

## עבודת 2: תמורה, 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 ולא נימוק, אפילו נכון, לא תתקבל.
- 3) יש לרשום ליד כל תשובה את מספר של השאלה שעליה אתם עונים.

### מועד הגשה

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

### אופן הגשה

- 1) קראו היטב את השאלות. עליכם לענות על כל השאלות בעבודה זו.
  - 2) הגשת העבודה תהיה דרך אתר הקורס במודול בלבד בלבד. הגשת העבודה היא **בזוגות**.
  - 3) כיצד להגיש?
- א) יש לסרוק או להמיר את העבודה לקובץ pdf ולהגיש אותו (סרייקה לא ברורה או מוטשטשת לא תיבדק).
- ב) שם הקובץ שיוגש למערכת ההגשה יהיה מסטר ת"ז של המגיש. לדוגמה: 123456789.pdf.
- 4) בקובץ המוגש יש להוסיף את התיעוד הבא בעמוד הראשון (בעברית או באנגלית, לבחירתכם). יש לשנות את השם שלהם שלכם ואת תעודה זההות לתעודה זההות שלכם. ובמוקם סולמי יש לכתוב את מסטר העבודה.
- Assignment: #  
Author: Israel Israeli, ID: 01234567
- 5) לאחר שהעליתם את הקבצים שלכם למודול, הורידו אותם מהמודול למחשב שלכם וודאו כי הקבצים תקינים וכי העלייתם את הקבצים נכונים והמלאים. לאחר תום מועד ההגשה לא יתקבלו ערעורים על כך שהעליתם קבצים לא תקינים או שהעליתם בטעות קבצים אחרים / לא נכוןים.

### שאלות

- 1) שאלות בנוגע לעבודה יש לשאול בפורום באתר המודול של הקורס או בשעות קבלה של המתרגל/ת האחראי/ת בלבד. אין לשאול שאלות במיל לא למתרגל האחראי ולא למתרגלים/מטריצים אחרים.
- 2) ניתן לשאול שאלות הבקרה ומיקוד על המשימות שבעבודה במידה ומשימה מסוימת לא ברורה. לא ניתן לשאול על הפתרונות שלכם. לדוגמה, לא ניתן לשאול האם הפתרון שלי נכון, לא ניתן לשאול למה הפתרון לא עובד, וכדומה.

**שונות**

- 1) השאלות בעבודה זו הינה שות משקל. ככלומר, משקל כל שאלה הוא 100 חלקים מסך השאלות בעבודה.
- 2) בשאלת מרובת סעיפים, הסעיפים הם שווים משקל. ככלומר משקל כל סעיף הוא משקל השאלה כולה חלקי מספר הסעיפים השאלה.

בצלחה!

## עבודת 2: תמורה, צופן אניגמה, קריפטו-אנליזה וצופן RSA

### שאלה 1 (10 נקודות)

VSLBHPNAQRPELCGGUVFZRFFNTRCYRNFRJEVGRLBHEANZRURER

### שאלה 2 (10 נקודות)

הטקסט הבא

BXNKJLGZ

הוצפן ע"י צופן אניגמה עם המשקפת המשותנה

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

מצאו את הטקסט המקורי.

### שאלה 3 (10 נקודות)

הטבלה הבאה מראה מילימ אופייניות מהודעות מוצפנות מאותו יום.

WWODFS	YASEQM	JZKNIC	FSZWUW	JBNPLY	CFWXVB
DLVQMF	VBRULE	GYACDP	KTESYU	AMJLZV	IRLGNI
PEQITH	XONKHK	UNBJWX	LVIHPT	ZCFRSL	BJXAEZ
NQTVCJ	MHGPOA	TDDMJR	QXCBGN	PHPHORD	RUUWKQ
SGMTXO	EIVZBF				

**a)** הוכחו כי התמורות המתאימות של צופן אניגמה הן:

$$\Delta_4 \Delta_1 = (\text{JNVU}) (\text{ZRYE}) (\text{GCXKSTMPI}) (\text{ALHOFWDQB}) ,$$

$$\Delta_5 \Delta_2 = (\text{HO}) (\text{XG}) (\text{DJETY}) (\text{MZIBL}) (\text{FVPRNW}) (\text{AQCSUK}) ,$$

$$\Delta_6 \Delta_3 = (\text{MOS}) (\text{CNK}) (\text{BXZW}) (\text{YGAP}) (\text{FLITJV}) (\text{QHDREU}) .$$

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

MWORVZ

חשבו את הטקסט המקורי.

**שאלה 4 (10 נקודות)**

הtekst הבא הוכפן 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 XHVVFFA ZY CUZX CFOO TF UDR ADYC KDSPFC CD ULMF KHY

היעזרו בкриיפטו-אנליזה כדי למצוא את הטקסט המקורי.

**שאלה 5 (10 נקודות)**תהי  $\Sigma \rightarrow \Sigma$ :  $\pi$  תמורה מעל אלפבית  $\Sigma$ . הוכחו או הפריכו ע"י דוגמה נגדית את הטענות הבאות:(א) אם  $\pi$  מחזורי באורך  $k$  אז  $\pi^k = \text{id}$ .(ב) אם  $\pi$  מחזורי באורך  $k$  אז  $k$  הוא השלים הקטן ביותר עבורו  $\pi^k = \text{id}$ .**שאלה 6 (10 נקודות)**תהי  $\Sigma$  אלפבית בעל  $n$  אותיות. כלומר  $n = |\Sigma|$ . נסמן ב-  $S_n$  הקבוצה של כל התמורות האפשריות מעל  $\Sigma$ .

הוכחו את הטענה הבאה:

אם קיימת Tamura  $\alpha \in S_n$  כך שלכל  $\beta \in S_n$  מתקיים:

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

$$\text{או } \alpha = \text{id}.$$

**שאלה 7 (10 נקודות)**

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

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

ההצפנה של הודעה היא

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

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

(ב) חשבו את הטקסט המקורי שאليس שלחה.

**שאלה 8 (10 נקודות)**

פתרו את המערכת משוואות הבאה בעזרת המשפט השאריות הסיני:

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27}.$$

 **שאלה 9 (10 נקודות)**

פתרו את המערכת משוואות הבאה:

$$13x \equiv 4 \pmod{99}$$

$$15x \equiv 56 \pmod{101}.$$

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

 **שאלה 10 (10 נקודות)**בוב בונה מפתח ציבורי ומפתח סודי של צופן RSA עם הפרמטרים  $b = 31$ ,  $q = 41$ ,  $p = 37$ .(א) חשבו את  $n$  ו-  $a$ .(ב) אליס מצפינה את הטקסט הגלוי `bccc`. מהי הטקסט מוצפן שהוא שולחת לבוב?(ג) הוכחו שהפענוח של הטקסט מוצפן שמצאתם בסעיף ב' נותן `bccc`.

רמז:

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

 **שאלה 11 (10 נקודות)**

נתון הטקסט גלי

`thefutureisgood`

והtekst מוצפן שלו

`FOPBVFWDFCCGMAT`

הtekst הוצפן עם צופן היל. מצאו את המפתח.