קריפטוגרפיה – מועד א'

כולל תיקונים בזמן הבחינה

202-2-5871

סמסטר א' תשע"ד

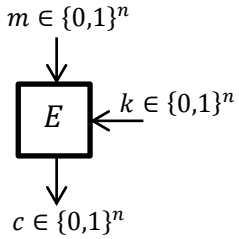
19.1.2014

הנחיות:

1. בטופס הבחינה 3 עמודים מלבד עמוד 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 [39 נקודות]

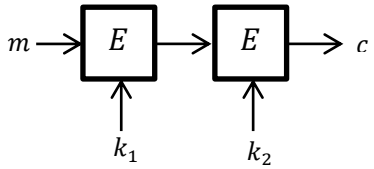


יהיו E אלגוריתם הצפנה ו- D אלגוריתם פענוח של מערכת הצפנה במפתח פרטי, כאשר:

- ההודעות, המפתחות, וההצפנות הם מחרוזות של n ביטים.
- לכל m, k מתקיים ש- $D(E(m,k),k) = m$.
- לכל מסר m ולכל צופן c קיים מפתח יחיד k כך ש- $E(m,k) = c$.

סעיף א [12 נקודות]

נגדיר אלגוריתם הצפנה E_2 באופן הבא. בהינתן מפתח $k = (k_1, k_2) \in \{0,1\}^{2n}$ והודעה $m \in \{0,1\}^n$, נגדיר $E_2(m,k) = E(E(m,k_1),k_2)$.
בציור:



הוכיחו כי לכל הודעה $m \in \{0,1\}^n$ ולכל הצפנה $c \in \{0,1\}^n$ יש בדיוק 2^n מפתחות $k \in \{0,1\}^{2n}$ כך ש- $E_2(m,k) = c$.

סעיף ב [12 נקודות]

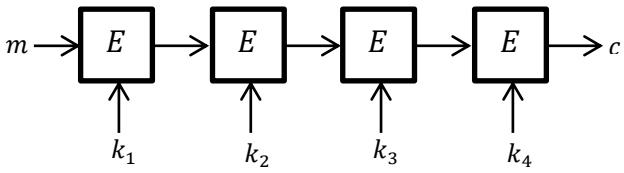
נתונים הודעה $m \in \{0,1\}^n$ והצפנה $c \in \{0,1\}^n$. הראו אלגוריתם בזמן בערך 2^n וזיכרון בערך 2^n המוצא את כל המפתחות $k \in \{0,1\}^{2n}$ כך ש- $E_2(m,k) = c$.

סעיף ג [15 נקודות]

נגדיר אלגוריתם הצפנה E_4 באופן הבא. בהינתן מפתח $k = (k_1, k_2, k_3, k_4) \in \{0,1\}^{4n}$ והודעה $m \in \{0,1\}^n$ נגדיר:

$$E_4(m,k) = E(E(E(E(m,k_1),k_2),k_3),k_4).$$

בציור:



נתונים 2 זוגות הודעות והצפנות $(m_1, c_1), (m_2, c_2)$, ונתונה הפרוצדורה הבאה (בה השורה האחרונה חסרה):

לכל $x \in \{0,1\}^n$ בצע:

- רשום את כל המפתחות k_1, k_2 כך ש- $x = E(E(m_1,k_1),k_2)$, וליד כל זוג כנ"ל רשום את $E(E(m_2,k_1),k_2)$.
- רשום את כל המפתחות k_3, k_4 כך ש- $c_1 = E(E(x,k_3),k_4)$, וליד כל זוג כנ"ל רשום את $D(D(c_2,k_4),k_3)$.
- השלימו .....

השתמשו בפרוצדורה הנ"ל, והראו אלגוריתם בזמן בערך 2^{2n} וזיכרון בערך 2^n המוצא את כל המפתחות k_1, k_2, k_3, k_4 שמצפינים את m_1 ל- c_1 ואת m_2 ל- c_2. הסבירו את נכונות האלגוריתם ונתחו זמן ריצה וזכרון.

שאלה 2 [39 נקודות]

נתון פרוטוקול ה- OT הבא. **קלטים:** בוב מחזיק $x_0, x_1 \in \{0,1\}$. אליס מחזיקה $s \in \{0,1\}$.

<u>תחילה אליס מבצעת:</u>

- מגרילה q ראשוני כך ש- $p = 2q + 1$ ראשוני.
- מוצאת $h \in \mathbb{Z}_p$ שהסדר שלו הוא q.
- מגרילה $b \in \mathbb{Z}_q$ באקראי.
- אם $s = 0$ אזי:
  מחשבת $B_0 = h^b \bmod p$
  מגרילה $B_1 \in QR_p$ באקראי
- אם $s = 1$ אזי:
  מגרילה $B_0 \in QR_p$ באקראי
  מחשבת $B_1 = h^b \bmod p$

שולחת לבוב את p, h, B_0, B_1.

<u>לאחר מכן בוב מבצע:</u>

- מגריל $a_0, a_1 \in \mathbb{Z}_q$ באקראי.
- מחשב עבור $i \in \{0,1\}$:
  $A_i = h^{a_i} \bmod p$
  $C_i = B_i^{a_i} \cdot h^{x_i} \bmod p$
- שולח לאליס את A_0, C_0, A_1, C_1.

סעיף א [9 נקודות]

איך אליס משחזרת את הביט x_s?

סעיף ב [10 נקודות]

הוכיחו כי בוב לא לומד שום מידע על s.

סעיף ג [10 נקודות]

הסבירו מדוע אליס לא לומדת שום מידע על x_{1-s}. מותר להסתמך על בטיחות מערכת ההצפנה של $ElGamal$.

סעיף ד [10 נקודות]

הוכיחו כי אם אליס רמאית אז היא יכולה ללמוד בצורה יעילה את שני הביטים.

שאלה 3 [22 נקודות]

יהי p ראשוני. בשאלה זו הניחו כי p ידוע לכולם (למצפין, למפענח, ולתוקף).

סעיף א [8 נקודות]

נגדיר את אלגוריתם ההצפנה הבא (הצפנה במפתח פרטי).

קלטים: מפתח סודי r כך ש- $\gcd(r, p-1) = 1$, והודעה $m \in \mathbb{Z}_p$.

פלט: $c = m^r \bmod p$.

הראו כיצד בהינתן r ו- c ניתן לפענח את m.

סעיף ב [6 נקודות]

נתון מספר r כך ש- $\gcd(r, p-1) = 1$.

הוכיחו כי הפונקציה $f(x) = x^r \bmod p$ היא פרמוטציה על איברי $\mathbb{Z}_p$.

סעיף ג [8 נקודות]

נתונה קריפטוגרמה c.

הראו כי אם לתוקף מותר לבקש פענוחים של כל קריפטוגרמה $c_i \neq c$, אזי הוא יכול לפענח את c ביעילות (התוקף מכיר את p).