7.12.2014

קריפטוגרפיה: תרגיל 3

<u>הגשה</u>: יום א' 21.12.14 לתא 78 בקומה 1 בניין 37 (שימו לב שרשום על התא "אורי שטמר"). 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:

$$x \equiv a \pmod{p}$$
$$x \equiv a \left(\mathrm{mod}\frac{m_1}{p}\right)$$
$$x \equiv b \left(\mathrm{mod}\frac{m_2}{p}\right)$$

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:

$$c = m^e \pmod{N} = m^e \quad \longleftarrow \text{מעל השלמים}$$

(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

הזכרו בהתקפה שראינו בכיתה על שימוש ב Textbook RSA במקרה שבו לכמה נמענים שונים יש את אותה החזקה הציבורית $e = 3$ (אבל מודולוסים N_i שונים).
בשני הסעיפים הבאים נראה מתקפות על המקרה בו לכמה נמענים שונים יש אותו המודולוס N, אבל חזקות e_i שונות.

נניח שכל העובדים בחברה מסויימת משתמשים במערכת *Textbook RSA* על מנת להצפין הודעות.
בנוסף, נניח כי כל עובדי החברה משתמשים באותו מודולוס ציבורי N, אבל לכל עובד יש חזקה ציבורית ופרטית משלו e_i, d_i.
כלומר, לכל עובד i יש מפתח פרטי (N, d_i) ומפתח ציבורי (N, e_i) כך ש- $e_i \cdot d_i \equiv 1 \pmod{\phi(N)}$.

סעיף א
הראו איך עובד i יכול לפענח הודעות שהוצפנו עבור עובד j.

סעיף ב
בסעיף הקודם ראינו כי עובדי החברה יכולים לפענח הודעות של עובדים אחרים. בסעיף זה נראה מתקפה הניתנת לביצוע גם ע"י גורם חיצוני (ללא ידיעת אף אחד מהמפתחות הסודיים d_i).
נניח כי עבור זוג עובדים i, j מתקיים $\gcd(e_i, e_j) = 1$, ונניח כי אותה הודעה m מוצפנת ונשלחת גם לעובד i וגם לעובד j.
הראו יריב יעיל אשר מסוגל לשחזר את m בהינתן $c_i = m^{e_i} \bmod N$ ו- $c_j = m^{e_j} \bmod N$.
(היריב יודע את N, e_i, e_j).

שאלה 5

סטודנט בקורס קריפטוגרפיה הציע את הנחת הקושי הבאה (המוגדרת באמצעות משחק נגד יריב):

משחק עם פרמטר n:
- הגרל ראשוני p בן n ביטים בהתפלגות אחידה.
- הגרל בהתפלגות אחידה $e \in \mathbb{Z}_{p-1}$ ו- $m \in \mathbb{Z}_p^*$.
- חשב $y = [m^e \bmod p]$.
- היריב $\mathcal{A}$ מופעל על הקלטים p, e, y ופולט $\hat{m} \in \mathbb{Z}_p^*$. היריב מנצח אם $[\hat{m}^e \bmod p] = y$.

הסטודנט טען כי סיכויי הניצחון של כל יריב פולינומי הם זניחים כפונקצייה של n.
הוכיחו כי הסטודנט טעה.