

עבודת 2: תמורות, צופן אניגמה, קריפטו-אנליזה וצופן RSA

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: עבודה-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: עבודה-ירמיהו-תז-123456789-גל-113114115.pdf

(4) בקובץ המוגש יש להוסיף את התיעוד הבא בעמוד הראשון (בעברית או באנגלית, לבחירתכם). יש לשנות את השם שלכם ואת תעודת הזהות לתעודת הזהות 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.

בהצלחה!

עבודת 2: תמורות, צופן אניגמה, קריפטו-אנליזה וצופן RSA**שאלה 1 (10 נקודות)**

VSLBHPNAQRPELCGGUVFZRFFNTRCYRNFRJEVGRLBHEANZRURER

שאלה 2 (9 נקודות)

הטקסט הבא

BXNKJLGZ

הוצפן ע"י צופן אניגמה עם המשקפת המשתנה

$$\pi = (AG) (XI) (LP) (HD) (ES) (TY) .$$

מצאו את הטקסט הגלוי.

שאלה 3 (9 נקודות)

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

WWODFS	YASEQM	JZKNIC	FSZWUW	JBPNLY	CFWXVB
DLVQMF	VBRULE	GYACDP	KTESYU	AMJLZV	IRLGNI
PEQITH	XONKHK	UNBJWX	LVIHPT	ZCFRSL	BJXAEZ
NQTV CJ	MHGPOA	TDDMJR	QXC BGN	HPHORD	RUUYKQ
SGMTXO	EIVZBF				

(א) הוכיחו כי התמורות המתאימות של צופן אניגמה הן:

$$\begin{aligned} \Delta_4 \Delta_1 &= (JNVU) (ZRYE) (GCXKSTMPI) (ALHOFWDQB) , \\ \Delta_5 \Delta_2 &= (HO) (XG) (DJETY) (MZIBL) (FVPRNW) (AQCSUK) , \\ \Delta_6 \Delta_3 &= (MOS) (CNK) (BXZW) (YGAP) (FLITJV) (QHDREU) . \end{aligned}$$

(ב) נניח כי התמורות $\Delta_6 \Delta_3, \Delta_5 \Delta_2, \Delta_4 \Delta_1$ הן בסדר ריבסקי. נתון הטקסט הבא שהוצפן ע"י צופן אניגמה:

MWORVZ

חשבו את הטקסט הגלוי.

שאלה 4 (9 נקודות)

הטקסט הבא הוצפן ע"י צופן אפיני:

BDHS CZTF ZX OZTZCFA ADYC RLXCF ZC OZMZYP XDTFDYF FOXFX
OZKF ADYC OZMF CUF SFXHOCX DK XDTFDYF FOXFX CUZYJZYP
ADYC RDSSB LQDHC CUF KHCHSF SFTFTQFS VDTIOFTFYCX KDSPFC
CUF ZYXHOCX ADYC RDSSB RULC DCUFS IFDIOF CUZYJ ZK
BDH XHVFFFA ZY CUZX CFOO TF UDR ADYC KDSPFC CD ULMF KHY

היעזרו בקריפטו-אנליזה כדי למצוא את הטקסט הגלוי.

שאלה 5 (9 נקודות)

תהי $\pi : \Sigma \rightarrow \Sigma$ תמורה מעל אלפבית Σ . הוכיחו או הפריכו ע"י דוגמה נגדית את הטענות הבאות:

(א) אם π מחזור באורך k אזי $\pi^k = \text{id}$.

(ב) אם π מחזור באורך k אזי k הוא השלם הקטן ביותר עבורו $\pi^k = \text{id}$.

שאלה 6 (9 נקודות)

תהי Σ אלפבית בעל n אותיות. כלומר $|\Sigma| = n$. נסמן ב- S_n הקבוצה של כל התמורות האפשריות מעל Σ . הוכיחו את הטענה הבאה:
אם קיימת תמורה $\alpha \in S_n$ כך שלכל $\beta \in S_n$ מתקיים:

$$\alpha\beta = \beta\alpha$$

אז $\alpha = \text{id}$.

שאלה 7 (9 נקודות)

אליס שולחת לבוב ההודעה. אליס מצפינה את ההודעה ע"י צופן RSA עם הפרמטרים

$$b = 107, \quad p = 73, \quad q = 31.$$

ההצפנה של ההודעה היא

$$y = \text{DED}.$$

(א) הוכיחו כי המפתח הציבורי הוא $(a, p, q) = (323, 73, 31)$.

(ב) חשבו את הטקסט הגלוי שאליס שלחה.

שאלה 8 (9 נקודות)

פתרו את המערכת משוואות הבאה בעזרת המשפט השאריות הסיני:

$$\begin{aligned}x &\equiv 12 \pmod{25} \\x &\equiv 9 \pmod{26} \\x &\equiv 23 \pmod{27}.\end{aligned}$$

שאלה 9 (9 נקודות)

פתרו את המערכת משוואות הבאה:

$$\begin{aligned}13x &\equiv 4 \pmod{99} \\15x &\equiv 56 \pmod{101}.\end{aligned}$$

רמז: השתמשו באלגוריתם המוכלל של אוקליד ואחר כך המשפט השאריות הסיני.

שאלה 10 (9 נקודות)

בוב בונה מפתח ציבורי ומפתח סודי של צופן RSA עם הפרמטרים $p = 37, q = 41$ ו- $b = 31$.

(א) חשבו את n , $\phi(n)$ ו- a .

(ב) אליס מצפינה את הטקסט הגלוי `bcci`. מהי הטקסט מוצפן שהיא שולחת לבוב?

(ג) הוכיחו שהפענוח של הטקסט מוצפן שמצאתם בסעיף ב' נותן `bcci`.

רמז:

$$(-11)(1440) + (511)(31) = 1, \quad (-9)(41) + (10)(37) = 1.$$

שאלה 11 (9 נקודות)

נתון הטקסט גלוי

thefutureisgood

והטקסט מוצפן שלו

FOPBVFWDFFCCGMAT

הטקסט הוצפן עם צופן היל. מצאו את המפתח.