



הנדסת תכנה

# קריפטולוגיה 1

(61117)

סיכום הקורס וオスף מבחנים

חברת זו המשויכת למאגר חומר עזר אקדמי של אגודות הסטודנטים אורט בראודה, נכתבה ע"י סטודנטים הולמים במקלה ואחריות השימוש בה מוטלת על המשתמש בלבד.



## קרייטולוגיה 1

סיכון הקורס, אוסף מבחנים

סמסטר ב' תשע"ד

**שם המרצה:** פרופ' זאב וילקוביץ'

**נערר ונכתב ע"י:** שמעון ארזואן



# קריפטולוגיה 1 – סיכון החומר

כותב : שמעון ארזואן.

סיכום הרצאות שנערכו בסמסטר אביב 2014, מרצה הקורס: ולדימיר (זאב) וולקוביץ.

סילבוס הקורס הוא:

- .1. מבוא לצפנים קלאסיים.
- .2. אריתמטיקה מודולרית.
- .3. ניתוח של הצפנים הקלאסיים.
- .4. שימוש בתורת האינפורמציה.
- .5. Block Ciphers and the Data Encryption Standard (DES)
- .6. ניתוח של האלגוריתם DES.
- .7. אלגוריתמים קריפטוגרפיים של תורה המספרים.
- .8. מערכת Diffie-Hellman
- .9. מבוא למערכות Public-Key
- .10. מערכת RSA
- .11. פרוטוקולי Public-Key



## תוכן

7	מבוא.....
7	מחלק משותף הגדול ביותר – GCD –Greatest Common Divisor .....
7	אלגוריתם אוקלידי למציאת מחלק משותף הגדול ביותר .....
8	מציאת הופכי באמצעות אלגוריתם אוקלידי .....
8	משפט אוילר .....
8	משפט פרמה הקטן .....
9	מציאת הופכי באמצעות משפט אוילר .....
9	משפט השאריות הסיניים .....
11	אלגוריתמים של הצפנה .....
11	אלגוריתם הפצנה סימטרי .....
11	הודעה בלתי מוסתרת - Unhidden messages .....
11	התקפה איטרטיבית - The Iterative Attack .....
11	One Time Pad .....
12	Shift Cipher – אלגוריתם הזזה .....
12	<b>התקפות על האלגוריתם .....</b>
12	Linear Cipher – אלגוריתם לינארי .....
13	התקפות על האלגוריתם .....
13	מציאת הודעות בלתי מוסתרות .....
14	Exponential Cipher – אלגוריתם אקספוננציאלי .....
15	מציאת הודעות בלתי מוסתרות .....
15	איך נמצא את היוצר .....
16	Substitution Ciphers .....
16	Block Ciphers .....
16	Hill Cipher .....
20	מציאת הודעות בלתי מוסתרות .....
22	Permutation Cipher .....
22	Vigenère Cipher .....
23	תורת המידע בкриיפטולוגיה .....
23	זיכרון על נוסחאות של הסתבות .....
23	אנטרופיה .....
24	DES .....
24	הקדמה .....
24	תיאור האלגוריתם .....
27	פונקצייה .....
28	פרוצדורות הרחבת מפתח .....
28	מתකפה על האלגוריתם .....

28.....	מפתח ב-DES
29.....	Double DES
30.....	ECB – Electronic Codebook
30.....	CBC – Cipher Block Chaining
31.....	Diffie-Hellman Algorithm
32.....	RSA
32.....	<b>הקדמה</b>
32.....	<b>תיאור</b>
32.....	מספר טוב לשמש כבסיס במערכת RSA אם הוא מקיים .....
32.....	למה האלגוריתם נחשב לבטוח .....
33.....	מציאת הודעות בלתי מוסתרות .....
34.....	air נתן לפרוץ .....
35.....	Hash functions
35.....	Hash functions <b>הסביר</b>
35.....	תכונות פונקציה Hash
35.....	The Birthday Paradox
37.....	חתימה דיגיטלית .....
37.....	Digital Signatures <b>הסביר</b>
37.....	אלגוריתמים לחתימה דיגיטלית .....
38.....	אוסף מבחנים ופתרונות .....

# מבוא

מחלק משותף הגדול ביותר – GCD – Greatest Common Divisor

מחלק משותף מקסימלי של שני מספרים שלמים הוא המספר הגדול ביותר שמחולק את שניהם. למשל, המחלק המשותף המקסימלי של 12 ו-18 הוא 6. אם קיבלנו כי  $\text{gcd}(a, b) = 1$  אז  $a, b$  זרים.  
תוכנות :

$$\begin{aligned}\text{gcd}(a, b) &\geq 1 \\ \text{gcd}(a, a) &= |a| \\ \text{gcd}(a, 0) &= |a| \\ \text{gcd}(a, 1) &= 1 \\ \text{gcd}(a, b) &= \text{gcd}(b, a) \\ \text{gcd}(ax, bx) &= x * \text{gcd}(a, b) \\ \text{gcd}(a, ax + b) &= \text{gcd}(a, b) \\ \text{gcd}(a, b) = d &\Rightarrow \text{gcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1\end{aligned}$$

אלגוריתם אוקלידי למציאת מחלק משותף הגדול ביותר

פסאודו-קוד של האלגוריתם:

```

GCD( u , v )
1. if v = 0
2.   return u
3. else
4.   return GCD( v , u mod v )

```

$$\text{gcd}(u, v) \rightarrow u = v * q + r \quad (r = u \bmod v)$$

$$\text{gcd}(v, r)$$

דוגמא לחישוב:

$$\text{gcd}(175, 63) \quad .1$$

$$\text{gcd}(175, 63) \rightarrow 175 = 63 * 2 + 49$$

$$\text{gcd}(63, 49) \rightarrow 63 = 49 * 1 + 14$$

$$\text{gcd}(49, 14) \rightarrow 49 = 14 * 3 + 7$$

$$\text{gcd}(14, 7) \rightarrow 14 = 7 * 2 + 0$$

$$\text{gcd}(7, 0) = 7$$

$$\text{קיים שארית } 0, \text{ לנכון } \text{gcd}(175, 63) = 7$$

$$\text{gcd}(101, 44) \quad .2$$

$$\text{gcd}(101, 44) \rightarrow 101 = 44 * 2 + 13$$

$$\text{gcd}(44, 13) \rightarrow 44 = 13 * 3 + 5$$

$$\text{gcd}(13, 5) \rightarrow 13 = 5 * 2 + 3$$

$$\text{gcd}(5, 3) \rightarrow 5 = 3 * 1 + 2$$

$$\text{gcd}(3, 2) \rightarrow 3 = 2 * 1 + 1$$

$$\text{gcd}(2, 1) = 1$$

## מציאת הופכי באמצעות אלגוריתם אוקלידיים

בכדי להשתמש באלגוריתם זה חשוב להבין:

אם  $\text{gcd}(a, b) = d$  מחלק את  $a$  ואת  $b$  אזי קיימים שלמים  $s, t$  כך ש:

$$d = a * s + b * t$$

אם מתקיים כי  $1 = \text{gcd}(a, b)$  או באמצעות אלגוריתם זה ניתן למצוא את  $t, s$  כך ש:

$$1 = a * s + b * t$$

למעשה  $s$  הוא הופכי כלפי של  $a$  מודולו  $b$  אחר :

$$as = 1 \pmod{b}$$

מבנה האלגוריתם – נניח כי נרצה למצוא  $a^{-1} \pmod{m}$ , כאשר אנחנו מציגים את כל המשוואות תהליך החישוב.

1. נחשב  $\text{gcd}(a, m)$  באמצעות אלגוריתם אוקלידי, כאשר אנחנו מציגים את כל המשוואות תהליך החישוב.

2. אם מצאנו כי  $\text{gcd}(a, m) \neq 1$  אז לא קיים הופכי.

3. אם  $\text{gcd}(a, m) = 1$ , נverb על המשוואות הכל מהמשווהה שבה מצאנו שארית 1

( $r=1$ )  $a = b * q + r$ , עבור כל משווהה נבודד באגף אחד את השארית, באופן רקורסיבי החל מהמשווהה האחרון שמצאנו וציב שאריות אלו במשוואות שהיו לפניה. נשים לב כי בכל איטרציה נשאיר את השלמים של

האיטרציה הבאה, ככלمر לא נבצע חיבור של 2 שותפות שקיבלו.

דוגמא לenthalיך תמחיש בצורה טוביה את האלגוריתם:

$$\text{נרצה למצוא } 44^{-1} \pmod{101}$$

ראשית נחשב את  $\text{gcd}(101, 44)$

$$\text{gcd}(101, 44) \rightarrow 101 = 44 * 2 + 13$$

$$\text{gcd}(44, 13) \rightarrow 44 = 13 * 3 + 5$$

$$\text{gcd}(13, 5) \rightarrow 13 = 5 * 2 + 3$$

$$\text{gcd}(5, 3) \rightarrow 5 = 3 * 1 + 2$$

$$\text{gcd}(3, 2) \rightarrow 3 = 2 * 1 + 1$$

$$\text{gcd}(2, 1) = 1$$

$$\begin{aligned} 1 &= 3 - 1 * 2 = 3 - 1 * (5 - 1 * 3) = -1 * 5 + 2 * 3 = -1 * 5 + 2 * (13 - 5 * 2) \\ &= 2 * 13 - 5 * 5 = 2 * 13 - 5 * (44 - 13 * 3) = -5 * 44 + 17 * 13 \\ &= -5 * 44 + 17(101 - 44 * 2) = 17 * 101 - 39 * 44 \end{aligned}$$

לאחר פעולות האלגוריתם קיבלנו כי :

$$1 = 17 * 101 - 39 * 44 \pmod{101} = -39 * 44 \pmod{101} = 62 * 44 \pmod{101}$$

מכאן קיבלנו כי :

$$44^{-1} \pmod{101} = 62$$

## משפט אוילר

אם  $a$  שלם זר למספר טבעי  $n$  אז:

$$a^{\theta(n)} \equiv 1 \pmod{n}$$

( $\theta$ ) זאת פונקציה אוילר זהו מספר המספרים הטבעיים הקטנים ל- $n$  הזרים לו.

פירוק של  $n$  למספרים ראשוניים:

$$\theta(n) = n * \left(1 - \frac{1}{p_1}\right) * \left(1 - \frac{1}{p_2}\right) * \dots * \left(1 - \frac{1}{p_k}\right)$$

לדוגמה:

$$10 = 2 * 5$$

$$\theta(10) = 10 * \left(1 - \frac{1}{5}\right) * \left(1 - \frac{1}{2}\right) = 10 * \frac{4}{5} * \frac{1}{2} = 4$$

לכן נוכל להשתמש במספט אוילר ולומר כי:  $\text{gcd}(7, 10) = 1$

$$7^{\theta(10)} = 1 \pmod{10}$$

$$7^4 = 1 \pmod{10}$$

## משפט פרמה הקטן

זהה הרחבה למשפט אוילר: יהי  $p$  מספר ראשוני, אם  $a$  שלם זר ל- $p$ , אז :

$$a^{p-1} \equiv 1 \pmod{p}$$

## מציאת הופכי באמצעות משפט אוילר

באמצעות משפט אוילר ניתן למצוא הופכי, בנוסף באמצעותו ניתן להקל על חישוב מודולו במספר בחזקה גדולה.

דוגמא:

$$\text{נרצה למצוא הופכי ל-7 ביחס למודולו } 25, \text{ כלומר } 7^{-1} \text{ mod } 25.$$

נניח כי בדקנו כי אכן קיים הופכי ל-7 ביחס למודולו 25, אך משפט אוילר נסיק כי

$$7^{\theta(25)} = 1 \text{ mod } 25$$

$$7^{\theta(25)-1} * 7 = 1 \text{ mod } 25$$

נניח כי חישבנו ומצאנו:  $\theta(25) = 20$ .

$$7^{20-1} * 7 = 1 \text{ mod } 25$$

$$7^{19} * 7 = 1 \text{ mod } 25$$

מכיוון שיש הופכי ניתן לכפול בו:

$$7^{19} * 7 * 7^{-1} = 1 * 7^{-1} \text{ mod } 25$$

כלומר קיבלנו כי:

$$7^{-1} = 7^{19} \text{ mod } 25$$

$$\text{נותר רק לחשב מהו } 7^{19} \text{ mod } 25$$

לרוב נחשב זו ע"י חילוק החזקה לחולקים שאת הפתרון שלHon קל לחשב:

$$7^{19} \text{ mod } 25 = 7^{2^9} * 7 \text{ mod } 25$$

$$7^2 \text{ mod } 25 = 49 \text{ mod } 25 = -1$$

$$7^{2^9} * 7 \text{ mod } 25 = (-1)^9 * 7 \text{ mod } 25 = -7 \text{ mod } 25 = 18$$

מכאן קיבלנו כי:

$$7^{-1} = 7^{19} \text{ mod } 25 = 18$$

## משפט השאריות הסיניים

בהתנן מערכת משוואות מודולאריות

$$\begin{cases} x \equiv r_1 \text{ mod } m_1 \\ x \equiv r_2 \text{ mod } m_2 \\ \dots \\ x \equiv r_k \text{ mod } m_k \end{cases}$$

כאשר כל ה-  $m_i$  זרים זה לזו, למערכת יש פתרון ייחיד מודולו  $m_1 * m_2 * \dots * m_k$  והוא

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \dots + M_k s_k r_k$$

כאשר לכל  $i$   $M_i * s_i \equiv 1 \text{ mod } m_i$  והוא הפתרון היחיד למשוואה  $M_i = \frac{m_1 * m_2 * \dots * m_k}{m_i}$

משוואה זו שקולה למשוואה  $s_i = M_i^{-1} \text{ mod } m_i$

כלומר – עליינו לפתור תחילה את המערכת

$$\begin{cases} M_1 * s_1 \equiv 1 \text{ mod } m_1 \\ M_2 * s_2 \equiv 1 \text{ mod } m_2 \\ \dots \\ M_k * s_k \equiv 1 \text{ mod } m_k \end{cases}$$

דוגמא:

$$\begin{cases} x^b = x \text{ mod } 19 \\ x^b = x \text{ mod } 17 \end{cases}$$

נשתמש במשפט השאריות הסיניים:

$$\begin{array}{ll} m_1 = 19 & m_2 = 17 \\ M_1 = 17 & M_2 = 19 \end{array}$$

$$c_1 = M_1^{-1} \bmod m_1 , \quad c_2 = M_2^{-1} \bmod m_2$$

$$c_1 = M_1^{-1} \bmod m_1 = 17^{-1} \bmod 19$$

ראשית נבדוק אם קיימים זרים, נבדוק האם 17 ו-19 הם זרים, מכיוון ששניהם מספרים ראשונים אז  $\gcd(19,17)=1$ , ולכן לפי משפט אולר ניתן גם להסיק כי :

$$17^{\theta(19)} \equiv 1 \bmod 19$$

$$17^{\theta(19)-1} * 17 \equiv 1 \bmod 19$$

$$17^{18-1} * 17 \equiv 1 \bmod 19 \quad (\theta(19) = 18)$$

$$17^{17} * 17 \equiv 1 \bmod 19$$

כלומר קיבלנו כי :

$$17^{-1} \equiv 17^{17} \bmod 19 \equiv (17^2)^8 * 17 \equiv 289^8 * 17 \equiv 4^8 * 17 \equiv 5 * 17 \equiv 9 \bmod 19$$

$$17^{-1} \equiv 9 \bmod 19$$

$$c_2 = M_2^{-1} \bmod m_2 = 19^{-1} \bmod 17 = 2^{-1} \bmod 17$$

(כי 17 ראשוני) ולכן לפי משפט אולר ניתן גם להסיק כי :

$$12^{\theta(17)} \equiv 1 \bmod 17$$

$$12^{\theta(17)-1} * 12 \equiv 1 \bmod 17$$

$$\theta(17) = 16$$

$$12^{16-1} * 12 \equiv 1 \bmod 17$$

$$12^{15} * 12 \equiv 1 \bmod 17$$

כלומר קיבלנו כי :

$$\begin{aligned} 2^{-1} &\equiv 12^{15} \bmod 17 = 12^{2^7} * 12 = 8^7 * 12 = 8^{2^3} * 8 * 12 = 64^3 * 96 = 13^3 * 11 = 4 * 11 \\ &= 10 \end{aligned}$$

$$2^{-1} \equiv 10 \bmod 17$$

קיבלונו כי :

$$m_1 = 19 \quad m_2 = 17$$

$$M_1 = 17 \quad M_2 = 19$$

$$c_1 = 9 \quad c_2 = 10$$

$$x \equiv r_1 * M_1 * c_1 + r_2 * M_2 * c_2 \equiv r_1 * 17 * 9 + r_2 * 19 * 10 \equiv 153r_1 + 190r_2 \bmod 19 * 17$$

## אלגוריתמים של הצפנה

נדיר הגדרות בסיסיות שאיתן נשמש עבור כל סוג של אלגוריתם הצפנה:

**M** מילה שיש להצפין. (לפעמים נרשם  $x$ )  
**k** מפתח הצפנה.  
**c** מילה מוצפנת. (לפעמים נרשם  $y$ )  
 **$E_k(M)$**  פונקציה הצפנה שמצפינה את מילה  $M$  לפי מפתח  $k$ .  
 **$D_k(c)$**  פונקציה פיענוחה שפענחת את  $c$  לפי מפתח  $k$ .

### אלגוריתם הפצנה סימטרי

באלגוריתם זה מפתח הצפנה ישמש גם כמפתח הפיענוח./algoritmim או השולח והמקבל חיבים מראש להסכים בינויהם על מפתח. המפתח חייב להיות פרט פרטי השולח והמקבל, אחרת יהיה ניתן לעזוב את המידע. ישנו שני סוגי של אלגוריתמים סימטריים:  
 1. Stream algorithms – בכל פעם מגיע בית (או יותר) ומצביעים רק אותה.  
 2. Block algorithms – בכל פעם מצביעים קבוצה (בלוק) של ערכים בו זמן.

### הודעה בלתי מוסתרת - Unhidden messages

הודעה  $x$  תיקרא הודעה בלתי מוסתרת אם מתקיים:

$$E_k(x) = x$$

### התקפה איטרטיבית - The Iterative Attack

נניח כי ישנו אלגוריתם הצפנה ידוע, אם ידוע לנו  $c$  ונרצה למצוא את  $M$  ניתן לבצע התקפה איטרטיבית. בהתקפה זו אנחנו בכל פעם נצפן בעורת האלגוריתם את הטקסט המוצפן עד שנגיע לטקסט בМОצפן המקורי. נתון  $c_0$ 想找  $M$  כך ש:  $E_k(M) = c_0$ . אוז נחשב:

$$E_k(c_0) = c_1$$

$$E_k(c_1) = c_2$$

$$E_k(c_2) = c_3$$

...

$$E_k(c_j) = c_{j+1}$$

...

$$E_k(c_n) = c_0$$

במצב זהמצאנו את  $M = c_n$  שבעזרו קיבלנו  $c_0 = E_k(M)$ . אנחנו נצליח למצוא את  $M$  מכיוון שאלגוריתם ההצפנה נותן לנו ערכים סופיים בצורה מעגלית, אך לאחר זמן מה נצליח לקבל את ההודעה.

נשים לב שאנו מקבלים רק מידע על איזה הודעה הצפנו ולא מהו המפתח.

### One Time Pad

ישו 2 משתמשים Alice ו-Bob שורצים לדבר ביניהם. הרעיון סביב השיטה הנ"ל הוא שלשניהם תהיה רשות מפתחות גדולות, כך שבכל איטרציה המפתח יוחלף באחריו בראשימה. ההצפנה והפענוח יהיה ע"י פעולה XOR בין המפתח ל- Plaintext (ההודעה שאותה נרצה להצפין) רשות המפתחות יכולה להתකבל במספר אופנים:  
 • לשני הצדדים יש את אותה מכונה שגירילה באופן זהה מספרים אקראיים.

- לשני הצדדים יכול להיות נוסחת שעלה סמך המפתח הקודם בונה מפתח חדש, לדוגמה:  $a * k_{i-1} + b \mod n$ .
- לשני הצדדים יש טבלה סטטית המכילה מפתחות, שני הצדדים יכולים להצפין טקסטים כאורך הטבלה.

תרונות:

- השיטה לא רגישה להתקפה סטטיסטית.
- השיטה מבטיחה Perfect Secrecy

חרוגות:

- צריך לבצע סyncron בין שני הצדדים בכדי לדעת איזה מפתח הוא הנכחי.
- צריך למצוא שיטה בכדי להסכים על טבלת המפתחות.
- השיטה נהייה בעייתית במיוחד כאשר יש מספר רב של משתמשים באותו הצופן. ראשית צריך לחלק לנולם את אותה טבלה מה שמעלה את הסיכוי לחשיפתה ובנוסף כאשר צריך צורך לשנות אותה צריך לעדכן את כלום בעבר טבלה.

## – אלגוריתם הזזה – Shift Cipher

יהיה  $a$  ב כלשו בגודל  $n$ , (נניח כי השתמש בא"ב האנגלית המכיל 26 אותיות) לכל אות בא"ב נקזה מספר בטוחה  $[0, n-1]$ .  
זהו סוג של צופן החלפה שככל אות בטקסט מוחלפת על ידי אות הנמצאת בהיסט קבוע כלשהו ממנו באלף-בית  
מפתח היה  $1 \leq k \leq n-1$ .

$$\begin{aligned} E_k(x) &= (x + k) \mod n \\ D_k(y) &= (y - k) \mod n \end{aligned}$$

הערה: עבור  $k = 3$  האלגוריתם יקרא "צופן קיסר" (Caesar Cipher)

### התקפות על האלגוריתם

- בהינתן  $M = c = E_k(M)$  ניתן לפרק את האלגוריתם ע"י ביצוע ברוט פורס למצוא את ה- $k$  המתאים, בכך שנעבור על כל ה- $k$  האפשריים.
- התקפה סטטיסטית - ניתן לעשות מיפוי סטטי של אותיות שהתדריות שהן מופיעות בשפה גדול. לדוגמה בשפה האנגלית האות e היא בעלת התדריות הגבוהה ביותר, לכן נעבור על כל טקסט מוצפן ונחש את האות בעלת התדריות הגבוהה ביותר ונניח שהיא e, בכך נוכל למצוא את k בקלות.

## – אלגוריתם לינארי – Linear Cipher

באלגוריתם זה המפתח יהיה זוג של מספרים  $(a, b) \in Z_n$  כאשר  $k = a$  והוא  $E_k(x) = (ax + b) \mod n$   
נשיב לב שכדי לפענה את ההודעה, חיבת להיות פונקציה הופכית, זה יקרה אם קיים הופכי לא- $a$  ביחס למודלו  $D_k(y) = a^{-1}(y - b) \mod n$

$$\begin{aligned} D_k(y) &= a^{-1}(y - b) \mod n = a^{-1}((ax + b) \mod n - b) \mod n \\ &= a^{-1}(ax + b - b) \mod n = a^{-1}ax \mod n = x \mod n \\ &a^{-1}a \mod n = 1 \end{aligned}$$

זה כמובן מתקיים כאשר  $a^{-1}a \mod n = 1$

נשים לב כי ערך  $a$  יכול להיות כל מספר שנבחר והוא לא משנה לנו בפיענוחו لكن קיימים חאפשויות.  
מכאן שמספר הערכים התקנים של  $a$  שנייתן לבחורו הוא כל הערכים שוררים לא- $n$ , מספר זה שקול ל- $\theta(n)$   
ומכאן שכך האפשרויות של המפתחות הקיימים עבור  $Z_n$  הוא:  $n * \theta(n)$ .

דוגמא:  $n = 26$ ,  $k = (7,3)$   
 $7^{-1} = 15 \text{ mod } 26$

$$E_k(x) = (7x + 3) \text{ mod } 26$$

$$D_k(y) = 15(y - 3) \text{ mod } 26 = 15y - 45 \text{ mod } 26 = 15y - 19 \text{ mod } 26$$

התקפות על האלגוריתם

- בהינתן 2 הודעות בלתי מוצפנות יחד עם ההצפנה שלהם, ניתן להרכיב מערכת משוואות לינאריות המכילה 2 משוואות עם שני נעלמים ובכך למצוא את  $a, b$ .

$$(ax_1 + b) \text{ mod } n = y_1$$

$$(ax_2 + b) \text{ mod } n = y_2$$

סוגי התקפות:

– בסוג התקפה זה אנחנו נבחר הודעות בעלי החיבות מיחודה שבuzzerten ניתן לפרוץ את Chosen plaintext •

האלגוריתם יחסית בקלות, לדוגמא אם נבחר  $0 = x$  אז נוכל לשירות למצוא את  $b$ .

$$E_k(0) = (a * 0 + b) \text{ mod } n = b \text{ mod } n$$

מציאת הודעות בלתי מוסתרות

עבור צופן לינארי  $x = (ax + b) \text{ mod } n$   $E_k(x) = (ax + b) \text{ mod } n$  כלומר נקבל כי

$$(a - 1)x \text{ mod } n = -b$$

קיים מושואה לינארית, יכול להיות שאין לה פתרון, כמו פתרונות או פתרון יחיד.

נחשב את  $(a - 1, n) = g = \text{gcd}(a - 1, n)$ .

אין פתרון - אם  $g$  לא מחלק את  $b$

יש  $g$  פתרונות – אם  $g$  שונה מ-1 יש לנו  $g$  פתרונות.

איך נמצא אותם:

$$\frac{(a-1)}{g}x \text{ mod } \frac{n}{g} = -\frac{b}{g}$$

נרכיב מושואה חדשה, נчисל  $\frac{n}{g}$ .

$$\left(\frac{(a-1)}{g}\right)^{-1} \text{ mod } \frac{n}{g} = b^{-1}$$

או נכפול את המושואה שקבענו בהופכי:

$$b^{-1} * \frac{(a-1)}{g}x \text{ mod } \frac{n}{g} = b^{-1} * -\frac{b}{g}$$

$$x = \left(b^{-1} * -\frac{b}{g}\right) \text{ mod } \frac{n}{g}$$

קיבלנו ערך של הודעה בלתי מוסתרת  $x$ ,  
 nimim leb ci kiblano paturon achad, kiblano zotzai ci be'atzem paturon be'uya acheret mahava be'notona, lken shear haftaronot shel be'uya  
 ha'mekorit yihya:

$$x_t = x + \frac{n}{g} * t$$

רץ על מספר הפתרוןות האפשריים.

דוגמא: נמצא את הודעה בלתי מוסתרת עבור  $27$   
 $E_K(x) = (11x + 3) \text{ mod } 27 = x$

נפתרו את המשוואה הבאה:

$$(11x + 3) \text{ mod } 27 = x$$

$$10x \equiv -3 \text{ mod } 27 \equiv 24 \text{ mod } 27$$

מספר הפתרוןות למשואה הוא  $\text{gcd}(27, 10) = 1$ .  
 נחפש את  $10^{-1} \text{ mod } 27$ .

נמצא את האיבר ההופכי באמצעות אלגוריתם אוקלייד.

ראשית נחשב את ה- $\text{gcd}(27, 10)$

$$\begin{aligned}
\gcd(27, 10) &\rightarrow 27 = 10 * 2 + 7 \\
\gcd(10, 7) &\rightarrow 10 = 7 * 1 + 3 \\
\gcd(7, 3) &\rightarrow 7 = 3 * 2 + 1 \\
\gcd(3, 1) &= 1 \\
1 &= 7 - 2 * 3 = 7 - 2(10 - 1 * 7) = -2 * 10 + 3 * 7 = -2 * 10 + 3(27 - 2 * 10) \\
&= 3 * 27 - 8 * 10
\end{aligned}$$

לאחר פעולות האלגוריתם קיבלנו כי :

$$1 \equiv 3 * 27 - 8 * 10 \pmod{27} \equiv -8 * 10 \pmod{27} \equiv 19 * 10 \pmod{27}$$

מכאן קיבלנו כי :

$$10^{-1} \pmod{27} \equiv 19$$

$$\text{נכפול את המשווה } 10x \equiv 24 \pmod{27}$$

$$10^{-1} * 10x \equiv 10^{-1} * 24 \pmod{27}$$

$$x \equiv 19 * 24 \pmod{27} \equiv 456 \pmod{27} \equiv 24 \pmod{27}$$

$$\text{מספר הפתרונות למשווה יחיד } , \gcd(27, 10) = 1 , \text{ הוא } 24$$

### – אלגוריתם אקספוננציאלי . Exponential Cipher

באלגוריתם זה המפתח הוא זוג  $(a, b)$  הנקרא  $k$  והצפנה תהיה:

$$E_k(x) = (ax^b) \pmod{n}$$

הפענוח יהיה:

$$D_k(y) = (a^{-1}y)^c \pmod{n}$$

$$c = b^{-1} \pmod{\theta(n)}$$

**הערות חשובות:**

לא כל זוג מספרים יכול להיות מפתח. ברור כי כדי שזוג יהיה מפתח חייב להיות לפונקציה שהוא מרכיב פונקציה הופכית, והוא מתקיים כאשר:

- קיים הופכי לא- $a$  ביחס למודולו  $n$ . כלומר:

$$\exists a^{-1} \pmod{n} \Leftrightarrow \gcd(a, n) = 1$$

נשים לב כי מספר האברים הזוגים  $\theta(n)$  הם :  $\theta(\theta(n))$ , ולכן יש  $\theta(\theta(n))$  ערכים אפשריים לא- $a$ .

- קיים הופכי לא- $b$  ביחס למודולו  $\theta(n)$ . כלומר:

$$\exists b^{-1} \pmod{\theta(n)} \Leftrightarrow \gcd(b, \theta(n)) = 1$$

נשים לב כי מספר האברים הזוגים  $\theta(\theta(n))$  הם :  $\theta(\theta(\theta(n)))$ , ולכן יש  $\theta(\theta(\theta(n)))$  ערכים אפשריים לא- $b$ .

מכאן שמספר הזוגות היילולים להיות מפתח הם:  $\theta(n) * \theta(\theta(n))$

דוגמא:

$$\begin{aligned}
D_k(y) &= (18^{-1}y)^c \pmod{31} \quad \text{נתון נוסחת צופן מעירכי } E_K(x) = (18x^{13}) \pmod{31} \\
&\quad \text{נמצא את נוסחת הפענוח, } c = 13^{-1} \pmod{\theta(31)}
\end{aligned}$$

נចטרך למצוא את:

$$18^{-1} \pmod{31}$$

$$13^{-1} \pmod{30}$$

נמצא את האיבר ההפוך  $18^{-1} \pmod{31}$  באמצעות אלגוריתם אוקלידי.

ראשית נחשב את ה- $\gcd(31, 18)$

$$\begin{aligned}
\gcd(31, 18) &\rightarrow 31 = 18 * 1 + 13 \\
\gcd(18, 13) &\rightarrow 18 = 13 * 1 + 5 \\
\gcd(13, 5) &\rightarrow 13 = 5 * 2 + 3 \\
\gcd(5, 3) &\rightarrow 5 = 3 * 1 + 2 \\
\gcd(3, 2) &\rightarrow 3 = 2 * 1 + 1 \\
\gcd(2, 1) &= 1
\end{aligned}$$

$$\begin{aligned}
1 &= 3 - 1 * 2 = 3 - 1(5 - 1 * 3) = -1 * 5 + 2 * 3 = -1 * 5 + 2(13 - 2 * 5) = 2 * 13 - 5 * 5 \\
&= 2 * 13 - 5 * (18 - 1 * 13) = -5 * 18 + 7 * 13 = -5 * 18 + 7(31 - 1 * 18) \\
&= 7 * 31 - 12 * 18
\end{aligned}$$

לאחר פעולות האלגוריתם קיבלנו כי :  
 $1 \equiv 7 * 31 - 12 * 18 \pmod{31} \equiv -12 * 18 \pmod{31} \equiv 19 * 18 \pmod{31}$   
 מכאן קיבלנו כי :  
 $18^{-1} \pmod{31} \equiv 19$

מצא את האיבר ההפכי  $13^{-1} \pmod{30}$  באמצעות אלגוריתם אוקלייד.  
 $\text{gcd}(30, 13)$

$$\begin{aligned}
\text{gcd}(30, 13) &\rightarrow 30 = 13 * 2 + 4 \\
\text{gcd}(13, 4) &\rightarrow 13 = 4 * 3 + 1 \\
\text{gcd}(4, 1) &= 1
\end{aligned}$$

$$1 = 13 - 3 * 4 = 13 - 3(30 - 2 * 13) = -3 * 30 + 7 * 13$$

לאחר פעולות האלגוריתם קיבלנו כי :  
 $1 \equiv -3 * 30 + 7 * 13 \pmod{30} \equiv 7 * 13 \pmod{30}$   
 מכאן קיבלנו כי :  
 $13^{-1} \pmod{30} \equiv 7$   
 מצאנו את  $c = 7$  ואת  $a = 19^{-1}$ , מכאן שימושה הפינונה תוויה:  
 $D_k(y) = (19y)^7 \pmod{31}$

#### מציאת הודעות בלתי מוסתרות

נשים לב כי תמיד קיים פתרון טריויאלי  $x = 0$ .  
 עבור  $0 \neq x$  :

אם  $a$  ראשון או עבור כל  $x$  קיים הופכי ביחס למודולו  $a$ , ולכן ניתן לכפול את המשווה בהופכי זה ולקבל:  
 $ax^{b-1} = 1 \pmod{a}$   
 מצא את הופכי של  $a$  ביחס למודולו  $a$  וככפול בו את המשווה נקבל:  
 $x^{b-1} = a^{-1} \pmod{a}$   
 למשווה הזאת יש מספר פתרונות, הדרך הטובה ביותר למציאו אותן הוא באמצעות יוצר.  
 נגיד  $g \in Z_n$  יוצר של חבורת  $Z_n$ . נסמן  $g = g^t$ ,  $x = g^a$ ,  $a = g^t$ ,  $t$ . נציג וביקבב:  
 $ax^{b-1} = 1 \pmod{a} \rightarrow g^a g^{t(b-1)} = g^0 \pmod{a}$   
 מכאן נקבל כי :  $a + t(b-1) = 0 \pmod{\theta(n)}$  (נובע משפט פרמה הקטן).

לאחר שנמצא את היוצר, נמצא את  $a = g^a \pmod{a}$ . (נשים לב כי למציאו את  $a$  זאת בעיה לוגריתמים שהחישבו המודולרי לא יודע להתמודד איתה, שכן לפחות מה שיש לעשות זה לזרוק מספרים ולהתפלל שימושו יתרוף)  
 לאחר שמצאנו את  $a$  קיבלנו משווה בנעלם אחד,  $t$ . נמצא את  $t$  ונציב אותו ב- $n = g^t \pmod{a}$  כדי לקבל את כל ההודעות הבלתי מוסתרות.

#### איך נמצא את היוצר

נחפש את כל המחלקים של  $(n)^\theta$ , נניח כי הם  $n_l, n_1, n_2, \dots, n_k$ . נבחר מספרים החל מ-2 והלאה, כל מספר זה נעללה בחזקה של כל המחלקים של  $(n)^\theta$  מודולו  $n$ , נניח כי בחרנו ב- $k$  איזי נחשב :

אם מקבל מספר שונה מ-1 עבור כל חישוב, איזי יוצר, אחרת הוא לא יוצר ונמשיך לחפש הלאה.  
 נבין כי אם קיבלנו 1 לא משנה באיזו חזקה נבעור יישורות למספר הבא.  
 נשים לב כי ישנו מספר יוצרים אפשריים, סה"כ מספר היוצרים הם :  $\theta(\theta(n))$   
 איך נמצא את שאר היוצרים, נעללה את היוצר שמצאנו בחזקה של כל האיברים הזוגיים  $l-1, l, \dots, n$ .

## Substitution Ciphers

כל אות באلف הבית תוחלף באות אחרת. ליתר דיוק, תמורה של הא"ב תיבחר ומופעלת על הטקסט. צפוני: הוזה, לינארו ומערכותיהם דוגמאות של צפוני חילוף. מכיוון שהודעה מוצפנת שומרת הסטטיסטייה של מופע של אותיות בשפה, ניתן תדרות (התקפה סטטיסטית) הוא דרך ייעילה לשבור צפנים אלו.

## Block Ciphers

"שנム אלגוריתמי החלפה המחליפים בדיקות אחת, כלומר את הטקסט המקורי תוחלף עם אות אחרת בטקסט המוצפן. בغالל תכונה זו ניתן לבצע התקפה סטטיסטית עליהם. נרצה למנוע התקפה זו, לשם כך בכל פעם נקודד בлок של אותיות. הרבה אלגוריתמים בкриptoלוגיה מקודדים בЛОקים ולא אותיות בודדות, לדוגמה: DES , AES , Hill .

## Hill Cipher

נתון טקסט  $X = (x_1, x_2, \dots, x_k)$  נתולק את הבלוק זה לתחי בלוקים  $(a_1, a_2, \dots, a_m)$ .  
 כך שבלוק הוא בגודל  $m$ ,  $x_1 = (a_1, \dots, a_m), x_2 = (a_{m+1}, \dots, a_{2m})$ .  
 אם  $|K|$  לא מחלק ב- $m$  אז בבלוק האחרון  $a_k$  נרפס אפסים לקבל גודל  $m$  של הבלוק.  
 באלגוריתם זה המפתח יהיה מטריצה ריבועית  $K_{m \times m}$ .  
 ההצפנה תהיה:

$$E_K(\vec{x}) = \vec{x} * K \bmod n$$

הפענוח יהיה:

$$E_K(\vec{y}) = \vec{y} * K^{-1} \bmod n$$

לא כל מטריצה יכולה להיות מפתח, כדי שמטריצה כלשהי תהיה מפתח חייב להתקיים:  
 $\exists K^{-1} \bmod n \Leftrightarrow \gcd(|K|, n) = 1$

כלומר אם הדטרמיננטה של  $K$  זורה לח אויל- $K$  קיימת מטריצה הופכית.  
 מספר המפתחות האפשריים אלו הם מספר המטריצות הפיכות במודולו  $n$ .

**דוגמא:**

נתון אלפבית אנגלי בן 26 אותיות. השתמש בצופן היל (HILL) עם גודל בלוק  $m=3$  ונתקבל טקסט מוצפן:  
 $F B R T L W U G A J Q I N Z T H H X T E P H B N X S W$

מצא את מטריצת המפתח ואת הטקסט המקורי אם ידוע שהtekסט המקורי מסתומים ב- **JAMESBOND** ?

נתון טקסט מוצפן  $\vec{y}$  ונתון חלק מ- $\vec{x}$ , נצטרכן למצוא את מטריצת  $K$ ,

ונגיד את מטריצת  $K = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ , נרצה למצוא את כל הנעלמים.

בכדי לעשות זאת נצטרכן למצוא 9 מושוואות לניאירות שלא קיימת ביניהן תלות. נמצאו מושוואות אלו באמצעות הטקסט המקורי והמוצפן הנתון לנו.

