# קריפטוגרפיה - מועד א'

## 202-1-5351
## סמסטר א' תשע"ג
## 27.1.2013

הנחיות:

1. בטופס הבחינה 3 דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 3 שאלות שמשקלן אינו שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להתעכב זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
8. מותר להסתמך על משפטים שהוכחו בהרצאות, אך יש לצטט אותם במדויק.
9. אם אתם מסתמכים על טענות שהוכחו בתרגילי בית יש להוכיח אותם.
10. **במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.**

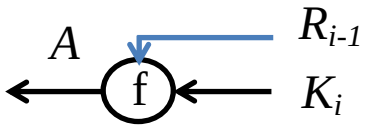
בהצלחה!

# שאלה 1 [42 נקודות]

שאלה זאת עוסקת במערכת ההצפנה DES.

### סעיף א [8 נקודות]

נתבונן בפונקציית f המופעלת בכל שלב במערכת DES כאשר הקלט שלה הוא מפתח $K_i$ באורך 48 ביטים ו- $R_{i-1}$. נסמן את הפלט של f ב- $A$.

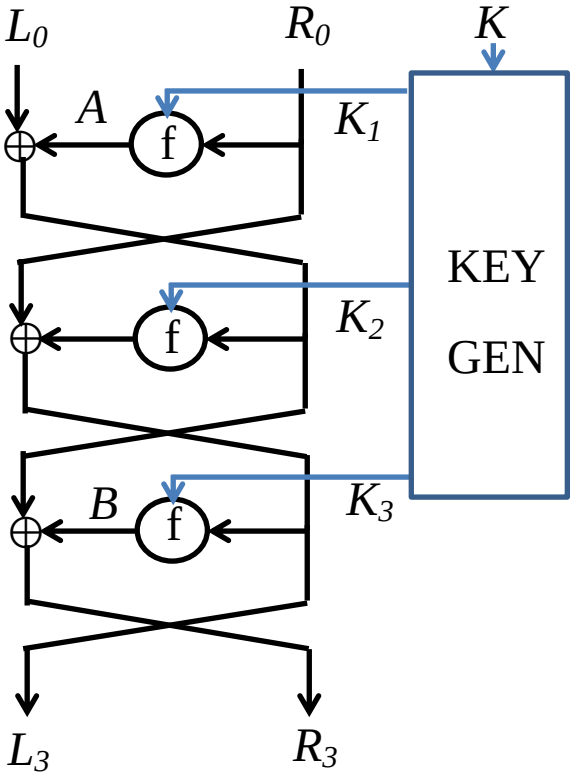



הראו כי לכל $\mathbf{R_{i-1}}$, ו- $\mathbf{A}$ קיים לפחות מפתח אחד $\boldsymbol{K_i}$ כך ש- $\boldsymbol{A = f(R_{i-1}, K_i)}$.

### סעיף ב [8 נקודות]

נסמן את החצי הימני של המפתח $K_i$ ב- $K_{i,R}$ (כאשר $K_{i,R}$ הוא באורך 24 ביטים). הראו אלגוריתם יעיל (בסיבוכיות $O(1)$) שמקבל כקלט $R_{i-1}$, $K_{i,R}$ ו- $A$ ובודק אם קיים מפתח $K_i$ כך ש- $K_{i,R}$ הוא החצי הימני שלו ומתקיים $A = f(R_{i-1}, K_i)$. שימו לב כי האלגוריתם שלכם אינו מקבל את החצי השמאלי של המפתח. הסבירו מדוע האלגוריתם שלכם נכון.

בסעיפים הבאים נתבונן במערכת ההצפנה DES עם 3 סיבובים (ללא הפרמוטציה ההתחלתית) עם אלגוריתם יצירת המפתחות כמו ב- DES הרגיל. באלגוריתם יצירת המפתחות הקלט הוא מפתח $K$ באורך 56 ביטים. ממפתח זו מייצרים שלושה מפתחות $K_1, K_2$ ו- $K_3$. המערכת מתוארת באיור הבא:



**סעיף ג [8 נקודות]**

נסמן ב- $A$ את הפלט של ההפעלה הראשונה של f במערכת וב- $B$ את הפלט של ההפעלה השלישית של f במערכת. הראו כי

$$A \oplus B = L_0 \oplus R_3 .$$

**סעיף ד [18 נקודות]**

באלגוריתם יצירת המפתחות ב- DES מחלקים את המפתח $K$ באורך 56 ביטים לשני מפתחות $\mathrm{K_L}, \mathrm{K_R}$, כל אחד באורך 28 ביטים, כאשר $K_L, K_R$ הם החצי הימני והשמאלי של $K$ בהתאמה. המפתח $K_i$ של סיבוב $i$ הוא באורך 48 ביטים, נסמן את החצי הימני והשמאלי שלו ב- $K_{i,R}$ ו- $K_{i,L}$ בהתאמה. המפתח $K_{i,R}$ מיוצר מ- $\mathrm{K_R}$ והמפתח $K_{i,L}$ מיוצר מ- $K_L$.

