יסודות הקריפטוגרפיה שיעור 7#

תזכורת:

<u>משפט המספרים הראשוניים</u>: חסם למספר הראשוניים עד מספר x הוא: $\pi(x) \cong \frac{x}{\ln x}$. באינטרוול מספיק גדול ניתן לאמוד חסם למס' הראשוניים שמכיל. בדיקת ראשוניות אקראית רצה ב-$O(n^3)$ ודטר' ב-$O(n^6)$.

החבורה הכפלית $\mathbb{Z}_m^*$:

- נסמן $m = pq$ ו-$\mathbb{Z}_m^* = \mathbb{Z}_{pq}^*$ מכיל את כל המספרים בטווח $[1, \dots, pq-1]$.
- גודל הקבוצה: $\phi(pq) = \phi(p) \cdot \phi(q) = (p-1)(q-1) = m - (p+q) + 1$
- לכל $x \in \mathbb{Z}_m^*$: $x^{(p-1)(q-1)} = 1 (\mathrm{mod}\, pq)$.
- לחבורה הכפלית הזו אין יוצרים כפליים.

שורשים ריבועיים של 1 ב-Z_{pq}^*:

נרצה לספור שורשים ריבועיים ב-Z_{pq}^* ונתחיל מ-1: 1 – ברור; -1 – שהוא $pq-1$ - כמעט ברור; מה עוד?

ידוע כי ב-$\mathbb{Z}_p^*$ יש ל-1 שני שורשים ריבועיים והם $1, p-1$. כנ"ל ב-$\mathbb{Z}_q^*$: $1, q-1$. שורש ריבועי של 1 ב-Z_{pq}^* צריך לקיים: $y^2 = 1 (\mathrm{mod}\, pq)$ אז $y^2 = 1 (\mathrm{mod}\, p), y^2 = 1 (\mathrm{mod}\, q)$. לפי משפט השאריות הסיני מקבלים של-1 יש 4 שורשים ריבועיים.

<u>כללי</u>:

נניח z הוא ריבוע ב-Z_{pq}^*, כלומר קיים t כך ש-$t^2 = z (\mathrm{mod}\, pq)$. מכאן ישר מקבלים 4 שורשים:

- $t \cdot 1$
- $t \cdot (-1) = t(pq-1)$
- $t \cdot a$
- $t \cdot b$

כאשר a, b הם שורשי יחידה שאינם ± 1 שקיבלנו קודם. לכן ההעתקה $x \to x^2 (\mathrm{mod}\, q)$ היא 4 ל-1, ל-$\frac{1}{4}$ מהאיברים הם ריבועיים (יש להם מקור) ו-$\frac{3}{4}$ אינם ריבועיים. הערה: ל-$\mathbb{Z}_{pqr}^*$ ההעתקה היא 8 ל-1 (p, q, r ראשוניים).

<u>טענה</u>:

אם e זר ל-$(p-1)(q-1)$ אז $x \to x^e (\mathrm{mod}\, pq)$ היא העתקה חח"ע ועל של Z_{pq}^* (ויכול לשמש כבסיס להצפנה – אחרי הפעלת שיקול דעת; למשל $e = 1$ לא רעיון טוב לשימוש). מ-$xgcd$ קיים f, d כך ש-$f \cdot (p-1)(q-1) + de = gcd = 1$ ולכן $d \cdot e = 1 + \underset{=-f}{C}(p-1)(q-1)$.

נסמן $y = x^e$ ואז: $y^d = (x^e)^d = x^{ed} = x^{1+C(p-1)(q-1)} = x$ ולכן $y \to y^d$ היא ההעתקה ההפוכה ל-$x \to x^e$.

RSA:

- המידע הפרטי של בוב: p, q ראשוניים גדולים.
- מידע פומבי: $m = pq, e$ כאשר e זר ל-$\phi(m) = (p-1)(q-1)$.
- עוד מידע פרטי: d הזר ל-$\phi(m)$ כך ש-$d \cdot e = 1 (\mathrm{mod}\, \phi(m))$.

הודעות יהיו איברים ב-$\mathbb{Z}_m$ (בד"כ ב-$\mathbb{Z}_m^*$), כלומר $[1, \dots, m-1]$.

- הצפנה: $P \to C \coloneqq P^e (\mathrm{mod}\, m)$.
- פענוח: $C \to P = C^d = P^{de} = P (\mathrm{mod}\, m)$.

אם $P = 0$ אז כלום לא קורה (וסודיות לא נשמרת). אם $P > 0$ אבל $P \notin \mathbb{Z}_m^*$ אז $1 < \gcd(P, m) > m$ ולכן לא מאפשר פירוק. לכן ההודעות שניתנות להצפנה בדרך זו היא $P \in Z_{pq}^*$.

<u>דוגמא</u>: במצגת שיעור 7, שקופית 13.

<u>הערה</u>: החישובים x^e מתבצעים מודולו $p \cdot q$ אבל ניתן לחסוך זמן אם בחזקה נעבוד עם $e \bmod \phi(pq)$. למשל:

$$x^{9337} (\mathrm{mod}\, 2773) = x^{9337 (\mathrm{mod}\, 2668)} (\mathrm{mod}\, 2773)$$

וכך מזרזים אתהחישוב בחזקה.

כמה חזק *RSA*:

מציאת d לדרך הפענוח המוצעת שקולה למציאת פירוק, ולכן פענוח RSA קשה לכל היותר כמו פירוק. אבל, יתכן שקיימת דרך אחרת קלה יותר, שכמובן טרם נמצאה.

