05.12.12

קריפטוגרפיה: תרגיל 3

הגשה: יום ד' 19.12.12 בהרצאה ב 16:10. ההגשה בזוגות או ביחידים.

שאלה 1

סעיף א

פתרו את מערכת המשוואות הבאה בעזרת משפט השאריות הסיני:

$$x \equiv 12 \pmod{25}$$
$$x \equiv 18 \pmod{23}$$
$$x \equiv 10 \pmod{31}$$

סעיף ב

פתרו את מערכת המשוואות הבאה בעזרת משפט השאריות הסיני והאלגוריתם למציאת הופכי:

$$37x \equiv 11 \pmod{98}$$
$$41x \equiv 31 \pmod{103}$$

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 $\mathcal{Z}_p^*$ ו- r מספר טבעי. נסמן $\alpha = \gcd(r,p\text{-}1)$. 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- $\mathcal{Z}_p^*$ 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 $M \in \mathcal{Z}_N^*$ כך ש- $\mathrm{RSA}(M,(N,e))=M$. הוכיחו כי מספר נקודות השבת של (N,e) ב- $\mathcal{Z}_N^*$ הוא $\gcd(e\text{-}1,q\text{-}1) \cdot \gcd(e\text{-}1,p\text{-}1)$.

הדרכה: השתמשו במשפט השאריות הסיני.

שאלה 4

יהיו p מספר ראשוני גדול מ-2.

תזכורת, QR_p היא קבוצת כל השאריות הריבועיות ב $\mathbb{Z}_p^*$, ו- QNR_p היא קבוצת כל האיברים ב $\mathbb{Z}_p^*$ שאינם שאריות ריבועיות.

סעיף א

הוכיחו כי אם $a,b \in \mathrm{QR}_p$ אזי $a \cdot b \in QR_p$.

סעיף ב

הוכיחו כי אם $a \in \mathrm{QR}_p$ ו- $b \in \mathrm{QNR}_p$ אזי $a \cdot b \in QNR_p$.

סעיף ג

הוכיחו כי $a^{(p-1)/2} \equiv \pm 1 (\mathrm{mod}\ p)$ לכל $a \in \mathbf{Z}_p^*$.

סעיף ד

הוכיחו כי אם $a,b \in \mathrm{QNR}_p$ אזי $a \cdot b \in QR_p$.