יסודות הקריפטוגרפיה שיעור 5#

הראנו כי בכל שדה $GF(p^k)$ יש איברים פרמיטיביים, נרצה למצוא דרך יעילה למצוא איבר פרמיטיבי בשדה.

דרך אחת למצוא איבר פרמיטיבי:

מגרילים איבר בשדה x שאינו 0. יש לו סיכוי טוב להיות שורש פרימיטיבי כי יש הרבה כאלה, ולכן נבדוק את הסדר שלו. נניח שנתון פירוק $\Pi_{i=1}^{s} p_i^{e_i} = p^k - 1$ כאשר p_i ראשוניים ו-$e_i \geq 1$. נסמן: $|x| = m = \Pi_{\substack{i=1 \\ 0 \leq f_i \leq e_i}}^{s} p_i^{f_i} < p^k - 1$. קיים j כך ש-$f_j < e_j$ $1 = x^{\frac{p^k-1}{p_j}}$.

כל איבר מחלק את סדר החבורה שהוא $p^k - 1$, ורוצים לוודא עבור x האם הסדר שלו הוא $p^k - 1$ (ואז הוא פרימיטיבי), ולכן נבדוק $\forall 1 \leq 1 \leq s$ האם $x^{\frac{p^k-1}{p_i}} \stackrel{?}{=} 1$ וזה אמ"מ x הוא שורש פרימיטיבי (איבר פרימיטיבי). הבעיה היא הפירוק לגורמים ראשוניים, המשפיעה על יעילות האלגוריתם. סה"כ האלגוריתם הוא $O(\log^3 p)$ (חישוב $x^m \bmod p$).

***Quadratic Residues* – שאריות ריבועיות:**

מספרים שהם ריבוע שלם של מספרים אחרים ב-$\mathbb{Z}_m$.

עבור $m \geq 2$ ו-$0 \neq x \in \mathbb{Z}_m$, x הוא שארית ריבועית מודולו m אם קיים $y \in \mathbb{Z}_m$ כך ש-$y^2 \equiv x (\bmod m)$.

עבור $\mathbb{Z}_p^* =< g \geq \{g^1, \dots, g^{p-1}\}$ מתקיים $x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$ עבור שאריות ריבועיות – דרך אחת לבדוק האם מספר הוא שארית ריבועית. דרך אחרת היא לבדוק האם מספר מקיים $g^{\frac{p-1}{2}} = (g^{p-1})^t \cdot g^{\frac{p-1}{2}} = g^{(p-1)t+\frac{p-1}{2}} = (g^{2t+1})^{\frac{p-1}{2}} \neq 1$ (=1), וזו בדיקה שאיבר הוא לא שארית ריבועית. אם כן כדי לבדוק האם מספר הוא שארית ריבועית מעלים אותו בחזקה $\frac{p-1}{2}$.

<u>דרך יעילה לחישוב $x^n \bmod m$</u>:

נסתכל על הפירוק הבינארי של n: $n = n_0 + 2n_1 + 4n_2 + \cdots + 2^k n_k$, ואז: $x^n = x^{n_0} \cdot \dots \cdot (x^k)^{n^k}$ – כאשר חישוב המכפלות הפנימיות של x הוא סה"כ $2(k-1)$ כפלים ו-$k = \log_2 n$. לכן כאשר מחשבים $x^{\frac{p-1}{2}} \bmod p$ העלות היא $O(\log^3 p)$.

אם $m = pq$ אז:

$$\begin{cases} x = y^2 \bmod p \\ x = z^2 \bmod q \end{cases} \Rightarrow x = w^2 \bmod m, y = w \bmod p, z = w \bmod q$$

אם יודעים לפרק את m אז קל לחשב שאריתצ ריבועית, ואם לא אז קשה לחשב את m. כלומר, אם יודעים את $p.q$ אז קל לעשות את המעבר מ-y, z ל-w ולהיפך, אחרת מציאת w ש-x הוא הריבוע שלו היא שאלה קשה.

***The DL (discrete logarithm) problem*:**

תהי G חבורה ציקלית, כלומר $G =< g \geq \{g^1, \dots, g^{|G|}\}$. אם לוקחים x כללי בחבורה אז מתקיים $x \in G \Rightarrow x = g^i$. בהינתן x רוצים למצוא את ה-i שמקיים זאת. בעצם רוצים לחשב את $dl_g(x) = i$. דיסקרטי – משום שזה כפל בחבורה. אם $G = \mathbb{Z}_p^*$, תחת האילוץ ש-$p-1$ הוא בעל גורם ראשוני גדול, הבעיה היא קשה (פונקציה חד כיוונית).

