קריפטוגרפיה - מועד ב'

202-1-5351
סמסטר א' תשע"ג
18.2.2013

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.
10. **במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.**

בהצלחה!

שאלה 1 [29 נקודות]

נשתמש ב DES כדי לבנות פונקציית hash עם גודל תחום קבוע. נגדיר $h:\{0,1\}^{112} \to \{0,1\}^{64}$ ע"י:

$$h(x_1, x_2) = DES(DES(0^{64}, x_1), x_2)$$

כאשר $|x_1| = |x_2| = 56$.

סעיף א [15 נקודות]

הראו אלגוריתם שרץ בזמן (בערך) 2^{56} שמקבל ערך y ומוצא x_1, x_2 כך ש $h(x_1, x_2) = y$, או מכריז כי אין x_1, x_2 כנ"ל. בשלב ראשון האלגוריתם מחשב לכל x_2 את $z = DES^{-1}(y, x_2)$, וממיין את רשימת הזוגות (z, x_2) על פי z.

סעיף ב [14 נקודות]

הראו אלגוריתם אקראי שרץ בזמן (בערך) 2^{32} ומוצא התנגשות בהסתברות גבוהה.

שאלה 2 [40 נקודות]

סעיף א [10 נקודות]

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

סעיף ב [10 נקודות]

נתון ראשוני p כך ש $p \equiv 3 \pmod 4$. הוכיחו כי לכל $a \in \mathbb{Z}_p$, בדיוק אחד מבין a ו- $-a$ הוא שארית ריבועית מודולו p.

סעיף ג [10 נקודות]

נתונים שני ראשוניים p, q כך ש $p, q \equiv 3 \pmod 4$, ויהי $N = p \cdot q$. הוכיחו כי לכל $a \in \mathrm{QR}_N$ קיים יחיד $b \in \mathrm{QR}_N$ כך ש $b^2 \equiv a \pmod N$.

סעיף ד [10 נקודות]

נתונה מערכת ההצפנה הבאה:

- **יצירת מפתחות:**
  הגרל p, q 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** $m \in \mathbb{Z}_N$
  $$E(m, N) = m^2 \bmod N .$$

נניח כי אליס הצפינה הודעה $m \in \mathrm{QR}_N$. הסבירו איך מפענח שמחזיק את המפתח הפרטי ומקבל קריפטוגרמה C יכול לחשב את ההודעה שהוצפנה. שימו לב כי המפענח יודע כי $m \in \mathrm{QR}_N$.

שאלה 3 [31 נקודות]

1. מערכת הצפנה עם מפתח פרטי (E, D, Gen) נקראת <u>נכונה</u> אם כל הודעה m המוצפנת במפתח מפוענחת במפתח ל- m.
2. מערכת הצפנה עם מפתח פרטי (E, D, Gen) נקראת <u>בטוחה</u> אם היא בטוחה על פי ההגדרה שניתנה בכיתה.

סעיף א [7 נקודות]

נתונות 2 מערכות הצפנה עם מפתח פרטי

$$(E_1, D_1, Gen_1)$$
$$(E_2, D_2, Gen_2)$$

ידוע כי שתיהן נכונות, אך בדיוק אחת מהן בטוחה. לא ידוע מי מהן היא המערכת הבטוחה. בנוסף, נתונה סכמה לחלוקת סוד 2 מתוך 2. מוצעת מערכת ההצפנה הבאה:

- **יצירת מפתחות:**
  הרץ Gen_1 לקבלת k_1, הרץ Gen_2 לקבלת k_2.
  המפתח הסודי: (k_1, k_2).
- **הצפנה של הודעה m:**
  חלק את m על פי סכמה לחלוקת סוד 2 מתוך 2. נסמן את החלקים ב- s_1, s_2.
  חשב $C_1 \leftarrow Enc_1(s_1, k_1)$ ו- $C_2 \leftarrow Enc_2(s_2, k_2)$
  פלוט את ההצפנה $C = (C_1, C_2)$.

הראו כיצד לפענח הודעה במערכת והסבירו מדוע המערכת הנ"ל היא נכונה, ומדוע היא בטוחה.

סעיף ב [12 נקודות]

נתונות 3 מערכות הצפנה. ידוע שלפחות 2 מהן נכונות ושלפחות 2 מהן בטוחות. לא ידוע איזה מהן בטוחות ואיזה מהן נכונות. הראו מערכת הצפנה העונה על הדרישות הבאות:

1. המערכת משתמשת רק במערכות הצפנה הנתונות ובסכמת חלוקת סוד לפי בחירתכם.
2. המערכת בטוחה.
3. מפענח אשר יודע אילו מבין שלושת המערכות הן הנכונות, יכול לפענח הצפנות (המצפין <u>לא</u> יודע מיהן הנכונות ומיהן הבטוחות).

הסבירו מדוע המערכת שבניתם עונה לדרישות 2 ו- 3.

סעיף ג [12 נקודות]

נתונות 5 מערכות הצפנה. ידוע שלפחות 4 מהן נכונות ושלפחות 4 מהן בטוחות. לא ידוע איזה מהן בטוחות ואיזה מהן נכונות. הראו מערכת הצפנה נכונה ובטוחה המשתמשת רק במערכות הצפנה הנתונות ובסכמת חלוקת סוד לפי בחירתכם.

<u>שימו לב</u>: כאן גם המצפין וגם המפענח לא יודעים מיהן המערכות הבטוחות ומיהן המערכות הנכונות.

הסבירו מדוע המערכת שבניתם עונה לדרישות.