יסודות הקריפטוגרפיה שיעור 6#

נושא היום הוא בדיקת ראשוניות. בהמשך נדבר בעיקר על *RSA* כמערכת דוגמא למערכת הצפנה פומבית. שבוע שעבר דיברנו על החלפת מפתחות של *DH* ושם צריך מספר p ראשוני גדול, אך הוא לא חייב להיות סודי. ב-*RSA* המפתח מורכב ממכפלה של שני ראשוניים שאינם ידועים. לכן חשוב ב-*RSA* שנוכל לבחור ראשוניים גדולים ו"סודיים". לשם כך צריך את משפט המספרים הראשוניים – שיש מאגר גדול של מספרים ראשוניים ושניתן יהיה לבדוק ראשוניות. בשיעור הבא נדבר על אלגוריתמים לפירוק (פירוק ראשוניים אינו קל).

ראינו שבכל שדה, בפרט ב-$\mathbb{Z}_p$ יש איברים פרימיטייבים היוצרים את החבורה $\mathbb{Z}_p^*$. מה קורה עבור m המורכב משני גורמים ראשוניים מוכפלים?

משפט: ב-$\mathbb{Z}_m^*$ עבור m המורכב <u>משני גורמים אי זוגיים ראשוניים</u> אין איברים פרימיטיביים.

אם כן m שכן יש בו איברים פרימיטייבים מקיים: $m = 2^k p^l, k, l \geq 1$ או p^l או 2^k. דוגמא: עבור $m = 25 = 5^2$ מתקיים ש-3 הוא איבר פרימיטיבי של $\mathbb{Z}_{25}^*$.

משפט המספרים הראשוניים:

ישנם אינסוף מספרים ראשוניים. נניח כי יש מספר סופי של ראשוניים k. נסתכל על המספר $p_1 \cdot p_2 \cdot \dots p_k + 1$ - אותו אף אחד מהמספרים $p_1, \dots, p_k$ לא מחלק. זה לא אומר שהוא ראשוני, אבל הגורמים שלנו אינם אלה בהכרח ולכן בהכרח קיימים עוד מספרים ראשוניים.

זה לא אומר לנו דבר על צפיפותם של הראשוניים. נסמן $\pi(x)$ כמספר הראשוניים עד x. למשל $\pi(30) = 4 + 4 + 2 = 10$ (חלוקת הסכום לפי מספר הראשוניים בכל עשירייה עד30). מתקיים: $\pi(x) \cong \frac{x}{\ln x}$ ועבור $x \geq 55$: $\frac{x}{\ln x - 4} \leq \pi(x) \leq \frac{x}{\ln x + 2}$.

נסמן p_n המספר הראשוני ה-nי, אז מתקיים: $n \ln n + n \ln \ln n > p_n > n \ln n + n(\ln \ln n - 1)$.

<u>מסקנות</u>:

1. יש הרבה מספרים ראשוניים.
2. אם בוחרים באקראי מספר בן n ספרות, הסיכוי שהוא ראשוני הוא בערך $\frac{1}{n}$. **<u>חשוב לדעת מסקנה זו</u>**.

אנלוגית ראשוניות לפולינומים: פולינום <u>אי-פריק</u>. נסתכל על פולינום עם משתנה אחד מדרגה k מעל $GF(p)$, כמה מהם אי-פריקים?

ראשית, יש סה"כ p^k פולינומים בשדה; נסמן את N_k כמספר האי פריקים, ומתקיים שהוא בערך $N_k \cong \frac{p^k}{k}$.

<u>השערת *Goldbach*</u>: כל מספר זוגי טבעי גדול מ-2 ניתן לייצוג כסכום של שני מספרים ראשוניים.

כיצד בודקים ראשוניות:

רוצים להיות מסוגלים לבדוק האם מספר נתון הוא ראשוני. הבדיקה שנבצע היא למעשה בדיקת <u>אי-ראשוניות</u>. אם המספר הוא לא ראשוני נניח בהסתברות $\frac{1}{2}$, אז כל בדיקה כזו תיתן עד שהמספר מורכב. לאחר 100 בדיקות כאלה נדע בהסתברות גבוהה עם סיכוי טעות של $\frac{1}{2^{100}}$ האם המספר ראשוני.

בהינתן מספר בן n ביטים רוצים לבדוק האם מספר הוא פריק. בעיית ההחלטה הזו היא ב-NP, כאשר העד הוא גורמי המספר. באופן דטרמניסטי לא ניתן למצוא גורמים אלו בזמן פולי". מצד שני, בעיית החיפוש, כלומר בהינתן מספר n יש למצוא את הגורמים שלו – זו לא בעיה שקולה לבעיית ההחלטה.

<u>האם יש דרך טובה יותר לבדיקת פריקות/ראשוניות מאשר בדיקת כל הגורמים?</u>

Solovey-Strassen, 1977: כדי להראות ש-m פריק מספיק להראות עדות שהוא לא מתנהג כמו ראשוני, ועדות זו לא כוללת גורם ראשוני של m.