נבחר בבלוקים הבאים :

$x$	...	...	J	A	M	E	S	B	O	N	D
$y$	...	X	T	E	P	H	B	N	X	S	W

$$(O, N, D) \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = (X, S, W)$$

$$(E, S, B) \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = (H, B, N)$$

$$(J, A, M) \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = (T, E, P)$$

נאחד את כל נתונם וنمיר את האותיות למספרים:

$$\begin{pmatrix} J & A & M \\ E & S & B \\ O & N & D \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} T & E & P \\ H & B & N \\ X & S & W \end{pmatrix}$$

<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>	<b>K</b>	<b>L</b>	<b>M</b>
0	1	2	3	4	5	6	7	8	9	10	11	12
<b>N</b>	<b>O</b>	<b>P</b>	<b>Q</b>	<b>R</b>	<b>S</b>	<b>T</b>	<b>U</b>	<b>V</b>	<b>W</b>	<b>X</b>	<b>Y</b>	<b>Z</b>
13	14	15	16	17	18	19	20	21	22	23	24	25

$$\begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 19 & 4 & 15 \\ 7 & 1 & 13 \\ 23 & 18 & 22 \end{pmatrix}$$

מצא את K באופן הבא:

$$\begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix}^{-1}$$

ראשית נבדוק האם קיימים:

מצא את המטריצה ההפוכה בשיטת המשלים האלגברי:  
הnbsp; : **det**

$$\begin{aligned} \det\left(\begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix}\right) &= \left| \begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix} \right| \\ &= 9 \cdot (18 \cdot 3 - 1 \cdot 13) - 0 + 12 \cdot (4 \cdot 13 - 18 \cdot 14) \\ &= 9 \cdot 41 + 12 \cdot (-200) = -2031 \equiv 23 \text{ mod } 26 \end{aligned}$$

ובצע חישוב בשיטת המינורים:

$$\begin{aligned} \begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix} &\rightarrow \begin{pmatrix} 18 \cdot 3 - 1 \cdot 13 & -(4 \cdot 3 - 1 \cdot 14) & 4 \cdot 13 - 18 \cdot 14 \\ -(0 \cdot 3 - 12 \cdot 13) & 9 \cdot 3 - 12 \cdot 14 & -(9 \cdot 13 - 0 \cdot 14) \\ 0 \cdot 1 - 12 \cdot 18 & -(9 \cdot 1 - 12 \cdot 4) & 9 \cdot 18 - 0 \cdot 4 \end{pmatrix} \\ &= \begin{pmatrix} 41 & 2 & -200 \\ 156 & -141 & -117 \\ -216 & 39 & 162 \end{pmatrix} \equiv \begin{pmatrix} 15 & 2 & 8 \\ 0 & 15 & 13 \\ 18 & 13 & 6 \end{pmatrix} \text{ mod } 26 \end{aligned}$$

נשחלף את המטריצה:

$$\begin{pmatrix} 15 & 0 & 18 \\ 2 & 15 & 13 \\ 8 & 13 & 6 \end{pmatrix}$$

נחלק את המטריצה המשוחלפת ב-**det** שמצאנו, חילוק זה הוא הכפלת בהופכי של **det**  
**det** = 23

נמצא  $23^{-1} \bmod 26$ , באמצעות אלגוריתם אוקלידיים:

$$26 = 23 * 1 + 3$$

$$23 = 3 * 7 + 2$$

$$3 = 2 * 1 + 1$$

$$1 = 3 - 2 * 1 = 3 - 1(23 - 3 * 7) = 3 * 8 - 23 * 1 = -23 + 8 * (26 - 23 * 1)$$

$$= 8 * 26 - 9 * 23$$

$$8 * 26 - 9 * 23 \bmod 26 \equiv -9 * 23 \bmod 26 \equiv 1$$

$$23^{-1} \bmod 26 \equiv -9 \equiv 17$$

$$17 \begin{pmatrix} 15 & 0 & 18 \\ 2 & 15 & 13 \\ 8 & 13 & 6 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 255 & 0 & 306 \\ 34 & 255 & 221 \\ 136 & 221 & 102 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 21 & 0 & 20 \\ 8 & 21 & 13 \\ 6 & 13 & 24 \end{pmatrix} \bmod 26$$

לסיכום:  
קיבלו כי:

$$\begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 21 & 0 & 20 \\ 8 & 21 & 13 \\ 6 & 13 & 24 \end{pmatrix} \bmod 26$$

נמצא את מטריצה  $K$ :

$$\begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 19 & 4 & 15 \\ 7 & 1 & 13 \\ 23 & 18 & 22 \end{pmatrix}$$

כפול בהופכי שמצאנו:

$$\begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 9 & 0 & 12 \\ 4 & 18 & 1 \\ 14 & 13 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 19 & 4 & 15 \\ 7 & 1 & 13 \\ 23 & 18 & 22 \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 21 & 0 & 20 \\ 8 & 21 & 13 \\ 6 & 13 & 24 \end{pmatrix} \begin{pmatrix} 19 & 4 & 15 \\ 7 & 1 & 13 \\ 23 & 18 & 22 \end{pmatrix} = \begin{pmatrix} 859 & 444 & 755 \\ 598 & 287 & 679 \\ 757 & 469 & 787 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 1 & 7 \end{pmatrix} \bmod 26$$

מצאנו את מטריצת המפתחה:

$$K = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 1 & 7 \end{pmatrix}$$

בכדי למצוא את הטקסט המקורי יש ללחשב את  $K^{-1}$ :  
מצא את המטריצה ההופכית בשיטת המשלים האלגברי:

.1. נחשב  $\det K$ :

$$\begin{aligned} \det \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 1 & 7 \end{pmatrix} &= \left| \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 1 & 7 \end{pmatrix} \right| \\ &= 1 * (1 * 7 - 3 * 1) - 2 * (0 * 7 - 3 * 3) + 1 * (0 * 1 - 1 * 3) = 4 + 18 - 3 \\ &= 19 \end{aligned}$$

.2. נבצע חישוב בשיטת המינוראים:

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 1 & 7 \end{pmatrix} \rightarrow \begin{pmatrix} 1 * 7 - 3 * 1 & -(0 * 7 - 3 * 3) & 0 * 1 - 1 * 3 \\ -(2 * 7 - 1 * 1) & 1 * 7 - 1 * 3 & -(1 * 1 - 2 * 3) \\ 2 * 3 - 1 * 1 & -(1 * 3 - 1 * 0) & 1 * 1 - 2 * 0 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & 9 & -3 \\ -13 & 4 & 5 \\ 5 & -3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 4 & 9 & 23 \\ 13 & 4 & 5 \\ 5 & 23 & 1 \end{pmatrix} \text{ mod } 26$$

3. **נשחלה את המטריצה:**

$$\begin{pmatrix} 4 & 13 & 5 \\ 9 & 4 & 23 \\ 23 & 5 & 1 \end{pmatrix}$$

4. נחלק את המטריצה המשוחלפת ב-**det** שמצאנו, חילוק זה הוא הכפלה בהופכי של :

$$\det = 19$$

נמצא  $19^{-1} \text{ mod } 26$ , באמצעות אלגוריתם אוקליידי:

$$\gcd(26, 19) \rightarrow 26 = 19 * 1 + 7$$

$$\gcd(19, 7) \rightarrow 19 = 7 * 2 + 5$$

$$\gcd(7, 5) \rightarrow 7 = 5 * 1 + 2$$

$$\gcd(5, 2) \rightarrow 5 = 2 * 2 + 1$$

$$\gcd(2, 1) = 1$$

$$\begin{aligned} 1 &= 5 - 2 * 2 = 5 - 2 * (7 - 1 * 5) = -2 * 7 + 3 * 5 = -2 * 7 + 3 * (19 - 7 * 2) \\ &= 3 * 19 - 8 * 7 = 3 * 19 - 8 * (26 - 19 * 1) = 11 * 19 - 8 * 26 \\ &11 * 19 - 8 * 26 = 11 * 19 \text{ mod } 26 \\ &19^{-1} \text{ mod } 26 = 11 \end{aligned}$$

$$11 \begin{pmatrix} 4 & 13 & 5 \\ 9 & 4 & 23 \\ 23 & 5 & 1 \end{pmatrix} \text{ mod } 26 \equiv \begin{pmatrix} 44 & 143 & 55 \\ 99 & 44 & 253 \\ 253 & 55 & 11 \end{pmatrix} \text{ mod } 26 \equiv \begin{pmatrix} 18 & 13 & 3 \\ 21 & 18 & 19 \\ 19 & 3 & 11 \end{pmatrix}$$

לסיכום:  
קיבלו כי :

$$K^{-1} = \begin{pmatrix} 18 & 13 & 3 \\ 21 & 18 & 19 \\ 19 & 3 & 11 \end{pmatrix}$$

**הערה:**

אם המטריצה הייתה  $2 \times 2$  היינו מוצאים מטריצה הופכית באופן הבא:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

דרך נוספת עבור מטריצות יותר גדולות היא להציג מטריצה מימין למטריצה היחידה, לדרג את המטריצה החדשה כך שבעד שמאל נקבל מבנה של מטריצה יחידה.

**הערה חשובה:**

לפעמים נקבל  $\chi$  שהוא לא ראשוני, ולכן לא ניתן להשתמש בתנאי  $n$  ש  $|K| \neq 0 \text{ mod } n$  במקורה זה נhapus את כל המחלקים של  $\chi$  ונרכיב את מערכת המשוואות הבאה:  
נניח כי המחלקים של  $\chi$  הם :  $n_1, n_2 \dots n_k$

$$\gcd(|K|, n) = 1 \Leftrightarrow \begin{cases} |K| \neq 0 \text{ mod } n_1 \\ |K| \neq 0 \text{ mod } n_2 \\ \dots \\ |K| \neq 0 \text{ mod } n_k \end{cases}$$

עכשו נוכל להשתמש בתנאי כך שכל המשוואות יתקיימו.

לדוגמא:

$$\text{בצופן HILL עם מטריצה-מפתח } \begin{pmatrix} 2a & 13 \\ 15 & a \end{pmatrix} \text{ מעל אלף-בית האנגלית בן 26 אותיות.}$$

עבור איזה ערכים של  $a$  המטריצה מגירה צופן?  
מטריצת  $K$  יכולה להיות מפתח כאשר קיימים  $K^{-1}$  (כלומר  $K$  הפיכה)

$$\exists K^{-1} \text{ mod } 26 \Leftrightarrow \gcd(|K|, 26) = 1 \Leftrightarrow |K| \neq 0 \text{ mod } 26$$

$n$  ראשון : הראשית נחשב את  $\det(K)$

$$\det\begin{pmatrix} 2a & 13 \\ 15 & a \end{pmatrix} = 2a * a - 13 * 15 = 2a^2 - 195 \equiv (2a^2 + 13) \text{ mod } 26$$

26 לא ראשוני לכן לא נוכל להשתמש בתנאי ש:  $|K| \neq 0 \text{ mod } 26$   
המחלקים של 26 הם 2, 13: לכן, אם מתקיים  $1 = \gcd(|K|, 26) = |K|$  לא מחלק ב-2 או ב-13,  
כלומר:

$$\gcd(|K|, 26) = 1 \Leftrightarrow \begin{cases} |K| \neq 0 \text{ mod } 13 \\ |K| \neq 0 \text{ mod } 2 \end{cases}$$

עכשו ניתן להשתמש בתנאי כך ש: נמצא  $a$  ו  $|K| \neq 0 \text{ mod } 13$  -  $a_0 \neq 0 \text{ and } a_1 \neq 13$

$$|K| \neq 0 \text{ mod } 13$$

$$(2a^2 + 13) \neq 0 \text{ mod } 13$$

$$(2a^2) \neq 0 \text{ mod } 13$$

$$a_0 \neq 0 \text{ and } a_1 \neq 13$$

$$|K| \neq 0 \text{ mod } 2$$

$$(2a^2 + 13) \neq 0 \text{ mod } 2$$

$$(13) \neq 0 \text{ mod } 2$$

לכל  $a$ ,

מכאן ש: מטריצת  $K$  הפיכה כאשר

$$a_0 \neq 0 \text{ and } a_1 \neq 13$$

לסיכום:

מטריצת  $K$  תהיה מפתח עבור כל ערכי  $a$ , פרט ל: 0, 13

מציאת הודעות בלתי מוסתרות

$$x * K = x \text{ mod } n$$

$$x * (K - I) = 0 \text{ mod } n$$

• נשים לב כי תמיד קיימים פתרון טריוויאלי  $x = 0$ .

• אם  $-K$  קיים ערך עצמי אחד  $= \lambda$  אז יש לו בנוסף הודעות בלתי מוסתרות לא טריוויאליות.

בשביל למצואו ע"ע מחשבים  $0 = K - \lambda I$ , נשים לב כי אם נציג  $\lambda = 0$  ונבדוק אם  $0 = |K - I|$  אזי, אם מתקיים השוויון:  $\lambda = 0$  הוא ע"ע של  $K$ .

אם  $0 \neq |K - I|$  אז  $|K - I|$  הפיכה כלומר ניתן לומר כי יש פתרון ייחודי והוא טריוויאלי.

$$\gcd(|K - I|, n) = 1 \Leftrightarrow |K - I| \neq 0 \text{ mod } n$$

$n$  ראשון : פתרון ייחודי

כמו שראינו, לעיתים נקבל  $0$  שהוא לא ראשוני, ולכן נhapus את כל המחלקים של  $0$  ובעזרתם נרכיב את מערכת המשוואות

הבאיה:

נניח כי המחלקים של  $0$  הם:  $n_1, n_2, \dots, n_k$

$$\gcd(|K - I|, n) = 1 \Leftrightarrow \begin{cases} |K - I| \neq 0 \text{ mod } n_1 \\ |K - I| \neq 0 \text{ mod } n_2 \\ \dots \\ |K - I| \neq 0 \text{ mod } n_k \end{cases}$$

עכשו נוכל להשתמש בתנאי כך שככל המשוואות יתקיימו.

הערה חשובה מאוד – לעיתים יכולם לשאול אותנו לחפש  $a$  שעבורו יש הודעות בלתי מוסתרות, חשוב קודם לבדוק עבור איזה  $a$  מטריצת  $K$  יכולה להיות מפתח. ישנו מקרים בהם נמצא ערכים שיכולים בתאoria להיות כאלה שיש להם הודעות בלתי מוסתרות (לפי חישוב הדטרמיננטה) אבל, בפועל אלו ערכים ש- $K$  לא יכול להיות מפתח עבורם.

דוגמא:

בצופן HILL עם מטריצה-מפתח  $\begin{pmatrix} 2a & 13 \\ 15 & a \end{pmatrix}$  מעל אלף-בית האנגלית בן 26 אותיות.  
עבור איזה ערכים של  $a$  הקטנים מ-13 מספר ההודעות הבלתי מוסתרות הוא המינימלי?

ראשית נמצאת ערכיו  $a$  שעבורם קיימות הודעות בלתי מוסתרות:

$$x * K = x \bmod 26$$

$$x * (K - I) = 0 \bmod 26$$

אם  $I - K$  הפיכה אז יש פתרון יחיד והוא טריוויאלי.

$$\Leftrightarrow \gcd(|K - I|, 26) = 1$$

**נחשב את  $(K - I)$ :**

$$\det \begin{pmatrix} 2a - 1 & 13 \\ 15 & a - 1 \end{pmatrix} = (2a - 1) * (a - 1) - 13 * 15 = (2a - 1) * (a - 1) - 195 \\ \equiv (2a^2 - 2a - a + 1 + 13) \bmod 26 \equiv (2a^2 - 3a + 14) \bmod 26$$

. נשים לב כי מטריצת  $I - K$  הפיכה עם מתקיים התנאי  $= 1$

המחלקים של 26 הם : 1,2,13 וכך, אם מתקיים  $= 1$

או ניתן לומר כי  $|I - K|$  לא מתחלק ב-2 או ב-13, כלומר:

$$\gcd(|K - I|, 26) = 1 \Leftrightarrow \begin{cases} |K - I| \neq 0 \bmod 13 \\ |K - I| \neq 0 \bmod 2 \end{cases}$$

נמצא  $a$  כך ש:  $|K - I| \neq 0 \bmod 2$  וגם  $|K - I| \neq 0 \bmod 13$

$$|K - I| \neq 0 \bmod 13$$

$$(2a^2 - 3a + 14) \neq 0 \bmod 13$$

$$(2a^2 - 3a + 1) \neq 0 \bmod 13$$

$$(a - 1)(2a - 1) \neq 0 \bmod 13$$

$$a_0 \neq 1 \quad , \quad 2a - 1 \neq 0 \bmod 13$$

$$2a \neq 1 \bmod 13$$

כל לראות כי ההפכי של 2 הוא 7, נכפול ב-7:

$$7 * 2a \neq 7 * 1 \bmod 13$$

$$a \neq 7 \bmod 13$$

$$a_0 \neq 1, a_1 \neq 7$$

$$|K - I| \neq 0 \bmod 2$$

$$(2a^2 - 3a + 14) \neq 0 \bmod 2$$

$$(-3a) \neq 0 \bmod 2$$

$$a \neq 0 \bmod 2$$

$$a \neq 0$$

מכיוון שצמצמנו את  $a = 26$  נצטרך להתחשב בזיה בפתרון שקיבלנו כלומר:

עבור  $|K - I| \neq 0 \bmod 13$ ,  $a \neq 1, 7$  קיבלו נס

כלומר  $(a \neq 1, 14, 7, 20) a \neq (1 + 13k) \bmod 26, (7 + 13k) \bmod 26$

עבור  $|K - I| \neq 0 \bmod 2$ ,  $a \neq 0$  קיבלו נס

. $(a \neq 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) a \neq (0 + 2k) \bmod 26$

נתבונן בערכים הקטנים מ-13 (על פי נתוני השאלה)

קיבלו כי עבור  $a \neq 0, 1, 2, 4, 6, 7, 8, 10, 12$   $\gcd(|K - I|, 26) = 1$

**נשים לב** ש-0 הוא לא בתחום הגדרה שלנו (עבור  $a=0$  המטריצה לא מהוות מפתח), וכך נעיף אותו.

**או במלילים אחרות** – ערכיו  $a$  שעבורם קיימת הודעה בלתי מוסתרת אחת,

$$a = 3, 5, 9, 11$$

זהו בעצם מספר ההודעות הבלתי מוסתרות המינימליים.

### הערות על האלגוריתם

- קל לפירץ אותו בזמנים אם נתון הودעה + הודעה מוצפנת, ניתן להרכיב מערכת משוואות (חשוב מאוד שהמשוואות יהיו בלתי תלויות – שכן יש לבחור את סוג ההודעות בהכמה).

## Permutation Cipher

זהו מקרה פרטי של צופן היל שבו מטריצה של הבלוק שאותו רוצים להצפין. מה שעצם עושים זה לוקחים את מטריצה היחידה I ומחליפים בין העמודות שבה.

לדוגמא: נרצה להצפין את הבלוק  $(a, b, c)$ , נחליף בין עמודות מטריצה היחידה:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = K$$

$$(a, b, c) \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = (b, c, a)$$

קיבלו פרמוטציה של הבלוק המקורי.

## Vigenère Cipher

עבור מפתח  $K = (k_1, k_2, \dots, k_m)$  הצופן יחושב על סמך הנוסחה:  
 $E_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m) \bmod n$   
 הפיענוח יחושב על סמך הנוסחה הבאה:  
 $D_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m) \bmod n$

נשים לב שגם בעצם הרחבה של צופן קיסר, בצופן קיסר כל ערכי המפתח שוויים.

## תורת המידע בкриптולוגיה

התקפות על צפנים نوعדו לחושף מידע על ההודעה שהוצפנה או אפילו את ההודעה עצמה או מידע על הצופן כגון מידע על המפתח. כאשר נרצה לנתח התקפות ועמידות של צפנים, נצרך להשתמש במושגים יותר ברורים של מידע. לשם כך נשחטש במושגים מתחום תורה המידע (information theory).

חוֹרָה עַל נוֹסְחָות שֶׁל הַסְּתָבָרוֹת.

נוסחת הסתברות מותנית:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

נוסחת בייס:

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

### אנתרופופיה

האנתרופופיה היא שמתאר את מידת האי וודאות של המערכת.

נוסחת האנתרופופיה:

$$H(X) = - \sum_{x \in X} \Pr(x) * \log \Pr(x)$$

תכונות:

$$H(X) \geq 0$$

$$H(X) \leq \log_2 |X|$$

$$H(X, Y) \leq H(X) + H(Y)$$

אנתרופופיה משותפת:

$$H(X, Y) = - \sum_{x \in X} \sum_{y \in Y} \Pr(x, y) * \log \Pr(x, y)$$

אנתרופופיה מותנית – נשתחז בנוסחה זו כאשר ניתנת לנו התקפה כלשהי  $X$  והתפלגות הערכים לפני התקפה  $Y$ . ונרצה לדעת מה האנתרופופיה לאחר התקפה.

$$H(Y|X) = \sum_{x \in X} \Pr(x) * H(Y|X=x)$$

נוסחת כל השרשרת:

$$H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

$$D(P(x) || Q(x)) = \sum_{x \in X} \Pr(x) * \log \left( \frac{\Pr(x)}{Q(x)} \right)$$

$$I(X, Y) = D(P(x, y) || P(x) * P(y)) = \sum_{x \in X} \sum_{y \in Y} \Pr(x, y) * \log \left( \frac{\Pr(x, y)}{\Pr(x) * \Pr(y)} \right)$$

$$I(X, Y) = H(X) + H(Y) - H(X, Y) = H(X) + H(Y) - H(Y) - H(X|Y) = H(X) - H(X|Y)$$

$$I(X, X) = H(X)$$

$$L(C) = \sum_{i=1}^m P_i * l_i$$

אם  $L(C) = H(X)$  קוד אופטימלי.  
לכן  $L(C) \geq H(X)$  האופטימלי.

# DES

## הקדמה

IBM בראשי תיבות DES - הוא תקן הצפנה נתונים שפותח ב- 1975 על ידי IBM בשיתוף פעולה עם הסוכנות לביטחון לאומי של ארה"ב. DES הוא צופן בלוקים סימטרי איטרטיבי. הפונקציה הפנימית של האלגוריתם מתבצעת בששה עשר סבבים על בלוק מידע בגודל 64 סיביות, בעזרת מפתח סודי בגודל 64 סיביות (שמתוכם רק 56 סיביות בשימוש) ומפעילה פלט בגודל זהה. צופן DES מבוסס על רעיון שנראה צופן מרוכב שהוא שילוב של החלפה ותמורה לייצרת פונקציה חזקה.

## תיאור האלגוריתם

הקלט הוא בלוק טקסט קריא בגודל 64 סיביות ומפתח הצפנה סודי  $K$  בגודל 64 (בפועל 56) סיביות. מפתח - באמצעות פרוצדורת הרחבת מפתח מרחיבים ומחלקים את המפתח ל-16 מקטעים בני 48 סיביות, כל אחד מהם משמש עבור סבב אחד.

- מכינים 8 תיבות החלפה (S-box) סטטיות  $S_1, S_2, \dots, S_8$  המיצגות פונקציות שמחזירות פלט של 4 סיביות עבור קלט של 6 סיביות. תיבות ההחלפה מוצגות באמצעות טבלה. תיבות ההחלפה הנקראת S-box קיצור של Substitution box מייצגת פונקציות החלפה אי-ליינאריות. תיבות ההחלפה של DES הן מקור בטיבוחתו, הפונקציות שהן מייצגות הן הפעולות האי-ליינאריות היחידות המופעלות על הקלט ואלמלה הן צופן DES לפיריצה בקלות.

<table border="1" style="border-collapse: collapse; text-align: center;"> <thead> <tr> <th>32</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th></tr> </thead> <tbody> <tr><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr> <tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr> <tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td></tr> <tr><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr> <tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr> <tr><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr> <tr><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td><td>1</td></tr> </tbody> </table> <p style="text-align: center;"><i>E</i></p>	32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21	22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1	<table border="1" style="border-collapse: collapse; text-align: center;"> <thead> <tr> <th>16</th><th>7</th><th>20</th><th>21</th></tr> </thead> <tbody> <tr><td>29</td><td>12</td><td>28</td><td>17</td></tr> <tr><td>1</td><td>15</td><td>23</td><td>26</td></tr> <tr><td>5</td><td>18</td><td>31</td><td>10</td></tr> <tr><td>2</td><td>8</td><td>24</td><td>14</td></tr> <tr><td>32</td><td>27</td><td>3</td><td>9</td></tr> <tr><td>19</td><td>13</td><td>30</td><td>6</td></tr> <tr><td>22</td><td>11</td><td>4</td><td>25</td></tr> </tbody> </table> <p style="text-align: center;"><i>P</i></p>	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25
32	1	2	3	4	5																																																																												
4	5	6	7	8	9																																																																												
8	9	10	11	12	13																																																																												
12	13	14	15	16	17																																																																												
16	17	18	19	20	21																																																																												
20	21	22	23	24	25																																																																												
24	25	26	27	28	29																																																																												
28	29	30	31	32	1																																																																												
16	7	20	21																																																																														
29	12	28	17																																																																														
1	15	23	26																																																																														
5	18	31	10																																																																														
2	8	24	14																																																																														
32	27	3	9																																																																														
19	13	30	6																																																																														
22	11	4	25																																																																														

**התיבה E (קייזור של Expansion)** - היא תיבת תמורה/הרחבה, שתפקידה בנוסף להרחב את הקלט מ-32 סיביות ל-48 סיביות.

**התיבה P (קייזור הרחבה של Permutation)** - היא תיבת תמורה סטטית נוספת שמירה את הקלט בסוף כל סבב תוך שמירה על גודלו - 32 סיביות.

**מכנים תיבות החלפה IP (קייזור של Initial Permutation)** - היא תיבת תמורה שתפקידה להחליף את המידע של הקלט

<table border="1" style="border-collapse: collapse; width: 100px; height: 100px;"> <tr><td>58</td><td>50</td><td>42</td><td>34</td><td>26</td><td>18</td><td>10</td><td>2</td></tr> <tr><td>60</td><td>52</td><td>44</td><td>36</td><td>28</td><td>20</td><td>12</td><td>4</td></tr> <tr><td>62</td><td>54</td><td>46</td><td>38</td><td>30</td><td>22</td><td>14</td><td>6</td></tr> <tr><td>64</td><td>56</td><td>48</td><td>40</td><td>32</td><td>24</td><td>16</td><td>8</td></tr> <tr><td>57</td><td>49</td><td>41</td><td>33</td><td>25</td><td>17</td><td>9</td><td>1</td></tr> <tr><td>59</td><td>51</td><td>43</td><td>35</td><td>27</td><td>19</td><td>11</td><td>3</td></tr> <tr><td>61</td><td>53</td><td>45</td><td>37</td><td>29</td><td>21</td><td>13</td><td>5</td></tr> <tr><td>63</td><td>55</td><td>47</td><td>39</td><td>31</td><td>23</td><td>15</td><td>7</td></tr> </table>	58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4	62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8	57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3	61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7	$IP$	<table border="1" style="border-collapse: collapse; width: 100px; height: 100px;"> <tr><td>40</td><td>8</td><td>48</td><td>16</td><td>56</td><td>24</td><td>64</td><td>32</td></tr> <tr><td>39</td><td>7</td><td>47</td><td>15</td><td>55</td><td>23</td><td>63</td><td>31</td></tr> <tr><td>38</td><td>6</td><td>46</td><td>14</td><td>54</td><td>22</td><td>62</td><td>30</td></tr> <tr><td>37</td><td>5</td><td>45</td><td>13</td><td>53</td><td>21</td><td>61</td><td>29</td></tr> <tr><td>36</td><td>4</td><td>44</td><td>12</td><td>52</td><td>20</td><td>60</td><td>28</td></tr> <tr><td>35</td><td>3</td><td>43</td><td>11</td><td>51</td><td>19</td><td>59</td><td>27</td></tr> <tr><td>34</td><td>2</td><td>42</td><td>10</td><td>50</td><td>18</td><td>58</td><td>26</td></tr> <tr><td>33</td><td>1</td><td>41</td><td>9</td><td>49</td><td>17</td><td>57</td><td>25</td></tr> </table>	40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31	38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29	36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27	34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25	$IP^{-1}$
58	50	42	34	26	18	10	2																																																																																																																												
60	52	44	36	28	20	12	4																																																																																																																												
62	54	46	38	30	22	14	6																																																																																																																												
64	56	48	40	32	24	16	8																																																																																																																												
57	49	41	33	25	17	9	1																																																																																																																												
59	51	43	35	27	19	11	3																																																																																																																												
61	53	45	37	29	21	13	5																																																																																																																												
63	55	47	39	31	23	15	7																																																																																																																												
40	8	48	16	56	24	64	32																																																																																																																												
39	7	47	15	55	23	63	31																																																																																																																												
38	6	46	14	54	22	62	30																																																																																																																												
37	5	45	13	53	21	61	29																																																																																																																												
36	4	44	12	52	20	60	28																																																																																																																												
35	3	43	11	51	19	59	27																																																																																																																												
34	2	42	10	50	18	58	26																																																																																																																												
33	1	41	9	49	17	57	25																																																																																																																												

מציעים תמורה חד פעמית על כל סיביות הקלט באמצעות תיבת תמורה סטטית הנקראת  $IP$ .

ובסיוום כל 16 הסבבים מעבירים את הפלט בתיבת התמורה ההפוכה לה  $IP^{-1}$ .

לפעולה זו אין השפעה משמעותית על בטיחות הצופן כיון שאינה תלואה במפתח ההצפנה ומקובל להעתלם ממנה שמנתחים את הצופן.

לא ברורה לゲMRI הסיבה לתוספת זו, יש הסברים כי היא נועדה להאט את האלגוריתם במכונן.

סדר הפעולות בכל הסבבים זהה.

תחילה מחלקים את קלט האלגוריתם לשני חצאים  $L_0, R_0$  בהתאם ובכל סבב מבצעים כדלהלן:

$$L_i = R_{i-1}$$

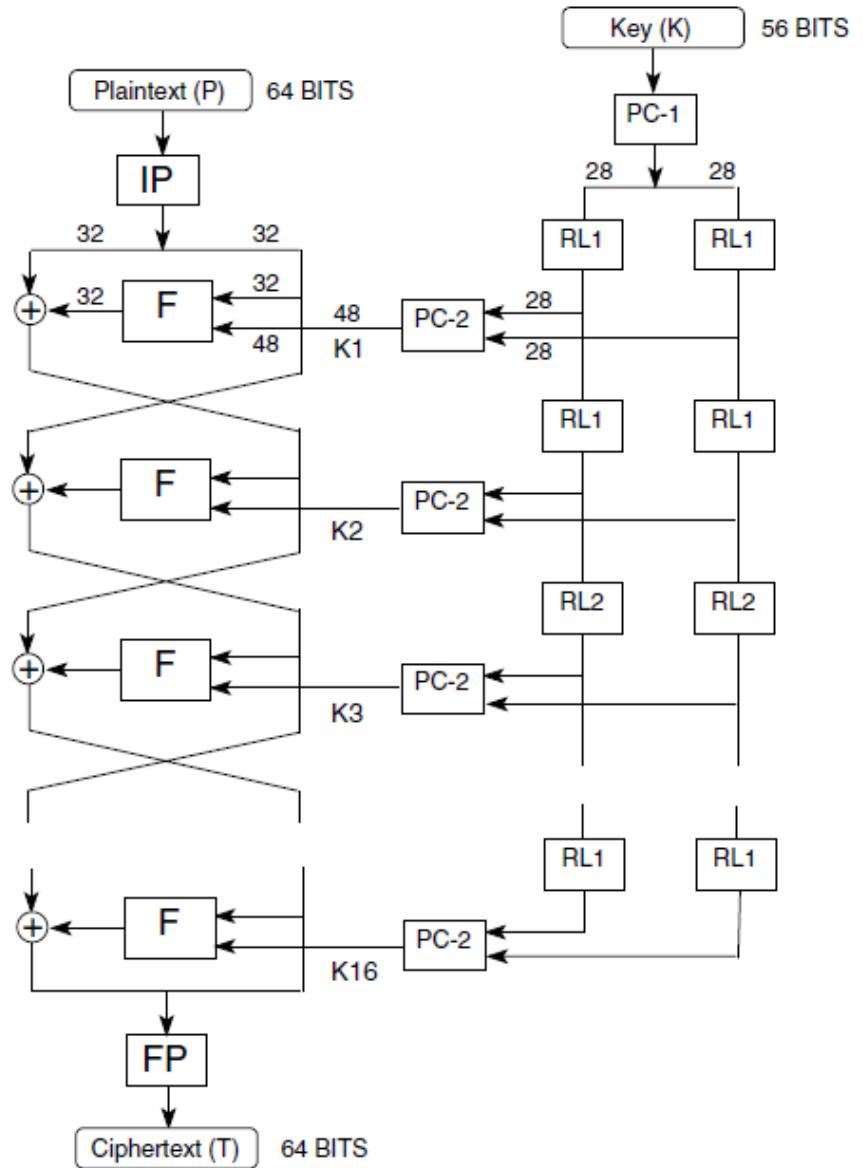
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

$$f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

פעולות הפונקציה  $f$  מתבצעת רק על מחצי הקלט (היינו 32 סיביות).

המחצית השנייה מועברת לסבב הבא ללא שינוי.

**פונוח - DES** היינו צופן סימטרי ועל כן פועלות הפונוח דומה לפועלות ההצפנה. על מנת לפונוח בלוק של 64 ביטים מוצפנים, נעביר אותו במערכת ה-DES-אך נבצע את תהליך **the Round Functions**-בצורה הפוכה (נכנים את המפתחות בסדר הפוך). בסוף התהליך יתקבל כפלט המידע המקורי שהוצפן.



## פונקציה F

מקבלת חלק של מילה בגודל 32 ביט ומספר בגודל 48 ביט.

$$f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

הפונקציה  $f$  מורכבת משילוב הפונקציות המתוירות:

- הפונקציה E "ומגדילה" את הקלט לפולט של 48 סיביות (כל סיבית קלט אחת משפיעה על פולט הפונקציה לפחות פעם אחת).

$$E(R_{i-1})$$

- מבצעים XOR בין הערך המורחב למפתח

$$E(R_{i-1}) \oplus K_i$$

- מחלקים את התוצאה ל-8 חלקים כל אחד בגודל 6 ביט.

$$E(R_{i-1}) \oplus K_i = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$$

$$B_i = b_1 b_2 b_3 b_4 b_5 b_6$$

- לכל  $B_i$  קיימת תיבת החלפה S-Box מבוצעת פולה לא-لينארית על הקלט:

- נתבונן בשורה ה- $r = b_1 b_6$  (נمير את הערך לדציג מי מבינארי).

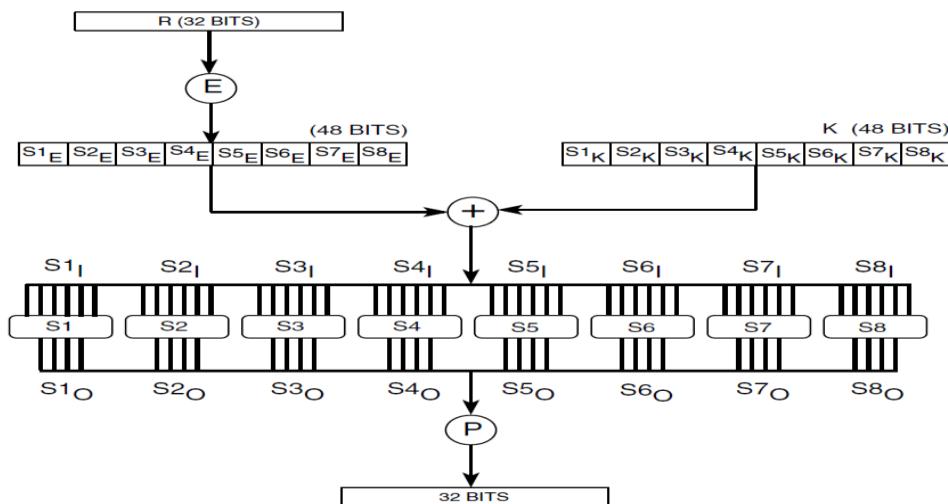
- נתבונן בעמודה  $c = b_2 b_3 b_4 b_5$  (נمير את הערך לדציג מי מבינארי).

- נחשב  $C_i$ ,  $S_i[r, c] = C_i$ , כאשר  $C_i$  בגודל 4 ביט.

- קיבל  $C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8$  מספר בגודל 32 ביט.

- נעביר את  $C$  בפונקציה P המפתח את הקלט לערכים בגודל 32 סיביות.

$$P(C)$$



## פרוצדורת הרחבת מפתח

להרחבת המפתח, צופן DES משתמש בשתי טבלאות סטטיות  $PC1, PC2$

$C$							
57	49	41	33	25	17	9	
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
$D$							
63	55	47	39	31	23	15	
7	62	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	13	28	20	12	4	
$PC1$				$PC2$			

המפתח מורחב ל-16 בלוקים בני 48 סיביות כל אחד.

מתעלמים מהסיביות  $(k_8, k_{16}, \dots, k_{64})$  – כל בית 8 בפתח מהוות בית ביקורת, יש בית ביקורת כי חשוב מאוד שלא יהיו לנו טיעות בפתח כי אז כל הקידוד יהיה טוען. בית הביקורת – הוא בית שמשלים את מספר האדמים שהוא ב-7 הביטים לפניו במספר אי-זוגי.

באמצעות טבלה  $PC1$  מחלקים את 56 הסיביות האפקטיביות לשני משתנים  $D, C$  בני 28 סיביות כל אחד. עבור כל סיבב מוצעים הזה מהוות לשלאל (Rotate left) של סיביות המשתנים  $D, C$ , בתבנית אחת או שתים בהתאם לערך התלוי במיקום הסיביות, עבור סיבבים 1,2,9,16 מזויים ב-1 עבור יתר מזויים ב-2 משתמשים בטבלה  $PC2$  כדי לשרר את סיביות המשתנים לבлок מפתח בגודל 48 סיביות.

$$\begin{aligned} PC1_1 &= C_0 D_0 \\ C_i &= Shift\ Left\ i\ (C_{i-1}) \\ D_i &= Shift\ Left\ i\ (D_{i-1}) \\ K_i &= PC2(C_i D_i) \end{aligned}$$

## מתקפה על האלגוריתם

- .1 brute force – יש לנו סה"כ  $2^{56}$  אפשרויות של ערכים למפתחות, ניתן לעבור על כל אפשרויות. ברור כי התקפה זו לא מעשית, ידרשו שנים בכדי לפצח את הצופן.
- .2 ניתן להוריד את מספר המפתחות פי 2 –  $2^{55}$  וזה מכיוון שיש לנו סימטריה במקרה המשלים,  $y = E_K(x) \quad \bar{y} = E_{\bar{K}}(\bar{x})$
- .3 התקפה דיפרנציאלית – אם נתבונן על מילת קוד + מילה מוצפנת המתאימה לה, נוכל למצוא מידע נוסף על האלגוריתם, יותר נכון לומר שניתן למצוא שעבור צדים מסוימים נקבל התפלגות לא אחידה. בכך נוכל להוריד את מרחב האפשרויות למפתח שלנו, ב-DES עם 16 סיבובים נוכל לבדוק  $2^{47}$  מפתחות.
- .4 התקפה לינארית – משתמש על מבנה האלגוריתם ומנסה למצוא מקומות בהם חישוב ה-XOR נתון לנו מידע לגבי חלק מהbiteים של המפתח. יכול להוריד לנו את מרחב הפתרונות ל- $2^{43}$ .