אם נתון i, חישוב g^i היא בעיה קלה. הבעיה ההפוכה קשה (אך כריעה). האלג' הנאיבי יעבור על כל i אפשרי ויבדוק האם $x = g^i$, אז עבור תנאים מסויימים חישוב זה יהיה קשה וארוך חישובית.

***Diffie & Hellman*:**

חלוקת מפתח לשני חלקים, מפתח פומבי k_E ומפתח k_d *decryption* שהוא מפתח משותף לשני הצדדים. נסתכל על המקרה בו לשני הצדדים יש מפתח משותף ויריב מאזין. סימונים:

- A מספר ראשוני גדול p, g איבר פרימיטיבי ב-$\mathbb{Z}_p^*$.
- אליס (אחד הצדדים) בוחרת $a \in [0, \dots, p-2]$ ושולחת $x = g^a \bmod p$ לבוב (מועבר בערוץ מאובטח).
- בוב עושה אותו דבר עם b ושולח את $y = g^b$ לאליס (מועבר בערוץ מאובטח).

רוצים ש-p יהיה מהצורה $p = 1 + (small\ factors) \cdot (\boldsymbol{one}\ large\ factor)$.

כעת אליס מחשבת את המפתח: $(g^b)^a = g^{ba}$. גם בוב יכול לעשות את אותו דבר: $(g^a)^b = g^{ab}$. כל החישובים הללו פשוטים. מי שהאזין לקו יודע את g^a, g^b, ונשאלת השאלה האם מידע זה מספיק כדי לחשב את g^{ab} (בעיה זו שונה מבעיית DL) בזמן טוב. מפתח זה מסומן $DH\ key$.

אם היה קל לפתור את DL, היה קל למצוא את $DH\ key$. אבל, זה רק אומר ש-DL קשה מ-DH. ובכל זאת, DH היא בעיה מספיק קשה (לא נפתרה מאז 1976). כעת ניתן להשתמש ב-g^{ab} להצפנה כלשהי, למשל AES. נשים לב כי $a \to g^a \bmod p$ הוא מיפוי יחיד עבור $2 \le a \le p-2$. מה צריך להוכיח:

- נכונות הפרוטוקול: שכל אחד מהצדדים יוכל לבצע את הפרוטוקול מהצד שלו ולקבל בסוף מפתח משותף.
- אבטחה: שהפרוטוקול יהיה בטוח.
- אבטחה חזקה: רוצים שיריב שאוסף את כל האינפורמציה הפומבית, כגון p, g, g^a, g^b, לא יוכל למצוא את a, b אלא בדרך קשה חישובית (לא NP-קשה, אך קשה), והאינפורמציה הפומבית לא משפרת את סיכוייו לפענח את המפתח.

הערה: וריאציה של האלגוריתם לבנות את המפתח g^{a+b} למשל אינה טובה כי קל לבנות את המפתח הזה מהמידע הפומבי.

<u>אלגוריתם DF לא מספק את הדרישה השלישית</u>:

נראה ש-DH כן חושף מידע על המפתח עצמו. למרות שלא ידוע דבר על a, בהינתן g^a כן ניתן לבדוק בקלות האם מספר זה הוא שארית ריבועית או לא:

$$a \coloneqq a_0 + 2a_1 \Rightarrow g^a\ is\ a\ QR \Leftrightarrow a_0 = 0$$

כלומר, אם a אי זוגי, אז מה שקיבלנו הוא לא שארית ריבועית. כלומר, כל מי ששומע את התקשורת יכול לגלות את ה-lsb של a ושל b. לפי זה ניתן לגלות גם האם $a \cdot b$ הוא מספר זוגי, ולכן ניתן לגלות האם g^{ab} הוא שארית ריבועית או לא.

אם כן, ניתן לשפר ע"י בחירה מראש של a, b אי זוגי – ואז המידע הפומבי לא מסגיר מידע חדש על a, b. כעת המידע הפומבי הוא g, p, g^a, g^b והעובדה ש-a, b אי זוגיים. כמו כן p יבחר מהצורה $p = 2q - 1$, כלומר 2 הוא גורם קטן של $p - 1$.

ישנן דוגמאות נוספות של DH בחבורות אחרות, כמו החבורה האדיטיבית $(\mathbb{Z}_p, +)$ או החבורה המולטיפליקטיבית $(\mathbb{Z}_p, \cdot)$ או עקומים אליפטיים.

<u>שימושים ל-DF</u>:

במצגת.

שאר ההרצאה היתה הדגמה ב-$sage$. פונקציות חשובות:

- $timeit(< action >)$: מחזיר את זמן החישוב של הפעולה.
- חישוב מודולו #1: $\bmod(prod([x] * x), y)$ - איטי.
- חישוב מודולו #2: $prod(\bmod(x, y), x)$ - מהיר.

...