05/12/2013

קריפטוגרפיה: תרגיל 3

<u>הגשה</u>: יום ד' 18/12/13 ב- 14:10 בהרצאה. ההגשה בזוגות או יחידים.

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 $\frac{m_1}{p}$ ו את $\frac{m_2}{p}$. נסתכל על מערכת המשוואות:

$$x \equiv a \ (mod\ m_1)$$
$$x \equiv b \ (mod\ m_2)$$

סעיף א

הוכיחו כי אם $a \not\equiv b \ (mod\ p)$ אזי אין למערכת פתרון.

סעיף ב

הוכיחו כי אם $a \equiv b \ (mod\ p)$ אזי למערכת קיים **לפחות** פתרון אחד.
רמז: התבוננו במערכת המשוואות הבאה:

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

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

סעיף ג

הוכיחו כי אם $a \equiv b \ (mod\ p)$ אזי מספר הפתרונות ב- $\mathbb{Z}_{m_1 \cdot m_2}$ של מערכת המשוואות הוא p.

שאלה 2

יהיו N,e,d כמו ב- RSA. כלומר, $N = p\,q$ עבור שני ראשוניים אי-זוגיים p ו- q שונים זה מזה, e ו-d כך ש- $\gcd(e,\varphi(N))=1$ ו- $e\ d \equiv 1 \pmod{\varphi(N)}$. הוכיחו בעזרת משפט השאריות הסיני כי לכל $a \in \mathbf{Z}_N - \mathbf{Z}_N^*$ מתקיים כי אם $b=a^e \bmod N$ ו- $c=b^d \bmod N$, אזי $a=c$.

שאלה 3

סעיף א

יהי g יוצר של Z_p^* ו- r מספר טבעי. נסמן $\alpha = \gcd(r,p-1)$. הוכיחו כי $x^r \equiv 1 \pmod p$ אם ורק אם קיים j, כאשר $1 \le j \le \alpha$, כך ש- $x \equiv g^{j(p-1)/\alpha} \pmod p$. כמה מספרים ב- Z_p^* מקיימים $x^r \equiv 1 \pmod p$?

סעיף ב

יהיו p ו- q ראשוניים שונים זה מזה ו- $N=pq$. נקודת שבת של מפתח ה- RSA הציבורי (N,e) היא הודעה $M \in Z_N^*$ כך ש- $RSA_{(N,e)}(M)=M$. הוכיחו כי מספר נקודות השבת של (N,e) ב- Z_N^* הוא $\gcd(e-1,q-1) \cdot \gcd(e-1,p-1)$.
<u>הדרכה</u>: השתמשו במשפט השאריות הסיני.

שאלה 4

יהיו p ראשוני אי-זוגי ו- g יוצר של $\mathbb{Z}_p$.

סעיף א

יהיו (p,g,a) ו- (p,g,A) מפתח פרטי וציבורי בהתאמה עבור מערכת ההצפנה של ElGamal, כאשר $A \equiv g^a \ (mod\ p)$, ותהיינה $M_1, M_2 \in \mathbb{Z}_p^*$ שתי הודעות. עבור $j = 1,2$ נסמן ב $\left(B_j, C_j\right)$ הצפנה של M_j בעזרת מחרוזת אקראית a_j, כלומר

$$B_j \leftarrow g^{b_j} \ (mod\ p) \quad \text{ו-} \quad C_j \leftarrow A^{b_j} \cdot M_j \ (mod\ p)$$

הוכיחו כי $(B_1 \cdot B_2, C_1 \cdot C_2)$ היא הצפנה חוקית של ההודעה $M_1 \cdot M_2$, כאשר כל הכפלים הם ב- $\mathbb{Z}_p^*$.

סעיף ב

הראו שמערכת ההצפנה של ElGamal אינה עמידה בפני התקפת קריפטוגרמה נבחרת (כפי שראינו בכיתה עבור RSA). המתקיף בהתקפה שלכם ראשי לבקש פיענוח של קריפטוגרמה אחת בלבד.