## מפתח ב-DES

נשים לב שבאלגוריתם DES יש מקרים בהן המפתח יקרא "מפתח חלש", בקרה זה נקבע כי עבור כל תתי המפתחות שאנו מייצרים עברו כל סיבוב של האלגוריתם, כל המפתחות שוים:  $K_1 = K_2 = \dots = K_{16}$ :  
לדוגמא:

$$K = [01]^8 \rightarrow (00000001)^8$$

שניהם מקבל 56 הביטים נקלע 56 אפסים.

$$K = [FE]^8 \rightarrow (11111110)^8$$

שניהם מקבל 56 הביטים נקלע 56 אחדים.

למה לא נכון להשתמש באלגוריתם במפתח חלש ב-DES?  
כי מפתח חלש לא מŻפין אף הודעה כי אחריו 2 איטרציות הוא משוחרר את ההודעה, ככלומר מקבל כי:

$$\begin{aligned} E_K(x) &= y \\ E_K(y) &= x \end{aligned}$$

- נשים לב כי אם נתנו לנו איזושהו מספר ועלינו לבדוק אם הוא מפתח נהיה חיבם לבודק:
1. האם הוא תקין – כולם האם כל בית 8 בו משלים את מספר האחדים-ב-7 הביטים לפני לא-זוגי.
  2. האם הוא מפתח חלש.

קיימים גם מפתח חצי חלש, שבו חלק מהפעמים נקבל תתי מפתחות שווים.

נשים לב שמדובר  $2^{56}$  מפתחות אפשריות יש לנו  $2^{12} = 2^6(2^2 + 3 * 2^2 + 3 * 2^4)$  אפשרויות לבחור מפתח חלש וחצי חלש מכאן שהסתברות לבחור מפתח כזה היא :

$$\frac{2^{12}}{2^{56}} = \frac{1}{2^{44}} = 5.6 * 10^{-14}$$

הסתברות נמוכה מאוד.

הערה – מפתח חלש ב-DES לא מצפין  $2^{32}$  הודיעות, ככלומר יש לנו  $2^{32}$  הודיעות בלתי מוסתרות

## Double DES

נרייך מילת טקסט על אלגוריתם DES פעמים כך שבכל פעם נבצע את הקידוד עם מפתח אחר. בכך מרחיב האפשרויות למפתחות שלנו מגיע ל:  $2^{56} * 2^{56} = 2^{112}$ .

מתתקפת Meet in the middle – באמצעות התקפה זו ניתן באופן אקספוננציאלי להפיחת את מספר התמורה brute force הנדרשת כדי לפענן טקסט שהוצפן על ידי יותר מפתח אחד.

ב-DES התקפה זו עוזרת לנו לבדוק רק  $2^{56}$  אפשרויות של מפתחות ולא  $2^{112}$

$$C = E_{K_1}(E_{k_2}(x))$$

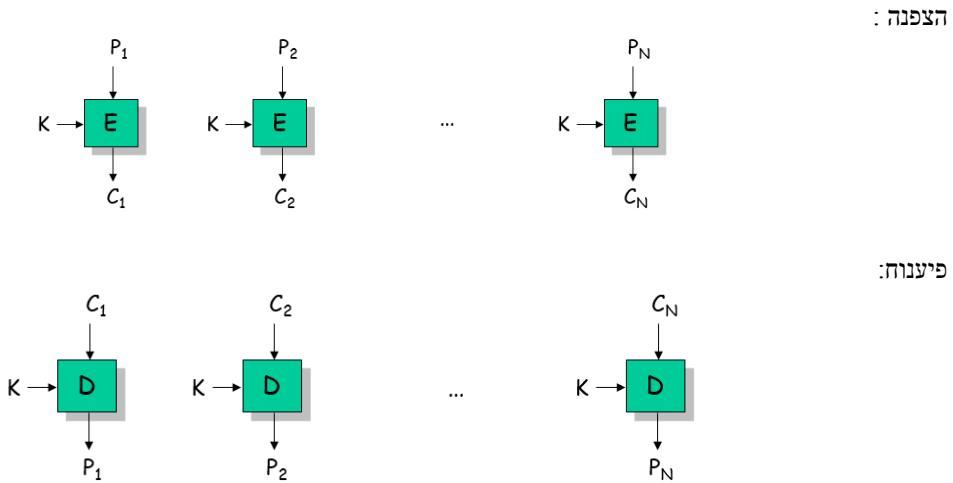
$$D_{K_1}(C) = E_{k_2}(x)$$

- עבור ( $C$ ) יש לנו סה"כ  $2^{56}$  מפתחות, ניתן למצוא את ערכיו ( $D$ ) עבור כל מפתח כזה. נמיין את התוצאות שקיבלנו. כל זה ניתן לעשות בסיבוכיות של  $2^{56}$ .
- באותו אופן, נמצא את כל ערכי ( $x$ ) עבור כל מפתח כזה ונמיין את התוצאות, גם כאן יש לנו סה"כ  $2^{56}$  מפתחות. כל זה ניתן לעשות בסיבוכיות של  $2^{56}$ .
- נמצא ערכים שווים ב-2 המערךיים שקיבלנו, ובכך נמצא את זוגות החזודים של המפתחות אפשריים. זמן החיפוש הוא גם בסדר גודל של  $2^{56}$ .
- נבצע את תהליך זה שוב עבור הודעה אחרת.
- נבצע חיתוך בין זוגות המפתחות עבור כל הודעה, ונמצא את זוג המפתחות המתאים (הסתברות שהוא זוג בחיתוך שאינו זוג המפתחות קטנה מאוד)

ראינו כי ניתן להוריד משמעותית את זמן ההתקפה.

## ECB – Electronic Codebook

בשיטתה זו בכל פעם נצפין בלוק באופן בלתי תלוי בבלוקים האחרים.

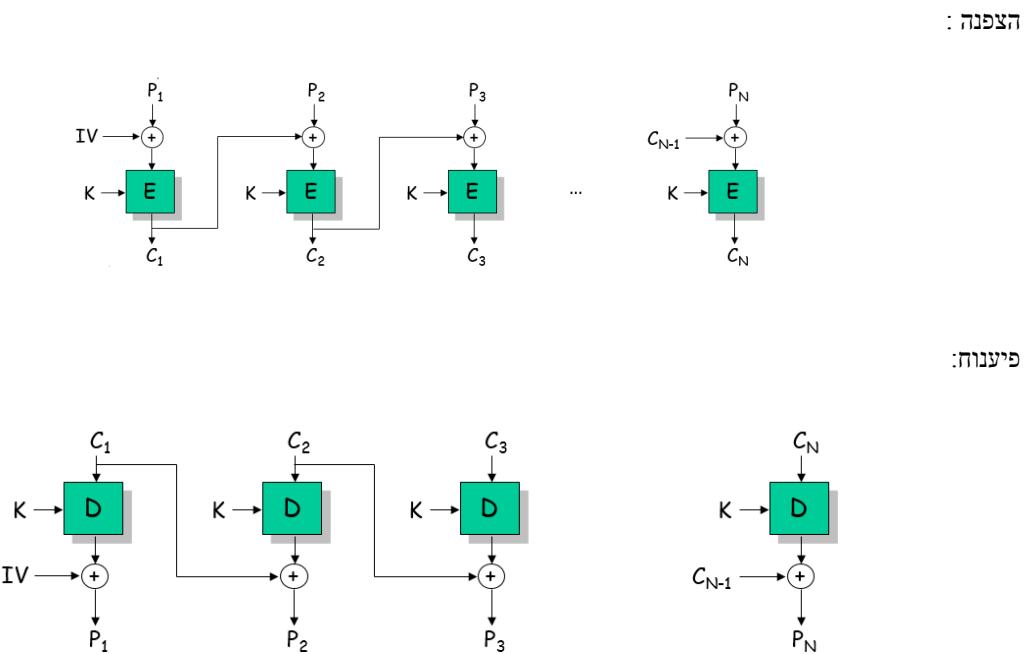


- יתרונות:
  - טעות בקידוד בלוק לא משפיע על קידוד בלוקים אחרים.

- חסרונות:
  - בלוקים זהים יקודדו תמיד לאותו בלוק.
  - ניתן להשתמש בהתקפה סטטיסטית.

## CBC – Cipher Block Chaining

בשיטת ההצפנה זו, ישנה תלות לא רק במפתח אלא גם בוקטור התחלתי (IV). הצפנה הבלוק משפיעה על הבלוק הבא. הוקטור התחלתי יכול לשנות את ההצפנה עבור קלטים זרים.



יתרונות:

- עדין נגד התקפות סטטיסטיות.
- בלוקים זהים יכולים להיות מוצפנים לערבים שונים.
- שינוי וקטור התחלתי משפייע על תוצאות הקידוד – בשיטה זו אנו מוחקים את האבטחה באמצעות שימוש בוקטור,
- את הוקטור ניתן להעביר המידע מכוון.

הסכנות:

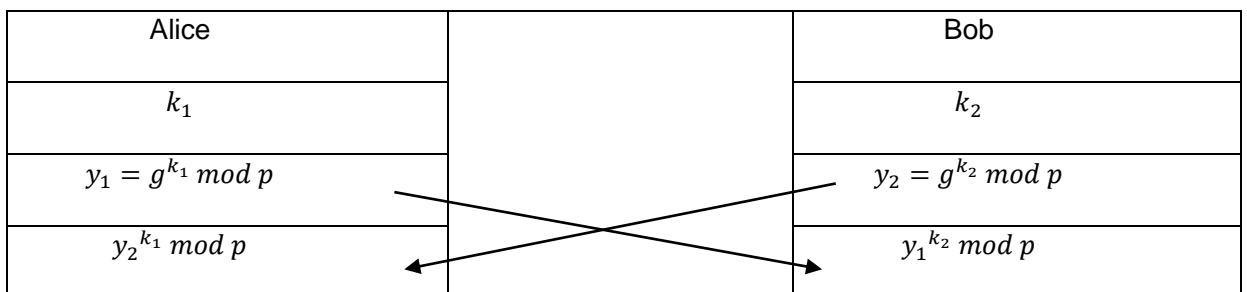
- טעות בקידוד בלוק משפייע על קידוד בלוקים אחרים.
- ניתן לבצע התקפה ע"י הכנסת טעות בבייט אחד, טעות זו תהיה גם בבלוק הבא בדיקת אותו הביט, בכך ניתן להזזה בית ספציפי בפתח ובכך להוריד את מס' האפשרויות של המפתחות.
- נדרש למצוא דרך להסכים על הוקטור  $\text{IV}$  (נניח לשלווה אותו מוצפן בזרה כלשהו).

## Diffie-Hellman Algorithm

זהו אלגוריתם להעברת מפתח. נתון  $p$  ויוצר  $g$ . נתון מפתחות פרטיים  $k_1, k_2$ .

המפתח המשותף ייחסב יהיה:

תהליך ה- Diffie Hellman יהיה באופן הבא :



ישריך לדעת לבוחר  $k$  בהכמה:

- נבחר  $k$  שהוא לא חלק של  $(n)$ , כי אם הוא כן, יהיה ניתן בקלות למצאו אותו – אם ישב מאזין זדוני לקו שבו תסדר את המידע שלו, המאזין יוכל למצוא בקלות את ה- $k$  שלה בכך שהוא פשוט עבר על כל החלקים של  $(n)$ .

הסביר נוסף: נשים לב שם נעללה יוצר בחזקה שהיא זרה ל- $n$  נקבל יוצר נוסף. אם מפתח  $k$  הוא זר ל- $n$  אז הערך  $g^k$  הוא יוצר ולכן אם נעללה אותו בחזקות שונות נוכל להגיע לכל מרחב המפתחות הציבוריים. לעומת זאת אם נבחר  $k$  שאינו זר ל- $n$  נוכל להגיע רק מתחת קבוצה של מפתחות פומביים ובכך להיות יותר רגילים למתקפה מצאה.

# RSA

## הקדמה

**RSA** היא שיטת הצפנה אסימטרית דטרמיניסטית. האלגוריתם מבוסס על רעיון המפתח הפומבי ומסתמך על בעיית פירוק לגורמים.

## תיאור

1. בוחרים שני מספרים ראשוניים  $q, p$  כאשר  $2 < q \neq p$ . ערכיהם אלו צריכים להיות ערך באותו תחום כלומר יחסית קרובים זה לזה, בנוסף  $\gcd(p-1, q-1)$  צריך להיות קטן.
2. מוחשבים  $n = p * q$ .
3. מוחשבים  $\theta(n) = (p-1)(q-1)$ .
4. בוחרים שלם  $n < b < 1$  שהוא זר ל- $\theta(n)$ , כלומר  $1 = \gcd(b, \theta(n))$ .
- a. נשים לב כי  $b$  הוא תמיד יהיה מספר אי זוגי, וזה מכוון ש  $(q-1)(p-1) \equiv 1 \pmod{\theta(n)}$  הוא מספר זוגי, ולכנן אם  $a$  היה זוגי ה- $\gcd$  שלהם היה שווה לאחד.
- b. יש לנו סה"כ  $\theta(n)$  אפשרויות למפתח.
- c. נשים לב כי עבור  $b$  יש לנו באופן אוטומטי אחד ערכי  $a$ .
- d. נועד לפבחור  $b$  כזה שעבورو מספר ההודעות הבלתי מסוות הוא נמוך ככל האפשר.
5. מוצאים  $a$  כך שיתקיים  $ab \equiv 1 \pmod{\theta(n)}$ .

**פומבי:**

$n$  •

$b$  •

**פרטי:**

$q, p$  •

$a$  •

**הצפנה:**

$$E(x) = x^b \pmod{n}$$

**פיענוח:**

$$D(y) = y^a \pmod{n}$$

מספר טוב לשימוש בסיסים במערכת **RSA** אם הוא מקיים

- הוא פריק ל-2 במספרים ראשוניים.
- לא מתפרק ב-2 (כי אז יהיה קל למצוא את הפירוק שלו)
- מספר שהוא לא ריבוע של מספר כלשהו (ישנם אלגוריתמים שיכלו למצוא את הפירוק במחירות ובנוסף נקבל כי  $b=p$ )
- לא מספר ראשוני.

למה האלגוריתם נחשב לבתו

- בשביל הפיענוח אנו חיבם שהיה לנו מפתח פרטי  $a$ , כדי למצוא אותו נהיה חייבים לדעת את  $q, p$  שגם הם פרטיים. כדי למצוא אותם ככלمر למצוא את הפירוק  $q = n$  נדרש לעבור על מספר אפשרויות רבות,  $n$  הוא מספר ענק, לכן נדרש לעבור כל  $\sqrt{n}$  איברים (זאת כמוות עצומה – לרוב יהיה מספר בעל 1024 ביטים).
- **Discrete Logarithm Problem** – לא ניתן לחשב  $\log_b x$  בחישוב מודולרי ולכנן לא ניתן למצוא באמצעותו את  $a$ .
- לא קיימת פונקציה שורש בחישוב מודולרי, יודעים את  $b$  אבל לא ניתן למצוא את  $x^b$ .

## מציאת הודעות בלתי מוסתרות

לכל מערכת RSA יש לפחות 9 הודעות בלתי מוסתרות.

מספר ההודעות הבלתי מוסתרות הוא:

$$(1 + \gcd(b - 1, p - 1)) * (1 + \gcd(b - 1, q - 1))$$

הודעה בלתי מוסתרת מוגדרת כ:

$$E(x) = x^b = x \bmod n$$

באופן אוטומטי ניתן לראות כי  $0, 1 = x$  הן שאリות של הודעות בלתי מוסתרות טריויאליות. מכיוון ש- $b$  הוא אי זוגי ניתן לומר כי גם  $-1 = x$  היא שאリת הודעה בלתי מוסתרת טריויאלית.

בנוסף לשאリות אלו ( $\pm 1 = x$ ) יכולים להיות עוד שאリות של הודעות בלתי מוסתרות לא טריויאליות. **נשים לב** – הודעה בלתי מוסתרת מורכבת מזוגות של שאリות בהמשך נראה איך מוצאים אותם.

אנחנו יודעים כי יש לנו 3 הודעות בלתי מוסתרות עבור כל חלק של  $n$ , בנוסחה  $1 + \gcd(b - 1, p - 1)$

ה-1 מאפיין את שאリת 0

$\gcd$  מאפיין את שאר השאリות אם יוצא כי  $p-1 = 2g$  אז יש לנו רק הודעות בלתי מוסתרות טריויאליות (כי יש לנו בודאות שאリות  $\pm 1$ ).

איך נמצא את ה Hodoutes :

ראשית נגידר את מערכת המשוואות:

$$x^b = x \bmod n \Leftrightarrow \begin{cases} x^b = x \bmod p & , \quad x = 0, \pm 1 \\ x^b = x \bmod q & , \quad x = 0, \pm 1 \end{cases}$$

נשים לב כי ניתן למצוא 9 הודעות בלתי מוסתרות טריויאליות עבור כל  $n$  מתאים.

נשתמש במשפט השאריות הסיניים, נמצא את :

$$\begin{aligned} m_1 &= q & m_2 &= p \\ M_1 &= p & M_2 &= q \\ c_1 &= M_1^{-1} \bmod m_1 & c_2 &= M_2^{-1} \bmod m_2 \end{aligned}$$

$$x \equiv r_1 * M_1 * c_1 + r_2 * M_2 * c_2 \bmod n$$

נציב במקום  $r_1, r_2$  את השאリות  $\pm 1, 0$  ונמצא את ה Hodoutes .

$r_1 \backslash r_2$	0	1	-1
0			
1			
-1			

אם נקבל כי  $(b - 1, p - 1) = 2g$  גדול מ-2 – כלומר קיימות ה Hodoutes בלתי מוסתרות לא טריויאליות, נדרש למצוא את השאリות המתאימות להן, לשם כך נפעיל הצורה הבאה:

נזכיר כי ה Hodoutes בלתי מוסתרות מוגדרות (נתבונן רק עבור החלק של  $p$ )

$$M^b = M \bmod p$$

$M = 0$  זהה ה Hodעה טריויאלית.

נתבונן במקרה שבו  $M \neq 0$ , נחלה את המשווה ב- $M$ : נשים לב כי מכיוון ש- $p$  ראשוני בהכרח קיים הופכי.

$$M^{b-1} = 1 \bmod p$$

נמצא יוצר  $g$  של  $Z_p$ .

נגידר:  $M = g^\alpha$ , אז

$$g^{\alpha b-1} = 1 \text{ mod } p$$

נשים לב כי משווה זו נכונה אם  $\alpha(b-1) = 0 \text{ mod } \theta(p)$  כלומר  $\alpha(b-1) = 0 \text{ mod } (p-1)$

נשים לב כי כבר מצאנו  $2 > d$  מתחולק ב- $d$  ומcause שŁemشوואה יש  $d$  פתרונות, נחלק את המשווה ב- $d$ .

$$\frac{\alpha(b-1)}{d} = 0 \text{ mod } \frac{(p-1)}{d}$$

נשים לב כי  $\alpha = 0$  הוא פתרון, لكن סט הפתרונות שלנו יהיה  
 $x_i = 0 + t * \frac{(p-1)}{d} \quad t = 0, 1, \dots, d-1$   
 נשים לב שבמקרה הפתרונות שמצאנו יהיה לנו גם את  $1 \pm$ .  
 את תחילה זה עשינו על  $p$  באופן סימטרי ניתן לעשות אותו גם על  $q$   
 (נעשה זאת כמובן רק במקרה ש  $(\gcd(b-1, q-1) > 2)$ )

את השאריות שמצאנו נוסיף לטבלה של השאריות.  
 נשים לב שם מבקשים למצוא הודעות בלתי מוסתרות לא טריויאליות, הודעות אלו הן כל זוגות השאריות כך שלפחות אחת מהשאריות לא טריויאלית.

### איך ניתן לפרקן

1. brute force - מה שלא ידוע זה  $a$ , מכיוון שהבעה היא Discrete Logarithm Problem נצטרך לעבור על כל הטענות האפשריות של  $a$ , דבר שיקח שנים.
2. Cycle Attack – אנחנו מוצאים התקפה איטרטיבית וסופרים את מספר האיטרציות שעשינו עד אשר קיבל את הטקסט המקורי.

# Hash functions

## הסבר Hash functions

פונקציה זו מקבל הودעה באורך שרירוני ומחזירה ערך בעל גודל קבוע. תפקיך פונקציה זו היא להבטיח שלמות, כלומר לבדוק שכל הودעה שנשלחה לא השתנה בדרך ע"י גורם עוין. ניתן לומר שפונקציה היא וריאציה מתוחכמת לשימוש ב-CRC-*b*. בפונקציה זו המיפוי יכול להיות רבים לאחר, במקרה כזו יכול להיות התנגשות, כלומר הודעות שונות ימופו באותו ערך. למעשה בפונקציות אלו קשה למצוא התנגשויות כאלה.

### תכונות פונקציה Hash

- הפונקציה צריכה להיות קלה לחישוב.
- התנגשות חלשה – בהינתן הודעה  $x$  קשה למצוא הודעה  $y$  כך שיתקיים  $h(x) = h(y)$ .
- התנגשות חזקה – קשה למצוא שתי הודעות  $y, x$  כך שיתקיים  $h(x) = h(y)$ .
- קשה לשחזר את ערך הפונקציה, כלומר  $y$  למצוא  $x$  שקיימים  $h(x) = h(y)$ .

### The Birthday Paradox

אנו משתמשים בפרדוקס זה כדי לדעת את ההסתברות להתנגשות בין הודעות. נעשה את האנלוגיה הבאה:  
נניח כי אנשים הם הודעות, וימם זה מקומות עליהם הודעות מעוברת בפונקציה  $h$ -hash, נרצה לחשב מהי ההסתברות להתנגשות, כלומר שקיים לפחות 2 הודעות שմופות לאותו ערך.  
הבעיה שколה לבעה הבאה:  
נתון חדר שבו יש  $k$  אנשים ומספר ימים  $n$ .

מהי ההסתברות שיהיו לפחות 2 אנשים בתחום החדר שנולדו באותו יום?

- עבור כל איש יש  $n$  ימים בהם הוא יכול להיוולד, מכאן מספר האפשרויות של כל האנשים להיוולד ביום כלשהו הוא  $n^k$ .

נניח כי כל האנשים נולדו ביום אחר, אזי: לאיש הראשון יש  $n$  אפשרויות, לשני יש  $n-1$  ועוד הלאה, מכאן שמספר האפשרויות לכך הוא :

שההסתברות שכולם נולדו ביום אחר היא:

$$P = \frac{n!}{(n-k)!} = \frac{n!}{n^k(n-k)!} = \frac{n * (n-1) * (n-2) * ... * (n-k+1)}{n * n * ... * n} \\ = \left(1 - \frac{1}{n}\right) * \left(1 - \frac{2}{n}\right) * ... * \left(1 - \frac{k+1}{n}\right)$$

נעזר בפרק טילור  $x$ ,  $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^k}{k!}$ , אנחנו יכולים להעזר בקרוב זה רק אם  $k > n$ .

נקבל כי:

$$\left(1 - \frac{1}{n}\right) * \left(1 - \frac{2}{n}\right) * ... * \left(1 - \frac{n-1}{n}\right) \approx e^{-\frac{1}{n} - \frac{2}{n} - \dots - \frac{k+1}{n}} = e^{-\frac{1}{n} * \frac{k(k+1)}{2}} \approx e^{-\frac{k^2}{2n}}$$

מצאנו קירוב להסתברות שככל אחד נולד ביום אחר.

- ההסתברות שמשלימה: קיים לפחות 2 אנשים שנולדו באותו יום היא :

$$1 - e^{-\frac{k^2}{2n}}$$

כלומר ההסתברות של התנגשות עבור  $k$  הודות ו- $\epsilon$  ערכי פונקציה ה-**hash** היא

$$1 - e^{-\frac{k^2}{2n}}$$

## User Identification

נניח ב- **User** וב- **Server**, **User** רוצה לבצע **Log-in** ל- **Server**.  
ל- **Server** יש רשימה מפתקות עבור כל **User** במערכת.  
**Server**-ה שולח מספר רנדומלי  $R$  ושולח אותו ל- **User**.  
ה- **User** יבצע  $E_k(H(R))$  וישלח לה **Server**.  
ה- **Server** יחשב גם  $E_k(H(R))$  ויאזנו בין מה שהוא קיבל למה שהוא חישב.

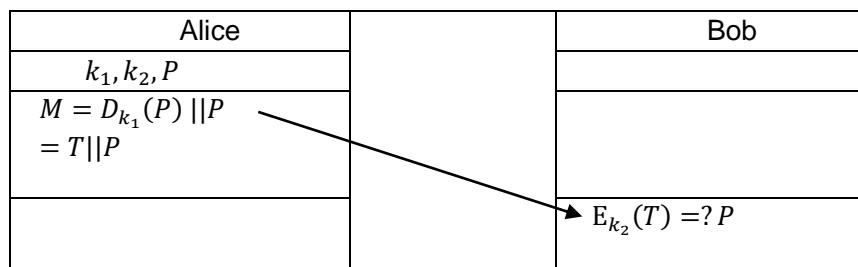
# חתימה דיגיטלית

## הסבר Digital Signatures

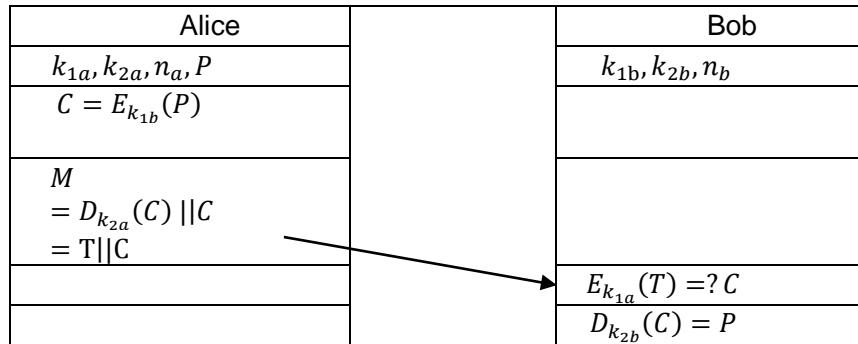
- חתימה דיגיטלית זהו כלי המדמה אישור לפעולה מסוימת, בדומה לחתימה ידנית על מסמך.
- כלומר באמצעות חתימה זו ניתן לדעת מי שלח הודעה מסוימת.
- חתימה דיגיטלית יכולה להיות שימוש ברשות האינטרנט, במיללים וכו'.
- תקבידה הוא להבטיח שלמות בהעברת ההודעה, כלומר שאף אחד לא שינה אותה בדרך.
- חתימה דיגיטלית מספקת:
- .1. איזומת Authentication – ניתן לדעת מי כתוב את ההודעה.
  - .2. שלמות הנתונים Data Integrity – ההודעה לא השתנה בדרך.
  - .3. אי הכחשה Non-Repudiation – מי שחתום על ההודעה בודאות כתוב אותה, לא ניתן להתכחש לו.

## אלגוריתמים לחתימה דיגיטלית

- .1. אליס מייצר 2 מפתחות  $k_1, k_2$  כאשר את  $k_2$  היא מפרסמת.  
יהי הודעה  $P$  כלשהי.



- .2. אליס מייצר 2 מפתחות  $k_{1a}, k_{2a}, n_a$  כאשר את  $k_{1a}$  היא מפרסמת.  
בוב מייצר 2 מפתחות  $k_{1b}, k_{2b}, n_b$  כאשר את  $k_{1b}$  היא מפרסמת.



$n_a, n_b$  אלו פרמטרים אשר מגדרים את הגודל של המפתחות, בעזרתם ניתן לקבוע אם איזה מפתח נשימוש ראשון בתהליך, כלומר בכך לא לאבד מידע נצטרכן תמיד להציג קודם עם המפתח בעל האורך היותר גדול ולאחריו להשתמש עם המפתח הקטן.  
התהליך המתואר בתרשימים מתאים למקרה שבו  $n_a < n_b$

# **אוסף מבחנים ופתרונות**



# **מכללת אורט בראודה**

## **ORT BRAUDE COLLEGE**

100

**לפני הchèלה הבדיקה אנה קרא בעיון את ההוראות ומלא את הפרטים בכתב יד ברורה:  
(שים לב, מחרות הבדיקה נסרקות למאגר נתונים. יש להקפיד שלא לкопל / לתלוש / לכתב בכתבים)**

מועד מיוחד  מועד ב'  מועד א'

# **מחברת בתיינה**

סמסטר: א - ב - קיץ

- כתוב את תשובהתיק בכתב ברור ובעט בלבד בשני העמודים של כל דף.
  - הנך רשאי להקדיש עמוד שלם, או מספר עמודים שלמים לטיותה.
  - אם תכתוב טיטה, הקדש לה את העמוד הימני ואת העתקה לנקי בעמוד השמאלי.
  - העבר קו על אותם החלקים מהטיטה או מהעבודה הנקייה, שאינך רוצה שהבוחן יקרה.
  - אין לשימוש בכל נייר אחר.
  - אם מחברת זו לא תספק לך נא לבקש גליונות נוספים מהמשגיח/ה.
  - מחברות המבחן הן מחברות המכללה ורכושה ועל כן יש להזכירן למשגיח/ה בכל תנאי.
  - כל העבודה, כולל טיטה וחישובי עזר צריים להיכتب במחברת זו בלבד.

**שמור על טוהר הבחינה!  
הישגיות בירושה היא  
הדרך היחידה להצלחה!**



14

מג' פידורי

מחברת מס' \_\_\_\_\_ מטור \_\_\_\_\_



(19) 308884154 ת.ג.  
בוחינה: 06001002252



**אין** **לכתוב** מעבר ל~~קו~~ האדום משני צדי הדף.  
ש **לכתוב** את הבדיקה בעט (כחול / שחור) בלבד.

308884154 יוניברסיטאות

מחלוקת עכרכ

## מקצוע הבדיקה

M222 כיתה

7/2/90 תאריך

## שם המרצה

יועצת יציאה לשירותים

如需更多帮助，請訪問 [我們的網站](#) 或撥打 [電話](#)。

Digitized by srujanika@gmail.com

[www.ncbi.nlm.nih.gov](http://www.ncbi.nlm.nih.gov) [www.ncbi.nlm.nih.gov/entrez](http://www.ncbi.nlm.nih.gov/entrez) [www.ncbi.nlm.nih.gov/blast](http://www.ncbi.nlm.nih.gov/blast)

טוויס  
טוויסטופס מלאוה לשאלון מבתן

שם הקורס: קרייפטולוגיה 1	שם לימוד: ג'
אס' הקורס: 61117	שם המרצה: פרופ/ה זאב וולקוביץ'
אס' סמסטר: א'	מסלול / מגמה: הנדסת תוכנה
מועד הבחינה: א' 07/02/2010	תאריך הבחינה: א'
משך הבחינה: 180 דקות 14 <sup>00</sup>	משך הבחינה: 180 דקות 14 <sup>00</sup>

הוראות לנבחן ולמשגיח

1. יש להחזיר את השאלון בסוף הבחינה.
2. יש לענות על כל השאלות.
3. ניתן להשתמש רק בדף נוסחאות מצורף בטופס.
4. לא ניתן להשתמש בחומר עזר אחר.
5. ניתן לכתוב בעט בלבד.
6. כל העבודה, כולל טיוטה והישובי עוזר, צריכה להיכתב במחברת הבחינה בלבד ו/או בשאלון (כמפורט בסעיף 7) ואינו להשתמש בכל נייר אחר.
7. יש לענות על הבחינה בטופס שאלון הבחינה בלבד.
8. המחברות לא יידקן.
9. טפסי השאלון יידקנו.
10. אין לחלק לסטודנטים פתקי שאלות.
11. היכן שדרושים הסברים תן/י הסבר.
21. אין להעביר כל חומר בין הסטודנטים.
31. מס' הנקודות לכל שאלה נתון בסוגרים אחרי השאלה.

**ב ה צ ל ח ה !!!**

### שאלה מס' 1

נתון אלףית בן 29 אותיות.

א. רשום את הנוסחה לפיענוח של האופן:  $E(x) = 20 \cdot x^5 \pmod{29}$  ( 10 נקודות )

$$\frac{y = 20x^5 (29)}{(20^{-1}y)^{5-1}} \quad : \quad \text{NCLC, J013}$$

$$\underline{20^{-1} = 29 = 20 \cdot 1 - 9 / 9 \cdot 29 - 13 \cdot 20}$$

$$\begin{array}{c} 9 \cdot (29 - 20) - 4 \cdot 20 \\ 9 \cdot 9 - 4 \cdot 20 \\ 9 - 4 \cdot (20 - 9 \cdot 2) \end{array}$$

$$\begin{array}{l} 9 = 2 \cdot 4 + 1 \\ 1 = 9 - (4 \cdot 2) \\ \boxed{20 \cdot 1 = 16} \\ \hline 5 \cdot 1 = \cancel{6}17 \end{array} \Rightarrow x = (16 \cdot y)^{17} = \boxed{7 \cdot y^{17}}$$

אלא אם בדוחשיות ברלמי מופתרות לאוות  $E(x) = 20 \cdot x^5 \pmod{29}$

$$x = 20x^5 \quad (29)$$

92 1110 1962 on 29 c 60

~~2831,22~~ 67c ~~all notes add 1~~ 2831,22

~~\* - o - i - sk' a' c -~~

122 nn'2 'sietz 29 -e 56208

John G. Smith John G. Smith

$x=0(29)$ : the next problem is very similar.

$$\frac{11 \equiv 6 \pmod{29}}{(\epsilon)}$$

$$29 = 5 \cdot 5 - 4$$

$$5 = 4 \downarrow$$
~~$$5 = 2 \cdot 2 + 1$$~~

$$\underline{\theta(29) = 28}$$

~~$$16 \cdot 5^{-1} \pmod{28}$$~~

$$5 \cdot 5^{-1} = 1 \pmod{28}$$

$$28 = 5 \cdot 5 + 3$$

$$5 = 3 + 2$$

$$3 = 2 + 1$$

$$1 = 3 - 2 \Rightarrow$$

$$3 = (5 - 3)$$

$$2 \cdot 3 = 5$$

$$2 \cdot (28 - 5 \cdot 5) = 5$$

$$2 \cdot 28 - \underbrace{11 \cdot 5}$$

$$-11 = \boxed{17} \pmod{28}$$

$$16 \cdot 17 = \pmod{29}$$

$$16 \cdot (16^8)^2 =$$

$$16 \cdot (16)^2 = \boxed{7}$$

שאלה מס' 2 (10 נקודות)

כיצד ניתן להשתמש בהתקפה "meet in the middle" על- מנת להתקיף את הצופן 4DES הבניוי

?  $E_{k_1} \left( D_{k_2} \left( D_{k_3} \left( E_{k_4}(x) \right) \right) \right)$  באופן הבא:  $k_4, k_3, k_2, k_1$  על ארבעה מפתחות שונים

~~השאלה מילוה בפער~~

שאלה מס' 3

הוחלט לבצע החלפת מפתחות באמצעות מערכת Diffie-Hellman על בסיס 43 והיוצר הקטן ביותר.

Alice משתמש במפתח  $a = 5$  ו- Bob משתמש במפתח  $b = 3$ .

12 asfc jen.

$$2^{56} \cdot 2^{56} \cdot 2^{56} + 2^{56} \cdot 3(252^{56} \cdot 1022^{56}) =$$

$\text{O}_2^{168} \Rightarrow$

~~Piano Chords~~ -  
~~Meet in~~ -  
~~meet in the middle~~

*[Handwritten signature]*

*John 710-751*

152 Met-in-the-middle 2,222 a eners 152  
152 Sc 11012 e 152 n

$$O(2^{224})$$

W. J. GUNN N.Y.C. ~~Hill~~ 251

א. חשב את המפתח המשותף. (10 נקודות)

14, 21, 28, 35, 42 : 43 31, 37, 41, 43, 49

1, 2, 3, 6, 7, 14, 21, 42 : 42 6, 12, 24, 48

$$2 \vdash 2^{14} = 1 \Rightarrow 2311 \text{ es } 2311 \text{ G.P}$$

$$3 \vdash 3^6 = 41$$

$$3 \vdash 3^7 = 37$$

$$3^{14} = (3^7)^2 = (37)^2 = 36$$

$$3^{21} = (3^7)^3 = (37)^3 = 42$$

$$3^{42} = 1$$

נוסף

: סדרת

22

Bob

Alic

(10)

$$3^3$$

$$3^5$$

$$28^3 = 22$$

$$27^5 = 22$$

~~22, 8, 22, 22, 22~~

ב. איזה מה מפתחות הפרטיים  $b=7$  או  $b=11$  נראה לך טוב יותר? נמק את תשובתך (10 נקודות)

71 = 61, 21, 16, 22, 22

105, 8(43)=425 25 66 7 e 6662

(10)

110006 6 6662 b=7 = 2 2221 p6

721 p6 V 11058, 81111 11111

nonsp peak 42 622  $\delta = 11 - 2$

201 : 216 b=11 125, 8m en

ג. סטודנט עשה טעות בחישובים ובחר כיווצר  $7 = g$ . מה הטעות הבחרה? (5 נקודות)

43 SW 731' E8 g=7

25 do season Diffie-Hellman p/c

ארצנו, צהיר, 208, מס' 630, מ-20.8.1947.

ל'ג נובמבר 1931, ירושלים ופאל

order 7135 for 65 '9, wards

Now I am for open attack). If you

שאל'ה מס' 4

א. תאר מערכת RSA הבנויה על בסיס  $N = 667$ . (10 נקודות)

C. McCullough

$$(p, q, N, \alpha_b) \Rightarrow p = 23, q = 29, N = 667$$

$$a \cdot b = 1 \quad (\theta(n) = a \cdot b = 1 \quad (616))$$

לפנינו ישנו גורם ב, א

ונדריך את  $a$  שSEND, 16 כפונקציית פירסום.