תארו אלגוריתם בסיבוכיות $2^{28}$ שמקבל כקלט הודעות $\mathrm{M_1}$ ו- $\mathrm{M_2}$ וההצפנות שלהם במערכת הנ"ל $\mathrm{C_1}$ ו- $\mathrm{C_2}$, ומוצא את $\mathrm{K_R}$. הניחו כי קיים בדיוק מפתח אחד $\mathrm{K_R}$ המצפין את זוג ההודעות לקריפטוגרמות המתאימות.

# שאלה 2 [38 נקודות]

בסעיפים הבאים $p, q$ הא ראשוניים שונים כך ש- $p, q \equiv 3 \pmod 4$ ו- $N = p \cdot q$.

**סעיף א [6 נקודות]**

הוכיחו כי $(N - p - q + 5)/8$ הוא מספר שלם.

**סעיף ב [10 נקודות]**

הוכיחו כי $a^{(N-p-q+1)/2} \equiv 1 \pmod N$ לכל $a \in \mathbb{Z}_N^*$.

**סעיף ג [6 נקודות]**

הוכיחו כי $a^{(N-p-q+1)/4} \equiv 1 \pmod N$ לכל $a \in \mathrm{QR}_N$.

**סעיף ד [8 נקודות]**

הוכיחו כי אם $a \in \mathrm{QR}_N$ ו- $b = a^{(N-p-q+5)/8} \bmod N$ אזי $a \equiv b^2 \pmod N$.

**סעיף ה [8 נקודות]**

נתאר מערכת להצפנה עם מפתח ציבורי.

**יצירת מפתחות:**

הגרל $p, q$ הא ראשוניים גדולים כך ש- $p, q \equiv 3 \pmod 4$ וחשב $N = p \cdot q$.

מפתח פרטי: $p, q$. מפתח ציבורי: $N$.

**הצפנה של הודעה $m \in \mathbb{Z}_N^*$ כך ש- $1 \le m < N/2$:**

$$\mathrm{E}(m, N) = m^2 \bmod N .$$

הסבירו איך מפענח שמחזיק את המפתח הפרטי ומקבל קריפטוגרמה $C$ יכול לחשב 2 הודעות שאחת מהן היא ההודעה שהוצפנה.

# שאלה 3 [20 נקודות]

השאלה הבאה עוסקת בסכמות לחלוקת סוד ל- $n$ משתתפים שנסמנם $p_1, \dots, p_n$. נתבונן בסכמה הבאה לחלוקת סוד $s \in \{0,1\}$:

1. המחלק מגריל ביט $a_0 \in \{0,1\}$ בהתפלגות אחידה ומחשב $a_1 = a_0 \oplus s$.
2. עבור $1 \leq i \leq n/2$ החלק של משתתף $p_i$ הוא $a_0$ ועבור $n/2 < i \leq n$ החלק של משתתף $p_i$ הוא $a_1$.

## סעיף א [5 נקודות]

הסבירו מדוע כל משתתף לא לומד כל מידע על הסוד.

## סעיף ב [5 נקודות]

הסבירו מדוע זוג משתתפים $p_i, p_j$ עבור $i < j$ יכול לשחזר את הסוד **אם ורק אם** $i \leq n/2$ ו- $n/2 < j$.

## סעיף ג [10 נקודות]

יהי $\ell = \lceil \log n \rceil$. עבור $i \in \{1, \dots, n\}$ נסתכל על $i = i_1 \dots i_\ell$ הייצוג הבינארי של $i$. לדוגמא, עבור $n = 7$ נקבל כי $3 = 011$.

נתבונן בסכמה הבאה לחלוקת סוד $s \in \{0,1\}$:

1. המחלק מגריל $\ell$ ביטים $a_{1,0}, \dots, a_{\ell,0}$, כל ביט בהתפלגות אחידה ובאופן בלתי תלוי בביטים האחרים.
   המחלק מחשב $a_{k,1} = a_{k,0} \oplus s$ עבור $1 \leq k \leq \ell$.
2. החלק של משתתף $p_i$ עבור $i = i_1 \dots i_\ell$ הוא $a_{1,i_1}, a_{2,i_2}, \dots, a_{\ell,i_\ell}$.

לדוגמא, החלק של משתתף 3 הוא $a_{1,0}, a_{2,1}, a_{3,1}$.

הסבירו מדוע כל משתתף לא לומד כל מידע על הסוד וכיצד כל זוג משתתפים יכול לשחזר את הסוד.