16.4.01 עמוס ביימל

קריפטוגרפיה – תרגיל 3

הגשה ב-30.4.01 בהרצאה.

שאלה 1

יהי $N = p \cdot q$ עבור שני ראשוניים אי-זוגיים p ו- q $(p \neq q)$. ויהיו e ו-d כך ש-$\gcd(e, \varphi(N)) = 1$ ו- $e \cdot d \equiv 1 \pmod{\varphi(N)}$. כלומר, N, e, d הם כמו ב-RSA. הוכיחו בעזרת משפט השאריות הסיני כי לכל $a \in \mathcal{Z}_N \setminus \mathcal{Z}_N^\star$ מתקיים כי אם $b = a^e \bmod N$ ו-$c = b^d \bmod N$, אזי $a = c$.

שאלה 2

יהי $N = p \cdot q$ עבור p, q ראשוניים אי-זוגיים $(p \neq q)$.

1. יהי g יוצר של $\mathcal{Z}_p^*$ ו-r מספר טבעי. נסמן $\alpha = \gcd(r, p-1)$. הוכיחו כי $x^r \equiv 1 \pmod{p}$ אם ורק אם קיים j, כאשר $1 \leq j \leq \alpha$, כך ש- $x \equiv g^{\frac{p-1}{\alpha} \cdot j} \pmod{p}$.
   כמה מספרים ב- $\mathcal{Z}_p^*$ מקיימים $x^r \equiv 1 \pmod{p}$?
2. נקודת שבת של מפתח RSA ציבורי (N, e) היא הודעה $M \in \mathcal{Z}_N^*$ כך ש- $RSA(M, (N, e)) = M$. הוכיחו כי מספר נקודות השבת של (N, e) ב- $\mathcal{Z}_N^*$ הוא $\gcd(e-1, p-1) \cdot \gcd(e-1, q-1)$.
   הדרכה: השתמשו במשפט השאריות הסיני.

שאלה 3

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

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

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

   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 4

פיענוח הודעה ב- על ידי מחזיק המפתח הפרטי מתבצע ע"י $O(\log d)$ כפלים. לחסוך בסיבוכיות הפיענוח הוצע לבחור d קטן. אולם, בהרצאה נראה כי אם המפתח הפיענוח d ב-RSA קטן, אזי המערכת אינה בטוחה, כלומר, ניתן לפענח גם ללא המפתח הפרטי.

בשאלה זו נראה שיטה איך לשפר את סיבוכיות הפיענוח ע"י מחזיק המפתח הפרטי 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.

הערה: אפשר להניח כי המפתח הפרטי מכיל מידע נוסף שעוזר לייעל את החישוב. פרטו מהו מידע זה והסבירו למה ניתן לחשבו באופן יעיל בזמן יצירת המפתחות.