$M$  מוגדר כמספר פירסום של  $b$ .

$$\frac{N}{M} = C^b = ab \quad \text{ונכון כן } 2216 \neq 872$$

$$\therefore \exists k \in \mathbb{Z} \quad M = M^{ba} \quad (\text{נוכיח})$$

$$\therefore \exists k \in \mathbb{Z} \quad N^{bk} = ab \quad (\text{נוכיח})$$

ב. מצא את כל הבודאות הבלתי מוסתרות לכל מפתח. (15 נקודות)

~~$p=23$~~

~~$q=29$~~

$$M = 0, 1, -1 = 22$$

$$0, 1, -1 = 28$$

$$23 \quad 29 \quad \text{נתקה}$$

$$M(0, 0) = 0$$

$$M(0, 1) = 552$$

$$M(0, -1) = 115$$

$$M(1, 0) = 116$$

$$M(1, 1) = 668 = 1$$

$$M(1, -1) = 231$$

$$M(-1, 0) = 551$$

$$23 \quad 29 \quad \text{נתקה}$$

$$1, 0, 2, 2, 1$$

$$(23 \cdot 24Y_1 + 4 \cdot 29Y_2) = x(N)$$

$$23 \quad 29 \quad \text{נתקה}$$

$$N \quad \text{נתקה}$$

$$N = 867$$

$$15$$

!4 25re

6c

PLS 5125 P.C. 23 a,b 7063

$$\theta(n) = (p-1)(q-1) = \theta(1) \cdot 5$$

pen 287e 25 dr mon 513107  
21375 373e 5622 p,q 56 pens  
1-  $\sqrt{D}$  in p" sick 22 610001/56 56 56  
1562 6820 7232 .513d 220n n pen  
28n

כָּלְבָן

11' N dice 2831.77 CM  
11' 27.3 mm CB  
11' 27.0 mm CA

$$m^b(N) \equiv c \pmod{N}$$

१८४

$$c^a \equiv m^{b^a} \equiv m \pmod{N}$$

$$a \cdot b = \tau(\theta(b)) \cdot c \quad \text{Sdp}$$

לפניהם נתקיימה מלחמת מלחמות, ולבסוף נכבשו ירושלים על ידי הרומיים.

$$M(-1, 1) = 436$$

$$M(-1, -1) = 666$$

שאלה מס' 5 (10 נקודות)

סטודנט החליט להעלות את המהירות של DES ולכן הוא עשה את השינוי באלגוריתם: מפתח לא מחלק בשני חזאים וההוזה הциיקלית מתבצעת לכל ה- 56 ביטים, אחרי כל הזזה, 48 הביטים השמאליים מהווים מפתח הנוכחי מצאו את המפתחות החלשים.

~~מפתח קידום מתקדם~~

~~המקורה מכך מכך מכך~~

~~ריבוקה טען שטחן גאנדרה ריבוקה~~

~~בנוסף ל- 48 ביטים, נקבעו 10 ביטים נוספים.~~

$$1) \frac{0 \dots 0}{0-48} \xrightarrow{\text{48-56}} \frac{0 \dots 0}{48-56} \xrightarrow{\text{6,1}} \text{10}$$

$$2) \frac{1 \dots 1}{0-48} \xrightarrow{\text{48-56}} \frac{1 \dots 1}{48-56} \xrightarrow{\text{6,1}} \text{10}$$

שאלה מס' 6 (10 נקודות)

יהיו  $d$  ו-  $q$  ראשוניים גדולים ו-  $N = pq$ . נבחר  $g$  כך ש-  $\gcd(g, \phi(N)) = 1$ .

הוכיחו כי קיימים שלמים  $j, i$ , כאשר  $j < i < 0$ , כך ש-  $(g^i \equiv g^j \pmod{\phi(N)})$ .

## Euler-Fermat Sc Lecns 28

~~first~~  $\rightarrow \text{if } \gcd(g, \phi(n)) = 1 \text{ then}$

~~then~~  $\because p, q \text{ are } i, j \text{ such that}$

$$g^{\phi(\phi(n))^i} = g^{\phi(\phi(n))^j} \pmod{\phi(n)} = \\ 1^i = 1^j \pmod{\phi(n)}$$

Q

~~so~~,  $j = 3, i = 21 \text{ and}$

$$g^{\phi((p-1)(q-1))^1} = g^{\phi((p-1)(q-1))^3} \pmod{\phi(p-1)(q-1)}$$

~~so~~  $\therefore p, q | N = p \cdot q \rightarrow \text{if } p, q \text{ are such that}$

$$\phi(n) = (p-1)(q-1)$$

DEFINITION

$$g^1 = 1^3 \pmod{(p-1)(q-1)}$$

### BLOCK-CIPHERS .1

,  $e(X_m) = Y_m$  PLAINTEXT

can  $X_m = (x_1, x_2, \dots, x_m)$  block of the words of

. CIPHERTEXT  $Y_m = (y_1, y_2, \dots, y_m)$

### Euler-Fermat Theorem .2

for all  $a \in \mathbb{Z}$  such that  $\gcd(a, n) = 1$  we have

$$a^{n-1} \pmod{n} = 1$$

3. English alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

**פתרון של המבחן 01/03/2010  
בקורס: קריפטולוגיה 1 / 61117**

שאלה מס' 1 (15 נקודות)

נשתמש בצופן היל (HILL) עם גודל בלוק  $m = 3$  ומפתח  $K$  מעל אלפבית בן 29 אותיות ( $n=29$ ). מצא את כל ההודעות הבלתי מוסתרות.

$$K = \begin{pmatrix} 1 & 0 & 17 \\ 3 & 1 & 2 \\ 2 & 15 & 1 \end{pmatrix}$$

פתרונות:

$\det K = (-29 + 17 \cdot 43) \bmod 29 = (17 \cdot 14) \bmod 29 = 6$  ומפני שמתקיים התנאי הפיכות של מטריצה  $K$  או  $\gcd(\det K, n) = 1$  ניתן להשתמש במטריצה  $K$  כמפתח בצופן היל. ההודעות הבלתי מוסתרות הן פתרונות של המשוואה  $X \cdot K = X \cdot I$  או  $(K - I) \cdot X = 0$ . מפני ש-

$$\gcd(11, 29) = 1 \quad \det(K - I) = \det \begin{pmatrix} 0 & 0 & 17 \\ 3 & 0 & 2 \\ 2 & 15 & 0 \end{pmatrix} = 17 \cdot 45 \bmod 29 = 11$$

הפייה ויש למשווה רק פתרון טריוויאלי  $X = 0$ .

שאלה מס' 2 (10 נקודות)

Bob בונה את צופן היל (HILL) עם מפתח A וчисב שמספר ההודעות הבלתי מוסתרות שווה לשתיים. לאחר מכן Alice החליטה לשנות את הצופן ולהשתמש במטריצה  $(A - I)^m$ , בטור המפתח. כיצד

ניתן להעריך את הבחירה של Alice ?

•  $\text{N}^{\text{NO}_3^-}$  :  $\text{N}^{\text{H}_3^+}$  :  $\text{N}^{\text{NH}_2^-}$  :  $\text{N}^{\text{NH}_3^+}$  :  $\text{N}^{\text{NH}_2^-}$  :  $\text{N}^{\text{NH}_3^+}$  :  $\text{N}^{\text{NH}_2^-}$

$A\vec{x} = \vec{x}$  ပါမ်မှာ,  $\boxed{x=1}$  မျှတော်းပါ။

גָּמְנִים וְעַמְקִים

$$\|A - I\| = 0 \iff (\forall i=1) \|A - I\|_i = 0 \iff \text{All } a_{ii} = 1$$

$$\text{If } \lambda_1, \lambda_2, \dots, \lambda_n \text{ are eigenvalues of } A, \text{ then } \det(A - \lambda I) = (\lambda_1 - \lambda)(\lambda_2 - \lambda) \cdots (\lambda_n - \lambda)$$

מגניט פיזיקי הנק במקלט אפלטון, מ

לעומת הדוגמה הקודמת, מטרת הפעלה היא  $(A - I)^{-1}$ , כלומר  $A^{-1}$ .

גראן: אם יתאפשר מילוי נסיבותם של גורמים

**שאלה מס' 3 (10 נקודות)**

הסברתו של אחת הבודעה עליה - 0.5 (הסתברויות אחרות שוות בינהן). איזה מידע גוטן הסימן?

הסתברות של אחת ההודעות עוללה - 0.5 (הסתברות אורה או לא שותה ב-50%). רוחן ונטחן ארכויים 8 (וושטן ג'טס) נזקם  $P_i = \frac{1}{8}$ ,  $1 \leq i \leq 8$

$$H(X) = \sum_{i=1}^8 p_i \cdot \log_2 \frac{1}{p_i} \dots$$

... =  $\sum_{i=1}^8 \frac{1}{8} \cdot \log_2 8 = 1 \cdot \log_2 2^3 = \boxed{3}$

$$(2 \leq i \leq 8) \quad p_i = \frac{1-\frac{1}{2}}{8-1} = \frac{1}{14} - 1 \quad p_1 = \frac{1}{2} \Rightarrow 100, 778$$

1(r) {3n p0nd}

לעומת זו הערך המרבי של ה Entropy (בנוסף לערך ה-Entropy)

$$H(Y) = \sum_{i=1}^8 p_i \cdot \log_2 \left( \frac{1}{p_i} \right) = \frac{1}{2} \cdot \log_2 2 + 7 \cdot \frac{1}{14} \cdot \log_2 14 = \\ = \frac{1}{2} + \frac{1}{2} \cdot \log_2 14 \approx \boxed{2.403}$$

הערך המרבי של Entropy

$$I = H(X) - H(Y) \approx 0.596$$

שאלה מס' 4 (15 נקודות)

תאר את שיטת הפענוח של האלגוריתם DES וסביר את נכונותה.

השיטה הינה פונקציית פולינום, כלומר  $f(x) = ax^2 + bx + c$ , כאשר  $a, b, c$  הם קבועות.

$$f(x) = IP^{-1}(R_{16} L_{16}) \text{ (1)}$$

: 830 + 38  $i+16$  7128 (2)

$$(L_i) \rightarrow R_{i-1} \quad (2.1)$$

$$(R_i \oplus f(L_i, k_i)) \rightarrow L_{i-1} \quad (2.2)$$

$$IP \left( IP^{-1}(L_0 R_0) \right) : \text{נטען} \quad (3)$$

במקרה הראשון (3)

$$L_0 R_0 \text{ נסימן} \quad (4)$$

Given:  $L_0 R_0$ , INPUT  $\rightarrow$   $x$  ו-  $y$

ונז\_outer, והוא גודל של 80bit. סימון מילוי מושג ב- $k_i$ .

ונז\_outer  $\neq$  סימון גודל. אולם, אם נז\_outer ישייך ל- $y$  (ולו לא ל- $x$ )

<sup>4</sup> נז\_outer ו- $y$  ישייכו לאותה פונקציית פולינום. נז\_outer נז\_outer ישייך ל- $x$  ו- $y$  ישייך ל- $k_i$ .

שאלה מס' 5 (15 נקודות)

נבחר  $N = 899$  כבסיס למערכת RSA.

מצא את כל המפתחות הציבוריים שעבורם מספר ההודעות הבלתי מוסתרות שווה ל- 105.

$$P=29, q=31 \quad \text{נוסף } N=899 \quad 29 \cdot 31 = 899$$

(15)

נמצא  $k$  כך ש  $105 \mid (N-1)^k - 1$

$$\text{נמצא } k = \frac{(1+9\gcd(k-1, P-1))(1+9\gcd(k-1, q-1))}{(1+9\gcd(k-1, 28))(1+9\gcd(k-1, 30))} = 105$$

$$(1+9\gcd(k-1, 28)) \cdot (1+9\gcd(k-1, 30)) = 105$$

$$105 = 3 \cdot 5 \cdot 7$$

$$1+9\gcd(k-1, 28) = 15 \quad ; \quad \text{נמצא } k \text{ כך ש}$$

$$1+9\gcd(k-1, 30) = 7 \quad ; \quad \text{נמצא } k$$

$$(1+9\gcd(42, 28)) \cdot (1+9\gcd(42, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=43 \quad (1)$$

$$(1+9\gcd(126, 28)) \cdot (1+9\gcd(126, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=127 \quad (2)$$

$$(1+9\gcd(294, 28)) \cdot (1+9\gcd(294, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=295 \quad (3)$$

$$(1+9\gcd(378, 28)) \cdot (1+9\gcd(378, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=379 \quad (4)$$

$$(1+9\gcd(462, 28)) \cdot (1+9\gcd(462, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=463 \quad (5)$$

$$(1+9\gcd(546, 28)) \cdot (1+9\gcd(546, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=547 \quad (6)$$

$$(1+9\gcd(714, 28)) \cdot (1+9\gcd(714, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=715 \quad (7)$$

$$(1+9\gcd(798, 28)) \cdot (1+9\gcd(798, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=799 \quad (8)$$

$$(1+9\gcd(882, 28)) \cdot (1+9\gcd(882, 30)) = 15 \cdot 7 \quad \Leftarrow \quad k=883 \quad (9)$$

5

שאלה מס' 6 (15 נקודות)

נ霏

בנה מערכת Diffie-Hellman על בסיס 2 וכאשר מודול החישוב הוא אחד מהגורמים של בסיס המ מערכת RSA בשאלה מס' 5. מצא את המפתח המשותף אם המפתחות הפרטיים שווים ל- 5 ו- 7.

$$1. \quad \begin{array}{ccccccccc} 2^5 & 12 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ \boxed{P=29} & \boxed{Z_{29}} & & & & & & & \end{array} \quad (15)$$

רעיון,  $2^{5+1} \equiv 31 \pmod{29}$

$$\therefore \boxed{g = 31}, \quad g^{k_1+k_2} \quad \text{לפניהם}$$

$$\begin{aligned} (2^5)^7 \pmod{29} &\equiv 3^7 \pmod{29} \equiv \\ &\equiv 3 \cdot (3^3)^2 \pmod{29} \equiv 3 \cdot (-2)^2 \pmod{9} \equiv \\ &\equiv \boxed{12 \pmod{29}} \quad \text{לפניהם} \quad \therefore \end{aligned}$$

שאלה מס' 7 (20 נקודות)

ו- Bob רצו לבנות מערכת התקשורת כולל חתימה דיגיטלית בין הצדדים. בנה אותה אם ידוע לך מהם משתמשים במערכת RSA כך ש-  $N_1 = 77$  הוא בסיס המערכת של Bob ו-  $N_2 = 143$  הוא בסיס המערכת של Alice. בחר מפתחות ורגן חולופי הועדות עם החתימות: Alice שולחת OK- YES.

: Bob → Alice (rsa) נכון או לא נכון (20-)

$k_1, k_2 = 1 \pmod{\phi(n)}$	$\gcd(k, \phi(n)) = 1$	$\phi(N_2) = 120$	$N_1 = 77$	$\phi(N_1) = 60$
$k_1^{(1)} = 13$	ריבוע	$k_1^{(1)} = 7$	ריבוע	$k_2^{(1)} = 43$
$k_2^{(1)} = 37$	ריבוע	$k_2^{(1)} = 43$	ריבוע	$7 \cdot 43 = 1 \pmod{60}$
$13 \cdot 37 = 1 \pmod{120}$				

$$\left. \begin{array}{l} E_{k_1^{(1)}} \left( E_{k_2^{(1)}}(M) \right) \\ D_{k_1^{(1)}} \left( D_{k_2^{(1)}}(C) \right) \\ E_{k_1^{(2)}} \left( E_{k_2^{(1)}}(M) \right) \\ D_{k_1^{(2)}} \left( D_{k_2^{(2)}}(C) \right) \end{array} \right\} \begin{array}{l} \text{:Bob ל Alice (rsa)} \\ \text{:Bob ל Alice (rsa)} \\ \text{:Bob ל Alice (rsa)} \\ \text{:Alice ל Bob (rsa)} \end{array}$$

$$\left. \begin{array}{l} E_{k_1^{(1)}}(M) = M^7 \pmod{77} \\ E_{k_2^{(1)}}(M) = M^{43} \pmod{77} \end{array} \right\} \begin{array}{l} \text{מודולו 77} \\ \left( \begin{array}{l} E_{k_1^{(2)}} = M^{13} \pmod{143} \\ E_{k_2^{(2)}} = M^{37} \pmod{143} \end{array} \right) \end{array}$$

Bob

: Bob -f YES paris Alice

24 18

4

Y for Paris j'ad

$$\text{Y nos: } E_{k_2}^{(2)} = (24)^{37} \pmod{143} \equiv$$

-08

$$\equiv (12 \cdot 2)^{37} \equiv 12 \cdot \underbrace{(12^2)^{18}}_1 \cdot 2 \cdot 2^{36} \equiv 12 \cdot 1 \cdot 2 \cdot 2^{36} \equiv$$

$$\equiv 12 \cdot 2 \cdot \underbrace{(2^{12})^3}_9 \equiv 12 \cdot 2 \cdot 9^3 \equiv 24 \cdot \underbrace{(4 \cdot 23)^3}_{23^3} \equiv$$

$$\equiv 24 \cdot 64 \cdot 12 \equiv \underbrace{12^2}_{1} \cdot 128 \equiv \boxed{128 \pmod{143}}$$

$$E_{k_1}^{(1)}(143) = 143^7 \pmod{77} \equiv (66)^7 \pmod{77} \equiv$$

$$\equiv (-11) \cdot (-11)^3 \cdot (-11)^3 \equiv (-11) \cdot (-11) \cdot (-11) \cdot (-11)^2 \equiv$$

$$\equiv 11^2 \cdot 11^2 \cdot 11^2 \cdot (-11) \equiv 44 \cdot 44 \cdot (-11) \equiv \underbrace{44^2}_{1} \cdot 44 \cdot (-11) \equiv \boxed{55 \pmod{77}}$$

Alice -f O nro bob

nro

$$\text{O nro: } E_{k_2}^{(1)}(14) = 14^{43} \pmod{77} = \boxed{10}$$

$$E_{k_1}^{(2)}(\cancel{\text{nro}}) = \boxed{c^{13} \pmod{143}}$$



## טופס מלאוה לשאלון מבחן

שם הקורס: קרייפטולוגיה 1	שנת לימוד: ג'
מספר הקורס: 61117	שם המרצה: פרופ' זאב וולקוביץ'
מספר סטטוס: ב'	מסלול / מגמה: הנדסת תוכנה
מועד הבחינה: ב' 11/08/2010	תאריך הבחינה: ב'
שעת הבחינה: 14 <sup>00</sup>	משך הבחינה: 180 דקות

## הוראות לנבחן ולמשגיח

- .1. יש להציג את השאלון בסוף הבחינה.
- .2. יש לענות על כל השאלות.
- .3. ניתן להשתמש רק בדף נוסחאות מצורף בטופס.
- .4. לא ניתן להשתמש בחומר עזר אחר.
- .5. ניתן לכתוב בעט בלבד.
- .6. כל העבודה, כולל טויטה וחישובי עוזר, צריכה להיות במחברת הבחינה בלבד ו/או בשאלון (כמפורט בסעיף 7) ואין להשתמש בכל נייר אחר.
- .7. יש לענות על הבחינה בטופס שאלון הבחינה בלבד.
- .8. המחברות לא יידקנו.
- .9. טפסי השאלון יידקנו.
- .10. אין לחלק לסטודנטים פתקי שאלות.
- .11. היכן שדרושים הסברים תני הסבר.
- .12. אין להעביר כל חומר בין הסטודנטים.
- .13. מס' הנקודות לכל שאלה נקבע בסוגרים אחרי שאלה.
- .14. כל שאלה 10 נקודות.

**ב ה צ ל ח ה !!!**

שאלה מס' 1

נתון טקסט אנגלי גדול המוצפן בעורת צוֹפָן הַהְזֹנָה. האות כי נפוצה בטקסט המוצפן היא T.  
 4                  19  
 $E \rightarrow T \Rightarrow K = 15$                   10-

⇒

D ← S

O ← D

G ← V

(?)

DOG

שאלה מס' 2

במערכת מפתחות של צוֹפָן כלשהו יש 32 מפתחות. כחוצאה מהתקפה סטטיסטית מקבלים שהסתברות של מפתח אחד שווה ל- 0.6, הסתברות של מפתח שני שווה ל- 0.3 והסתברויות אחרות שוות אחת לשניה. מהו המידע שנדרש לנו להתקפה הסטטיסטית אם לפניה ההסתברויות של כל המפתחות יהיו שוות מבחינת הפרש הערכים של האנטרופיה.

$$P(K_1) = 0.6$$

$$P(K_2) = 0.3$$

$$P(K_i) = \frac{1}{300}$$

$$H(Y) = \log_2 32 = 5$$

$$H(H(Y)) = -0.6 \log_2 0.6 - 0.3 \log_2 0.3 - \sum_{i=1}^{30} \frac{1}{300} \log_2 \frac{1}{300} = 0.963 + 0.822$$

$$I = 5 - 1.785 \approx 3.214$$

1.785

שאלות מס' 3

Bob שלא למד מספיק טוב את המ鏘וע "криיפטולוגיה 1", החליט להעלות את סיבוכיות צופן DES ולהשתמש בצופן כפול עם מפתחות שונים (DOUBLE DES). Alice שנכחה בכל הרצאות אמרה ל- Bob שהרעיון שלו לא טוב. מדוע Alice צודקת?

10) (k) BOB receives files from Alice 1993

תבונת פונקציית נגזרת של פונקציה

لار جو جاں اور میں اسیں پسیں Meet in the milk zone

2) 032 k 1870 2) > 8 (2.  $^{56}(\text{Og}_2^{56})$ , 281 102N)

203 Bob /25 2001 11/8/2001 pf sk

Millions      13.7M      left      16.0M      3WFF

מִתְּוָאֵר וְמַבְּרָכָה בְּזֶבֶחַ וְמַזְבֵּחַ לְפָנֵי

גָּלְדִּים כַּלְמָנָה . שְׁלֹמֹה וְעַמְּלֵיכָם .

$$2^{5p} \left(\alpha\right)_2 2^{5k}$$

שאליה מס' 4

א. במערכת Diffie-Hellman כל משתמש בוחר מפתח. כמה אפשרויות לעשות זאת כך שהמפתח המשותף יהיה יוצר ? מודול מערכות הוא המספר  $d$ .

pk 7311 p2 9<sup>o</sup> sk 7311 9 pk

$$K_1 \cdot K_2 = d \text{ i.e. } p^3 \text{ and } \gcd(d, p-1) = 1 \text{ . note}$$

2016-131 (a) תיעוד מסמך רשות

$\Theta(\Theta(p))$

~~000~~ O'GARAHAN 'Je  
GIRNA 'Ife 

ב. חשב את המפתח המשותף בביטחון  $p=41$  ויוצר גדול יותר אם Alice משתמש במפתח  $k_1 = 5$   
- Bob משתמש במפתח  $k_2 = 3$

$$\text{לול}  
g^k \mod p \quad 13^5 \mod 41 \quad 6^2 \quad 12 \quad 6 \quad 35 \quad 16 \quad \text{ולול} \quad 10$$

$$\text{המפתח המשותף הוא } 35 \quad \text{gcd}(21, 40) = 1$$

3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39

לול  $g^k \mod p$   $13^5 \mod 41$   $6^2 \mod 41$   $35 \mod 41$

$$6^2 \mod 41 = g = 6^{21} = 35$$

ולול  $g^k \mod p$

$$35^{35} \mod 41 = 38$$

ולול  $g^k \mod p$

שאלות מס' 5

נתונה מערכת RSA הבנויה על בסיס 1271.

- א. מצא את כל ההודעות הבלתי מוסתרות עבור המפתח  $b=23$ .

10

$$n=1271$$

$$P=31 \rightarrow P-1=30 \quad \{1, 2, 3, 5, 6, 10, 15, 30\}$$

$$2^2=4, 2^3=8, 2^5=1 \Rightarrow 2^{311} \text{ ist } 2$$

$$3^2=9, 3^3=27, 3^5=26, 3^6=16, 3^{10}=(3^5)^2=26^2=25, 3^{15}=(3^5)^3=26^3=30, 3^{30}=(3^10)^3=26^3=1$$

$$M = 3^{\phi} \% P$$

7311 3 ←

$$M^k = M \% P$$

$$\Rightarrow 3^{\alpha K} = 3^{\alpha \% P} \Rightarrow 3^{\alpha(K-1)} = 1 \% P \Rightarrow \boxed{\alpha(K-1) = 0 \bmod \theta(\phi)}$$

$$22\alpha = 0 \bmod 30 / \circ 2$$

$$11x \equiv 0 \pmod{15} \Rightarrow x_1 = 0, x_2 = 15$$

$$1) M=0 \quad (\text{مثلاً})$$

$$2) \quad 3^0 = 1$$

$$3) \quad 3^{15} = 30 \quad (=1)$$

*✓ CNA*

$$q=41 \rightarrow q-1=40 \quad \{1, 2, 4, 5, 8, 10, \underline{20}, 40\}$$

(סימבוני וריאציות)

$$\boxed{g=6}$$

73/1'

$$6^\alpha = M \% q$$

כל  $M^k = M \% q$  כלומר אם מודולו

$$6^{2\alpha K} = 6^\alpha \% q \rightarrow 6^{\alpha(K-1)} = 1 \bmod q$$

$$2\alpha = 0 \bmod 40 \quad /:2$$

$$11\alpha = 0 \bmod 20$$

$$\alpha_1 = 0, \quad \alpha_2 = 20$$

$$1) M=0 \quad (\text{דרכו})$$

$$2) 6^0 = 1$$

$$3) 6^{20} = 40 = (-1)$$

$\downarrow$  סעיפים

<u>VIPON</u>									
$P=31$	0	0	0	1	1	1	-1	-1	
$q=41$	0	1	-1	0	1	-1	0	1	
	0	124	1147	1148	1	1024	123	247	1270

vipon יפה נסxfk fs

0, 124, 1147, 1148, 1, 1024, 123, 247, 1270.

ב. ההודעה  $C = 8$  התקבלה במערכת הנ"ל כתוצאה מהצפנה של הודעה  $M$  על ידי מפתח פתוח  $b=23$   
מצא את ההודעה המקורית  $M$

(10)

$$K_1 \cdot K_2 = 1 \pmod{\phi(n)}$$

$$23K_2 = 1 \pmod{1200}$$

$$\begin{array}{l} \gcd(1200, 23) = \\ 1200 = 23 \cdot 52 + 4 \end{array} \quad \begin{array}{l} \gcd(23, 4) = \\ 23 = 4 \cdot 5 + 3 \end{array} \quad \begin{array}{l} \gcd(4, 3) = \\ 4 = 3 \cdot 1 + 1 \end{array} \quad \begin{array}{l} \gcd(4, 1) = \\ \end{array}$$

$$l = 4 - 3 = 4 - (23 - 4 \cdot 5) = 4 - 23 + 4 \cdot 5 = 6 \cdot 4 - 23 = 6(1200 - 23 \cdot 52) - 23$$

$$6 \cdot 1200 - 312 \cdot 23 - 23 = 6 \cdot 1200 - 313 \cdot 23 \Rightarrow K_2 = 887$$

$$\begin{aligned} M &= 8^{887} \% 1271 = 8^5 \cdot 8^{882} \% 1271 = 993 \cdot (8^7)^{126} \% 1271 \\ &= 993 \cdot 2^{126} \% 1271 = 993 \cdot (2^9)^{14} \% 1271 = 993 \cdot 512^4 \% 1271 \end{aligned}$$

$$993 \cdot (512^3)^4 \% 1271 = 993 \cdot 4^3 \% 1271 = 2 \% 1271$$

שאלה מס' 6

נתונה מערכת KNAPSACK עם סדרה פומבית  $\{38, 7, 14, 47, 25\}$ . כמו כן ידוע שמודול  $N=50$ , והאיבר הראשון בסדרה סודית הוא  $a_1=2$ .

א. מצא את הסדרה הסודית.

$$\begin{aligned} 2x &= 38 \bmod 50 \Rightarrow \left\langle \begin{array}{c} 19 \\ 44 \end{array} \right\rangle \quad (10) \\ x &= 19 \quad \Leftarrow \text{סוד} \quad 44 \quad 14 \quad 50 \quad 25 \quad 47 \quad 44 \\ x^{-1} &= 29 \% 50 \end{aligned}$$

$$\begin{aligned} 38 \times 29 \bmod 50 &= 2 \\ 7 \times 29 \bmod 50 &= 3 \\ 14 \times 29 \bmod 50 &= 6 \\ 47 \times 29 \bmod 50 &= 13 \\ 25 \times 29 \bmod 50 &= 25 \\ \{2, 3, 6, 13, 25\} & \quad \text{Private.} \end{aligned}$$

ב. ההודעה המוצפנת היא  $C=10$ . מצא את ההודעה המקורית  $M$ .

$$\begin{aligned} C &= 10 \\ M &= x^{-1} \cdot c = 29 \cdot 10 = 40 \quad \Leftarrow = [M] \cdot A \\ C &= 10 \rightarrow \underline{\underline{0 \ 1 \ 0 \ 1 \ 0}} \quad (4) \quad (16) \end{aligned}$$

שאלה מס' 7 (10)

חשב את  $6^{6662} \mod 25$

$\begin{array}{r} 25 \\ \times 5 \\ \hline 125 \end{array}$

$$\varnothing(25) = 25 \left(\frac{1}{5}\right) = 20$$

$$6^{20} \equiv 1 \pmod{25} \quad (\text{מilk})$$

$$(6^{20})^{333} \cdot 6^2 = 1 \cdot 6^2 \% 25 = \boxed{11 \% 25}$$

## דף גוסחות

### Euler-Fermat Theorem .1

.  $a^{\varphi(n)} \mod n = 1$  מתקיים אם  $\gcd(a,n) = 1$

.  $a^{n-1} \mod n = 1$  אם  $n$  מספר ראשוני אז

. 2. גניחה ש-  $a^{\varphi(n)} \mod n = 1$  אזי למשווה  $ax \equiv b \pmod{n}$  יפייה בבדיקה  $g = \gcd(a,n)$ .  
פתרונות מהצורה:  $x = t\left(\frac{b}{g}\right)x_0 + s\left(\frac{n}{g}\right)$  כאשר  $t$  נוע בין 0 ל-1.  $x_0$  הוא פתרון של המשווה  $\left(\frac{a}{g}\right)x \equiv \left(\frac{n}{g}\right) \pmod{1}$ . לאחרת המשואה אינה ניתנת לפתרון.

### 3. משפט השארית הסיני:

יהיו  $d_1, d_2, \dots, d_t$  מספרים זרים בזוגות ו-  $d = d_1d_2 \dots d_t \mid n$ . אזי למערכת המשוואות

$$x \equiv m \pmod{d_i}$$

כאשר  $m$  נוע בין 1 ל- $d_i$ , יש פתרון משותף  $x$  בתחום  $[0, n-1]$ .

$$\frac{n}{d_i} * y_i \equiv 1 \pmod{d_i} \text{. CAN } x = \left[ \sum_{i=1}^t \left( \frac{n}{d_i} \right) y_i x_i \right] \pmod{n}$$

. 4. צופן RSA:  $E(x) = x^b \pmod{n}$

$n$  הוא מכפלה של שני מספרים ראשוניים שונים  $p, q$ .

### 5. האלפבית האנגלאי, קודים ושכיחיות /BALPIH/ :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
82	15	28	43	127	22	20	61	70	2	8	40	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
67	75	19	1	60	63	91	28	10	23	1	20	1

. 6. אנטרופיית המערכת  $H(K) = -\sum_{i=1}^n p_i \log(p_i)$ . CAN  $p_i$  הסתברות למצאה במצב  $i$   
כאשר  $i = 1, \dots, n$ .

**פתרון של המבחן 07/12/2012**  
**בקורס: קריפטולוגיה 1 /61117/**

**שאלה מס' 1**

על אלפבית בן  $n$  סימנים פונקציה מורכבת פועלת באופן הבא: בהתחלה מתבצעת פונקציה לiniarity  $n \bmod n = y = E(x) = (a \cdot x + b) \bmod n$  ולאחר מכן הפונקציה המערבית  $. z = E(y) = c \cdot y^d \bmod n$

- (א) נסח התנאים עבור פרמטרים  $n, a, b, c$  ו-  $d$  כדי שהפונקציה המורכבת תגדיר צופן המצפין את כל סימני הא"ב. (10 נקודות)

פתרון:

- (1)  $n$  - מספר טבעי גדול מ-1 ,  $/ \gcd(a,n)=1$
- (2)  $a$  - מספר זר ל-  $n$  ,  $/ \gcd(a,n)=1$
- (3)  $b$  - מספרשלם  $n > b > 0$
- (4)  $c$  - מספר זר ל-  $n$  ,  $/ \gcd(c,n)=1$
- (5)  $d$  - מספר זר ל-  $n$  ,  $/ \gcd(d,\theta(n))=1$

- (ב) אם  $n$  הוא קבוע איזה מספר הנוסחות (הביטוים) השונות של הצופן מוגדר לעיל (מספר הצירופים של פרמטרים שmericיבים נוסחות שונות)? (10 נקודות)

פתרון:

לפי סעיף א' מספר ערכים מתאימים לבחירה הוא:  
 $n - 1$ ,  $\theta(n) - 1$ ,  $\theta(\theta(n)) - 1$ ,  $\theta(\theta(\theta(n))) - 1$ . סה"כ לפי עקרון המכפל מספר האפשרויות הוא  $(n - 1) \cdot (\theta(n) - 1) \cdot (\theta(\theta(n))) - 1$ .

- (ג) בטא את נוסחת הפענוח לצופן זהה. (10 נקודות)

פתרון:

$$\begin{aligned} \text{נוסחה } (1) \quad x &= (y - b) \cdot a^{-1} \bmod(n) \quad \text{נובע ש- } y = (a \cdot x + b) \bmod(n) \\ \text{נוסחה } (2) \quad y &= (e \cdot z)^f \bmod(n) \quad \text{נובע ש- } z = c \cdot y^d \bmod(n) \\ &\quad . f = d^{-1} \bmod(\theta(n)) \quad \text{ו- } e = c^{-1} \bmod(n) \\ &\quad . x = ((e \cdot z)^f - b) \cdot a^{-1} \bmod(n) \quad \text{(2) ב- (1) נותנת נוסחה} \end{aligned}$$

**שאלה מס' 2**

נשתמש בצופן היל (HILL)  $Y = X \cdot K \bmod n$  עם גודל בלוק  $m = 3$  ומפתח  $K = \begin{pmatrix} 1 & 2 & a \\ a & 2 & 1 \\ 1 & 1 & 2a \end{pmatrix}$  מעלה"ב בן 29 אותיות.

- (א) לאילו ערכים של פרמטר  $a$  ניתן להשתמש במטריצה זו? (10 נקודות)

פתרון:

- מטריצה  $K$  הפיכה אם ורק אם  $\gcd(n, \det K) = 1$  ומפני שמספר  $n$  הוא ראשוני התנאי שקול לכך.

. נחשב  $\det K$  לפי השורה הראשונה:  $\det K \neq 0$

$$\det K = \det \begin{pmatrix} 1 & 2 & a \\ a & 2 & 1 \\ 1 & 1 & 2a \end{pmatrix} = 1 \cdot (2 \cdot 2 \cdot a - 1 \cdot 1) - 2 \cdot (a \cdot 2 \cdot a - 1 \cdot 1) + a \cdot (a \cdot 1 - 1 \cdot 2) = -3a^2 + 2a + 1$$

כל לראות ש-  $a_1 = 1$  הוא השורש אז  $-3a^2 + 2a + 1 = -(a-1)(3a+1)$  ופתרון של המשוואה

. כל ערכי פרט ל- 1 ו- 19 מתאימים.

(ב) נתון ש-  $a = 5$  . בטא נוסחה לפענו ופענה את  $(5,3,3)$  . (20 נקודות)

פתרון:

$$, (\det K)^{-1} = 23^{-1} \pmod{29} = 24, \det K = -3a^2 + 2a + 1 = -3 \cdot 25 + 2 \cdot 5 + 1 = -64 \equiv 23 \pmod{29}$$

$$K^{-1} = 24 \cdot \begin{pmatrix} 19 & 9 & 3 \\ 14 & 5 & 1 \\ -8 & -5 & -8 \end{pmatrix}^T = \begin{pmatrix} 21 & 17 & 11 \\ 13 & 4 & 25 \\ 14 & 24 & 11 \end{pmatrix}$$

$$X = Y \cdot K^{-1} = (5,3,3) \begin{pmatrix} 21 & 17 & 11 \\ 13 & 4 & 25 \\ 14 & 24 & 11 \end{pmatrix} = (12, 24, 18) \pmod{29}$$

ג) עברו אילו ערכים של  $a$  קיימות הודעות בלתי מוסתרות שונות מוקטור האפס ?

מצא את ההודעות האלו. (15 נקודות)

פתרון:

$(K - I)$  כמו בסעיף א', אם  $\det(K - I) \neq 0$  .  $X(K-I)=0 \Leftrightarrow XK=X$  . היפיכה ולהמערכת קיימים פתרון ייחודי  $X=0$  . נחשב שורשים המשוואה

$$\det(K - I) = \det \begin{pmatrix} 0 & 2 & a \\ a & 1 & 1 \\ 1 & 1 & 2a-1 \end{pmatrix} = -2(2a^2 - a - 1) + a(a-1) = -3a^2 + a + 2 = -(a-1)(3a+2)$$

. שני פתרונות הם  $a_1 = 1$  ו-  $a_2 = 9$

הערך הראשון לא מתאים לצוף.

