, \\ z_2 &= z_1^2 \bmod p = 26^2 \bmod 37 = 10, \\ z_3 &= z_2^2 \bmod p = 10^2 \bmod 37 = 26, \\ z_4 &= z_3^2 \bmod p = 26^2 \bmod 37 = 10. \end{aligned}$$

$$i \leftarrow 0, y \leftarrow 1$$

$$\begin{aligned} y &\leftarrow z_3 y \bmod p = 26 \bmod 37 = 26, \\ y &\leftarrow z_4 y \bmod p = (10)(26) \bmod 37 = 26. \end{aligned}$$

לכן:

$$(34^{12})^{-1} \equiv 34^{24} \bmod 37 \equiv 26 \bmod 37.$$

לפיכך:

$$x = (y_1^a)^{-1} (y_2) \bmod p = (34^{12})^{-1} (26) \bmod 37 \equiv (26)(26) \bmod 37 \equiv 10 \bmod 37.$$

לכן $x = 10 \rightarrow \text{BA}$.

שאלה 5