אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

קריפטוגרפיה - מועד ב'

202-1-5351
סמסטר א' תש"ע
24.2.2010

הנחיות:

1. בטופס הבחינה 2 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.
01. **במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.**

בהצלחה!

שאלה 1 [30 נקודות]

שאלה זאת עוסקת במערכת ההצפנה DES.

סעיף א [6 נקודות]

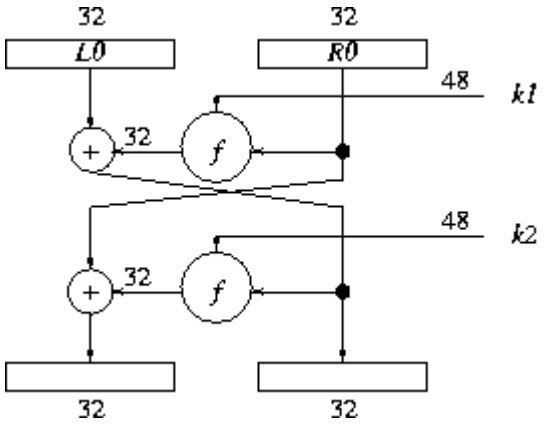
נסתכל על S-box כלשהי S_i עבור $1 \le i \le 8$. הסבירו בקצרה מדוע לכל פלט אפשרי $y \in \{0,1\}^4$ של S_i קיימים בדיוק 4 קלטים $x \in \{0,1\}^6$ ל- S_i עבורם מתקיים $S_i(x) = y$.

סעיף ב [11 נקודות]

נסתכל על פונקצית f של DES. נקבע הודעה שרירותית $M \in \{0,1\}^{64}$ ונסמן $M = L_0 R_0$, באשר $L_0, R_0 \in \{0,1\}^{32}$. הוכיחו כי לכל פלט אפשרי $y \in \{0,1\}^{32}$ של $f(R_0, k_1)$ קיימות בדיוק 2^{16} אפשרויות לבחירת $k_1 \in \{0,1\}^{48}$ עבורן מתקיים $f(R_0, k_1) = y$.

סעיף ג [13 נקודות]

נסתכל על גרסת DES בת שני סיבובים, עם שני מפתחות בלתי תלויים $k_1, k_2 \in \{0,1\}^{48}$, כמתואר באיור הבא:



במערכת זאת, אם ניקח שני זוגות הודעות וקריפטוגרמות $\langle M_1, C_1 \rangle, \langle M_2, C_2 \rangle$ אזי בהסתברות גבוהה יהיה לכל היותר מפתח $k = \langle k_1, k_2 \rangle$ יחיד שיעתיק כל M_i ל- C_i. הראו התקפה שזמן הריצה שלה הוא סדר גודל של $16 \cdot 2^6$ שבהינתן הזוגות $\langle M_1, C_1 \rangle, \langle M_2, C_2 \rangle$ מוצאת את המפתח $k = \langle k_1, k_2 \rangle$ שהצפין אותם.

שאלה 2 [30 נקודות]

בשאלה זו נתייחס לסכמה לחלוקת סוד הבאה עם שלושה משתתפים:

קלט: סוד $s \in \mathbb{Z}_p$ עבור $p > 2$ ראשוני שידוע לכל המשתתפים.

1. המחלק מגריל $r_1, r_2 \in \mathbb{Z}_p$ בהתפלגות אחידה ובאופן בלתי תלוי.
2. החלק של משתתף 1 הוא $(s + r_1 + 2r_2) \bmod p$.
3. החלק של משתתף 2 הוא $(2r_1 + r_2) \bmod p$.
4. החלק של משתתף 3 הוא $r_2 \bmod p$.

סעיף א [7 נקודות]

הוכיחו כי שלושת המשתתפים ביחד יכולים לשחזר את הסוד.

סעיף ב [8 נקודות]

הוכיחו כי אם $p = 3$ אזי משתתף 1 ומשתתף 2 יכולים לשחזר את הסוד.

סעיף ג [15 נקודות]

הוכיחו כי אם $p = 5$ אזי משתתף 1 ומשתתף 2 לא לומדים כל מידע על הסוד מהחלקים שלהם.

שאלה 3 [40 נקודות]

סעיף א [13 נקודות]

יהי p ראשוני כך ש- $p \equiv 3 (\mathrm{mod}\, 4)$. הוכיחו כי $-1 \notin \mathrm{QR}_p$.

סעיף ב [14 נקודות]

יהי p, q ראשונים כך ש- $p \equiv 3 (\mathrm{mod}\, 4)$, $q \equiv 3 (\mathrm{mod}\, 4)$ ו- $N = pq$. נתונה שארית ריבועית $a \in \mathrm{QR}_N$. הוכיחו כי <u>בדיוק</u> אחד מארבעת השורשים של a הוא שארית ריבועית מודולו N.

סעיף ג [13 נקודות]

נתאר גרסה של מערכת הצפנה של Rabin. אלגוריתם יצירת המפתחות:

1. הגרילו p, q ראשונים גדולים כך ש- $p \equiv 3 (\mathrm{mod}\, 4)$, $q \equiv 3 (\mathrm{mod}\, 4)$ וחשבו $N = pq$.

המפתח הציבורי: N.

המפתח הפרטי: p, q.

תחום ההודעות: QR_N.

ההצפנה של הודעה $m \in \mathrm{QR}_N$ היא $c \leftarrow m^2 \bmod N$.

הסבירו כיצד מפענח המחזיק במפתח הפרטי יכול לפענח את c בצורה יעילה.