לערך  $a_2 = 9$  נחפש פתרון כללי של המערכת:

$$\text{א.ז.א.}, \begin{cases} x_3 = t \\ x_2 = 16t \\ x_1 = 6t \end{cases} \Leftrightarrow \begin{cases} x_3 = t \\ 9x_2 = -t \\ 2x_1 + x_2 + x_3 = 0 \end{cases} \Leftrightarrow \begin{cases} 9x_2 + x_3 = 0 \\ 2x_1 + x_2 + x_3 = 0 \\ 9x_1 + x_2 + 17x_3 = 0 \end{cases}$$

.  $X = \{(6t, 16t, t), t \in \mathbb{Z}_{29}\}$  קבוצת ה Hodoot הבלתי מוסתרות היא

### שאלה מס' 3

נתונה מערכת ההצפנה :  $K = \{1, 2, 3\}$  ו-  $Y = \{A, B, C\}$ ,  $X = \{a, b, c\}$  לפי הטבלה:

k	E(a)	E(b)	E(c)
1	A	B	C
2	C	A	B
3	B	C	A

$$\text{בנחנה ש } P(k=2) = \frac{1}{4}, P(k=1) = \frac{1}{2} \text{ וגם } P(c) = \frac{1}{2}, P(b) = \frac{1}{6}, P(a) = \frac{1}{3} \text{ ו } P(k=3) = \frac{1}{4}$$

(א) חשב את התפלגות הסימנים המוצפנים  $\{Y\}$ . (10 נקודות)

פתרון:

$$P(A) = P(a) \cdot P(k=1) + P(b) \cdot P(k=2) + P(c) \cdot P(k=3) = \frac{1}{3} \cdot \frac{1}{2} + \frac{1}{6} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{3}$$

$$P(B) = P(a) \cdot P(k=3) + P(b) \cdot P(k=1) + P(c) \cdot P(k=2) = \frac{1}{3} \cdot \frac{1}{4} + \frac{1}{6} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} = \frac{7}{24}$$

$$P(C) = P(a) \cdot P(k=2) + P(b) \cdot P(k=3) + P(c) \cdot P(k=1) = \frac{1}{3} \cdot \frac{1}{4} + \frac{1}{6} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}$$

(ב) האם המערכת היא בעלת תכונה "perfect secrecy"? אם לא, אז בחר בתפלגות המפתח כך שהמערכת תהיה בעלת "perfect secrecy" (15 נקודות)

פתרון:

נבדוק את התכונה לתפלגות הנתון:

$$P(a | A) = \frac{P(a \& A)}{P(A)} = \frac{P(a) \cdot P(A | a)}{P(A)} = \frac{\frac{1}{3} \cdot \frac{1}{2}}{\frac{1}{3}} = \frac{1}{2} \neq \frac{1}{3} = P(a)$$

לכן המערכת היא בעלת תכונה "perfect secrecy"

נבחר בשביל קבועות המפתחות היחידה ונבדוק שזו המערכת היא בעלת תכונה "perfect secrecy".

במקרה זה קל לראות (כמו בסעיף א) ש-

לכל הودעה מקורית מתקיים:

$$P(x | y) = \frac{P(x \& y)}{P(y)} = \frac{P(x) \cdot P(y | x)}{P(y)} = \frac{\frac{1}{3} \cdot \frac{1}{3}}{\frac{1}{3}} = P(x)$$

ז.א. להתפלגות ייחודית המערכת היא בעלת תכונה "perfect secrecy".



## מכלחת אורט ברואודה ORT BRAUDE COLLEGE

לפני תחילת הבחינה אנא קרא בעיון את ההוראות ומלא את הפרטים בכתב יד ברוח:  
(שים לב, מתחבירות הבחינה נסrokות למאגר נתונים יש להקפיד שלא לкопל / לתלוש / לכתוב בכתב)

מועד א'  מועד ב'  מועד מיוחד

שם המושא 3/3

### מחברת בחינה

סמלטר: א - ב - קייז

- כל העבודה, כולל טיוטה וחישובי עור צרים מלהיכתב במחברות זו בלבד.
- שאלון הבחינה לא יבדק ע"י המרצה אלא אם צוין אחרת בשאלון, וכן יש לענות על כל השאלות במחברות הבחינה בלבד.
- אין להשתמש בכל נייר אחד.
- אם מחברת זו לא מספיק לך נא לבדוק גליונות נוספים מהמשגיח/ה.
- מחברות המבחן הן מחברות המכילה ורוכשה ועל כן יש להחזירן למשגיח/ה בכל תנאי.

- כתוב את תשובהתיק בכתב ברור וביגע בלבד בשני העמודים של כל דף.
- תוך רשיין להקדיש עמוד שלם, או מספר עמודים שלמים לטיוטה.
- אם כתוב טיוטה, הקדש לה את העמוד הימני ואת העתקה לנקי בעמוד השמאלי.
- הعبر קו על אותן החלקים מהטיוטה או מהעבודה חנוקה, שאין רוצה שהובוון יקרה.
- אין להשתמש בנוזל מהיקה (טיפקס).
- אסור לקרוע כל חלק שהוא מן המחברות או להשאיר עמודים חלקים בין התשובות.

**שמור על טוהר הבחינה!**  
**הישגים ביושר היא**  
**הדרך היהודית להצלחה!**



מס' סידורי:

מחברת מס' \_\_\_\_\_ מתוך \_\_\_\_\_ מחברות



ת.ז. 039701891  
בחינה: 006001004476

5



אין לכתרג מעבר לקו האודום משני צדי הדף.  
יש לנכון את הבחינה בעט (כחול / שחור) בלבד.

מס' ת"ז 1991

מחולקה בננה

מקצוע הבחינה קלטת פיקוד

ביתה M208

תאריך 5/3/12

שם המרצה prof. זילנארט עלייאן

שעת יציאה לשירותים

שעת חזרה לשירותים

+ 30

### טופס מלאוה לשאלון מבחן

שם הקורס: קרייפטולוגיה 1	שם לימוד: ג'
מספר הקורס: 61117	שם המרצה: פרופ' זאב ולקוביץ'
מספר סטטוס: א'	מסלול / מגמה: הנדסת תוכנה
מועד הבחינה: ב' 05/03/2012	תאריך הבחינה: ב'
משך הבחינה: 180 דקות	שעת הבחינה: 9:00

#### הוראות לנבחן ולמשגיח

1. יש להחזיר את השאלון בסוף הבחינה.
2. יש לענות על כל השאלות.
3. ניתן להשתמש רק בדף נוסחאות מצורף בטופס.
4. לא ניתן להשתמש בחומר עזר אחר.
5. ניתן לכתוב בעט בלבד.
6. כל העבודה, כולל טיוטה וחישובי עוזר, צריכה להיכתב במחברת הבחינה בלבד ו/או בשאלון (כמפורט בסעיף 7) ולא吟 להשתמש בכל נייר אחר.
7. יש לענות על הבחינה בטופס שאלון הבחינה בלבד.
8. המחברות לא ייבדקו.
9. טפסי השאלון ייבדקו.
10. אין להחלק לסטודנטים פתקי שאלות.
11. היכן שדרושים הסברים תוו/י הסבר.
12. אין להעביר כל חומר בין הסטודנטים.
13. מס' הנקודות לכל שאלה נתון בסוגרים אחרי השאלה.

**ב ה צ ל ח ה !!!**

סה"כ	6	5	4	3	2	1
94	10	10	10	10	10	14

1

שאלה מס' 1

ברצוננו להשתמש בצופן HILL עם מטריצת-מפתח  $\begin{pmatrix} 2 \cdot a & 13 \\ 15 & a \end{pmatrix}$  מעל אלף-בית האנגלית מורחב בן 29 סימנים.

א. עבור איזה ערכים של  $a$  המטריצה מדירה צופן? (10 נקודות)

סעיף א' גאוגרפיה ק-א. כב, כט ושבץ כנראה (גנרטר, ע"י) (4)

$$\gcd(\det K) = 1 \text{ או } \lambda \text{ זרולית } \Leftrightarrow \text{המקוינט } (\lambda) \text{ לא}$$

$$\det K = 2a^2 - 15 \cdot 13 = (2a^2 + 8) \mid 29.$$

$$2a^2 + 8 \equiv 0 \pmod{29} \quad \text{מ长时间, } 2a^2 \equiv -8 \pmod{29} \quad \text{מ长时间, } a^2 \equiv \frac{-8}{2} \pmod{29} \quad \text{מ长时间, } a^2 \equiv 4 \pmod{29} \quad \text{מ长时间, } a \equiv \pm 2 \pmod{29}$$

. א. ב' גנטוגרפיה (ג) פ.ר.ון, יג נושא כנראה ק-ט (10)

ב. מצא את ההודעות הבליי מוסתרות עבור ערך הפרמטר  $a=4$  (10 נקודות).

$$\tilde{x}K = \tilde{x} \quad \text{כעתו } \tilde{x} \text{ מושתרך והוא כפלי הנקוינט:} \quad K = \begin{pmatrix} 8 & 13 \\ 15 & 4 \end{pmatrix} \quad (10)$$

יעוד בזק  $K^{-1}$ ,  $\lambda=1$  ו-  $K-I$  פ"ג  $\lambda=1$  ו-  $K-I$  פ"ג

:  $K^{-1} = \frac{1}{29}(4 - 15, 13 - 8) = \frac{1}{29}(-11, 5)$  פ"ג  $K-I = \frac{1}{29}(8 - 15, 13 - 4) = \frac{1}{29}(-7, 9)$  פ"ג

$$\det \begin{pmatrix} 8 & 13 \\ 15 & 4 \end{pmatrix} = 21 - 195 = 0 \neq 0 \Rightarrow \text{המודולוס } 29 \text{ לא מחלק את }$$

ההמג'ר והמג'ר מושתרך והוא כפלי הנקוינט של הנקוינט.

$$\tilde{x}K = \tilde{x} \Rightarrow \tilde{x}K = \tilde{x}I \Rightarrow \tilde{x}(K-I) = 0$$

$$(x_1, x_2) \cdot \begin{pmatrix} 8 & 13 \\ 15 & 4 \end{pmatrix} = (0, 0)$$

$$\begin{cases} 7x_1 + 15x_2 = 0 \% 29 \\ 13x_1 + 3x_2 = 0 \% 29 \end{cases} \Rightarrow \begin{cases} 7x_1 = -15x_2 \\ 13x_1 = -3x_2 \end{cases} \Rightarrow \begin{cases} 7x_1 = 14x_2 \\ 13x_1 = 26x_2 \end{cases} \Rightarrow x_1 = 2x_2$$

תפלת השילוח נזקקה לשלוחה מוקדם כדי להניב תוצאות טובות.

$$\mathcal{M} = (2x, x).$$

$$M = \begin{pmatrix} 20, 10 \end{pmatrix} \Rightarrow \begin{pmatrix} 20, 10 \end{pmatrix} \begin{pmatrix} 8 & 13 \\ 15 & 4 \end{pmatrix} = \begin{pmatrix} 310, 300 \end{pmatrix} = \begin{pmatrix} 20, 10 \end{pmatrix} \quad \because \text{It's a } 1 \times N + 1 \times P$$

שאליה מס' 2

אם אפשר להשתמש בהתקפה "Meet in the Middle" נגד הצופן "Triple DES" ?

ככן" אוז הסבר באיזה **מקרה** ההתקפה היא אפקטיבית. (10 נקודות)

10

. TDES is Meet in the regular weekly meeting at 10:00 AM.

**הצ'קען** גיינט ווועגאַס כ. (זְפָנָן נְזָבֵן וְלִבְנֵי אֶרְזָה וְאֶרְזָה)

UNUNP (1') pic .  $2^{56} \cdot 2^{56} \cdot 2^{56} = 2^{168}$  - if brute force approach

$2^{56} \cdot 2^{56} = 2^{112}$  - If we're on the 77th floor, meet in the middle.

$\Sigma^{112}$  פירמה  $\Sigma^{57}$  - נ 130' מ' ג' 20ES-8 ערכו של ג' נ הינה נספח פון ורכ

וְאֵין כִּי-בָּא בְּמִזְרָחַ וְאֵין כִּי-בָּא בְּמִזְרָחַ (grate font) וְאֵין כִּי-בָּא בְּמִזְרָחַ (grate font) וְאֵין כִּי-בָּא בְּמִזְרָחַ (grate font)

### שאלה מס' 3

תאר והסביר את היתרונות והחסרונות של שיטת CBC בהצפנה 알고ריתם סימטרי (10 נקודות)

שאל'ה מס' 4

הסביר את הדרישות ל- HASH-פונקציה . (10 נקודות )

: 0/020 Hash 1"3)15an

① נסעה ברכבת מירושלים לאנטויניה; הינה אן, רוכב אנטויניה.

(2) נ.ג.ה. קלחן/בג'ן זיהוי, גענער זיך אַלטער גענער גענער (x) ה'.

(ג) נסחיה דודר מינימום: בז' נסחיה דודר מינימום  $y = 1$

10

שאלה מס' 5

נתונה מערכת RSA הבנויה על בסיס  $N = 667$ .

א. רשום את כל ההודעות הבלתי מוסתרות עבור מפתח כלשהו במערכת זו. (10 נקודות)

P.4

$$\begin{aligned}
 N &= 667, \quad P = 29, \quad q = 23, \quad \phi(N) = M^{-1} \cdot n = M^{-1} \cdot 667 \quad (\text{נקודות}) \\
 g &< \phi(29, 23) \quad (23, 6) \quad (6, 5) \quad | \quad 1 = 6 - 5 = 6 - (23 - 3 \cdot 6) = 4 \cdot 6 - 23 = 4 \cdot (29 - 23) - 23 = \\
 29 &= 1 \cdot 23 + 6 \quad 23 = 3 \cdot 6 + 5 \quad 6 = 3 + 1 \quad | \quad = 4 \cdot 29 - 5 \cdot 23 \Rightarrow \\
 \Rightarrow 29^{-1} &= 4 \cdot 23 \\
 23^{-1} &= 24 \cdot 29 \Rightarrow M = (29 \cdot 4 \cdot r_1 + 23 \cdot 24 \cdot r_2) \% 667 \\
 (0, 0) &\Rightarrow 0 \quad (1, 0) = 116 \quad (-1, 0) = 551 \\
 (0, 1) &\Rightarrow 552 \quad (1, 1) = 1 \quad (-1, 1) = 436 \\
 (0, -1) &\Rightarrow \cancel{115} \quad (1, -1) = 231 \quad (-1, -1) = 666
 \end{aligned}$$

(10)

ב. ההודעה  $C = 11$  התקבלה במערכת הנ"ל כחוצאת ההצפנה של הודעה  $M$  על-ידי מפתח פתוח  
b. מצא את ההודעה המקורית  $M$ . (10 נקודות)

(10)

$$\left\{ \theta(667) = 22.28 \right\} \quad (616, 123) \quad | \quad \text{123}$$

$$b=123 \Rightarrow 123 \cdot a = 1\% . 616 \Rightarrow \quad 616 = 5 \cdot 123 + 1 \quad | \quad 1 = 616 - 5 \cdot 123$$

$$\Rightarrow a = -5 = 611\% . 616 \Rightarrow a = 611 \quad \text{נוסף ל-616}$$

$$M = C^a \cdot 1.667 \Rightarrow 11^{611} \cdot 1.667 = 11^{616-5} = 11^{\theta(667)-5} = 11^{-5} =$$

$$= (11^{-1})^5 = (182)^5 = 182^4 \cdot 182 = 520\% . 667 \quad //$$

ג. תאר חתימה דיגיטלית אפשרית שימושה יכול לבצע במערכת זו. (10 נקודות)

(10)

ונראה כיצד ניתן לעשות זאת.

$$145 \cdot 17 = 1\% \cdot \frac{616}{145} \quad \Leftarrow \quad \text{2} = 1\% \cdot 616$$

$$c_2 = 145 \cdot 145 \cdot 17 \quad \text{אך} \quad c_2 = M^e \cdot M^d \quad \text{ולפיכך} \quad c_2 = M^{ed}$$

$(d, n, M, Y)$ : גרעין ופונקציית גיבוב

כאמור נבחרו  $\sqrt{n}$  אסימטרית כפונקציית גיבוב

לפיכך (הנורמה) מוגדרת כפונקציית גיבוב  $N$ , מוגדרת

$$z = M \quad \text{প্রিম} \quad \text{ז' נאצ'ן} \quad z = r^d \cdot n \quad : \text{ז' נאצ'ן} \quad \text{①}$$

לפיכך, נשים,

7. תאר וממש מספירת מערכת Diffie-Hellman הבניי על בסיס של הגורם הגדל של  $N$ .

(10 נקודות)

10

$$z_{29}^* - 2 \approx g = 2 \iff p-1 \text{ so } p \text{ prime} \quad i = \{2, 4, 7, 14\} \quad p=29 \\ p-1=28$$

$$\text{Alice: } a=17 \Rightarrow z^{17} \% 29 = 21 \quad \left. \begin{array}{l} \\ \end{array} \right\} \Rightarrow 21^{11} = 18^{17} \% 29 = 26 \% 29 \Rightarrow k=26$$

$$\text{Bob: } b=11 \Rightarrow z^{11} \% 29 = 18$$

$k$  הוא מילוי הנדרש.

Alice for  $k$  הינה הנדרש.

Bob for  $k$  הינה הנדרש.

שאלה מס' 6

**מערכת KNAPSACK** בנויה על סמך הסדרה הפומבית  $B=(46,14,51,24,16)$ , מודול חישוב

N=55 גורם סודי V=23. פענחו את ההוויה C=26 (נקודות 10).

$$\begin{array}{cccccc} & \text{: } 1, 8, \text{ Super increasing, } 2, 3, 5, 7, 11, 13, 17 \\ \hline (55, 23) & (23, 9) & (9, 5) & (5, 4) & | 1+5+4 = 5-(9-5) = 2 \cdot 5 - 9 = 2 \cdot (23-2 \cdot 9) - 9 = \\ 55 = 2 \cdot 23 + 9 & 23 = 2 \cdot 9 + 5 & 9 = 1 \cdot 5 + 4 & 5 = 4 + 1 & | = 2 \cdot 23 - 5 \cdot 9 = 2 \cdot 23 - 5 \cdot (55-2 \cdot 23) = 12 \cdot 23 - 5 \cdot 55 \end{array}$$

$$\Rightarrow V^{-1} = 12 \Rightarrow \begin{matrix} 12 \cdot 46 \% .55 = 2 \\ 12 \cdot 14 \% .55 = 3 \end{matrix} \Rightarrow A = (2, 3, 7, 13, 27)$$

$$12 \cdot 51 \% \cdot 55 = ?$$

$$12 \cdot 24 \% \cdot 55 = 13$$

$$12 \cdot 16\% \cdot 55 = 27$$

165-32-28

$$C = 26 \Rightarrow C_t = 26 \cdot 12\% \cdot 55 = 37 \Rightarrow \left[ \begin{array}{ccccc} 2 & 3 & 7 & 13 & 27 \\ 0 & 1 & 1 & 0 & 1 \end{array} \right]$$

$$M = 01101 = 13 \quad : 10^P_1$$

## דף נוסחות

### Euler-Fermat Theorem .1

. $a^{\theta(n)} \text{ mod } n = 1$  מתקיים אם  $\text{gcd}(a,n) = 1$

. $a^{n-1} \text{ mod } n = 1$  אם  $n$  מספר ראשוני או

### 2. משפט השארית הסיני:

יהיו  $d_1, d_2, \dots, d_t$  מספרים זרים בזוגות ו-  $d_1d_2\dots d_t = n$ . אזי למערכת המשוואות

$$x \text{ mod } d_i = x_i$$

כasher  $x$  נع בין 1 ל-  $t$ , יש פתרון משותף  $x$  בתחום  $[0, n-1]$ .

$$\frac{n}{d_i} * y_i \equiv 1 \pmod{d_i} \quad \text{כאז } x = \left[ \sum_{i=1}^t \left( \frac{n}{d_i} \right) y_i x_i \right] \text{ mod } n$$

### 3. הצופן RSA:

$E(x) = x^b \text{ mod } n$   $n$  הוא מכפלה של שני מספרים ראשוניים שונים  $p$  ו-  $q$ .

### 4. סימוביי הצופן KNAPSACK: $A = (a_1, a_2, \dots, a_n)$ - סדרה סודית,

$B = (b_1, b_2, \dots, b_n)$  - סדרה פומבית,  $V$  - גורם סודי.

### 5. האלפבית האנגלוי, קודים ושכיחויות /אלפית/ :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
82	15	28	43	127	22	20	61	70	2	8	40	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
67	75	19	1	60	63	91	28	10	23	1	20	1

**פתרון של המבחן 07/12/2012**  
**בקורס: קריפטולוגיה 1 /61117/**

**שאלה מס' 1**

על אלפבית בן  $n$  סימנים פונקציה מורכבת פועלת באופן הבא: בהתחלה מתבצעת פונקציה לiniarity  $n \text{ mod } n = E(x) = (a \cdot x + b) \text{ mod } n$  ולאחר מכן הפונקציה המערבית  $. z = E(y) = c \cdot y^d \text{ mod } n$

- (א) נסח תנאים עבור פרמטרים  $a, b, c$  ו-  $d$  כדי שהפונקציה המורכבת תגדיר צוף המצפין את כל סימני הא"ב. (10 נקודות)

פתרון:

- (1)  $n$  - מספר טבעי גדול מ-1 ,  $/ \text{gcd}(a,n)=1$
- (2)  $a$  - מספר זר ל-  $n$  ,  $/ \text{gcd}(c,n)=1$
- (3)  $b$  - מספרשלם  $0 \leq b < n$
- (4)  $c$  - מספר זר ל-  $n$  ,  $/ \text{gcd}(d,\theta(n))=1$
- (5)  $d$  - מספר זר ל-  $n$  ,  $/ \text{gcd}(d,\theta(n))=1$

- (ב) אם  $n$  הוא קבוע איזה מספר הנוסחות (הביטוים) השונות של הצופן מוגדר לעיל (מספר הצירופים של פרמטרים שmericיבים נוסחות שונות)? (10 נקודות)

פתרון:

לפי סעיף א' מספר ערכים מתאימים לבחירה הוא:  
 $n$  -  $\theta(n)$  -  $b$  ,  $a$  -  $\theta(\theta(n))$  -  $d$  . סה"כ לפי עקרון המכפל מספר האפשרויות הוא  $n \cdot \theta(n) \cdot \theta(\theta(n))$

- (ג) בטה את נוסחת הפענוח לצופן זהה. (10 נקודות)

פתרון:

$$\begin{aligned} \text{נוסחה } (1) \quad x &= (y - b) \cdot a^{-1} \text{ mod}(n) \quad \text{נובע ש- } y = (a \cdot x + b) \text{ mod } n \\ \text{נוסחה } (2) \quad y &= (e \cdot z)^f \text{ mod}(n) \quad \text{נובע ש- } z = c \cdot y^d \text{ mod } n \\ &\quad . f = d^{-1} \text{ mod}(\theta(n)) \quad \text{e} = c^{-1} \text{ mod}(n) \quad \text{כאן } (n) \\ &\quad . x = ((e \cdot z)^f - b) \cdot a^{-1} \text{ mod}(n) \quad \text{(2) נותנת נוסחה } (1) \end{aligned}$$

**שאלה מס' 2**

נשתמש בצופן היל (HILL)  $Y = X \cdot K \text{ mod } n$  עם גודל בלוק  $m = 3$  ומפתח  $K = \begin{pmatrix} 1 & 2 & a \\ a & 2 & 1 \\ 1 & 1 & 2a \end{pmatrix}$  מעלה"ב בן 29 אותיות.

- (א) לאילו ערכים של פרמטר  $a$  ניתן להשתמש במטריצה זו? (10 נקודות)

פתרון:

- מטריצה  $K$  הפיכה אם ורק אם  $\det K = 1$  ומפני שמספר  $a$  הוא ראשוני התנאי שקול לו

. נחשב  $\det K$  לפי השורה הראשונה:  $\det K \neq 0$

$$\det K = \det \begin{pmatrix} 1 & 2 & a \\ a & 2 & 1 \\ 1 & 1 & 2a \end{pmatrix} = 1 \cdot (2 \cdot 2 \cdot a - 1 \cdot 1) - 2 \cdot (a \cdot 2 \cdot a - 1 \cdot 1) + a \cdot (a \cdot 1 - 1 \cdot 2) = -3a^2 + 2a + 1$$

כל לראות ש-  $a_1 = 1$  הוא השורש אז  $-3a^2 + 2a + 1 = -(a-1)(3a+1)$  ופתרון של המשוואה

. כל ערכי פרט לו  $a_2 = 19$  והוא  $3a+1 \equiv 0 \pmod{29}$  מתאים.

(ב) נתון ש-  $a = 5$  . בטא נוסחה לפענו ופענה את  $(5,3,3)$  .  $(5,3,3)$  נקודות  
פתרון:

,  $(\det K)^{-1} = 23^{-1} \pmod{29} = 24$  ,  $\det K = -3a^2 + 2a + 1 = -3 \cdot 25 + 2 \cdot 5 + 1 = -64 \equiv 23 \pmod{29}$

$$K^{-1} = 24 \cdot \begin{pmatrix} 19 & 9 & 3 \\ 14 & 5 & 1 \\ -8 & -5 & -8 \end{pmatrix}^T = \begin{pmatrix} 21 & 17 & 11 \\ 13 & 4 & 25 \\ 14 & 24 & 11 \end{pmatrix}$$

$$X = Y \cdot K^{-1} = (5,3,3) \begin{pmatrix} 21 & 17 & 11 \\ 13 & 4 & 25 \\ 14 & 24 & 11 \end{pmatrix} = (12, 24, 18) \pmod{29}$$

ג) עברו אילו ערכי  $a$  קיימות הודעות בלתי מוסתרות שונות מוקטור האפס ?  
מצא את ההודעות הללו .  $(15$  נקודות $)$

פתרון:

$(K - I)$  כמ"ז בסעיף א', אם  $\det(K - I) \neq 0$  .  $X(K-I)=0 \Leftrightarrow XK=X$  .  
הפיכה ולהמערכת קיימים פתרון ייחודי  $X=0$  . נחשב שורשים המשוואה

$$\det(K-I) = \det \begin{pmatrix} 0 & 2 & a \\ a & 1 & 1 \\ 1 & 1 & 2a-1 \end{pmatrix} = -2(2a^2 - a - 1) + a(a-1) = -3a^2 + a + 2 = -(a-1)(3a+2)$$

. שני פתרונות הם  $a_1 = 1$  ו-  $a_2 = 9$

הערך הראשון לא מתאים לצוף.

לערך  $a_2 = 9$  נחפש פתרון כללי של המערכת:

$$\text{א.א.}, \begin{cases} x_3 = t \\ x_2 = 16t \\ x_1 = 6t \end{cases} \Leftrightarrow \begin{cases} x_3 = t \\ 9x_2 = -t \\ 2x_1 + x_2 + x_3 = 0 \end{cases} \Leftrightarrow \begin{cases} 9x_2 + x_3 = 0 \\ 2x_1 + x_2 + x_3 = 0 \\ 9x_1 + x_2 + 17x_3 = 0 \end{cases}$$

.  $X = \{(6t, 16t, t), t \in \mathbb{Z}_{29}\}$  קבוצת ה Hodoot הבלתי מוסתרות היא

### שאלה מס' 3

נתונה מערכת ההצפנה :  $K = \{1, 2, 3\}$  ו-  $Y = \{A, B, C\}$ ,  $X = \{a, b, c\}$  לפי הטבלה:

k	E(a)	E(b)	E(c)
1	A	B	C
2	C	A	B
3	B	C	A

$$\text{בנחנה ש } P(k=2) = \frac{1}{4}, P(k=1) = \frac{1}{2} \text{ וגם } P(c) = \frac{1}{2}, P(b) = \frac{1}{6}, P(a) = \frac{1}{3} \text{ ו } P(k=3) = \frac{1}{4}$$

(א) חשב את התפלגות הסימנים המוצפנים  $Y = \{A, B, C\}$ . (10 נקודות)

פתרון:

$$P(A) = P(a) \cdot P(k=1) + P(b) \cdot P(k=2) + P(c) \cdot P(k=3) = \frac{1}{3} \cdot \frac{1}{2} + \frac{1}{6} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{3}$$

$$P(B) = P(a) \cdot P(k=3) + P(b) \cdot P(k=1) + P(c) \cdot P(k=2) = \frac{1}{3} \cdot \frac{1}{4} + \frac{1}{6} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} = \frac{7}{24}$$

$$P(C) = P(a) \cdot P(k=2) + P(b) \cdot P(k=3) + P(c) \cdot P(k=1) = \frac{1}{3} \cdot \frac{1}{4} + \frac{1}{6} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}$$

(ב) האם המערכת היא בעלת תכונה "perfect secrecy"? אם לא, אז בחר בתפלגות המפתח כך שהמערכת תהיה בעלת "perfect secrecy" (15 נקודות)

פתרון:

נבדוק את התכונה להתפלגות הנתונה:

$$P(a | A) = \frac{P(a \& A)}{P(A)} = \frac{P(a) \cdot P(A | a)}{P(A)} = \frac{\frac{1}{3} \cdot \frac{1}{2}}{\frac{1}{3}} = \frac{1}{2} \neq \frac{1}{3} = P(a)$$

לכן המערכת היא בעלת תכונה "perfect secrecy"

נבחר בשביל קבועות המפתחות היחידה ונבדוק שזו המערכת היא בעלת תכונה

"perfect secrecy"

במקרה זה קל לראות (כמו בסעיף א) ש-  $P(A) = P(B) = P(C) = \frac{1}{3}$ , לכן לכל הودעה מקורית

מתקיים:  $x \in \{A, B, C\}$  ולכל הודעה מוצפנת  $y \in \{a, b, c\}$

$$P(x | y) = \frac{P(x \& y)}{P(y)} = \frac{P(x) \cdot P(y | x)}{P(y)} = \frac{\frac{1}{3} \cdot \frac{1}{3}}{\frac{1}{3}} = P(x)$$

ז.א. להתפלגות ייחודה המערכת היא בעלת תכונה "perfect secrecy".

**פתרונות של המבחן 25/01/2013**  
**בקורס: קרייפטולוגיה 1 /61117/ 1**

**שאלה מס' 1**

על אלפבית בן  $n = 26$  סימנים וגודל בлок  $3 = m$  צופן מורכב פועל באופן הבא:

$$\begin{aligned} \text{בהתחלת מתבצע צופן תמורה } \pi &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ ולאחר מכן מתבצע צופן היל} \\ &\cdot \begin{pmatrix} 1 & 2a & 1 \\ 3 & 0 & 2 \\ 2 & 3 & 2 \end{pmatrix} \text{ עם מפתח } E(X) = X \cdot K \end{aligned}$$

a) לאילו ערכי פרמטר  $a$  ניתן להשתמש以此 צופן זה? (20 נקודות)

פתרון:

$$\text{צופן תמורה הוא מקרה פרטי של צופן היל, בשאלה זאת עם מטריצה } \pi, \text{ כך } \pi = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

ש-  $E(X) = X \cdot [\pi]$ . לכן אנו מקבלים נוסחת הצופן המורכב  $K \cdot [\pi] \cdot X$ .

$$A = [\pi] \cdot K = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2a & 1 \\ 3 & 0 & 2 \\ 2 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 2 \\ 3 & 0 & 2 \\ 1 & 2a & 1 \end{pmatrix} \text{ היל עם מטריצה-מפתח}$$

התנאי הכרחי לקיום הצופן או הפיכות המטריצה הוא  $\det A \neq 0$ . כאן

$$\det A = 2 \cdot (-4a) - 3 \cdot 1 + 2 \cdot 6a = 4a - 3 \quad \text{ולכן התנאי הוא } 1 \neq 4a - 3$$

גורמים משותפים יותר מ-1 או ביטוי  $(4a - 3)$  לא מתחלק ב-2 וגם לא מתחלק ב-13,

ששקלול למערכת שני אי-שוויונים:  $(4a - 3) \neq 0 \pmod{2}$  שמתקיים לכל  $a$ , וגם

$$(4a - 3) \neq 0 \pmod{13} \Leftrightarrow 4a \neq 3 \pmod{13} \Leftrightarrow [4^{-1} \pmod{13} = 10] \Leftrightarrow a \neq 4 \pmod{13}$$

מן שאנו עובדים ב-  $Z_{26}$  התשובה הסופית  $a \neq 4$  וגם  $a \neq 17$ .

b) לאילו ערכי פרמטר  $a$  מספר הודעות בלתי מוסתרות הוא מינימלי ומעבר לכך ערך של פרמטר  $a$  מספר הודעות בלתי מוסתרות הוא מקסימלי? לערך זה מצא את כל ההודעות הבלתי מוסתרות. (20 נקודות)

פתרון:

התנאי שהודעה בלתי מוסתרת הוא  $X = X \cdot A$  או  $0 = X \cdot (A - I)$  שתלויב-

$$\det(A - I) = \det \begin{pmatrix} 1 & 3 & 2 \\ 3 & -1 & 2 \\ 1 & 2a & 0 \end{pmatrix} = 8 - 2a(-4) = 8(a + 1)$$

לכן יש שני מקרים אפשריים:

. במקורה זה מספר הודעות בלתי מוסתרות  $a = 25$  או  $a = 12$  .  $\text{gcd}(\det A, 26) = 26$  .**1**

$$\text{הוּא מְקַסִּימָלִי. נִמְצָא אֹתָן: } X \cdot \begin{pmatrix} 1 & 3 & 2 \\ 3 & -1 & 2 \\ 1 & 24 & 0 \end{pmatrix} = 0$$

$$\xrightarrow{\exists 5^{-1}(26)} \begin{cases} x_1 + 3x_2 + x_3 = 0 \\ 5x_1 + 5x_2 = 0 \\ 2x_1 + 2x_2 = 0 \end{cases} \xleftarrow{2R_1+R_2} \begin{cases} x_1 + 3x_2 + x_3 = 0 \\ 3x_1 - x_2 + 24x_3 = 0 \Leftrightarrow \\ 2x_1 + 2x_2 = 0 \end{cases}$$

2. פתרון כללי  $X = (t, -t, 2t)$

.**2**  $\text{gcd}(\det A, 26) = 2$

הערה (לא הכרחית): פתרית המערכת נותרת שני פתרונות ו-  $X_1 = (13, 13, 0)$  ו-  $X_0 = (0, 0, 0)$

**ג) נתון ש-  $a = 6$  . פענח את  $(13, 15, 13)$  . (20 נקודות)**

פתרון:

$$X = Y \cdot A^{-1} \pmod{n} \Leftrightarrow Y = X \cdot A \pmod{n}$$

$$\text{כآن: } A^{-1} \pmod{n} \text{ נחשב . } A = \begin{pmatrix} 2 & 3 & 2 \\ 3 & 0 & 2 \\ 1 & 12 & 1 \end{pmatrix}$$

$$\Leftrightarrow (\det A)^{-1} \pmod{26} = 5 \Leftrightarrow \det A = 4a - 3 = 21$$

$$A^{-1} = 5 \cdot \begin{pmatrix} 2 & -1 & 10 \\ 21 & 0 & 5 \\ 6 & 2 & 17 \end{pmatrix}^T = 5 \cdot \begin{pmatrix} 2 & 21 & 6 \\ -1 & 0 & 2 \\ 10 & 5 & 17 \end{pmatrix} = \begin{pmatrix} 10 & 1 & 4 \\ 21 & 0 & 10 \\ 24 & 25 & 7 \end{pmatrix}$$

$$X = (13, 15, 13) \cdot \begin{pmatrix} 10 & 1 & 4 \\ 21 & 0 & 10 \\ 24 & 25 & 7 \end{pmatrix} = (3, 0, 7) \pmod{26}$$

## שאלה מס' 2

מעל אלפבית בן n אותיות (n מספר ראשוני) פועל צופן מורכב משני שלבים: צופן ליניארי

וצופן מערכתי  $E(x) = c \cdot x^d \pmod{n}$  . **באיזה סדר** (מה בהתחלה

**ומה לאחר מכן** טוב יותר להשתמש בצלפים האלה ? נמק את תשובה.

פתרון:

אם בהתחלה אנו מצפנים בצלפן ליניארי ולאחר כך בצלפן מערכתי אז הצלפן המורכב נראה כ:

$$E(x) = c \cdot (ax + b)^d \pmod{n}$$

$$\dots \cdot n \cdot \theta(n) \cdot \theta(n) \cdot \theta(\theta(n))$$

אם מדר הפעולות הפוך אז הצופן המורכב נראה כ-  $E(x) = (acx^d + b) \bmod n$ . כאן אנו רואים רק 3 פרמטרים כי כפל  $ac$  הוא מספר אחד ושה"כ מספר צירופים שווה ל-

$$n \cdot \theta(n) \cdot \theta(\theta(n))$$

לכן סדר ראשון יותר עדיף.

### שאלה מס' 3

מערכת  $X$  יכולה להציג ב-  $n$  מצבים בלתי תלויים. לאיזו התפלגות הסתברותית האנטרופיה של המערכת מקסימלית ולאיזו התפלגות היא מינימלית? נמק והוכח את תשובהך. (20 נקודות)

פתרון:

האנטרופיה של המערכת שיכולה להציג ב-  $n$  מצבים עם התפלגות  $(p_1, p_2, \dots, p_n)$  שווה ל-

$$H(X) = -\sum_{i=1}^n p_i \log(p_i)$$

כि בקרה זה אין עדיפות בין מצבים ומשמעות האנטרופיה היא אי-ידיעה שלנו על מצב המערכת.

הוכחה פורמלית לא קשה, היא מהוות מיציאת אקסטרום של פונקציה

$$\sum_{i=1}^n p_i = 1 \quad \text{בתנאי} \quad F(p_1, \dots, p_n) = -\sum_{i=1}^n p_i \log(p_i)$$

משתנה חדש  $\lambda$  - כופל לגרנג' :

$$G(p_1, \dots, p_n, \lambda) = -\sum_{i=1}^n p_i \log(p_i) + \lambda \left( \sum_{i=1}^n p_i - 1 \right)$$

כדי למצא נקודת חסודה אנו גוזרים  $G$  לפי כל  $p_i$  ומשווים נגזרת ל- 0,

$$\frac{\partial G}{\partial p_i} = -\log p_i - \log e + \lambda = 0 \quad \text{מקבלים} \quad \log p_i + \lambda = \log e \quad \text{מכאן}$$

$$p_i = \frac{1}{n} \quad \text{לכל } i$$

האנטרופיה של המערכת שווה ל- 0 אם קיים מצב שהמערכת נמצאת במצב זה עם הסתבותות 1 (אין אי-ידיעה על מצב). בשפה מתמטית: קיימים  $i_0$  ו-  $j$  כך  $p_{i_0} = p_j = 1$  ולכל  $i \neq j$  בקרה זה כל המחברים בסכום  $H(X)$  שווים ל- 0 ( $t \cdot \log t \xrightarrow[t \rightarrow 0]{} 0$ ). זה ערך מינימלי כי כל המחברים בסכום  $H(X)$  הם אי-שליליים.

**פתרון של המבחן 08/02/2013**  
**בקורס: קריפטולוגיה 1 /61117/ 1**

**שאלה מס' 1**

נתון טקסט ארוך באנגלית ללא סימני פיסוק המוצפן על-ידי הצופן  $E(x) = (ax + b) \bmod 26$ . ידוע ששתי אותיות בעלות שכיחויות הכí גבוות הן V ו- M. האותיות מסודרות לפי סדר שכיחויות יורד.

(א) מצא את a ו- b. (8 נקודות)

**פתרון:**

בטבלה בדף הנוסחאות אנו רואים שכיחויות הכí גבוות הן e (שכיחות 12.7%) ו- t (שכיחות 9.1%). לכן כדי להניא ש- V היא תמונה של e ו- M היא תמונה של t:

$$\begin{array}{l} \left\{ \begin{array}{l} 4a + b \equiv 21 \% 26 \\ 19a + b \equiv 12 \% 26 \end{array} \right. , \quad \begin{array}{l} 4 = [e] \rightarrow [V] = 21 \\ 19 = [t] \rightarrow [M] = 12 \end{array} \end{array}$$

פתרונות המערכת נותנת  $a = 15$ ,  $b = 7$ ,  $15a \equiv 17 \% 26$ ,  $15^{-1} \% 26 = 15$ , מפני ש-  $15 \cdot 15^{-1} \% 26 = 1$ .