<u>המשפט הקטן של פרמה</u>: אם p הוא ראשוני ו- $1 \leq a \leq p - 1$ אז $a^{p-1} = 1 (\mathrm{mod}\, p)$. עבור m במקום p, מציאת a כזה היא עדות לכך ש- m הוא פריק אך לא נותן שום עדות למהם הגורמים של m. אבל, מספרי קרמייקל מקלקלים את הבדיקה הזו, אז נעשה שינוי באלגוריתם.

בהינתן m פריק, האם קיים עד פרמה a שמקיים $2 \leq a \leq m - 1$? **לא**, יש כמה כאלה שמבחן פרמה תמיד או כמעט תמיד נכשל עבורו.

<u>מספרי קרמייקל</u>: קיימים מספרים פריקים m שעבורם משפט פרמה הקטן נכשל, כלומר כמעט לכל a בתחום הנדרש מתקיים $a^{m-1} (\mathrm{mod}\, m) = 1$.

מספרים אלו מקיימים: $m = p_1 \cdot \dots \cdot p_k$ ולכל גורם מתקיים $p_i - 1$ מחלק את $m - 1$. מספרים אלו נדירים. ניתן לבנות מבחן שיבדוק האם מספר נתון הוא מספר קרמייקל, ואם לא נבצע עליו את האלגוריתם הרגיל.

מבחן מורחב לפריקות:

נרחיב את המבחן לשלוש בדיקות על $2 \le a \le m-1$:

- $\gcd(m,a) > 1$ - אזי m פריק.
- $a^{m-1} \neq 1$ - מבחן פרמה.
- $a^2 = 1 (\mathrm{mod}\, m)$ אבל $a \neq m-1$.

עבור מספר קרמייקל, צריך לבחור את a באופן הבא: $a = b^r$ כאשר $m-1 = 2r$, ו-b אינו עד מסוג 2 (כלומר $b^{m-1} = (b^r)^2 = 1 (\mathrm{mod}\, m)$.

<u>הכללה ל-m כללי</u>:

יהי $m-1 = 2^k \cdot r$ כאשר r אי-זוגי. לכל b מתקיים $b^{m-1} = (\dots((b^r)^2)^2 \dots)^2$ (k פעמים). אם בסוף התהליך $b^{m-1} \neq 1 (\mathrm{mod}\, m)$ אז b הוא עד מסוג 2. אם לא, נגדיר $a_0 = b^r, a_1 = a_0^2, \dots, a_k = a_{k-1}^2$, ואז $a_k = b^{m-1} (\mathrm{mod}\, m)$ וידוע כי זה שווה ל- 1. יהי j האינדקס הקטן ביותר שמתקיים עבורו $a_j = 1 (\mathrm{mod}\, m)$. אם $0 < j$ ו-$a_{j-1} \neq -1 (\mathrm{mod}\, m)$ אז a_{j-1} הוא עד טוב מסוג 3, ולכן m פריק. בחירת b המקיים אחד משני התנאים הנ"ל הוא <u>עד חכם</u>.

Rabin-Miller test:

אם m פריק אז לפחות $\frac{3}{4}m$ מספרים בטווח $1 \dots m$ הם עדים חכמים. כל b לוקח $O(\log^3 m)$ זמן בדיקה, אז אם בודקים $O(1)$ מהם מקבלים $O(\log^3 m)$ סיבוכיות זמן ריצת האלג'.

אז מבחן מילר-רבין הוא: מקבלים כקלט מספר m בן n ביטים. בוחרים 100 פעם $1 < b < m$ באקראי ובודקים האם הוא עד חכם. אם אחד או יותר b הוא עד חכם אז מוחזר ש-m הוא פריק, אחרת מוחזר שהוא ראשוני. זמן הריצה פולי' באורך הקלט, דהיינו n (מספר הביטים של m). אם m הוא ראשוני האלגוריתם <u>תמיד</u> יחזיר שהוא ראשוני (הטעות תיתכן בהסתברות נמוכה מאוד להחזיר על m פריק שהוא ראשוני. ההסתברות לטעות קטנה מ-$\left(\frac{1}{4}\right)^{100}$.

האלגוריתם הזה הוא ב-$RP \subseteq NP$ - פולי' הסתברותי עם טעות חד-צדדית (BPP – דו צדדית).

<u>אלגוריתם דטרמיניסטי לבדיקת ראשוניות</u>:

ב-2005 קבוצה של כמה הודים מצאו אלג' פולי' ב-$O(n^{12})$ לבדיקת ראשוניות דטר', שיותר מאוחר הורדה ל-$O(n^6)$. עדיין משתמשים באלגוריתם מילר-רבין כיוון שהטעות היא קטנה מאוד והביצועים הרבה יותר גבוהים.

הכפלת שלמים ופקטוריזציה כפונקציה חד-כיוונית:

<u>פונקציה חד כיוונית</u> היא פונ' שקל לחשב אותה בכיוון אחד, אך קשה לחשב את ההופכית שלה.

