תרגול מס' 3 במבוא לקריפטוגרפיה מודרנית

30 באוקטובר 2013

Decisional Diffie-Hellman

- תהי G חבורה ציקלית מסדר q עם יוצר g.
- בעיית Diffie-Hellman ב־G:

בעיית ההבחנה (Decisional־DH)

1. נגדיר שתי התפלגויות:

$$D_0 = \{g^x, g^y, g^{xy} : (x, y) \leftarrow Z_q^2\}$$

$$D_1 = \{g^x, g^y, g^z : (x, y, z) \leftarrow Z_q^3\}$$

2. קלט: $d_b \leftarrow D_b$ עבור $b \leftarrow \{0, 1\}$.
3. אתגר: נחש את b.

באיזה חבורות הבעיה קשה?

- דיברנו על החבורה Z_p^* המורכבת מהאיברים $\{1, 2, \ldots, p-1\}$ עם כפל מודולו ראשוני p ידוע כי קיים יוצר g. .
- מאמינים כי בעיית הלוגריתם הדיסקרטי ב־ Z_p^* קשה.
- גם CDH נחשבת קשה ב־ Z_p^*.
- האם DDH קשה ב־Z_p^*?

שאריות ריבועיות

הגדרה 0.1 (שארית ריבועית). נאמר כי איבר $s \in Z_p^*$ הוא שארית ריבועית (Quadratic Residue) אם קיים $r \in Z_p^*$ כך ש $s = r^2 \mod p$.

<u>הערה:</u> אפשר להגדיר גם בZ_N^*.

טענה 0.2 QR הנה תת־חבורה של Z_p^*.

הוכחה: מספיק לבדוק כי היא סגורה תחת הפעולה בחבורה:

$$s_1 = r_1^2, s_2 = r_2^2 \Rightarrow s_1 s_2 = (r_1 r_2)^2$$

■

טענה 0.3 יהי $g \in Z_p^*$ יוצר. אז:

1. $g \notin QR$.
2. לכל $a \in Z_p^*$, $a \in QR$ אמ"מ $a = g^k$ כאשר $k = 0 \mod 2$.

הוכחה: ■

1. נניח בשלילה כי $g = r^2$ עבור $r \in Z_p^*$, אז $g^{\frac{p-1}{2}} = r^{p-1} = 1$ (מדוע זו סתירה?)
2. נבחן את שני המקרים
   - נניח כי $k = 2n$, אז $a = g^k = g^{2n} = (g^n)^2 \mod p$.
   - נניח כי $k = 2n+1$, אז $a = g^k = g^{2n+1} = gg^{2n} \mod p$. מדוע $a \notin QR$?

מסקנה 0.4

1. $|QR| = \frac{p-1}{2}$.
2. $Z_p^* \setminus QR = gQR = \{gs : s \in QR\}$. האם זוהי חבורה?
3. יוצר של QR?

בדיקת ריבועיות

- איך ניתן לחשב ריבועיות? לוגריתם דיסקרטי?

טענה 0.5 (קריטריון אוילר) $a \in Z_p^*$ הוא שארית ריבועית אמ"מ $a^{\frac{p-1}{2}} = 1$.

- אם $a = r^2$, אז $a^{\frac{p-1}{2}} = r^{p-1} = 1$.
- אם $a \notin QR$, אז $a = gs$ עבור $s \in QR$ ולכן $a^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} s^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \neq 1$.
  (בתרגיל בית, במקרה זה $a^{\frac{p-1}{2}} = -1$)

בחזרה ל־DDH

טענה 0.6 DDH אינה קשה ב־Z_p^*. (בתרגיל בית - ניתן להבחין בפער $\frac{1}{2}$).

- דוג' לחבורה בה מאמינים ש־DDH קשה: מסתכלים על ראשוני $p = 2q + 1$ עבור ראשוני q. ומסתכלים על הבעיה בתת החבורה $G = QR$.