(ב) בטא את נוסחת הפענוח. (6 נקודות)

**פתרון:**

נוסחת הפענוח בצורה כללית היא  $D(y) = a^{-1} \cdot (y - b) \bmod n$ .  
 כאן  $n = 26$  ומסעיף א':  $a = 15$ ,  $b = 7$ .  
 לכן נוסחת הפענוח  $D(y) = 7(y - 13) \bmod 26 = (7y + 13) \bmod 26$ .

(ג) מצא את כל ההודעות הבלתי מוסתרות. (6 נקודות)

$\Leftarrow 15x + 13 \equiv x \pmod{26}$  המשווהה למציאת ההודעות הבלתי מוסתרות כאן היא  $14x \equiv 13 \pmod{26}$ .  
 למשווהה זו אין פתרונות, ז.א. אין לצופן זה ההודעות הבלתי מוסתרות.

**שאלה מס' 2 (10 נקודות)**

תאר והסביר את תהליך הפיענוח באלגוריתם DES.

**פתרון:**

לצורך הפיענוח בצדוף DES משתמשים באותו אלגוריתם ובאותה תוכנה שבצדפה וגם באותו מפתח, ז.א. השיטה החלופית לפענוח וסימטרית. פונקציית הפענוח של DES מקבלת ע"י הפעלה

אלגוריתם DES עצמו בשינוי הבא: באיטרציה הראשונה משתמשים ב- k16 (במקום ב- k1), באיטרציה השנייה משתמשים ב- k15 (במקום ב- k2, וכו').

הבלוק המוצפן שקלט לאלגוריתם DES הוא  $IP^{-1}(R_{16}, L_{16})$  (תמורת החצאים!).

שלב ראשון הוא תמורה התחלית IP שנوتנה. איטרציה ראשונה:

$$L'_0 = R_{16}, \quad R'_0 = L_{16}$$

$$R'_1 = L'_0 \oplus f(R'_0, K_{16}) = R_{16} \oplus f(L_{16}, K_{16}) \quad \text{מן ש-}$$

$$R'_1 = L_{15} \oplus f(R_{15}, K_{16}) \oplus f(L_{16}, K_{16}) = L_{15} \quad \text{או} \quad R_{15} = L_{16} \quad \text{ו} \quad R_{16} = L_{15} \oplus f(R_{15}, K_{16})$$

ואיתרציה הבאה נותנת:

$$R'_2 = L_{14} \oplus f(R_{14}, K_{15}) \oplus f(L_{15}, K_{15}) = L_{14} \quad \text{ו} \quad L'_2 = R'_1 = L_{15} = R_{14}$$

אחרי האיתרציה האחרונה מקבלים גם

$$IP^{-1}(R'_{16}, L'_{16}) = IP^{-1}(L_0, R_0) = IP^{-1}(IP(x)) = x$$

בסוף אנו חוזרים למקור:

### שאלה מס' 3 (10 נקודות)

תאר והסביר את הסיבוכיות של ההתקפה "Meet in the Middle" נגד צופן 4DES עם 4 מפתחות שונות.

פתרון:

כמו בהתקפה "Meet in the Middle" נגד צופן 2DES אנו צריכים למצא באמצע התקהיליך ולהשווות תוצאות הצפנה המקורי לכל מפתחות ותוצאות הפיענוח הבלוק המוצפן לכל מפתחות. ז.א. אנו צריכים להצפין ולפענח לכל צירופים של שני מפתחות ותהליך DES צריך לרוץ

$$2^{56} \cdot 2^{56} + 2^{56} \cdot 2^{56} = 2^{113}$$

### שאלה מס' 4 (10 נקודות)

הוחלט לבצע החלפת מפתחות באמצעות מערכת Diffie-Hellman על בסיס 29 והיוצר שונה מ-2 Alice משתמש במפתח  $K_1 = 5$  ו Bob משתמש במפתח  $K_2 = 7$ . חשב את המפתח המשותף.

פתרון:

נחפש יוצר של  $Z_{29}$  שונה מ-2. מפני ש-  $\theta(29) = 28$  אנו צריכים לבדוק מערכיהם:

$$3^7 = 27 \cdot 81 \equiv 12(29) \neq 1, \quad 3^4 = 81 \equiv 23(29) \neq 1, \quad 3^3 = 27 \equiv 10(29) \neq 1, \quad 3^2 = 9 \equiv 1(29) \neq 1$$

$$3^1 = 3 \quad \text{ולכן } g = 3 \quad \text{הוא יוצר של } Z_{29}$$

המפתח המשותף הוא  $K = 3^{5 \cdot 7 \% 29} = 3^{35 \% 29} \equiv 3^7 \% 29 \equiv 12$

### שאלה מס' 5 (10 נקודות)

שני חבירים החליטו לבנות מערכת הצפנה עם מפתח סודי המבוססת על הסדרה  $q \geq 2$  מסוג Super-Increasing מספר טבעי סודי ולא מוגדר מראש ו-  $p$  מספר ראשוני ידוע. תאר את מערכת החלפת המפתחות ושיטות ההצפנה ופענוח המערכת.

#### פתרון:

אם שניהם יודעים את הסדרה אז כל אחד יכול לחלק טקסט שלו לבLOCKים בני 6 ביטים, לחשב מכפלה סקלרית של BLOCK והסדרה ולשלוח לחבר שיכל بكلות לפותר את הביעת הילקוט.

לכן יש צורך לדעת מספר רק  $q$ . מערכת Diffie-Hellman נותנת לנו הפתרון:

$Z_P^*$  מספר ראשוני ידוע הוא מודול החישוב, מישחו אחד מחשב יוצר  $g$  של החבורה  $p$  ושולח לשני. אחר כך כל אחד בוחר מפתח פרטי וסודי והחלפת המפתחות בוצעה. כדאי לבחור מספר זר ל-  $(p, \theta)$ , או אי אפשר לקבל 1 כמפתח משותף.

### שאלה מס' 6 (10 נקודות)

.  $y = x^k \pmod{n}$  הצליה לעלות על זוג  $(x, y)$  כך ש- (1) במערכת RSA הכללית OSCAR יכול לחשב את המפתח הסודי  $k$ ? מה לפי דעתך הסיבוכיות הפתרון?

#### פתרון:

אין אפשרות אחרת פרט לשיטה Brute Force, ז.א. בדיקת כל ערכים של  $k$  מתחילה מ- 2 עד שהוא שווין. לפני שכל איטציה היא כפל ב-  $x$  לכן מקסימום ציריך לעשות  $(\theta(n) - 1)$  פעולות (הערכים המשמעותיים הם מ- 2 עד  $\theta(n) - 1$ ).

### שאלה מס' 7

נתונה מערכת RSA הבנויה על בסיס  $N = 391$ .

A. ההודעה  $C = 3$  התקבלה במערכת הנ"ל כתוצאת ההצפנה של הודעה  $M$  על-ידי מפתח פתוח  $b = 141$ . מצא את ההודעה המקורית  $M$ . (10 נקודות)

#### פתרון:

$$\theta(N) = 16 \cdot 22 = 352 \iff N = 17 \cdot 23$$

$$: a = b^{-1}(\theta(N)) = 141^{-1}(352)$$

$$a = 5 \text{ ז.א. } 1 = 141 - 2 \cdot (352 - 141 \cdot 2) = -2 \cdot 352 + 5 \cdot 141 \Leftrightarrow \begin{bmatrix} 352 = 141 \cdot 2 + 70 \\ 141 = 70 \cdot 2 + 1 \end{bmatrix}$$

$$\text{לכן } M = C^a(N) = 3^5(391) = 243$$

ב. רשום את כל ההודעות הבלתי מוסתרות עבור מפתחו **CLUSHER** זו . (10 נקודות)

פתרון:

נחפש את ההודעות הבלתי מוסתרות טריוויאליות שלא תלויות במפתח.

$$\begin{array}{l} x^{141} \equiv x(17) \\ x^{141} \equiv x(23) \end{array} \left. \begin{array}{l} x^b \equiv x(p) \\ x^b \equiv x(q) \end{array} \right\} \text{כך} \quad \text{התנאי ההפוך (10) שקול למערכת} \quad x^b \equiv x(N)$$

$$\text{נפתרו לפי משפט הסיני: } M_2 = 17, M_1 = 23, m_2 = 23, m_1 = 17$$

$$, C_2 = M_2^{-1} = 17^{-1}(23) = 19, C_1 = M_1^{-1} = 23^{-1}(17) = 6^{-1}(17) = 3$$

$$r_2 = 0, \pm 1, r_1 = 0, \pm 1 \text{ ונוסחת הפתרונות:}$$

$$x = (M_1 \cdot C_1 \cdot r_1 + M_2 \cdot C_2 \cdot r_2) \bmod N$$

$$\Leftrightarrow x = (23 \cdot 3 \cdot r_1 + 17 \cdot 19 \cdot r_2) \bmod 391 = (69 \cdot r_1 + 323 \cdot r_2) \bmod 391$$

$r_1$	0	0	0	1	1	1	-1	-1	-1
$r_2$	0	1	-1	0	1	-1	0	1	-1
$x$	0	323	68	69	1	137	322	254	390

ג. מצא את כל ההודעות הבלתי מוסתרות לא טריוויאליות עבור מפתח  $b=13$  . (10 נקודות)

פתרון:

נוסחה למספר ההודעות הבלתי מוסתרות היא

$$m = [1 + \gcd(12, 16)] \cdot [1 + \gcd(12, 22)] = 5 \cdot 3 = 15$$

מכאן נובע שקיים 6 הודעות הבלתי מוסתרות לא טריוויאליות. אנו מקבלים הן מצירופים של 2

פתרונות לא טריוויאליות של השוואת  $\bmod 17$  ו- 3 פתרונות טריוויאליות של השוואת  $\bmod 23$

נפתרו את קיימים יוצרים, למשל  $g = 3$  / קל לבסוף ש-

$s = g^t$  /. פרט לפתרון  $s_0 = 0$ ,  $n$  חפש פתרונות בצורה  $3^3 \neq 1, 3^4 \neq 1, 3^6 \neq 1$

$$\begin{aligned}
 13t \equiv t \pmod{\theta(17)} &\iff 13t \equiv t \pmod{\theta(17)} \iff g^{13t} = g^t(17) \\
 &\iff 3t \equiv 0 \pmod{4} \iff 12t \equiv 0 \pmod{\theta(16)} \iff
 \end{aligned}$$

t	0	4	8	12
s	1	13	-1	4

פתרונות המבוקשים הם  $s_4 = 13$  ו-  $s_3 = 4$ . הצגה בנוסחה מסיע ב' נותנת :

$r_1$	4	4	4	13	13	13
$r_2$	0	1	-1	0	1	-1
x	276	208	344	115	47	183



# **מכללת אורט בראודה ORT BRAUDE COLLEGE**

	שאלה 1
	שאלה 2
	שאלה 3
	שאלה 4
	שאלה 5
	שאלה 6
	ציון הבחינה

**לפני תחילת הבחינה אני קראי/י בעין את ההוראות ומלא/י את כל הפרטים בכתב ברוח:**  
(שים לב, מחברות הבחינה נסrokות למאגר נתונים. יש להקפיד  
שלא להפוך /لتולש / לכתוב בצלבים)

מועד מיוחד     מועד ב'     מועד א'

מחברת בחינה

שם המשגיח

סמסטר: א - ב - קיץ

22116

## **אין לתלוש דפים מהחברות**

שמור על טוהר הבחינה!

## הישגים ביושר היא הדרך היחידה להצלחה!



עמך, פידורי

מחברות מט' – מתר – מחריות



(14) 303624597 ת.ת  
006100010689 דוחן



וְאֶלְעָזָר בֶּן־מִתְּנַחַת כָּבֵד בָּקָה

אין לכתוב מעבר לכך האדום משנה צדי הדף.  
יש לכתוב את הבדיקה בעט (כחול / שחור) בלבד.

303624597 דן, ע"י

מחלקת ב (פ.כ)

## מבחן הרצאות

M112

15/07/12

תאורים

שעת יציאה לשירותים	שעת חזרה משירותים				

303624597

טופס מלאוה לשאלון מבחן

שם הקורס: קריופטולוגיה 1	שנת לימוד: ג'
שם המרצה: פרופ' זאב וולקוביץ' שם המתרגם: ד"ר לאוניד מוריונסקי	מספר הקורס: 61117
מסלול / מגמה: הנדסת תוכנה	מספר סטודנט: ב'
תאריך הבחינה: 15/07/2013	מועד הבחינה: א'
משך הבחינה: 180 דקות	שעת הבחינה: 9 <sup>00</sup>

הוראות לבבוחן ולמשגיח

1. יש להזכיר את השאלון בסוף הבחינה.
2. יש לענות על כל השאלות.
3. ניתן להשתמש רק בדף נוטחות מצורף בטופס.
4. לא ניתן להשתמש בחומר עזר אחר.
5. ניתן לכתוב בעט בלבד.
6. כל העבודה, כולל טיוטה וחישובי עוזר, צריכה להופיע במחברת הבחינה בלבד ו/או בשאלון (כמפורט בסעיף 7) ולאין להשתמש בכלל נייר אחר.
7. יש לענות על הבחינה בטופס שאלון הבחינה בלבד.
8. ניתן להשתמש במחשבון.
9. טפסי השאלון ייבדקן, המתרבויות לא ייבדקו.
10. אין להחלק לסטודנטים פתקי שאלות.
11. היכן שדרושים הסברים תני הסבר.
12. אין להעביר כל חומר בין הסטודנטים.
13. מס' הנקודות לכל שאלה נתון בסוגרים אחרי שאלת.

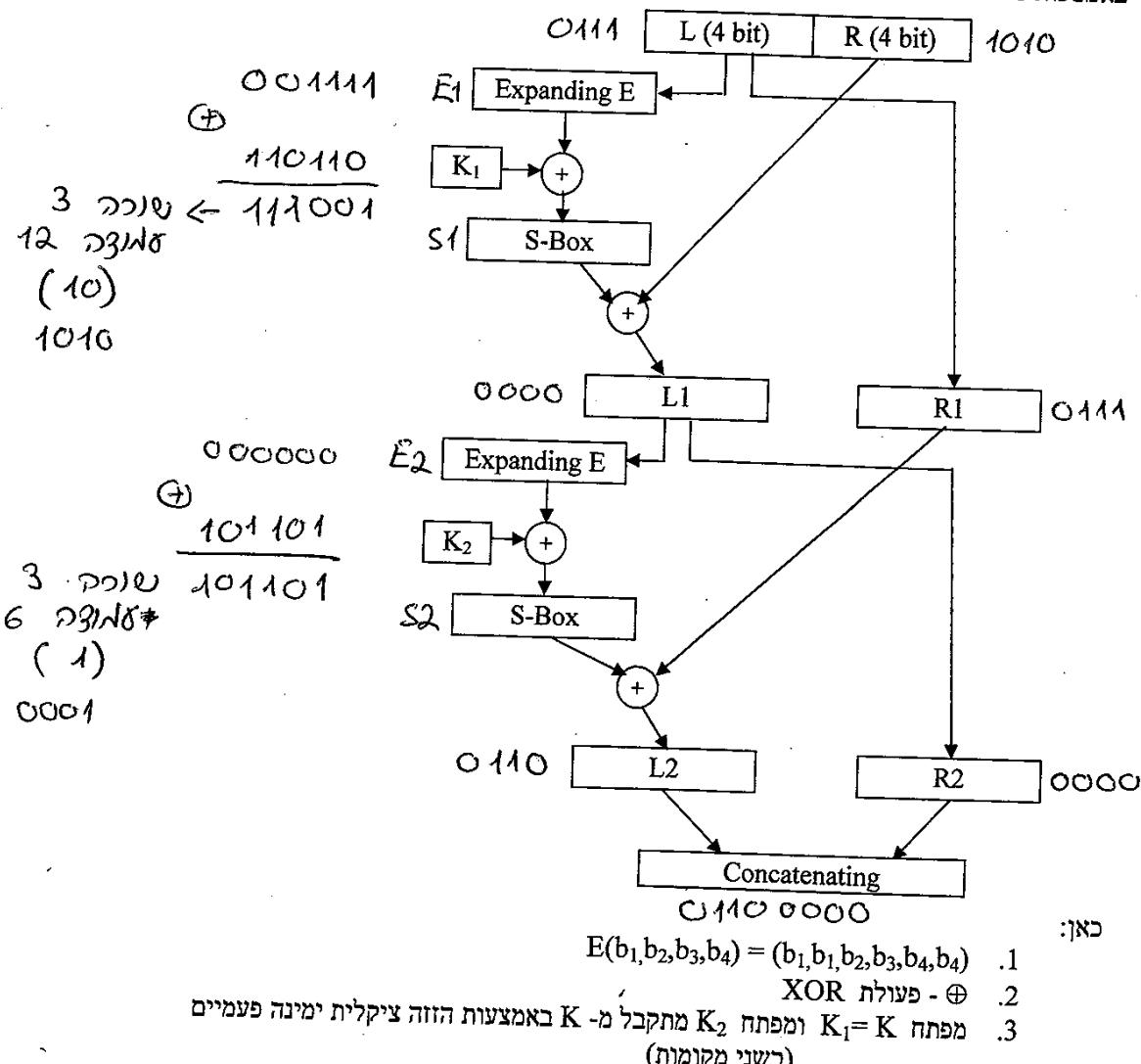
**בַּהֲצִלְתָּה !!!**

סה"כ	6	5	4	3	2	1
90	7	23	20	5	10	25

שאלה מס' 1

לפניך צופך SD המציג מחרוזת  $(b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8)$  באורך של 8 ביטים

באמצעות מפתח K של 6 ביטים באופן הבא:



כאן:

✓

$$E(b_1, b_2, b_3, b_4) = (b_1, b_1, b_2, b_3, b_4, b_4) .1$$

.2 פועלות -  $\oplus$

.3 מפתח K =  $K_1 = K_2$  ומפתח K מתקבל מ-K באמצעות הזזה ציקלית ימינה פעמיים (בשני מקומות)

✓

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

a) הצפן את String =  $(01111010)$  באמצעות המפתח  $K = (110110)$ . (10 נקודות)

✓

10

$$R_1 = L = 0111, R = 1010$$

$$E(L) = 001111 \oplus 110110 = 111001 \xrightarrow{\text{Sbox}} (R) 1010 \oplus 1010 = 0000$$

$$L_1 = 0000, R_1 = 0111$$

$$E(L_1) = 000000 \oplus 101101 = 101101 \xrightarrow{(1)} 0001 \oplus 0111 = 0110$$

$$L_2 = 0110, R_2 = L_1 = 0000$$

$$E(01111010) = 01100000 //$$

ב) האם ניתן להשתמש ב- SD לצורך פענוח הודעות שהוצפנו ע"י SD? אם לדעתך ניתן לפענוח SD וنمך את תהליך הפענוח. אם לדעתך אי אפשר אז הסבר怎ן כדי צריך לשנות את SD לצורך קבלת אלגוריתם הנינתן לפענוח עצמי. (10 נקודות)

10-

\* קבוצות הוכחה, גן כינס פסקום בסיסי SD נס

סב מוקטינים לאנרגיה וטמפרטורה מוגברת, סב

.DES - 2

\* צב. ד. ג'ון מילר פסקום בסיסי SD, נס

פאלט מושג מילויים

$k_2' = k_1$ ,  $k_1' = k_2$  במעבר בין סט, מושג כפולה  $L' = R$ ,  $R' = L$  DES  
 $L = 0110$ ,  $R = 0000$  מושג נורמלי  
 $L = 0000$ ,  $R = 0110$  מושג נורמי  $R_{\text{new}} = L$ ,  $L_{\text{new}} = R$  מושג נורמי

$\boxed{L_1 \quad | \quad L_2}$  מושג  $L_2 - L_1$  מושג  
1/1/k  
2/2/2

ג) איזה מפתחות הם חלשים ("חלש" כמו במערכת DES)? (5 נקודות)

レスון מס' 1 DES "קליפה" מושגים יתירים הם מושגים

ויבאים מצהה בזיהה - קיפוף shift - קיפוף קיפוף

000000	מושגים יתירים מושגים
111111	
101010	
010101	

שאלה מס' 2 (10 נקודות)

תאר את התקפה "Meet in the Middle" לזוג מפתחות DOUBLE DES עם שני מפתחות  $k_1, k_2$

והסביר את סיבוכיותה שלה.

(10)

תאר את התקפה "Meet in the Middle" לזוג מפתחות DOUBLE DES

תאר את התקפה "Meet in the Middle" לזוג מפתחות DOUBLE DES

Meet in the middle תאר את התקפה "Meet in the Middle" לזוג מפתחות DOUBLE DES

תאר את התקפה "Meet in the Middle" לזוג מפתחות DOUBLE DES

נוסף היפוך, וכך נסבכ בפונקציית פולינום (P) אמצעי

(c) יישר שיבור פולינומי (P) אמצעי

היפוך יישר שיבור פולינומי (P) אמצעי

היפוך יישר שיבור פולינומי (P) אמצעי

$O(2^{56})$  - כמות היפוכים כפולה ב- $2^{56}$

$O(2^{56} \log 2^{56})$  (חסכון מ- $2^{56} \times 2^{56}$ )

ונזק כושי נסבכ בפונקציית פולינום (P) אמצעי

בנ"ט כושי נסבכ בפונקציית פולינום (P) אמצעי

רעיון קידום שיבור פולינומי (P) אמצעי

היפוך שיבור פולינומי (P) אמצעי

לכ"כ  $O(2^{56} \log 2^{56})$

### שאלה מס' 3 (10 נקודות)

נתונה מערכת הצפנה :  $K = \{1, 2, 3\}$  ,  $Y = \{A, B, C\}$  ,  $X = \{a, b, c\}$  שמצוינה לפי הטבלה:

K	E(a)	E(b)	E(c)
1	A	B	C
2	B	C	A
3	C	B	B

5

.  $P(a) = P(b) = P(c)$  בהנחה שהמפתח במערכת נבחר באופן אחידתognam

? "perfect secrecy" האם המערכת היא בעלת

$P(x|y) = P(x)$  כן Perfect Secrecy

כן כי אם ידועות Y לא ידועות X

X יתגלו רק אם ידועות Y

Complex numbers first, k=3 many ways

Խնամքը ուղղված է բարեկարգ լոյզի համար կողմէց պահանջման

• 13211 916317 2011, k=3 h12N2

$$H_0 = \sum_{i=1}^3 \frac{1}{3} \log_2(3) = 1.584$$

$$H(Y|k=3) = P(A) + P(B) + P(C) = 0 + \frac{2}{3} \log_2 \left(\frac{3}{2}\right) + \frac{1}{3} \log_2 (3) = 0.917$$

שאליה מס' 4

בוחלט בראש המפלגה מפתחות באמצעות מערכת Diffie-Hellman עם בסיס 43 והיוצר הקטן

ביזום בר-ע' משמש בפתח Alice ו- Bob  $K_A = 5$  ו-  $K_B = 7$  משתמש בפתח

א. בזאר אם במלחמה ממשות. (10 נקודות)

$\oplus(n)=42$  .  $29^{th}$  Jan Pp. 23<sup>rd</sup> at 8pm 02/01/2018

2018,  $\alpha/|Z_{43}^*|$  ပေါ်များ၏ အရွယ်,  $g^a$  ပြုလုပ်ချက်၏ အရွယ်

Ex 10) If  $y^n = p^n - 3^n$  where  $a \in \{2, 3, 6, 7, 14, 21, 42\}$

• (גַּדְעֹן וְיַעֲקֹב) כָּל הַמִּזְבֵּחַ וְכָל הַמִּזְבֵּחַ

22 - N' Shō p338 Shō p8

$$\underline{2^0, 2^2 = 4 \neq 1, 2^3 = 8 \neq 1, 2^6 = 64 = 21 \neq 1, 2^7 = 42 \neq 1, 2^{14} = 1 \rightarrow \text{do 3), kof 2}}$$

$$\underline{3^2 = 9 \neq 1, 3^3 = 27 \neq 1, 3^6 = 41 \neq 1, 3^7 = 37 \neq 1, 3^{14} = 36 \neq 1, 3^{21} = 42 \neq 1 \Rightarrow 23}, \quad 3$$

$$k = (3^5)^7 = (3^7)^5 \bmod 43 = 37^5 = \text{further details will follow}$$

$$= 7 \bmod 43$$

ב. Oscar חפס את המספרים שלחו Alice ו- Bob אחד לשני. איזה מהם מכיל יותר מידע

(10)

{37,36,42,6,7,13 when sum of digits is 30-238}

~~Z<sub>4,3</sub> 55 ut 23"8 (4') 5 mēnīs pēc 3102~~

$k_A = 5$  bura yk abd yk Nefy 233 Oscar wihai pdf

በዚህ የዚህ አገልግሎት ተከራክር ነው እና ስለዚህ የዚህ አገልግሎት ተከራክር ነው

שאליה מס' 5

לפניך מוגדרת מודולית RSA עם שניי אחד: היא בנויה על בסיס של מכפלת שלושה גורמים

.  $E(M) = M^b \mod(n)$ . הידועה  $M$  מוצפנת באמצעות הבא:  $n = 19 \cdot 23$

א. פענה הודעה  $C = 13$  אם מפתח ציבורי  $b = 6653$ . (10 נקודות)

$a \in \mathbb{Z}^{\times}_n$ ,  $a = b \pmod{n}$   $\Leftrightarrow$   $a^{-1}b \equiv 1 \pmod{n}$

$$n = 12673 \Rightarrow \phi(n) = 12673 \left(\frac{18}{19}\right) \left(\frac{22}{23}\right) \left(\frac{28}{29}\right) = 11088 = (p-1)(q-1)(r-1)$$

$$a = b^{-1} \bmod 11088 = 6653^{-1} \bmod 11088$$

$$\text{gcd}(11088, 6653) = \text{gcd}(6653, 4435) = \text{gcd}(4435, 2218) = \text{gcd}(2218, 2217) = 1$$

$$11088 = 1 \cdot 6653 + 4435, 6653 = 1 \cdot 4435 + 2218, 4435 = 1 \cdot 2218 + 2217, 2218 = 1 \cdot 2217 + 1$$

$$1 = 2218 - 1 \cdot 2217 = (\cancel{1} \cancel{2} \cancel{1} \cancel{8}) (\cancel{1} \cancel{2} \cancel{1} \cancel{3} - \cancel{1} \cancel{2} \cancel{1} \cancel{4}) = (1)2218 - (4435 - 1 \cdot 2218)$$

$$= (-1)^{4435} + (2) \cdot 2218 = (-1)^{4435} + 2(6653 - 1 \cdot 4435) = (2)6653 + (-3)^{4435}$$

$$= (2)6653 - 3(11088 - 1 \cdot 6653) = (-3)11088 + (5)6653 \Rightarrow a \equiv \underline{5 \text{ mod } 11088}$$

$y^a \mod 12673$  :  $a = 13$  כרך ו' סעיף 12.2.1.5

$$y = c = 13 \Rightarrow 13^5 \mod 12673 = 3776 \mod 12673 = p$$



ב. מהו המספר הידועות הבלתי מוסתרות המינימלי? נמק. (5 נקודות)

3

$$[1 + \gcd(b-1, p-1)] [1 + \gcd(b-1, q-1)] \text{ RSA } \text{סעיף 3}$$

$$[1 + \gcd(b-1, p-1)] [1 + \gcd(b-1, q-1)] [1 + \gcd(b-1, m)] \text{ RSA } \text{סעיף 3}$$

$$[1 + \gcd(6652, 18)] [1 + \gcd(6652, 22)] [1 + \gcd(6652, 28)] \text{ RSA } \text{סעיף 3}$$

$$\gcd(6652, 18) = \gcd(18, 10) = \gcd(10, 8) = \gcd(8, 2) = 2 \rightarrow \text{סעיף 3}$$

$$\gcd(6652, 22) = \gcd(22, 8) = \gcd(8, 6) = \gcd(6, 2) = 2 \rightarrow \text{סעיף 3}$$

$$\gcd(6652, 28) = \gcd(28, 16) = \gcd(16, 12) = \gcd(12, 4) = 4 \rightarrow \text{סעיף 3}$$

$$3 \times 3 \times 5 = \underline{\underline{45}} \quad \text{סעיף 3}$$

ג. תאר את המערכת חתימה דיגיטלית המבוססת על מערכת הצפנה RSA. (10 נקודות)

$(n, p, q, a, b)$  -> GND 5 w RSA 4275

Each year 2-5% of PBI is lost due

RSA  $\rightarrow$  extended: Private  $(p, q, a) \rightarrow$  Public -  $(n, b)$

19582 Copernicat 1230P<sub>E</sub>, 10/12/13 נסיעת מילוי

New entries (e.g. egg). cd to /var/ci to review

כט. גן"ג גנץ ראי כהנא זעט

प्रगति, का

envers des, RSA versa abzweig push A entren-

C ja3N7 at 221 p ja3N 183 C6P3 at 8

Suppose p' is a point on the line AB.

! עזבונו נחלה נדיה sk, A-N בפער P-f 223

שאלה מס' 6

**משבצת KNAKSACK** בנויה על סמך הסדרה הפומבית  $(5, 34, 44, 6, 41) = B$ , מודול חישוב

\*במקרה רהט סבכ אוויות נגם מילון מילון:  $N=53$  וגורם סודי  $V=29$ . פענח את ההודעה  $C=27$ . (10 נקודות)

$$29x \equiv 5 \pmod{53} \Rightarrow x \equiv 5(29^{-1}) \pmod{53} = 5 \cdot 11 \pmod{53} = 2 \pmod{53}$$

$$29x \equiv 34 \pmod{53} \Rightarrow x \equiv 34(29^{-1}) \pmod{53} \equiv 34 \cdot 11 \pmod{53} \equiv 3 \pmod{53}$$

$$29x \equiv 44 \pmod{53} \Rightarrow x \equiv 44(29^{-1}) \pmod{53} = 44 \cdot 11 \pmod{53} = 7 \pmod{53}$$

$$29x \equiv 6 \pmod{53} \Rightarrow x = 6(29^{-1}) \pmod{53} = 6 \cdot 11 \pmod{53} = 13 \pmod{53}$$

$$29x \equiv 41 \pmod{53} \Rightarrow x = 41(29^{-1}) \pmod{53} = 41 \cdot 11 \pmod{53} = 27 \pmod{53}$$

atk  $aN''pN \alpha = \{2, 3, 7, 13, 27\}$   $a^3 \mid 0 \quad a \mid 30 \quad atk3N$

! Super-Increasing atk

(11011)  $\oplus C = 27$   $\rightarrow$   $27 \mid 27$  atk  $a \mid 27$   $a \mid 27$  \*

$$27 \geq 27 \rightarrow P = \underline{\underline{\underline{\underline{\underline{1}}}}}$$

$$0 \quad (00001) \rightarrow 1$$

$$\underline{\underline{\underline{\underline{\underline{P=1}}}}} \quad \text{gcf} \text{ calculate gcd's}$$

$$\gcd(53, 29) = \gcd(29, 24) = \gcd(24, 5) = \gcd(5, 4) = 1 \quad \checkmark$$

$$53 = 1 \cdot 29 + 24, \quad 29 = 1 \cdot 24 + 5, \quad 24 = 4 \cdot 5 + 4, \quad 5 = 1 \cdot 4 + 1$$

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 = 5 - (24 - 4 \cdot 5) = (-1)24 + (5)5 = (-1)24 + 5(29 - 1 \cdot 24) = (5)29 + (-6)24 = \\ &= (5)29 - 6(53 - 1 \cdot 29) = (-6)53 + (11)29 \Rightarrow 29^{-1} \pmod{53} \equiv 11 \pmod{53} \end{aligned}$$

\*\*

## דף נסחות

### Euler-Fermat Theorem .1

לכל  $a \in \mathbb{Z}$  ש-  $\gcd(a,n) = 1$  מתקיים  $a^{\phi(n)} \mod n = 1$

אם  $n$  מספר ראשוני אז  $\phi(n) = n - 1$

### 2. משפט השארית הסיני:

יהיו  $d_1, d_2, \dots, d_t$  מספרים זרים בזוגות ו-  $d_1 d_2 \dots d_t = n$ . אזי למערכת המשוואות

$$x \equiv a_i \pmod{d_i} \quad i = 1, 2, \dots, t$$

כאשר  $a_i$  נוע בין 1 ל-  $d_i$ , יש פתרון משותף  $x$  בתחום  $[0, n-1]$ .

$$\frac{n}{d_i} * y_i \equiv 1 \pmod{d_i} \quad \text{כאן } y_i = \left[ \sum_{i=1}^t \left( \frac{n}{d_i} \right) x_i \right] \pmod{n}$$

### 3. הצופן RSA:

$n$  הוא מכפלה של שני מספרים ראשוניים שונים  $p$  ו-  $q$ .

### 4. סימוני הצלף KNAPSACK:

$A = (a_1, a_2, \dots, a_n)$  - סדרה סודית,  $N$  - מודול חישוב,

$B = (b_1, b_2, \dots, b_n)$  - סדרה פומבית,  $V$  - גורם סודי.

### 5. האלפבית האנגלאי, קודים ושכיחיות /BALFITH/ :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
82	15	28	43	127	22	20	61	70	2	8	40	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
67	75	19	1	60	63	91	28	10	23	1	20	1

**פתרונות של המבחן 31/01/2014**  
**בקורס: קריפטולוגיה 1 /61117/**

**שאלה מס' 1**

נתון הצופן  $K = \begin{pmatrix} a & 1 & a+1 \\ 1 & a & 1 \\ 3 & 3 & 5 \end{pmatrix}$ ,  $Y = X K \bmod 33$ . עבור איזה ערכים של פרמטר  $a$  מטריצת  $K$  מקסימלי?

מספר הודעות בלתי מוסתרות הוא מקסימלי ועבור איזה הוא מינימאלי? (10 נקודות)

פתרון:

חישוב בחوغ  $Z_{33}$ . התנאי הכרחי שמטריצה הפיכה מתקיים אם ורק אם

$$|K| = 3(1-a^2-a) - 3(a-a-1) + 5(a^2-1) = 2a^2 - 3a + 1 = (a-1)(2a-1)$$

הbianio זר עם 33 אם גורמים שלו לא מתחלקים גם ב- 3 וגם ב- 11, 2.א.

$$\left. \begin{array}{l} a \neq 1 \bmod 3 \\ a \neq 2 \bmod 3 \\ \cdot \quad a \neq 1 \bmod 11 \\ a \neq 6 \bmod 11 \end{array} \right\} \iff \left. \begin{array}{l} a-1 \neq 0 \bmod 3 \\ a-1 \neq 0 \bmod 11 \\ 2a-1 \neq 0 \bmod 3 \\ 2a-1 \neq 0 \bmod 11 \end{array} \right\}$$

לכן ערכים מתאימים הם: 0,3,9,15,18,21,24,27,30 רק.

$\iff X \cdot K \equiv X \bmod 33$  הודעות בלתי מוסתרות הן פתרונות השוואת

$$\left. \begin{array}{l} 2x_1 + x_3 \equiv 0 \bmod 33 \\ -5x_1 + (a-1)x_2 \equiv 0 \bmod 33 \\ (a-7)x_1 + x_2 \equiv 0 \bmod 33 \end{array} \right\}, \text{ כי } \left. \begin{array}{l} ax_1 + x_2 + 3x_3 \equiv x_1 \bmod 33 \\ x_1 + ax_2 + 3x_3 \equiv x_2 \bmod 33 \\ (a+1)x_1 + x_2 + 5x_3 \equiv x_3 \bmod 33 \end{array} \right\}$$

$$\left. \begin{array}{l} [(a-7)(a-1)+5]x_1 \equiv 0 \bmod 33 \\ x_2 \equiv (7-a)x_1 \bmod 33 \\ x_3 \equiv -2x_1 \bmod 33 \end{array} \right\} : (a-1)R_3 - R_2$$

אנו יכולים לחשב  $a \neq 1$

יחסים שני ושלישי הם חזרה ערכים לנקודות שווה למספר פתרונות של השוואת ראשונה ושוואת רשותה  $\gcd((a-2)(a-6), 33) = 1$ .

a	0	3	9	15	18	21	24	27	30
m	3	3	3	3	3	3	33	3	3

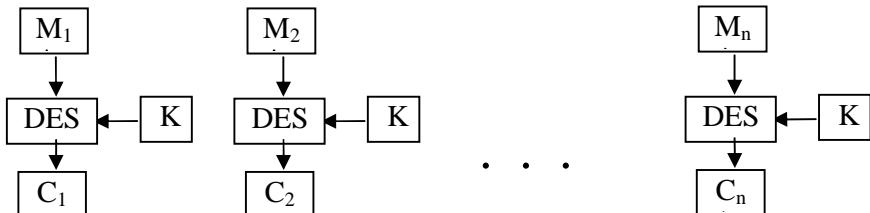
מכאן אנו רואים שמספר ה.ב.מ. מקסימלי ל- 24 והוא מינימלי לכל ערך אפשרי אחר.

## שאלה מס' 2

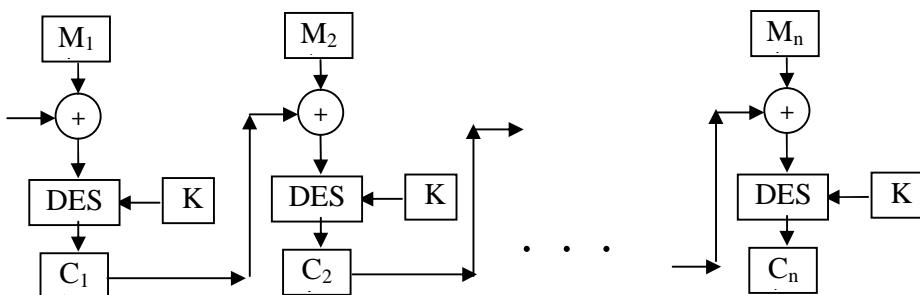
мар והסביר את היתרונות והחסרונות של השיטות ECB ו- CBC באלגוריתם הצפנה סימטרית.

