2.12.2015

קריפטוגרפיה: תרגיל 3

<u>הגשה</u>: יום ד' 16.12.15 בשעה 14:10 בהרצאה. ההגשה בזוגות או ביחידים.

שאלה 1

יהיו m_1 ו- m_2 טבעיים כך ש- $\gcd(m_1, m_2) = p$, כאשר p ראשוני ו- p איננו מחלק את $\frac{m_1}{p}$ ואיננו מחלק את $\frac{m_2}{p}$.
נסתכל על מערכת המשוואות הבאה:

$$x \equiv a \pmod{m_1}$$
$$x \equiv b \pmod{m_2}$$

סעיף א
הוכיחו כי אם $a \not\equiv b \pmod{p}$ אזי למערכת הנ"ל אין פתרון.

סעיף ב
הוכיחו כי אם $a \equiv b \pmod{p}$ אזי למערכת הנ"ל קיים לפחות פתרון אחד.

סעיף ג
הוכיחו כי אם $a \equiv b \pmod{p}$ אזי למערכת הנ"ל יש בדיוק p פתרונות בתחום $\mathbb{Z}_{m_1 \cdot m_2}$.

<u>רמז לסעיף ב:</u>
התבוננו במערכת המשוואות הבאה:

$$x \equiv a \pmod{p}$$
$$x \equiv a \pmod{\frac{m_1}{p}}$$
$$x \equiv b \pmod{\frac{m_2}{p}}$$

הערה: בפתרון עליכם גם להסביר מדוע זאת מערכת משוואות לגיטימית.

שאלה 2

יהיו N, e, d כמו ב- RSA. כלומר, $N = pq$ כאשר $p \neq q$ הם שני ראשוניים גדולים, ו- e, d הם כך ש- $\gcd(e, \phi(N)) = 1$ ו- $ed \equiv 1 \pmod{\phi(N)}$.
הוכיחו בעזרת משפט השאריות הסיני כי לכל $a \in \mathbb{Z}_N$ מתקיים:
אם $b = a^e \bmod N$ ו- $c = b^d \bmod N$, אזי $a = c$.

הערה: שימו לב כי ייתכן ש- $a \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$.

שאלה 3

הזכרו בהתקפה שראינו בכיתה על שימוש ב Textbook RSA להצפנת מסרים קצרים: בהצפנת מסר m כך ש- $m < N^{1/e}$ (כאשר (N, e) הוא המפתח הפומבי), נקבל:
$c = m^e \pmod{N} = m^e$ ← מעל השלמים
(ומעל השלמים אפשר לחשב שורש e-י ביעילות).

אליס רוצה לשלוח לבוב הודעה קצרה $m < N^{1/e}$, ובמטרה להימנע מההתקפה הנ"ל, היא שולחת לו הצפנה של $m' = 2^{100} \cdot m$.

הראו כיצד יריב אשר יודע כי אליס שולחת הצפנה של m עבור $m' = 2^{100} \cdot m$ יכול לתקן את המתקפה הנ"ל ולפענח ביעילות את m.

שאלה 4

היזכרו בהגדרת הבטיחות שניתנה בכיתה עבור מערכת הצפנה במפתח פומבי $\pi = (\text{Gen}, \text{Enc}, \text{Dec})$.

משחק הבחנה א (עם פרמטר n):

1. $(PK, SK) \leftarrow \text{Gen}(1^n)$.
2. בהינתן קלט PK, היריב $\mathcal{A}$ פולט זוג מסרים m_0, m_1 ממרחב המסרים של מערכת ההצפנה.
3. מגרילים בהתפלגות אחידה $b \in \{0,1\}$, ומחשבים קריפטוגרמה $c \leftarrow \text{Enc}(m_b, PK)$.
4. היריב $\mathcal{A}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{A}$ מנצח אם $\hat{b} = b$.

הגדרה א:

מערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{A}$ קיימת פונקציה זניחה $\text{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{A} \\ \text{במשחק א}\end{matrix}\right] \leq \frac{1}{2} + \text{negl}(n)$$

סעיף א

סטודנט בקורס טען שאפשר לפשט את משחק ההבחנה באופן הבא:
במקום לאפשר ליריב לבחור זוג מסרים m_0, m_1, נאפשר לו לבחור רק מסר אחד m. על מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של m לבין הצפנה של 1 (הניחו כי 1 נמצא במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ב (עם פרמטר n):

1. $(PK, SK) \leftarrow \text{Gen}(1^n)$.
2. בהינתן קלט PK, היריב $\mathcal{B}$ פולט מסר m ממרחב המסרים של מערכת ההצפנה.
3. מגרילים בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow \text{Enc}(m, PK)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow \text{Enc}(1, PK)$.
4. היריב $\mathcal{B}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ב:

מערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{B}$ קיימת פונקציה זניחה $\text{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{B} \\ \text{במשחק ב}\end{matrix}\right] \leq \frac{1}{2} + \text{negl}(n)$$

הוכיחו כי אם π אינה בטוחה לפי הגדרה ב אזי π אינה בטוחה לפי הגדרה א.
הדרכה: הניחו כי קיים יריב $\mathcal{B}$ המנצח במשחק ב בהסת' $\frac{1}{2} + \epsilon(n)$ והראו בעזרתו יריב $\mathcal{A}$ למשחק א.

סעיף ב

סטודנט אחר בקורס טען שאפשר לפשט עוד יותר את משחק ההבחנה:
לא נאפשר ליריב לבחור מסרים כלל, ועל מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של 1 לבין הצפנה של 2 (הניחו כי 1 ו- 2 נמצאים במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ג (עם פרמטר n):

1. $(PK, SK) \leftarrow \mathrm{Gen}(1^n)$.
2. מגרילים בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(1, PK)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(2, PK)$.
3. היריב $\mathcal{B}$ מקבל את PK ואת הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ג:

מערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{B}$ קיימת פונקציה זניחה $\mathrm{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{B} \\ \text{במשחק ג}\end{matrix}\right] \leq \frac{1}{2} + \mathrm{negl}(n).$$

הראו כי קיימת מערכת הצפנה במפתח פומבי אשר בטוחה לפי הגדרה ג <u>ולא</u> בטוחה לפי הגדרה א. ניתן להסתמך על הנחות הקושי שנלמדו בכיתה.

<u>רמז</u>: ניתן להתחיל ממערכת הצפנה כלשהי הבטוחה לפי הגדרה א ולשנות אותה בהתאם.