תכונות *RSA*:

ה-RSA הוא דטרמיניסטי. תכונה נוספת: RSA סגורה תחת כפליות, כלומר: $E(P_1 \cdot P_2) = E(P_1) \cdot E(P_2)$. אם כן RSA פגיעה תחת *chosen ciphertext attacks*, והיא לא פסאודו-ראנדומית. למשל: נניח נתון לנו $C \coloneqq E(x)$. היריב בוחר R אקראי ומחשב את $C' \coloneqq C \cdot R^e \bmod pq$ וזו הודעה אקראית ב-Z_{pq}^*. אם נדרוש את פענוח C' אז קיבלנו: $(C')^d = C^d \cdot R^{ed} = x \cdot R$. מכאן, ע"י הכפלה ב-$R^{-1}$ נקבל את x. שימוש ב-*padding* פותר משהו, לבדוק במצגת...

<u>שימוש ב-*CRT* להאצת *RSA*</u>: גם ל-e קטן ה-d צריך להיות גדול ולכן יש $2n$ העלאות בחזקה כדי לפתוח. יש n^3 פעולות על d בן n ביטים. בשימוש ב-CRT סה"כ: $2 \cdot \left(\frac{n}{2}\right)^3$ וזה שיפור בפקטור 4.

<u>שימוש ב-e קטן כדי להאיץ את תהליך ההצפנה</u>: במצגת.

תכונת *Random self reducibility* של *RSA*:

נסתכל על החוג Z_{pq}^* כעל מעגל. אם יש אחוז ε של הודעות אותן קל לפענח בלי מפתח, אז ניתן לפענח את כל המרחב ביעילות ε^{-1}. איך?

עבור x^e נכפיל אותו ב-R אקראי, ואז בהסתברות ε ניפול על מקום שקל לפענח. בהסתברות ε^{-1} ניפול על כזה.

<u>חתימות</u>:

רוצים שמחרוזת דיגיטלית תהווה חתימה ותוכל לקשר מסמך לאדם ספציפי. נרצה שחתימה כזו תהיה קשה לזיוף, המבוסס על בעיה חישובית. *Diffie Hellman* היו הראשונים שהציעו את זה, ומומש לראשונה ע"י *RSA*.

תהי E_A פונ' ההצפנה הפומבית של אליס ו-D_A פונקציית הפענוח הפרטית שלה. חתימה על הודעה M: $y = D_A(M)$, ונשלח את (M, y). במקרה זה M פומבי. כיוון שהיא היחידה שיכולה להפעיל את D_A, אז החתימה הזו ייחודית לה. כדי לוודא בצד השני שההודעה אחכן חתומה ע"י האדם המקורי, מחשבים את $E_A(y)$ ובודקים האם הוא שווה ל-M.

<u>כיצד מזייפים מסמך אקראי</u>: בוחרים R אקראי ומחשבים את $S =: E_A(R)$ ואז (S, R) הוא זוג טוב כי $R = D_A(S) = D_A\big(E_A(R)\big)$. זהו זיוף *existential forgery*. נראה שעם RSA ניתן לקבל גם זיופים מזיקים יותר.

פתרון ע"י *hash*:

מניחים כי H היא פונ' עמידה בפני התנגשויות פומבית. כדי לחתום על ההודעה M תחילה מבצעים עליה *Hashing*, ועל זה מבצעים חתימה. אם הפונ' H חזקה, החתימה תהיה חח"ע (בערך) להודעה. אז הזוג שנשלח הוא $\Big(M, D_A\big(H(M)\big)\Big)$.

באופן כללי, יש לחתימה 3 שלבים:

- יצירת מפתחות (כמו במערכות הצפנה).
- אלגוריתם חתימה: ייצור חתימה.
- אלגוריתם וריפיקציה: וידוא שהחתימה אכן מתאימה.

<u>אלגוריתם לפירוק פסרים טבעיים (*Polard*)</u>:

סיבוכיותו היא $2^{\frac{n}{4}}$; יש אלג' שסיבוכיותם היא 2^{n^c} עבור $c = \frac{1}{2}, \frac{1}{3}$.

נתבונן ב-$\mathbb{Z}_m$, ו-F פונקציה. ניקח x בתחום. נפעיל את F על x: $x, F(x), F^2(x), \dots$. כללית, המסלול של F חייב לחזור על עצמו כי המרחב $\mathbb{Z}_m$ סופי, ולכן יש חלק של לולאה שמתחיל עם זנב. אם F אקראית אז משיקולי פרדוקס היומולדת נקבל שגם הזנב וגם הלולאה הם בגודל בערך $\sqrt{\frac{\pi}{8}m}$ (תוחלת על כל F ועל כל x). נניח ש-$m = pq$ ו-F_p יהיה F מודולו p וכנ"ל לגבי F_q ושתיהן ב"ת. אם סוגרים לולאה F_p אך לא F_q אז זה אומר שיש לנו y ו-z כך שמתקיים: $y = z \pmod p$ וגם $y \neq z \pmod q$. במקרה זה נסתכל על $y - z$, הוא מתחלק ב-p אך לא ב-q.

איך מוצאים פונקציה אקראית? איך מגלים התנגשות?

גילוי התנגשות אפשר לעשות ע"י הרצת שני מצביעים, אחד בקצב 1 והשני בקצב כפול – שניהם יתנגשו בטוח.