פתרון:

ECB – Electronic Codebook



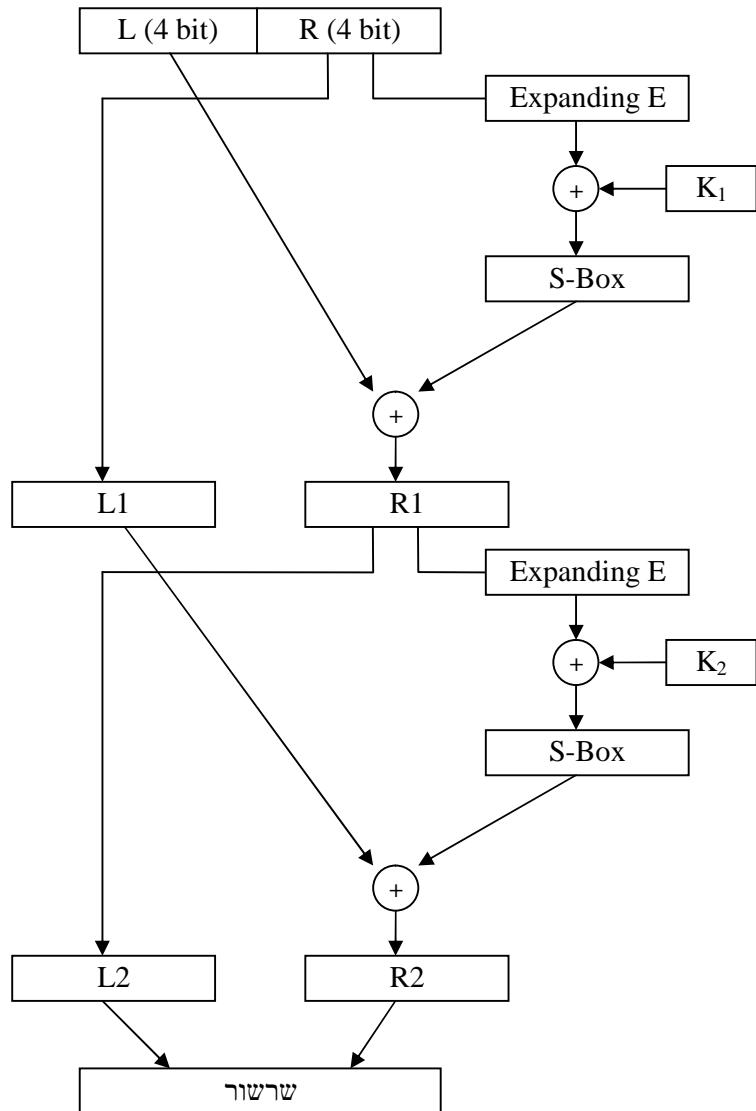
CBC – Cipher Block Chaining



היתרון של CBC בהשוואה עם ECB בлокים זהים לא מוצפנים עם אותה תוצאה.  
החסרון של CBC שטויות נגררת. זה לא אפשרית ב- ECB.

## שאלה מס' 3

לפניך צופק SD המצפין מחרוזת ( $b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8$ ) באורך של 8 ביטים  
באמצעות מפתח K של 6 ביטים באופן הבא:



כאן

1. פועלות XOR, S-Box ראה להלן,
2. E הופק 4 ביטים  $(b_1b_2b_3b_4)$  ל- 6 ביטים כדלקמן:  
 $(c_1c_2c_3c_4) = (1010) \oplus (b_1b_2b_3b_4)$
- זוג  $c_1c_2$  מגדיר את השורה ב- S-Box שבה אנו מצאים מספר  $c_1c_2c_3c_4$
- ומספר עמודה שלו בצדורה ביןארית (4 ביטים) מושרשים עם הזוג  $c_3c_4$ .
3. מפתח  $K_1 = K$  ומפתח  $K_2$  מתקיים  $K_2 = K$  באמצעות הזהות ציקלית ימינה בשני מקומות.

S-Box																
Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8

2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

. K= 011010 String=(10111010) ב암צעות המפתח

פתרונות:

$$L_0 = 1011$$

$$R_0 = 1010$$

$$E : 1010 \oplus 1010 = 0000 = (c_1 c_2 c_3 c_4) \Rightarrow$$

$$row = '00' = 0, \text{ number } 0 \text{ in column } 14 = '1110'$$

$$\Rightarrow E(R_0) = '111000' \Rightarrow '111000' \oplus '011010' = '100010'$$

$$r = 2, c = 1 \Rightarrow SBox(100010) = 1 = '0001'$$

$$L_1 = 1010$$

$$R_1 = 1011 \oplus 0001 = 1010$$

$$E : 1010 \oplus 1010 = 0000 = (c_1 c_2 c_3 c_4) \Rightarrow$$

$$row = '00' = 0, \text{ number } 0 \text{ in column } 14 = '1110'$$

$$\Rightarrow E(R_0) = '111000' \Rightarrow '111000' \oplus '100110' = '011110'$$

$$r = 0, c = 15 \Rightarrow SBox(011110) = 7 = '0111'$$

$$L_2 = 1010$$

$$R_2 = 1010 \oplus 0111 = 1101$$

$$Y = 10101101$$

ב) איך ניתן להשתמש ב- SD לצורך פענוח הודעות שהוצפנו ע"י SD? אם לדעתך ניתן לפענוח המספר ונמק את תהליך הפענוח. במקרה שלא, הסביר כיצד צריך לשנות את SD לצורך קבלת אלגוריתם הנitin לפענוח עצמי.

פתרונות:

אי אפשר להשתמש באלגוריתם.

אנו צריכים לעשות שינוי הבא: בסוף לשרשר בסדר הפוך.

כמו ב- DES רגיל במשך פיענוח אנו צריכים להשתמש במפתחות  $K_1, K_2$  בסדר הפוך.

#### שאלה מס' 4

מערכת RSA בנויה על בסיס 899.

א. הودעה C=3 התקבלה כתוצאה ההצפנה של הודעה M על ידי מפתח b=611. מצא

את M.

פתרונות:

$$\theta(N) = 28 \cdot 30 = 840 \iff N = 29 \cdot 31$$

$$: a = b^{-1}(\theta(N)) = 611^{-1}(840)$$

$$\begin{array}{c} 1=153-2\cdot(229-153)= \\ =-2\cdot229+3\cdot(611-2\cdot229)= \\ =3\cdot611-8\cdot(840-611)= \\ =-8\cdot840+11\cdot611 \end{array} \left[ \begin{array}{l} 840=611+229 \\ 611=229\cdot2+153 \\ 229=153+76 \\ 153=76\cdot2+1 \end{array} \right]$$

$$\text{לכן } M = C^a(N) = 3^{11}(899) = 44$$

**ב. מצא את כל ההודעות הבלתי מוסתרות עבור המפתח  $b=17$**

פתרונות:

התנאי החיפוש הודיעות בלתי מוסתרות ( $x(N)$ ) שקול למערכת  
 $\begin{cases} x^b \equiv x(p) \\ x^b \equiv x(q) \end{cases}$

$$\begin{cases} x^{17} \equiv x(29) \\ x^{17} \equiv x(31) \end{cases}$$

מספר ההודעות הבלתי מוסתרות הוא  $m = [1 + \gcd(16, 30)] \cdot [1 + \gcd(16, 28)] = 3 \cdot 5 = 15$   
 מכאן נובע שקייםות 15 ההודעות הבלתי מוסתרות והם מוגדרות על ידי צירופים של 5 פתרונות  
 $\mod 31$ . השווה ב-  $\mod 29$  ו- 3 פתרונות טריוויאליות של השוואת  $b$ .

נפתרו לפיה משפט הסיני:  $M_2 = 29, M_1 = 31, m_2 = 31, m_1 = 29$

$$, C_2 = M_2^{-1} = 29^{-1}(31) = 15, C_1 = M_1^{-1} = 31^{-1}(29) = 2^{-1}(29) = 15$$

ונוסחת הפתרונות  $x = (M_1 \cdot C_1 \cdot r_1 + M_2 \cdot C_2 \cdot r_2) \mod N$ , כאן  $r_i$  הם פתרונות של  
 $s^{17} \equiv s(31)$   $r_2 = 0, \pm 1$  ו-  $s^{17} \equiv s(29)$   $r_1 = 0, \pm 1$ .

נפתרו את  $s^{17} \equiv s(29)$ . בשדה  $Z_{29}$  קיימים יוצרים, למשל  $g = 2$  קל לבירוק ש-  
 $s_0 = 0$  פרט לפתרון  $2^2 \neq 1, 2^4 \neq 1, 2^7 \neq 1, 2^{14} \neq 1$   
 $\Leftarrow 17t \equiv t \mod \theta(29) \Leftarrow g^{17t} = g^t(29)$  אז  $s = g^t$   
 $\Leftarrow 4t \equiv 0 \mod 7 \Leftarrow 16t \equiv 0 \mod (28)$

t	0	7	14	21
s	1	12	-1	17

מציבים הערכים ומקבלים:

$$\Leftarrow x = (31 \cdot 15 \cdot r_1 + 29 \cdot 15 \cdot r_2) \mod 899 = 15 \cdot (31 \cdot r_1 + 29 \cdot r_2) \mod 899$$

ההודעות הבלתי מוסתרות טריוויאליות:

$r_1$	0	0	0	1	1	1	-1	-1	-1
$r_2$	0	1	-1	0	1	-1	0	1	-1
x	0	435	464	465	1	30	434	869	898

ההודעות הבלתי מוסתרות לא טריוויאליות:

$r_1$	12	12	12	17	17	17
$r_2$	0	1	-1	0	1	-1
$x$	186	621	650	713	249	278

ג. הוחלט לבצע החלפת מפתחות בשיטת Diffie-Hellman על בסיס הגורם הגדל  $q$  של המערכת הנ"ל, כאשר המפתחות הפרטיים של כל אחד מהמשתפים הם 5 ו- 7 בהתאם, חשב את המפתח המשותף.

פתרון:

$$\begin{aligned} N &= 31 \\ \theta(31) &= 30 \quad \text{אנו צריכים לבדוק מעירכים: } 2, 3, 5, 6, 10, 15 \\ 2^5 &\equiv 1 \pmod{31} \quad \text{מספר 2 הוא לא יוצר כי} \\ , 3^{10} &= 25(31) \neq 1, 3^6 \equiv 16(31) \neq 1, 3^5 = 243 \equiv 26(31) \neq 1 : 3 \quad \text{נבדק} \\ . Z_{31} & \quad \text{. } Z_{31} \text{ הוא יוצר של } g = 3 \quad 3^{15} \equiv 30(31) \neq 1 \\ . K &= 3^{5 \cdot 7 \% 31} = 3^{35 \% 31} \equiv 3^5 \% 31 \equiv 26 \quad \text{המפתח המשותף הוא} \end{aligned}$$

### שאלה מס' 5

האבטחה של RSA תלואה בשלוש פעולות מתמטיות שונות בלתי הפיכות. אחת מהן היא כפל של שני מספרים ראשוניים גדולים. אילו הן שתי פעולות אחרות?

פתרון:

2 פעולות אחרות הן:

א. עלייה בחזקה -  $E(x) = x^b$  וגם  $b$  הם ידועים אבל אי אפשר בזמן מתאים למצוא  $x$  (אין שורש באריתמטיקה מודולרית).

ב.  $(M_0, C_0)$  / Discrete Logarithm Problem / DLP - אם במשך התקפה קיבלנו זוג  $(M_0, C_0)$  /  $C_0 \equiv M_0^a \pmod{N}$  ואנו ידועים שקיים  $a$  ש- אבל לא יכולים בזמן מתאים לחשב מפתח סודי  $a$  (אין לוגריתם באריתמטיקה מודולרית).

### שאלה מס' 6

נתונה HASH פונקציה בעלת פלט באורך 16 ביט. אמד את ההסתברות ההתנגשות בקבוצאה של 256 הודעות שונות.

פתרון:

מבעיה "The Birthday attack" אנו יודעים שההסתברות ההתנגשות שווה ל-

$$P = 1 - e^{-\frac{k^2}{2N}} \quad \text{כאן } k = 256, N = 2^{16}, \text{ מספר ערכאים אפשריים } = \text{מספר "אנשים"} = 256. \text{ לכן } P = 0.393$$

שאלה מס' 7

נתונה מערכת KNAPSACK עם סדרה פומבית  $B = (17, 3, 20, 12, 7)$ . גם ידועים המודול חישוב  $N=31$  ואיבר גדול ביותר של סדרה סודית  $a_5=15$ .  
מצאו את הסדרה סודית ופענחו את ההודעה  $C=56$ .

פתרון:

מן ש-  $A \cdot V^{-1} \equiv 1 \pmod{31}$  ו-  $V=17$  ולכן  $V^{-1}=11$ .  
סדרה סודית היא  $A = V^{-1} \cdot B = 11 \cdot (17, 3, 20, 12, 7) = (1, 2, 3, 8, 15)$  וסכום ההודעה לפי הסדרה הסודית  $X_M = 56 \cdot 11 = 27(31)$ . פירוק לפי סדרה  $A$  נותן ייצוג בינארי של  $M$ :  
 $M = '10111' = 23$



# **מכללת אורט בראודה**

**לפני תחילת הבדיקה אנא קרא/י בעיון את ההוראות ומלא/י את כל הפרטים בכתב ברור:**  
(שים לב, מוחבות הבדיקות נסרקות למטרות נתוניות. יש להקפיד  
שלא לקלפל / לתלוש / לכתוב בצעבים)

	שאלה 1
	שאלה 2
	שאלה 3
	שאלה 4
	שאלה 5
	שאלה 6
	ציוון הבחינה

מועד א'  מועד ב'  מועד מ'

## מחברת בחרינה

סמסטר: א - ב - קיץ

፲፭፻፭

אין להלוש רפים מהמחברת

86

**שמור על טוהר הבחינה!  
הישגיות ביושר היא  
הדרך היחידה להצלחה!**



23

דס' סידורי

מחרבות מס' \_\_\_\_\_ מדור \_\_\_\_\_ מחברת מס'



(8) 201266129 .ת.ל  
בוחינן: 006110011309



**נא לבדוק מס' ת"ז במדבקה**

אין לכתוב מעבר לכך האדום משני צדי הדף.  
יש לכתוב את הבדיקה בעט (כחול / שחור) בלבד.

ס.נ.ת. 201266129

מחלקה **ויקרא**

מבחן היברידי

כיתה 203 מס' 12/11

שם המרצה בירוקו טריינינג וטכניון

~~11/11/11~~ 11/15

שעת יציאה לשירותים

שעת חזרה משירותים

—  
—  
—

*...and the world will be at peace.*

## טופס מלאווה לשאלון מבחן

שם הקורס: קרייפטולוגיה 1	שם לימודי: ג'
מספר הקורס: 61117	מרצה: פרופ' זאב ולקוביץ'
	מתרגלים: ד"ר רנטה אברוס ד"ר לאוניד מוריוזנסקי
מספר סמסטר: א'	מסלול / מגמה: הנדסת תוכנה
מועד הבחינה: ב' 19/02/2014	תאריך הבחינה:
שעת הבחינה: 9 <sup>00</sup>	משך הבחינה: 180 דקות

### הוראות לנבחן ולמישגית

1. יש להזכיר את השאלון בסוף הבחינה.
2. יש לענות על כל השאלות.
3. ניתן להשתמש רק בדף נוסחאות מצורף בטופס.
4. לא ניתן להשתמש בחומר עזר אחר.
5. **ניתן לכתוב בעט בלבד.**
6. כל העבודה, כולל פיזוטה וחישובי עזר, צריכה להיכתב במחברת הבחינה בלבד ו/או בשאלון (כמפורט בסעיף 7) ואין להשתמש בכלל נייר אחר.
7. יש לענות על הבחינה בטופס שאלון הבחינה בלבד.
8. ניתן להשתמש במחשבון.
9. **טפסי השאלון ייבדקן, המתריות לא ייבדקן.**
10. אין לחלק לסטודנטים פתקי שאלות.
11. הימן שדרושים הסברים תקיי הסבר.
12. אין להעביר כל חומר בין הסטודנטים.

**ב ה צ ל ח ה !!!**

1	2	3	4	5	6	7	8	סה"כ
10	7	10	10	33	10	10	10	100
7	5	8	8	3+10 10+10	5	10	10	86

שאלה מס' 1

$$K = \begin{pmatrix} a & 1 & a-1 \\ 1 & 2a & 1 \\ 2 & 3 & 1 \end{pmatrix}, Y = X K \bmod 37$$

עבור איזה ערכים של הפרמטר  $a$  מספר הודעות הבילתי מושטרות הוא מקסימלי ועבור איזה הוא מינימלי?  
(10 נקודות)

(1) רACION איזה אוסף גנרי סדרני?

$$\det K = a(2a-3) - 1(1-2) + (a-1)(3-4a) = \\ = 2a^2 - 3a + 1 + 3a - 4a^2 + 4a - 3 = 4a - 2a^2 - 2$$

לפניהם  $\det K \neq 0 \Leftrightarrow (4a - 2a^2 - 2, 37) = 1 \quad : \underline{f \parallel 3}$

$$4a - 2a^2 - 2 \neq 0 \pmod{37}$$

$$\begin{aligned} & 2a(2-a) \neq 2 \cdot 37 \\ & a(2-a) \neq 18 \cdot 37 \\ & a(2+36a) \neq 18 \cdot 37 \\ & a(1+18a) \neq 0 \pmod{37} \\ & a \equiv 3 \pmod{37} \\ & 1+18a \equiv 3 \pmod{37} \\ & 18a \equiv 2 \pmod{37} \\ & 18a \equiv 35 \pmod{37} \\ & a \equiv 33 \pmod{37} \\ & a \equiv 3 \pmod{37} \end{aligned}$$

$$= \begin{pmatrix} a & 1 & a-1 \\ 1 & 2a & 1 \\ 2 & 3 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a-1 & 1 & a-1 \\ 1 & 2a-1 & 1 \\ 2 & 3 & 0 \end{pmatrix}$$

$$(x \ y \ z) \begin{pmatrix} a-1 & 1 & a-1 \\ 1 & 2a-1 & 1 \\ 2 & 3 & 0 \end{pmatrix} = (0 \ 0 \ 0)$$

$$(k-I)^T = \begin{pmatrix} a-1 & 1 & 2 \\ 1 & 2a-1 & 3 \\ a-1 & 1 & 0 \end{pmatrix} \xrightarrow{R_3-R_1} \begin{pmatrix} 0 & 0 & 2 \\ 1 & 2a-1 & 3 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\begin{aligned} & \text{2nd row, } \\ & -a^2+2a-2=0 \quad \text{or} \quad a^2-2a+2=0 \quad (37) \\ & x_2 = \frac{2 \pm \sqrt{4-4}}{2} = \begin{cases} x_1=1 \\ x_2=1 \end{cases} \end{aligned}$$

$$2z=0$$

$$\begin{aligned} 1x + (2a-1)y + 3z &= 0 \Rightarrow -\frac{y}{a-1} + (2a-1)y = 0 \\ (a-1)x = -y \Rightarrow x &= \frac{-y}{a-1} \end{aligned}$$

$$y - (a-1)(2a-1)y = 0$$

$$y(1-2a^2+a+2a-1)=0$$

$$y(2a^2+3a)=0$$

$$2a^2+3a=0 \quad (37)$$

$$\therefore \text{or} \quad a=0$$

$$2a-3=0 \quad (37)$$

$$2a=3 \quad (37)$$

$$a=20 \quad (37)$$

u	v
1	21
2	22
3	23
4	24
6	26
9	27
12	28
18	38
36	56

7

$$\begin{aligned} & a=0 \quad \text{or} \quad k \quad \text{or} \quad 11k \\ & (2a^2+3a+2)=0 \quad (37) \\ & y=0 \quad (37) \\ & z=0, x=0 \quad (37) \\ & (0,0,0) \quad (37) \end{aligned}$$

$$(f_1, f_2, \dots, f_n) \in \Omega = \Omega(37)$$

$\alpha = 1$  (37)  $\rightarrow$   $\rho B \approx 137 M_{1.5}^2$   $\times$  many  $a$

אנו סבירים וסבירים וסבירים וסבירים

שאלות מס' 2

תאר את מערכת ONE TIME PAD ונמק יתרונות וחסרונות שלה. (7 נקודות)

כִּי-בְּעֵד כִּי-בְּעֵד כִּי-בְּעֵד כִּי-בְּעֵד

א. טב זהה הינה מילה גנטית נארנ.

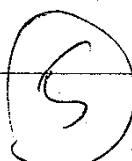
אל-מלאר: חוקן ה-רכוב, ה-הנימוחת ה-הטעה פ-ל-ל-ל-ל-ל

Another: Red official map of Canada, N.W.T.

אודה לך מילון פירוטי של המילים שפַתְתָה בפִתְתָה

$$K_{t+1} = a K_t + b(n) \quad \text{for } t \geq 0$$

the main role now has got - Indian firms



• R3177 D781B

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 2 & 3 & 1 \end{pmatrix}$$

$$(x \ y \ z) \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 2 & 3 & 1 \end{pmatrix} = (0 \ 0 \ 0)$$

$$x + y = 0 \Rightarrow x = -y \Rightarrow x = z$$

$$y + z = 0 \Rightarrow y = -z$$

$$2x + 3y = -z \Rightarrow 2z + 3 \cdot (-z) = -z$$

$$-z = -z$$

שאלה מס' 3

במערכת הצפנה קיימות 64 הודעות אפשריות עם הסתברויות שוות מראש אבל אם ידועה הودעה מוצפנת אז הסתברות של הודעה המקורית אחת היא שווה 0.5 והסתברויות הודעות אחרות שוות זו לזו. מהו המידע על הודעה מקורית שנוננתה הודעה מוצפנת? (10 נקודות)

$$P(x_i) = \frac{1}{64}$$

$$P(x_i | c_j) = \begin{cases} \frac{1}{2}, & i=j \\ \frac{1}{126}, & i \neq j \end{cases}$$

$$I = H(X) - H(X|C) = \log(64) - 3.5 \approx 2.5$$

$$H(X|C) = \sum_{c_i} p(c_i) H(X|c_i) \stackrel{3.5}{=} \sum p(c_i) \cdot 3.5 = 3.5$$

$$H(X|c_i) = \frac{1}{64} \cdot \log 2 + \frac{63}{126} \cdot \log(126) \stackrel{3.5}{=} 3.5$$

(8)

שאלה מס' 4

תאר את ההתקפה "Meet in the Middle" לצופן 4-DES עם כל מפתחות שונים והסביר את

סיבוכיות שלה. (10 נקודות) ויזען סולפְּגָעָה

$$E_{k_1}(E_{k_2}(E_{k_3}(E_{k_4}(x))) = y \quad \begin{matrix} \text{מתקפה} \\ \text{בינה} \\ \text{לפניהם} \end{matrix} \quad \begin{matrix} \text{x} \\ \text{y} \\ \text{y}^3 \end{matrix}$$

$$E_{k_3}(E_{k_4}(x)) = D_{k_2}(D_{k_1}(y))$$

$k_3, k_4$  הינו סדרה של  $k_1, k_2$  בירוב מקרים (בנוסף לדוגמה)

$$\text{RADIX}_2(y^3) \cdot 2^{112} + 2^{112} \quad \text{הציגי איזה סדרה?}$$

בנוסף לדוגמה, נשים לב ש $y^3$  מוגדרת כ $y^3 = y \cdot y \cdot y$ .

$$O(2^{113} \cdot \log(2^{112})) \quad \text{הו שיקול}$$

$$851 = 37 \cdot 23 \Rightarrow \phi(851) = 36 \cdot 22 = 792$$

שאלה מס' 5

מערכת RSA בניית על בסיס 1.

a. כמה מפתחות ציבוריים אפשריים קיימים במערכת זו? (3 נקודות)

$$\phi(b) \mid \phi(a) \quad b \cdot a = 1 (\phi(851)) \quad \text{בנוסף}$$

$$\phi(\phi(851)) = \phi(792) = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{10}{11} \cdot 792 = \underline{\underline{240}}$$

3

ב. הودעה 3 התקבלה כתוצאה ההצפנה של הודעה  $M$  על ידי מפתח  $b=679$ . מצא את  $M$ .  
(10 נקודות)

$$D = 679 \Rightarrow \alpha = 679^{-1} (\neq 92)$$

$$(792, 679) = (679, 113) = 679 - 6 \cdot 113 = 679 - 6(\neq 92 - 679) =$$

$$\neq 7 \cdot 679 - 6 \cdot 792 \Rightarrow \alpha = 7$$

$$M = D_7(3) = 3^7 (851) = 485 (851)$$

= 10

ג. מצא את כל ה教导ות הבלתי מוסתרות עבור המפתח  $b = 17$ . (10 נקודות)

רלו נולן גודן 60 נולן 55

$$m_1 = 23, M_1 = 37, m_2 = 37, M_2 = 23$$

$$C_1 = M_1^{-1}(m_1) = 14^{-1}(23) = 5(23)$$

$$C_2 = M_2^{-1}(m_2) = 23^{-1}(37) = 29(23)$$

$$(37, 23) = (23, 14) - (14, 9) - (9, 5) = 2 \cdot 5 - 9 =$$

$$= 2 \cdot (14 - 9) - 9 = 2 \cdot 14 - 3 \cdot 9 = 2 \cdot 14 - 3(23 - 14) = -3 \cdot 23 + 5 \cdot 14$$

$$= -3(23) + 5(37 - 23) = \underbrace{-8}_{C_2} \cdot 23 + 5 \cdot 37$$

$$m^{17} \equiv m(37)$$

$$m^{17} \equiv m(23)$$

רלו נולן 100% 3k

רלו נולן 100%

$$x = k_1 \cdot 667 + k_2 \cdot 185 (851)$$

רלו נולן 100%

$$\frac{(1 + \gcd(\underbrace{16, 36}_4)) (1 + \gcd(\underbrace{16, 22}_2))}{4} = 15$$

רלו נולן 100% .  $\sum_{37}^2$  מהן 6 רלו

$$36 = 2^2 \cdot 3^2 \Rightarrow \{2, 4, 6, 12, 3, 9, 18\} : 37 \rightarrow 31 \text{ by}$$

: 31 2 remain 130

$$2^2 = 4$$

$$2^4 = 16$$

$$2^3 = 8$$

$$2^6 = 27 \Rightarrow 1812$$

$$2^9 = 31$$

$$2^{12} = 26$$

$$2^{18} = 36$$

$$(2^\alpha)^k = (2^\alpha)(37) \quad \text{if } M = 2^\alpha \quad \text{by}$$

$$2^{k\alpha} = 1 \quad (37)$$

$$4\alpha = 0 \quad \Leftarrow 16\alpha = 0 \quad (37) = 0 \quad (36)$$

$\alpha = 0, 9, 18, 27$  : סדרה גיאומטרית עם ריבוע של 4 של

:  $Z_{37}^*$  → נספחים מימין → 31

$\alpha$	0	9	18	27
$m$	1	31	36	6

$$x = v_1 667 + v_2 185$$

(10)

$r_1$	0	0	0	1	1	1	-1	-1	-1	0	1	1	0	1	-1
$b_2$	0	1	-1	0	1	-1	0	1	-1	31	31	31	6	6	6
$X$	0	185	666	667	852	482	184	369	850	629	445	813	2975	75	443

ד. הוחלט לבצע החלפת מפתחות בשיטת Diffie-Hellman על בסיס הגורם הגדל  $g$  של המערכת הנ"ל, כאשר המפתחות הפרטיים של כל אחד מהמשתתפים הם 7 ו- 9 בהתאם, חשב את המפתח המשותף. איזה מהמפתחות הפרטיים יותר טוב או אין עדיפות? נמק את חשיבותך. (10 נקודות)

$$g = 37$$

$$p \cdot \mathbb{Z}_{37}^* \ni 83 \rightarrow 2e \text{ קבוצה } \mathcal{L}(p) \text{ נס饱ה}$$

$$2^{9 \cdot 7} \equiv 2^{63} = 2^{63 \bmod 36} = 2^{63 \bmod 36} = 2^{27} = 6 \quad (37)$$

$$83 \mid 2^9 \mid 83 \mid 2^7 \quad \text{יכלול נס饱ה}$$

$$(37 \cdot 71) \cdot 36 = 0(37) \mid 25 \mid 9 \mid 15$$

$$\text{לפנינו } 2^k \text{ דרכו שוכן נס饱ה}$$

Answers

שאלה מס' 9

תאר והסביר את "The Birthday attack" נגד פונקציית HASH. (10 נקודות)

ההתקפה נקראת: The Birthday Attack

ההתקפה מושגנת על: פונקציית HASH k (בדרך כלל)

ההתקפה מושגנת על: פונקציית HASH k (בדרך כלל)

ההתקפה מושגנת על: פונקציית HASH k (בדרך כלל)

$$1 - e^{-\frac{k^2}{2N}}$$

5

7n 4

שאלה מס' 7

מערכת KNAPSACK בנויה על סמך הסדרה הפומבית ( $B = (38, 4, 27, 35, 36)$ , מודול חישוב

$$N=53 \text{ וגורם סודי } V=19. \text{ פענח את ההודעה } C=14 \text{ נקודות) } . \\ (53, 19) = (14, 15) = (15, 4) = (4, 3) = 4 \cdot 3 = 4 - (15 - 4 \cdot 3) = 4 - 4 - 15 = \\ = 4(19 - 15) = 15 = 4 \cdot 19 - 5 \cdot 15 = 4 \cdot 19 - 5(53 - 2 \cdot 19) = (2) \cdot 19 - 5 \cdot 53$$

$$V^{-1} = 14(53)$$

$$A = \sqrt{B} = (1, 3, 7, 13, 27)$$

$$M' = V^{-1} \cdot C = 37 = 27 + 7 + 3 \Rightarrow M' = \begin{smallmatrix} 0 & 1 & 1 & 0 & 1 \\ 8 & 4 & & & 1 \end{smallmatrix} B$$

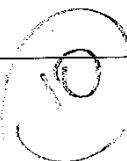
$$\boxed{M = 13}$$

ל.ג.  $M \rightarrow$  מילוי הרצף

$$4 + 27 + 36 = 14 \checkmark$$

$$M' \cdot V = 14 \checkmark$$

$$37 \cdot 19 = 14$$



ס.ג.:

שאלה מס' 8

ALICE ו- BOB משתמשים במערכת RSA כדי לשולח הודעה אחת לשני. פרמטרים של ALICE ושל BOB הם שונים, אבלקטיים  $n$  ו-  $e_2$  הם מספרים לא זרים. איך לפרק את המרכיבים (למזהה הפרמטרים)? (10 נקודות)

השאלה מבקשת למצוא את  $n$  והקיצור  $(N, e_2)$ .  
השאלה מבקשת למצוא את  $N$  ו-  $e_2$ .

10

### דף נוסחות

#### Euler-Fermat Theorem .1

לכל  $a \in \mathbb{Z}$  מתקיים  $\gcd(a,n) = 1 \Rightarrow a^{\phi(n)} \mod n = 1$

אם  $n$  מספר ראשוני אז  $a^{n-1} \mod n = 1$

#### 2. משפט השארית הסיני:

יהיו  $d_1, \dots, d_t$  מספרים זרים בזוגות ו-  $d_1 d_2 \dots d_t \mid n$ . אזי למערכת המשוואות

$$x \equiv a_i \pmod{d_i}, \quad i = 1, \dots, t$$

קיים פתרון משותף  $x$  בתחום  $[0, n-1]$ .

$$\frac{n}{d_i} * y_i \equiv 1 \pmod{d_i} \quad \text{כאן } x = \left[ \sum_{i=1}^t \left( \frac{n}{d_i} \right) y_i x_i \right] \pmod{n}$$

3. הצופן RSA:  $E(x) = x^b \pmod{n}$

$n$  הוא מכפלה של שני מספרים ראשוניים שונים  $p$  ו-  $q$ .

4. סימוני הצופן KNAPSACK:  $A = (a_1, a_2, \dots, a_n)$  - מודול חישוב,  $N$  - סדרה סודית,

$B = (b_1, b_2, \dots, b_n)$  - סדרה פומבית,  $V$  - גורם סודי.

#### 5. האלפבית האנגלי, קודים וশכיחיות / באליית :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
82	15	28	43	127	22	20	61	70	2	8	40	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
67	75	19	1	60	63	91	28	10	23	1	20	1

**פתרונות של המבחן 6/7/2014  
בקורס: קריפטולוגיה 1 / 61117/**

**שאלה מס' 1**

**מוגדר צוף**  $E(X) = \left[ (x_1, x_2) \cdot \begin{pmatrix} a & 1 \\ 2 & a-1 \end{pmatrix} + (2, 3) \right] \bmod 29$  **על א"ב**

**בנ" 29** אותיות: א"ב אנגלי (קודים 0-25) ועוד רווח, פסיק, נקודה עם קודים 26, 27 ו- 28 בהתאם. עבור כל ערך של פרמטר  $a$  מצא מספר הודעות בלתי מוסתרות והשכ אונן עבור  $a=6$ . (20 נקודות)

**פתרונות:**

1. קודם כל נחשב ערכים אפשריים של הפרמטר. ערך אפשרי אם בשילובו אפשר לפענה תוצאה הצפנה, ז.א. נסחת הצפנה היא הפיכה:

$$(y_1, y_2) = \left[ (x_1, x_2) \cdot \begin{pmatrix} a & 1 \\ 2 & a-1 \end{pmatrix} + (2, 3) \right] \bmod 29$$

ואנו יכולים למצוא  $x_1, x_2$  ונתנו יכו למצא  $X$  כפונקציה של  $Y$  אם

ורק אם מטריצה  $\begin{pmatrix} a & 1 \\ 2 & a-1 \end{pmatrix}$  היא הפיכה לפי  $\bmod 29$ . תנאי הפיכות הכרחי ומספיק הוא

$$\gcd(\det\begin{pmatrix} a & 1 \\ 2 & a-1 \end{pmatrix}, 29) = 1$$

ולפניהם  $\det\begin{pmatrix} a & 1 \\ 2 & a-1 \end{pmatrix} \neq 0$ , לכן  $a^2 - a - 2 \neq 0$  או  $a \neq 2$  ו-  $a \neq 28$ .

לפי הגדרה של הודעות בלתי מוסתרות  $X \equiv Y \bmod n$  וכאן  $X \equiv XA + B \bmod 29$ .

או  $X(A - I) \equiv -B \bmod 29$ . אם מטריצה  $(A - I)$  הפיכה אז קיים פתרון אחד ויחיד.

המקרה מתקיים, כמו בסעיף הקודם, אם ורק אם

$$\begin{cases} a \neq 0 \\ a \neq 3 \end{cases} \text{, } |A - I| = \begin{vmatrix} a-1 & 1 \\ 2 & a-2 \end{vmatrix} = a^2 - 3a = a(a-3) \neq 0 \bmod 29$$

$$\text{סתירה, } \begin{cases} -x_1 + 2x_2 = -2 \bmod 29 \\ x_1 - 2x_2 = -3 \bmod 29 \end{cases} \iff (x_1, x_2) \cdot \begin{pmatrix} -1 & 1 \\ 2 & -2 \end{pmatrix} = -(2, 3) \bmod 29 \text{ או } a = 0 \text{ אם}$$

$$\begin{cases} 2x_1 + 2x_2 = -2 \bmod 29 \\ x_1 + x_2 = -3 \bmod 29 \end{cases} \text{ אין פתרונות. גם ל- } a = 3 \text{ מקבלים שלמערכת}$$

$$\Leftrightarrow \begin{cases} 5x_1 + 2x_2 = -2 \pmod{29} \\ x_1 + 4x_2 = -3 \pmod{29} \end{cases} \Leftrightarrow (x_1, x_2) \cdot \begin{pmatrix} 5 & 1 \\ 2 & 4 \end{pmatrix} = -(2, 3) \pmod{29}$$

$$x_2 = 17 \text{ ו } x_1 = 16 \Leftrightarrow 9x_1 = -1 \pmod{29}$$

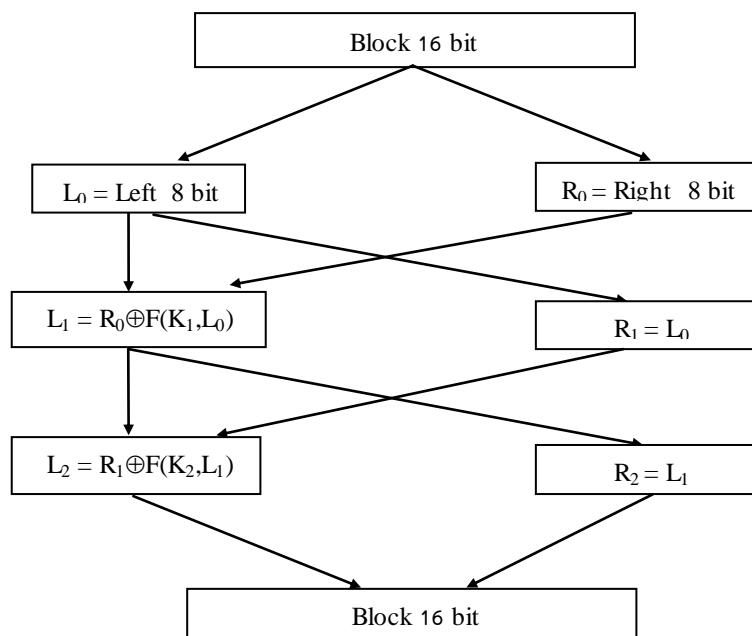
תשובה: לכל ערכים  $a$  חוץ מ- 0, 2, 3, 28 יש הودעה בלתי מוסתרת אחת,

אם  $a$  שווה 0 או 3 אז אין הודעות בלתי מוסתרות

. אם  $a = 6$  אז ה Hodua בלתי המוסתרת היא (16, 17)

## שאלה מס' 2

נתון אלגוריתם שמצוין בЛОקים של 16 סיביות באמצעות מפתח של 12 סיביות



כأن

1. מפתחות נוכחים:

$K_1$  הוא 8 סיביות הראשונות מצד שמאל של המפתח  $K$



$K_2$  הוא 8 סיביות הראשונות מצד ימין של המפתח  $K$



2. חשב פונקציה  $F$ :

א. שרשור  $K_i \oplus L_{i-1}$  (משמאלי) ו- 4 סיביות שלא ישמשו במפתח נוכחי:  $(K \setminus K_i) \parallel (K \setminus K_i)$

ב. מחלקים את השורה שקבלנו לשתי שורות באורך 6 ביט, לכל מהן נכנסים בו- S-box, מקבלים שתי תוצאות ומשרשרם אותן.

S-Box																
Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

(א) הצפן  $K = (10101010101010) \oplus (10101010101010)$  (10 נקודות).