הכפלת שני מספרים בני n ספרות לוקח $O(n^2)$ זמן; הפעולה ההפוכה של פירוק לגורמים לוקחת $2^{c \cdot n^{\frac{1}{3}}}$ זמן (לפי האלג' הטוב ביותר שקיים כיום). קל לבחור שני מספרים ראשוניים $p \cdot q$ וליצור את מכפלתם $m = p \cdot q$, הפירוק $m \to p, q$ קשה. נשאלת השאלה האם קושי זה יכול להוות בסיס למערכת הצפנות עם מפתח פומבי? (כן – RSA). אלג' החלפת המפתחות של DH לא עונה על כך.

RSA:

- האינפורמציה הפרטית של בוב היא p, q שני ראשוניים אקראיים.
- האינפורמציה הפומבית:
  - $m = p \cdot q$
  - חזקה e זרה ל-$\phi(m)$ שזה במקרה זה: $\phi(m) = (p-1)(q-1)$ – שזה מספר האיברים ב-$\mathbb{Z}_m^*$.
- מידע פרטי נוסף: d שהוא זר ל-$\phi(m)$ ומקיים $d \cdot e = 1 (\mathrm{mod}\, \varphi(m))$ (מתוך $xgcd$).

נסתכל על ההודעה $A \in \mathbb{Z}_m$. ההצפנה: $C := A^e (\mathrm{mod}\, m)$, C ישלח לבוב. פענוח: $C^d = A^{d \cdot e} = A (\mathrm{mod}\, m)$. נשים לב כי $A^{de} = A^1 (\mathrm{mod}\, m)$ כי $d \cdot e = 1 (\mathrm{mod}\, \phi(m))$, ובחוג שלנו שהוא $\mathbb{Z}_m^*$ מתקיים $A^{\phi(m)} = A^1 (\mathrm{mod}\, m) = A$.

<u>הערה</u>: אם $A \neq 0$ נמצא ב-$\mathbb{Z}_m \backslash \mathbb{Z}_m^*$ אז החשבונות לא עובדים, אבל A כזה יאפשר פירוק של m: $m > \gcd(A, m) > 1$ ולא סביר שנתקל בכזה A.

בניית הצפנת *RSA* :

חזקת ההצפנה e יכולה להיות קטנה, למשל אם $p \cdot q = 2 (\mathrm{mod}\, 3)$ אפשר לקחת $e = 3$. יתרונות: הצפנה מהירה – שני כפלים בלבד. חסרונות: ?.

<u>הערה</u>: אם היריב יודע ש-d קטן, הוא ינסה את כל האפשרויות ולכן זה רעיון רע.

בהינתן $m = pq$ ו-e, האם אפשר:

- לחשב את $\phi(p)$
- למצוא את d

חישוב $\phi(p)$ קשה כמו פירוק כי $\phi(p \cdot q) = (p-1)(q-1) = pq - q - p + 1$. נניח שהצלחנו לחשב את זה ונתון גם pq. ע"י חיסור נקבל $l \coloneqq p + q$. נפתור את זוג המשוואות: $\begin{cases} p \cdot q = m \\ p + q = l \end{cases}$ וכך נמצא את p, q. כלומר, חישוב $\phi(pq)$ שקול לפירוק, והוא קשה.

נניח יש אלג' למצוא את d מתוך pq ביחס ל-e הנתון. ידוע כי $de = 1 (\mathrm{mod}\, \phi(pq))$, כלומר יש C כך ש-$de = 1 + C \cdot \phi(pq)$. כלומר, אם יודעים לחשב את d אז (אם מחסירים 1) מתקבלת כפולה של $\phi(pq)$. מכאן (נראה בתרגול) ניתן למצוא את $\phi(pq)$ ומכאן לפרק.

משפט השאריות הסיני (*Chinese remainder theorem*) / *CRT* :

נניח $m_1, \dots, m_k$ טבעיים זרים בזוגות, כלומר $\gcd(m_i, m_j) = 1$ לכל i, j ו-$a_1, \dots, a_k$ טבעיים כך ש-$0 \le a_i \le m_i - 1$. אז יש x טבעי כך שלכל i מתקיים $x = a_i (\mathrm{mod}\, m_i)$ ויתרה מכך, בתחום $[0, (\pi_{m_i}) - 1]$ הוא יחיד.

<u>הערה</u>: ב-*sage* לגבי שניים, הפעולה היא: $CRT(a_1, a_2, m_1, m_2)$.

<u>הוכחה</u>: באינדוקציה.

עבור $k = 2$: רוצים x כך ש-$x = a_1 (\mathrm{mod}\, m_1), x = a_2 (\mathrm{mod}\, m_2)$. כיוון ש-$m_i$ זרים, אז יש $m_2^{-1} (\mathrm{mod}\, m_1)$ ו-$m_1^{-1} (\mathrm{mod}\, m_2)$ – הופכיים כפליים מודולו השני. נגדיר $x = a_1 \cdot m_2 \cdot \underbrace{(m_2^{-1} - 1 \bmod m_1)}_{< m_1} + a_2 \cdot m_1 \cdot \underbrace{(m_1^{-1} \bmod m_2)}_{< m_2}$.

...