עמוס ביימל 8.4.03

קריפטוגרפיה: תרגיל 3

הגשה: יום ג' 29/04/03 ב- 18:00 בשיעור.

שאלה 1

בשאלה זו נראה בעייתיות של מערכת ההצפנה RSA כאשר משתמשים ב- $e=3$ להצפין. יהי $N=pq$ מספר בין n ביטים שהוא מכפלה של שני ראשוניים גדולים כאשר $p<q<2\sqrt{N}$ ו- $\gcd(3,\varphi(N))=1$. המפתח הציבורי הוא $(N,3)$ והמפתח הפרטי הוא (N,d) כאשר $3\cdot d \equiv 1 (\mathrm{mod}\, \varphi(N))$, כלומר קיים שלם A כך ש- $3d = A\varphi(N)+1$.

סעיף א

הוכיחו כי $1 \le A \le 2$.

סעיף ב

הוכיחו כי $A \neq 1$. הסתמכו על העובדה כי $p>3$ ולכן 3 לא מחלק את p ואת q.

סעיף ג

הראו איך לחשב בזמן $O(n)$ את d בהינתן $\varphi(N)$ ו- N.

סעיף ד

הראו כי $N-4\sqrt{N}<\varphi(N)<N$.

סעיף ה

הראו איך איב, שיודעת מהו N, יכולה למצוא בצורה יעילה d' כך ש- $|d-d'|<3\sqrt{N}$. שימו לב: איב אינה יודעת מהו $\varphi(N)$.

שאלה 2

יהיו p ו- q ראשוניים אי-זוגיים כך ש- $p=2q+1$.

סעיף א

יהי $a \in \mathbb{Z}_p^*$ כך ש- $a \neq \pm 1 \pmod p$. הוכיחו כי אם a <u>אינו</u> יוצר של $\mathbb{Z}_p^*$, אזי a- הוא יוצר של $\mathbb{Z}_p^*$.

סעיף ב

הראו אלגוריתם דטרמיניסטי יעיל המוצא יוצר של $\mathbb{Z}_p^*$. מה סיבוכיות האלגוריתם שתיארתם?

שאלה 3

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 $M_1,M_2 \in \mathbb{Z}_p^*$ שתי הודעות. עבור j=1,2, הצפנו את M_j בעזרת מחרוזת אקראית a_j לקריפטוגרמה (A_j , C_j) כאשר $A_j \leftarrow g^{a_j} \pmod{p}$ ו- $C_j \leftarrow B^{a_j} M \pmod{p}$. הוכיחו כי $(A_1 \cdot A_2, C_1 \cdot C_2)$ היא הצפנה 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.

שאלה 4

בשאלה זו p הוא ראשוני גדול, ו- g הוא יוצר של $\mathbb{Z}_p^*$.

סעיף א

יהיו $a,b \in \{0,....,p-1\}$ ו- $K \equiv g^{ab} \pmod{p}$. הוכיחו כי K הוא שארית ריבועית מודולו p אם ורק אם a או b זוגיים. (שימו לב כי יתכן ש- $ab \geq p-1$).

סעיף ב

האם המפתח הנוצר בפרוטוקול של Diffie & Hellman להחלפת מפתחות מתפלג בצורה אחידה על $\mathbb{Z}_p^*$? הוכיחו תשובתכם.

סעיף ג

הוכיחו כי מאזין יכול לבדוק בצורה יעילה אם $K \equiv g^{ab} \pmod{p}$, המפתח הנוצר בפרוטוקול של Diffie & Hellman, הוא שארית ריבועית כאשר המאזין יודע מהם p, g ו- $A \equiv g^a \pmod{p}$, $B \equiv g \pmod{p}$.

סעיף ד

הוכיחו כי מאזין יכול לבדוק בצורה יעילה אם הודעה המוצפנת בשיטת ElGamal היא שארית ריבועית כאשר המאזין יודע מהו המפתח הציבורי ומהי הקריפטוגרמה.

שאלה 5

עבור מחרוזת בינארית A, נסמן ב- $\overline{A}$ את המחרוזת המשלימה (כלומר, המחרוזת בה כל אפס מוחלף באחד ולהפך).
הוכיחו כי $\mathrm{DES}(\overline{m},\overline{k}) = \overline{\mathrm{DES}(m,k)}$.
הסתמכו על העובדה כי המפתח k_i בכל איטרציה הוא תת-קבוצה של הביטים של המפתח k.