קריפטוגרפיה – תרגיל 3

הגשה ב-8.5.00 בתא הדואר שלי – 126.

שאלה 1

יהיו (p,g,b) ו-(p,g,B) מפתח פרטי וציבורי בהתאמה עבור מערכת ההצפנה של ElGamal, כאשר $B \equiv g^b \pmod p$. בנוסף יהיו $M_1, M_2 \in \mathcal{Z}_p^*$ שתי הודעות. נניח שעבור $j = 1,2$ הצפנו את M_j בעזרת מחרוזת אקראית r_j לקריפטוגרמה (R_j, y_j) כאשר

$$R_j \leftarrow g^{r_j} \bmod p \quad \text{ו-} \quad y_j \leftarrow B^{r_j} \cdot M \bmod p.$$

1. הוכיחו כי $(R_1 \cdot R_2, y_1 \cdot y_2)$ היא הצפנה של ההודעה $M_1 \cdot M_2$, כאשר כל הכפלים הם ב-$\mathcal{Z}_p$.
2. הראו שמערכת ההצפנה של ElGamal אינה עמידה בפני התקפת קריפטוגרמה נבחרת.

שאלה 2

יהי $N = p \cdot q$ עבור שני מספרים ראשוניים p,q כך ש-$p,q = 3 \pmod 4$. מטרת שאלה זו היא להראות אלגוריתם נוסף למציאת שורש מודולו N.

1. הוכיחו כי לכל $a \in \mathcal{Z}_N^*$ מתקיימים שני התנאים הבאים:

   $$a^{\varphi(N)/2} \equiv 1 \pmod p \text{, ו-} a^{\varphi(N)/2} \equiv 1 \pmod q.$$

   הסיקו כי $a^{\varphi(N)/2} \equiv 1 \pmod N$.
2. הוכיחו כי אם $a \in QR_N$ אזי $a^{\varphi(N)/4} \equiv 1 \pmod N$.
3. יהי $a \in QR_N$ ו-$b \leftarrow a^{(\varphi(N)+4)/8} \bmod N$. הוכיחו כי b הוא שורש של a, כלומר $a \equiv b^2 \pmod N$.

הערה: בכל הסעיפים יש להראות שהחזקות הן מספרים שלמים.

שאלה 3

בהרצאה טענו כי אם המפתח הפיענוח d ב-RSA קטן, אזי המערכת אינה בטוחה. בשאלה זו נראה שיטה איך לפענח ביעילות למרות ש-d לא יהיה קטן. יהיו e ו-d כך ש-$ed \equiv 1 \pmod{\varphi(N)}$, $d_1 \equiv d \pmod{p-1}$ ו-$d_2 \equiv d \pmod{q-1}$. הראו איך לפענח הודעות המוצפנות בעזרת המפתח (N,e) על ידי $O(\log d_1 + \log d_2)$ כפלים וחיבורים, כאשר p,d ו-q ידועים.

שאלה 4

מטרת שאלה זו להראות חולשה של מערכת החתימה של ElGamal כאשר החותם Bob לא משתמש בה נכון. נניח כי Bob חותם על שתי הודעות $m_1, m_2 \in \mathcal{Z}_p^*$ על ידי (γ, δ_1) ו-(γ, δ_2) בהתאמה (כלומר אותו ערך γ מופיע בשני החתימות). נניח בנוסף כי $\gcd(\delta_1 - \delta_2, p-1) = 1$.

1. הראו כיצד לחשב בצורה יעילה את k מתוך ההודעות, החתימות ומפתח הוידוא.
2. הראו כיצד למצוא בצורה יעילה את מפתח החתימה.