הגשה:
יום ד' 02.01.13 בהרצאה

קריפטוגרפיה: תרגיל 4

20.12.2012

שאלה 1

יהי $N = pq$ עבור p, q ראשוניים אי זוגיים.
יהי k כך ש- $(p-1)$ ו- $(q-1)$ מחלקים את k.
יהיו e, d כך ש- $e \cdot d \equiv 1 \ (mod\ k)$.

סעיף א

הראו ש- $M^{e \cdot d} \equiv M \ (mod\ N)$ לכל $M \in \mathbb{Z}_N$.
רמז: השתמשו במשפט השאריות הסיני.

סעיף ב

בכיתה הראינו שבהינתן d כך ש- $e \cdot d \equiv 1 \ \left(mod\ \phi(N)\right)$, יריב ל- Textbook RSA יכול לפענח הצפנות. הראו שזה אפשרי גם בהינתן d כך ש- $e \cdot d \equiv 1 \ \left(mod\ \frac{\phi(N)}{2}\right)$.
כלומר, הראו כיצד בהינתן N, e ו- d כנ"ל, ניתן לחשב ביעילות את M מתוך $M^e \ mod\ N$.

שאלה 2

בשאלה זו תראו שבעיית הלוג הדיסקרטי ניתנת לרדוקציה אקראית.
יהי p ראשוני ו- g יוצר של $\mathbb{Z}_p^*$.

סעיף א

הראו כי עבור $A, B, C \in \mathbb{Z}_p^*$ כך ש $C = A \cdot B$ מתקיים ש- $DL_g(C) = DL_g(A) + DL_g(B)$.

סעיף ב

i. הראו כי אם מגרילים $x \in \mathbb{Z}_{p-1}$ באקראי בהתפלגות אחידה, אזי $X = g^x \ mod\ p$ מתפלג אחיד ב $\mathbb{Z}_p^*$.

ii. נקבע $A \in \mathbb{Z}_p^*$ כלשהו. הראו כי אם מגרילים $y \in \mathbb{Z}_p^*$ באקראי בהתפלגות אחידה, אזי $z = y \cdot A \ mod\ p$ מתפלג אחיד ב $\mathbb{Z}_p^*$.

סעיף ג

הראו כי אם קיים אלגוריתם יעיל $\mathcal{A}$ שמוצא לוג דיסקרטי ל- $\frac{1}{2}$ מהאיברים ב- $\mathbb{Z}_p^*$, אזי קיים אלגוריתם אקראי יעיל $\mathcal{B}$ שמוצא לוג דיסקרטי לכל מספר ב- $\mathbb{Z}_p^*$ בהסתברות לפחות $\frac{1}{2}$.
כלומר, הראו אלג' $\mathcal{B}$ שבקלט p, g, A מוצא בהסתברות לפחות $\frac{1}{2}$ איבר a כך ש $A \equiv g^a \ (mod\ p)$.

שאלה 3

בכיתה הצגנו את הנחת הקושי של בעיית DDH בתת החבורה של השאריות הריבועיות עבור ראשוני בטוח. בשאלה זו תראו שהנחה דומה לא מתקיימת עבור החבורה $\mathbb{Z}_p^*$ עבור p ראשוני אקראי.

נגדיר את המשחק הבא:

(1) בחר באקראי ראשוני p בן n ביטים.

(2) בחר g יוצר של $\mathbb{Z}_p^*$.

(3) בחר באקראי $x, y \in \mathbb{Z}_{p-1}$ וחשב: $A = g^x \bmod p \quad , \quad B = g^y \bmod p$

(4) הגרל $d \in \{0,1\}$ באקראי.

אם $d = 1$ אזי חשב $C = g^{x \cdot y} \bmod p$.

אחרת הגרל $C \in \mathbb{Z}_p^*$ באקראי.

(5) היריב E מופעל על p, g, A, B, C ופולט ניחוש $\hat{d}$.

E מנצח אם $\hat{d} = d$.

הראו יריב E (אלג' הסתברותי פולינומיאלי ב n) כך ש

$$\Pr\left[\begin{matrix}\text{מנצח } E \\ \text{במשחק הנ"ל}\end{matrix}\right] \geq \frac{1}{2} + t$$

עבור $t > 0$ קבוע כלשהו.

שאלה 4

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

סעיף א

יהיו (p, g, b) ו- (p, g, B) מפתח פרטי וציבורי בהתאמה עבור מערכת ההצפנה של ElGamal, כאשר $B \equiv g^b \pmod p$, ותהיינה $M_1, M_2 \in \mathbb{Z}_p^*$ שתי הודעות.

עבור $j = 1,2$ נסמן ב (A_j, C_j) הצפנה של M_j בעזרת מחרוזת אקראית a_j, כלומר $A_j \leftarrow g^{a_j} \pmod p$ ו- $C_j \leftarrow B^{a_j} \cdot M_j \pmod p$.

הוכיחו כי $(A_1 \cdot A_2, C_1 \cdot C_2)$ 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).