פתרונות:

$$L_0 = 10101010$$

$$R_0 = 10101010$$

$$K_1 \oplus L_0 \parallel (K \setminus K_1) = 000000001010 \Rightarrow$$

$$\begin{aligned} 1. \text{row} = '00' = 0, \text{column} '0000' = 0 \\ \Rightarrow SBox(000000) = 14 = '1110' \end{aligned}$$

$$\begin{aligned} 2. \text{row} = '00' = 0, \text{column} '0101' = 5 \\ \Rightarrow SBox(001010) = 15 = '1111' \end{aligned}$$

$$F(K, L_0) = 11101111$$

$$L_1 = R_0 \oplus F(K, L_0) = 01000101$$

$$R_1 = 10101010$$

$$K_2 \oplus L_1 \parallel (K \setminus K_2) = 11101111010 \Rightarrow$$

$$\begin{aligned} 1. \text{row} = '11' = 3, \text{column} '1101' = 13 \\ \Rightarrow SBox(111011) = 0 = '0000' \end{aligned}$$

$$\begin{aligned} 2. \text{row} = '10' = 2, \text{column} '1101' = 13 \\ \Rightarrow SBox(111010) = 10 = '1010' \end{aligned}$$

$$F(K, L_1) = 00001010$$

$$L_2 = R_1 \oplus F(K, L_1) = 101000000$$

$$R_2 = 01000101$$

$$Y = 1010000001000101$$

ב. האם האלגוריתם ניתן לפענה. אם לא, נמק השינוי הנדרש. (5 נקודות).

פתרונות:

אי אפשר להשתמש באלגוריתם.

אנו צריכים לעשות שינוי הבא בסוף לשרשרת בסדר הפוך כמו ב- DES רגיל וגם במשך פיענוח אנו צריכים להשתמש במפתחות  $K_1, K_2$  בסדר הפוך.

ג. מצא את המפתחות החלשים. (5 נקודות)

מפתח חלש במשמעות DES אם המפתחות נוכחים  $K_2, K_1$  שוים, אבל כאן בבלאייטריציה עוד נستخدم במשלים למפתח נוכחי.

מחלקים מפתח  $K$  בשלושה חלקים כך שכל אחד בן 4 ביטים:  $K = P_1 \parallel P_2 \parallel P_3$  (|| - שרשור),

$$P_1 = P_2 = P_3 \quad K_2 = P_2 \parallel P_3 \quad \text{ו} \quad K_1 = P_1 \parallel P_2$$

### שאלה מס' 3

נתונה מערכת מבוססת על אותו העיקרון כמו RSA רק הבסיס הוא מכפלה של 3 מספרים

$$n = pqr$$

א) מה הוא מספר הודעות בלתי מוסתרות טריוויאליות ? נמק. (5 נקודות)

פתרון:

אנו מקבלים הודעות בלתי מוסתרות טריוויאליות מצירופי פתרונות טריוויאליים של השוואות לפי

$$3^3 \equiv 1 \pmod{r} \quad \text{ול} \quad 3^3 \equiv 0 \pmod{q} \quad \text{ול} \quad 3^3 \equiv 0 \pmod{p}$$

ב) אם  $n=385$  אז כמה הודעות בלתי מוסתרות יש למפתח פרטי  $K=11$  ? תן דוגמה של הودעה בלתי מוסתרת לא טריוויאלית (10 נקודות)

פתרון:

$$n = 385 = 5 \cdot 7 \cdot 11$$

$$m = (1 + \gcd(10, 4)) \cdot (1 + \gcd(10, 6)) \cdot (1 + \gcd(10, 10)) = 99$$

כל הודעות הן בלתי מוסתרות ודה באמה נכון לפי משפט פרמה להשוואה

$x^{11} \equiv 1 \pmod{11}$  בוחרים למשל  $x = 2$  ולהשואות לפי 5 ו- 7 פתרון טריוויאלי 0, ככלומר  $(0, 0, 2)$ .

$$X = x \cdot M_3 \cdot C_3 \pmod{n} = 2 \cdot 35 \cdot (35^{-1} \pmod{11}) = 2 \cdot 35 \cdot 6\%385 = 35$$

### שאלה מס' 4

הוחלט לבצע החלפת מפתחות בשיטת Diffie-Hellman על בסיס  $p=13$  ויוצר קטן ביותר.

ידוע שמפתח משותף שווה 8 ואחד ממפתחות פרטיים הוא 5 או מה מפתח פרטי שני ?

(10 נקודות)

פתרון:

לחפשו יוצר אנו הייבים לבדוק לשונות מ- 1 חזקת עם מעריכים שמקבלים  $\theta(13) = 12$  ג.א.

$$\text{בודקים } 2: g = 2^{12} \equiv 64 \pmod{13} \neq 12 \quad \text{לכן } g = 2 \text{ יוצר קטן ביותר.}$$

ידוע ש-  $2^{5k} \equiv 8 \pmod{13}$  אפשר בכוח גס :

K	1	2	3	4	5	6	7	8	9
$2^{5k} \pmod{13}$	6	10	8						

או

להשוו את החזקה ב-  $5^{-1} \equiv 5 \pmod{12} \iff 5k \equiv 3 \pmod{12} : \text{mod} \theta(n)$

תשובה:  $k = 3$

### שאלה מס' 5

מערכת RSA בנויה על בסיס 437.

- א. הودעה  $C=3$  התקבלה כתוצאת ההצפנה של הודעה  $M$  על ידי מפתח  $b=283$ . מצא את  $M$ . (10 נקודות)

פתרונות:

$$\theta(N) = 18 \cdot 22 = 396 \iff N = 19 \cdot 23$$

נחשב המפתח חסודי  $a = b^{-1}(\theta(N)) = 283^{-1}(396)$

$$\begin{array}{c} 1 = 57 - (113 - 57) = \\ = -113 + 2 \cdot (283 - 2 \cdot 113) = \\ = 2 \cdot 283 - 5 \cdot (396 - 283) = \\ = -5 \cdot 396 + 7 \cdot 283 \end{array} \quad \left[ \begin{array}{l} 396 = 283 + 113 \\ 283 = 113 \cdot 2 + 57 \\ 113 = 57 + 56 \\ 57 = 56 + 1 \end{array} \right] \quad \text{לכן } a = 7$$

$$M = C^a(N) = 3^7(437) = 2$$

- ב. תאר את המערכת חתימה דיגיטלית המבוססת על מערכת הצפנה RSA. (5 נקודות)

פתרונות:

שיטת חתימה דיגיטלית הכי מקובלות היא הצפנה באמצעות המפתח הפרטี้ של החותם:  $E_{k_2} = M^{k_2}(n)$  כאשר  $k_2$  מפתח פרטוי של החותם אבל קיימת שיטה חילופית בנויה על הצפנה חוזרת במפתח הפרטוי של החותם ומפתח הציבורי של המქבל. תשובה מסווג זהה גם מתקובלת בהסביר הנכון.

- ג. האבטחה של RSA מבוססת על שלוש עובדות של אРИתמטיקה רגילה ואריתמטיקה מודולרית. מה הן העובדות הללו? (10 נקודות)

פתרונות:

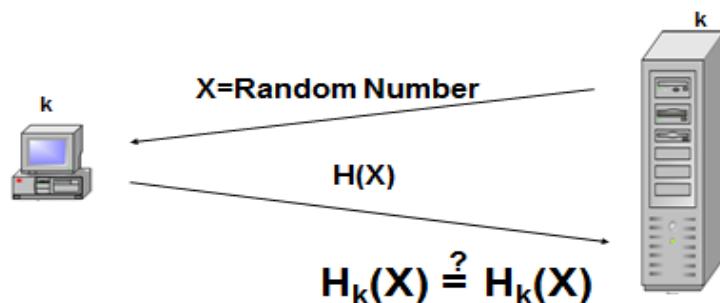
1. אי אפשר לפרק כפל של שני מספרים ראשוניים פרט לכוח גס (BRUTE FORCE).
2. עלייה בחזקה  $- E(x) = x^b$  וגם  $b$  הם ידועים אבל אי אפשר בזמן מתאים למצאו  $x$  (אין שורש באРИתמטיקה מודולרית).
3.  $(M_0, C_0)$  / Discrete Logarithm Problem / DLP /  $C_0 = E(M_0) \bmod N$  /  $(C_0)^a \equiv M_0 \pmod{N}$  אבל לא יכולים בזמן מתאים לחשב מפתח סודי  $a$  (אין לוגריתם באРИתמטיקה מודולרית).

## שאלה מס' 6

תאר והסביר פרוטוקול האימות המשמש ברשות (AIMOT) אויל SERVER CLIENT מבוסס על הצפנה של פונקציית הערבול (HASH FUNCTION) . (10 נקודות)

פתרונות:

### .AIMOT בעזרת HASH FUNCTION



- א) הרשת מقلל מספר אקראי גדול (64BIT) X ושולח אותו למשתמש.
- ב) המשתמש מחשב את הערך של פונקציית הערבול ומצביע אותו בפתחה הפרטי שלו ומחזיר לשרת.
- ג) הרשת מבצע אותן פעולה אם X ומשווה את התוצאות.
- ה) אם שתי התוצאות זהות אז תהליך האימות עבר בהצלחה.
- ו) לצורך ההבטחה אפשר לחזור על אותו תהליך.

	שאלה 1
	שאלה 2
	שאלה 3
	שאלה 4
	שאלה 5
	שאלה 6
	צוין הבחינה



לפני תחילת הבחינה אנא קרא/י בעיון את ההוראות ומלאי את כל הפרטים בכתב ברור:  
(שים לב, מחברות הבחינה נסרקות למאגר נתונים. יש להקפיד שלא לкопל / לתלוּש / לכתוב בכתב)

מועד א'  מועד ב'  מועד מיוחד

שם המשגיח טוויל

## מחברת בוחינה

סמסטר: א - ב - קיץ

14412

**אין לתלוּש דפים מהמחברת**

**שמור על טוהר הבחינה!**  
הישגים ביושר היא  
הדרך היחידה להצלחה!



מספר סידורי: 1

מחברת מס' \_\_\_\_\_ מטור \_\_\_\_\_ מחברות



ת.ז. 037036209  
בחינה: 006110015794



נא לבדוק מס' ת"ז במדבקה

אין לכתוב מעבר לכך האודום משני צד' הדף.  
יש לכתוב את הבחינה בעט (כחול / שחור) בלבד.

מס' ת"ז 037036209

מחלקה כימיה

מקצוע הבחינה קורס אינטנסיבי 1

כיתה M218

תאריך 06/07/2014

שם המרצה טוויל

שעת יציאה לשירותים 16:00

שעת חזרה משירותים 16:08

שים לב להנחיות הוחוקים. הרכבו לפניו הסיריקה. וכן אין לנתרן נז'

**טופס מלאוה לשאלון מבחן**

מרצים:	פרופ' זאב וולקוביץ'	שם הקורס:	קריפטולוגיה 1
מתרגם:	ד"ר רנטה אברוס	מספר הקורס:	61117
תאריך הבחינה:	6/07/2014	מחלקה:	הנדסת תוכנה
משך הבחינה:	180 דקות	שעת הבחינה:	14 <sup>00</sup>
מועד הבחינה:	אי' תשע"ד	סמסטר:	ב'

**הוראות לנבחן ולמשגיח**

1. יש לעות על הבחינה (לסמן X בסוגרים):
  - ( ) במחברת הבחינה בלבד
  - ( ) במחברת הבחינה ועל גבי טופס שאלון הבחינה
  - (X) בטופס שאלון הבחינה בלבד
2. המחברות יבדקו / לא יבדקו (נא לסמן בעיגול).
3. טפס השאלון (יבדקו) לא יבדקו (נא לסמן בעיגול).
4. ניתן / לא ניתן להשתמש בכל חומר עזר פרט ל \_\_\_\_\_ (נא לסמן בעיגול).
5. ניתן / לא ניתן להשתמש במחשבון (נא לסמן בעיגול).
6. יש / אין להקל לסטודנטים פתקי שאלות (נא לסמן בעיגול).
7. יש / אין לצרף את השאלון למחברת הבחינה בסוף הבחינה (נא לסמן בעיגול).
8. יש לענות על כל השאלות חלק השאלות (נא לסמן בעיגול).
9. מספר הנקודות לכל שאלה נתון בסוגרים ( ).
10. היקן שדרושים הסבירים ת/י הסבר.
11. כל העבודה, כולל טיזטה וחישובי עזר, צריכה להיות בכתב במחברת הבחינה בלבד / או בשאלון (כמפורט בסעיף 1) ואין להשתמש בכל נייר אחר.
12. אין להעביר כל חומר בין הסטודנטים.

1	2	3	4	5	6	סה"כ
20	20	15	10	25	10	100
20	20	15	10	25	10	100

**בצלחה!**



$$(x_1, x_2) \cdot \begin{pmatrix} a-1 & 2 \\ 1 & a-2 \end{pmatrix} = (-2, -3) \pmod{29}$$

נניח,  $\begin{pmatrix} a-1 & 2 \\ 1 & a-2 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  כי אם אז  $x_1, x_2 \in \mathbb{Z}_{29}$

$$\begin{pmatrix} a-1 & 2 \\ 1 & a-2 \end{pmatrix} = (a-1)(a-2) - 2 \equiv a^2 - 2a - a + 2 - 2 \equiv a^2 - 3a \equiv a(a-3) \not\equiv 0 \pmod{29}$$

$$a \not\equiv 0 \pmod{29} \quad a \not\equiv 3 \pmod{29}$$

הנראה אם  $a=2, 29 \mid 29a$  . אז  $a \not\equiv 0, 3 \pmod{29}$  ✓  
 $(n=2), \text{ונען ש} a \neq 0$

$$(x_1, x_2) \begin{pmatrix} -1 & 2 \\ 1 & -2 \end{pmatrix} = (-2, -3) \quad \underline{\text{אם } a=0}$$

$$(x_1, x_2) \begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix} = (-2, -3)$$

$$\begin{cases} x_1 = -2 \pmod{29} \\ -2x_1 = -3 \pmod{29} \end{cases}$$

$$\therefore \text{נמצא } x_1 \text{ של } 4 \equiv -3 \pmod{29}$$

$\text{נמצא } x \text{ של } 4x \equiv -3 \pmod{29}$  ✓

$\therefore a=3, a=6$   $\rightarrow$   $\text{not mod 29}$   $\Rightarrow$   $a \in \mathbb{P}_N$

$$\underline{\underline{a=3}} \quad (y_1, y_2) \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix} + (2, 3) = (x_1, x_2)$$

$$\begin{cases} 3x_1 + 2y_2 + 2 = x_1 \\ y_1 + 2y_2 + 3 = x_2 \end{cases} \rightarrow \begin{cases} 2y_1 + 2y_2 = -2 \\ y_1 + y_2 = -3 \end{cases} \rightarrow \begin{array}{l} x_1 = -3 - y_2 \\ \text{from } (1) \rightarrow 2(-3 - y_2) + 2y_2 = -2 \\ -6 - 2y_2 + 2y_2 = -2 \\ -6 = -2 \end{array}$$

$\rightarrow$   $\text{mod 29} \Rightarrow a=3$   $\rightarrow$   $a \in \mathbb{P}_N$

$$\underline{\underline{a=6}} \quad (y_1, y_2) \begin{pmatrix} 6 & 1 \\ 2 & 5 \end{pmatrix} + (2, 3) = (x_1, x_2)$$

$$\begin{cases} 6x_1 + 2y_2 + 2 = x_1 \\ y_1 + 5y_2 + 3 = x_2 \end{cases} \rightarrow \begin{cases} 5x_1 + 2y_2 = -2 \\ y_1 + 4y_2 = -3 \end{cases} \rightarrow x_1 = -4y_2 - 3$$

$$5(-4y_2 - 3) + 2y_2 = -2$$

$$-20y_2 - 15 + 2y_2 = -2$$

$$-18y_2 = 13 \text{ not mod 29}$$

$$\begin{array}{l} \text{from } (1) \rightarrow 6y_2 \equiv 13 \pmod{29} \\ 8 \cdot 11 \cdot y_2 \equiv 8 \cdot 13 \pmod{29} \end{array}$$

$$y_2 \equiv 104 \equiv 17 \pmod{29}$$

$$x_1 \equiv -4 \cdot 17 - 3 \equiv -71 \equiv 16 \pmod{29}$$

$$\rightarrow \text{IC mod 29 } \Rightarrow a=6 \rightarrow \mathbb{P}_N$$
  
$$(16, 17) \rightarrow \text{mod 29}$$

✓

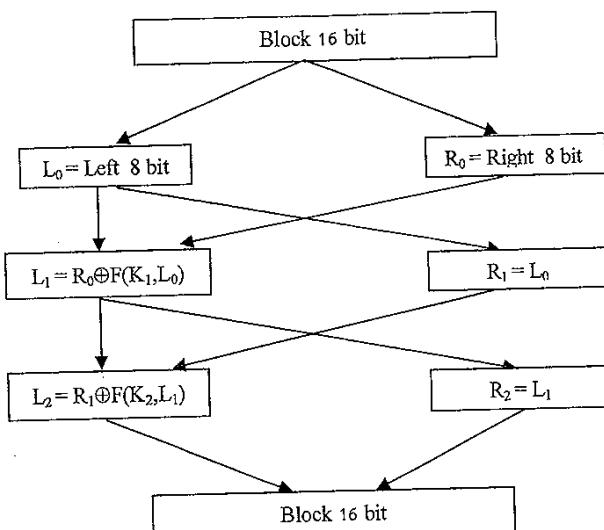
problem

$\text{mod 29} \Rightarrow a=3, 0$

$\text{mod 29} \Rightarrow a=3, 0, 2, 28$

שאל'ה מס' 2

נתון אלגוריתם שמצוין בЛОוקים של 16 סיביות באמצעות מפתח של 12 סיביות



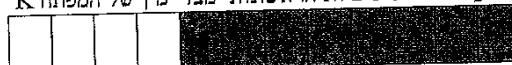
כאו

- ## 1. מפתחות נוכחים:

K<sub>1</sub> הוא סיביות הראשונות מציג שמל של המפה K



K<sub>2</sub> הוא סיביota הראשונית מצד ימיו של המפה K

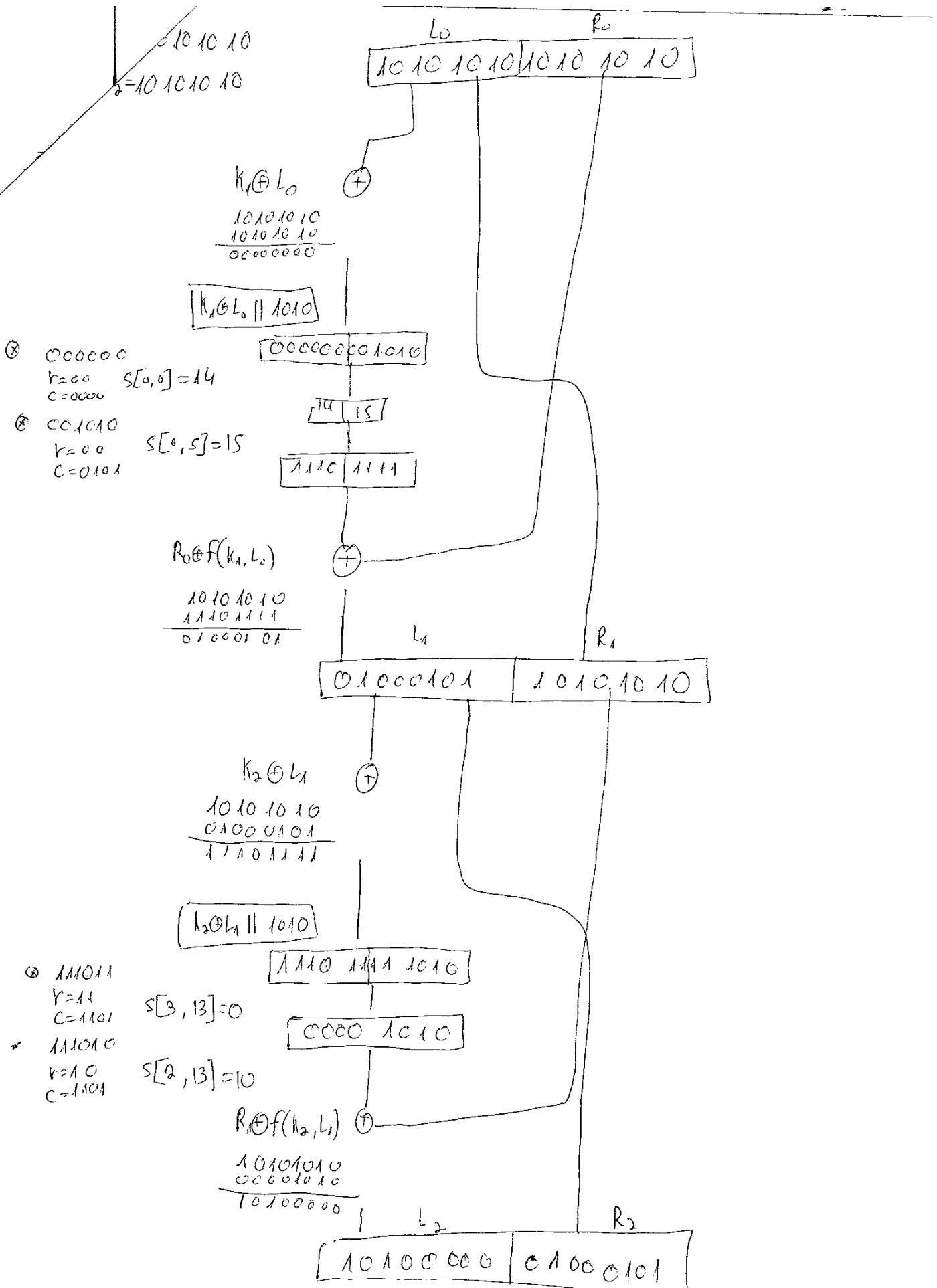


#### 2. חשוב פונקציה F :

- a. שרשור  $K_i \oplus L_{i-1}$  (משמאלי) ו- 4 סיביות שלא ישתמשו במפתח הנוכחי:  $(K_i \setminus K_j) \parallel (L_i \setminus L_j)$   
 b. מחלקים את השורה שקיבנו לשתי שורות באורך 6 ביט, לכל מהן נכנסים ב- S-box, מקבלים שתי תוצאות ומשרשים אותן.

S-Box																
Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

א) הצפן  $(1010101010101010)$  על ידי  $K = \begin{pmatrix} K_1 \\ K_2 \end{pmatrix} = \begin{pmatrix} 1010 & 1010 \\ 1010 & 1010 \end{pmatrix}$  נקבעות (



גומן תבור כ און גומן גומן

10

101010101010 1120 1010101010101010

三

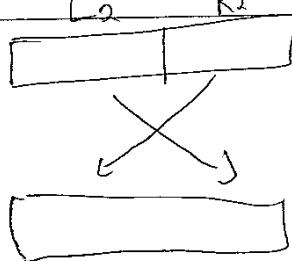
1010 0000 0100 0101

✓

ב) האם האלגוריתם נותן לפענה. אם לא, נמק השינוי הנדרש. (5 נקודות)

f. בנין דגון (בנין דגון), DES מופיע בזיהויים של מילים  
של מילון קבוצתי, כמו תבונת, מושג, מושג יפה  
ו<sub>1</sub> מושג יפה (בנין דגון) מופיע בזיהויים של מילים  
של מילון קבוצתי, כמו תבונת, מושג, מושג יפה  
ו<sub>2</sub> מושג יפה (בנין דגון) מופיע בזיהויים של מילים  
של מילון קבוצתי, כמו תבונת, מושג, מושג יפה

5



ג) מצא את המפתחות החלשים. ( 5 נקודות )

∴  $\text{H}_1 = \text{H}_2$  तो  $\text{H}_1$  का मैट्रिक्स अपने अपने उपरी नंबर वाले गणकों के समान है।

נניחו מערכת מבוססת על אותו העיקרון כמו RSA רק הבסיס הוא מכפלה של 3 מספרים ראשוניים  $n = pqr$

א) מה הוא מספר ההודעות הבלתי המוסתרות הטרייוויאליות ? נמק. (5 גנוזות )

לפנינו רשות  $n$  ומספרים  $a, b$  מ- $\mathbb{Z}$ . ניקח  $x = a + nb$  ו $y = b$ . אז  $x \equiv a \pmod{n}$  ו $y \equiv b \pmod{n}$ . ניקח  $d = \gcd(a, b)$ . אז  $a = dx$  ו $b = dy$ . ניקח  $m = \frac{a}{d} = \frac{dx}{d} = x$ . אז  $a = dm$  ו $b = d(m+1)$ . ניקח  $r = m+1$ . אז  $a = dr$  ו $b = d(r+1)$ . ניקח  $s = r+1$ . אז  $a = ds$  ו $b = d(s+1)$ . ניקח  $t = s+1$ . אז  $a = dt$  ו $b = d(t+1)$ . ניקח  $u = t+1$ . אז  $a = du$  ו $b = d(u+1)$ . ניקח  $v = u+1$ . אז  $a = dv$  ו $b = d(v+1)$ . ניקח  $w = v+1$ . אז  $a = dw$  ו $b = d(w+1)$ . ניקח  $x' = w+1$ . אז  $a = dw$  ו $b = d(x'+1)$ . ניקח  $y' = x'$ . אז  $x' \equiv a \pmod{n}$  ו $y' \equiv b \pmod{n}$ .

(ב) אם  $n=385$  אז כמה הודעות במלוי מוסתרות יש למפתח פרטי  $K=11$ ? תן דוגמה של הודעה בלתי מוסתרת לא טריוויאלית (10 נקודות)

$$\frac{1}{[1+g\text{cd}(b-1, p)] \cdot [1+g\text{cd}(b-1, q-1)] \cdot [1+g\text{cd}(b-1, r-1)]} \quad (10)$$

$$385 = 5 \cdot 7 \cdot 11 \quad \text{if } \begin{cases} n \equiv 1 \pmod{5} \\ n \equiv 1 \pmod{7} \\ n \equiv 1 \pmod{11} \end{cases}$$

$$\text{gcd}(10, 4) = 2, \text{gcd}(10, 6) = 2, \text{gcd}(10, 10) = 10$$

$$\frac{5 \cdot 7 \cdot [1+2] \cdot [1+2] \cdot [1+10] = 3 \cdot 3 \cdot 11 = 99}{(0, 0, 2) \rightarrow 10 \rightarrow 35} \quad \text{check} \quad (10)$$

$$\begin{aligned} x^1 &\equiv x \pmod{11} \\ x^2 &\equiv 1 \pmod{10} \end{aligned} \quad \text{check: } x^2 \equiv 1 \pmod{10} \quad \text{since } x^2 - 1 \equiv 0 \pmod{10} \quad \text{and } x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{10} \quad \text{so } x-1 \equiv 0 \pmod{10} \quad \text{and } x+1 \equiv 0 \pmod{10} \quad \text{but } x \neq 10 \quad \text{so } x \equiv 1 \pmod{10}$$

$$2 \text{ or } 11 \Rightarrow 10 \text{ check: } (10, 0, 10) \rightarrow 5, 7 \rightarrow 35 \quad \text{check: } 35 \rightarrow 35$$

#### שאלה מס' 4

הוחלט לבצע החלפת מפתחות בשיטת Diffie-Hellman על בסיס  $p=13$  וווצר קטן יותר. יוזע שפתח משותף שווה 8 ואחד מפתחות פרטיים הוא 5 איזה מפתח פרטי שני? (10 נקודות)

$$2, 3, 4, 6 : \begin{aligned} & \text{check: } g=2 \pmod{13} \quad g^2 \equiv 4 \pmod{13}, g^3 \equiv 8 \pmod{13} \\ & g^4 \equiv 16 \equiv 3 \pmod{13}, g^6 \equiv 64 \equiv 1 \pmod{13} \end{aligned}$$

$\begin{array}{c} g^{k_1 k_2} \not\equiv p \\ \Rightarrow \text{check Diffie-Hellman} \end{array}$

$$\begin{aligned} & g^{5k} \equiv 2^5 \pmod{13} \quad (g \equiv 2 \pmod{13}) \quad \text{check: } 2^5 \equiv 32 \equiv 9 \pmod{13} \\ & g^{5k} \equiv 9 \pmod{13} \quad \text{check: } 9 \equiv 3 \pmod{13} \quad \text{so } 5k \equiv 3 \pmod{12} \end{aligned}$$

$$5 \cdot 5k \equiv 5 \cdot 3 \pmod{12}$$

$$k \equiv 15 \equiv 3 \pmod{12}$$

$k=3$  check:  $g^{3 \cdot 5} \equiv 2^3 \pmod{13} \quad 2^3 \equiv 8 \pmod{13}$

(10)

5.3

$$2 \equiv 8 \pmod{13} \quad \text{זיהוי: } 2 \equiv 8 \pmod{13}$$

$$2^3 \equiv 2 \cdot 2 \cdot 2 = -1 \cdot -1 \cdot 8 \equiv 8 \quad \checkmark$$

שאלה מס' 5

מערכת RSA בנייה על בסיס 437.

א. הودעה  $C=3$  התקבלה כחומרה הצעינה של הודעה  $M$  על ידי מפתח  $b=283$ . מצא את  $M$ .

(10 נקודות)

10

$$M^{283} \equiv 3 \pmod{437} \quad \text{לפניהם, } 437 = 19 \cdot 23 \quad \text{ולפניהם } M \equiv 3 \pmod{23}$$

$$283 \cdot a \equiv 1 \pmod{23} \quad \text{לפניהם, } a \equiv 19 \pmod{23} \quad \text{ולפניהם } M \equiv 3 \pmod{19}$$

$$\phi(437) = 18 \cdot 22 = 396 \quad M \equiv 3^a \pmod{437} \quad \text{ולפניהם}$$

$$\text{לפניהם } a \equiv 19 \pmod{396} \quad \text{ולפניהם } b \equiv 283 \pmod{396}$$

$$396 = 283 \cdot 1 + 113$$

$$\text{gcd}(396, 283) = 113$$

$$\text{gcd}(283, 113) = 113 \cdot 2 + 57$$

$$\text{gcd}(113, 57) = 57 \cdot 1 + 56$$

$$\text{gcd}(57, 56) = 56 \cdot 1 + 1$$

$$1 = 57 - 1 \cdot 56 = 57 - 1 \cdot (113 - 1 \cdot 57) = -1 \cdot 113 + 2 \cdot 57 =$$

$$= -1 \cdot 113 + 2(283 - 2 \cdot 113) = 2 \cdot 283 - 5 \cdot 113 = 2 \cdot 283 - 5(396 - 1 \cdot 283)$$

$$= -5 \cdot 396 + 7 \cdot 283$$

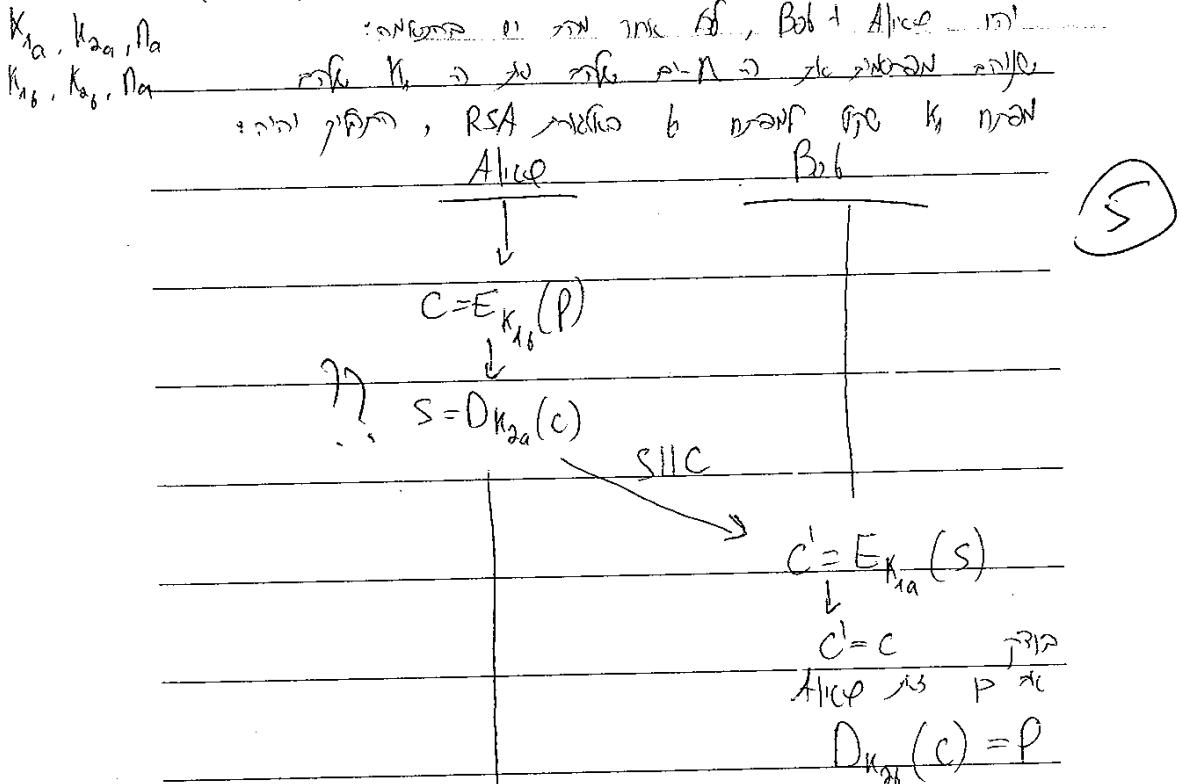
$$\text{ולפניהם, } a=7 \pmod{396}, \quad 283 \equiv 283 \pmod{396} \Rightarrow 283 \pmod{7}$$

$$M = 3^7 \equiv 2187 \equiv 2 \pmod{437}$$

$$\boxed{M = 2}$$

✓

ב. תאר את המערכת חתימה דיגיטלית המבוססת על מערכת הצפנה RSA. (5 נקודות)



ג. האבטחה של RSA מבוססת על שלוש עובדות של ארכיטקטורה רגילה וארכיטקטורה מודולרית. מה הן העובדות הללו? (10 נקודות)

$p, q$  ፳፻ ፳፻፻፻, ፲፻፻ ፳፻፻,  $n=p \cdot q$ , ፳፻፻፻፻፻ (1)

For plane  $y = \sqrt{n}$ ,  $\|f\|_2$  is  $\sqrt{n}$

רְבָעֵה בְּנֵי

פונקציית log  $\rightarrow$  מוגדרת כפונקציית כפוף (2)

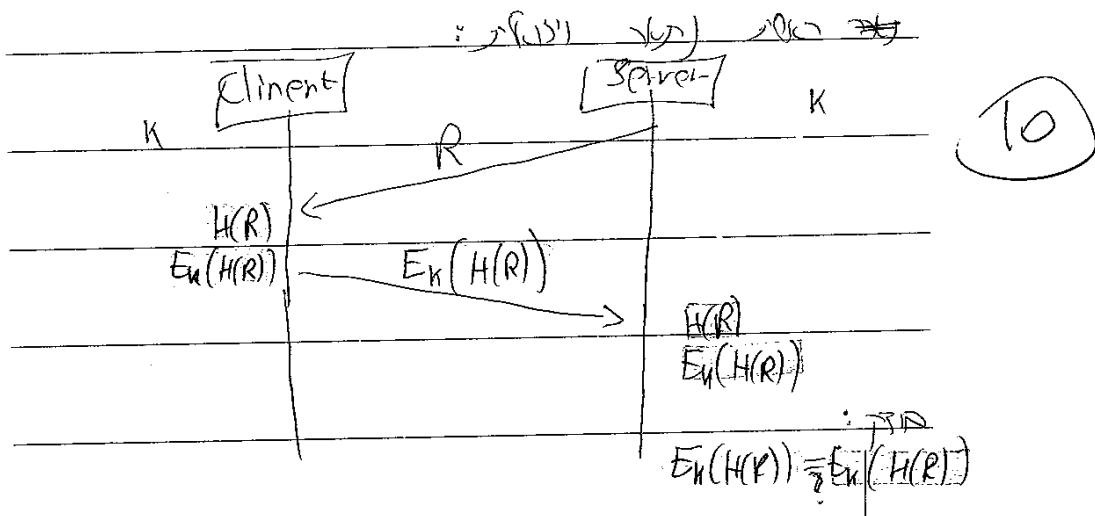
$$a \propto \log y \text{ if } C = y^a \quad \textcircled{1}$$

פונקציית חזקה  $\rightarrow$  מוגדרת כפונקציית כפוף (3)

$$\text{if } y \propto x^a \text{ if } y = x^b \quad \text{פונקציית חזקה}$$

### שאלה מס' 6

תאר והסביר פרוטוקול האימות המשמש ברשת (אימות SERVER מול CLIENT) מבוסס על הצפנה של פונקציית הערבול (HASH FUNCTION). (10 נקודות)



הצפנה של פונקציית הערבול היא:

הצפנה של פונקציית הערבול היא: פונקציית הערבול (H(R)) מושפעת רק מ-R. אם רוחב המפתח K הוא n ביטים, אז פונקציית הערבול תחזיר כיוון קיצור של n ביטים. אם רוחב המפתח K הוא n ביטים, אז פונקציית הערבול תחזיר כיוון קיצור של n ביטים.

פונקציית הערבול היא: פונקציית הערבול (H(R)) מושפעת רק מ-R. אם רוחב המפתח K הוא n ביטים, אז פונקציית הערבול תחזיר כיוון קיצור של n ביטים. אם רוחב המפתח K הוא n ביטים, אז פונקציית הערבול תחזיר כיוון קיצור של n ביטים.

### לפ' נוסחות

#### 1. Euler-Fermat Theorem

לכל  $a \in \mathbb{Z}$  ש- $\gcd(a,n) = 1$  מתקיים  $a^{\varphi(n)} \equiv 1 \pmod{n}$   
 אם  $n$  מספר ראשוני אז  $\varphi(n) = n - 1$

#### 2. משפט השארית הסינית

יהו  $d_1, d_2, \dots, d_t$  מספרים זרים בזוגות ו-  $n = d_1d_2 \dots d_t$ . אזי למערכת המשוואות  
 $x \equiv m \pmod{d_i} \quad i = 1, 2, \dots, t$

כאשר  $m$  נع בין 1 ל- $t$ , יש פתרון משותף  $x$  בתחום  $[0, n-1]$ .

$$\frac{n}{d_i} * y_i \equiv 1 \pmod{d_i} \quad \text{כאן } x = \left[ \sum_{i=1}^t \left( \frac{n}{d_i} \right) y_i x_i \right] \pmod{n}$$

#### 3. RSA:

הא  $(n, p, q, a, b)$  שבו  $(n, p, q)$  פומביים ו-  $(p, q, a, b)$  סודיים. כאן  $n$  הוא מכפלת  
 של שני מספרים ראשוניים שונים  $p$  ו-  $q$ , ו-  $b$  הפוכים זה לזה לפי מודול  $(n)$ .  
 נוסחת הצפנה  $E(x) = x^b \pmod{n}$

#### 4. האלפבית האנגלאי, קודים ושכיחויות /אלפיטה/ :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
82	15	28	43	127	22	20	61	70	2	8	40	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
67	75	19	1	60	63	91	28	10	23	1	20	1