קריפטוגרפיה

צופן RSA

1) משפט השאריות הסיני
2) משפט הקטן של פרמה
3) משפט אוילר
4) אלגוריתם RSA
   - Rabin
   - Shamir
   - Adleman
5) הצפנה ופענוח עם RSA
6) צופן אניגמה
7) ולמה: אניגמה ניתנת לפענוח
8) אל-גמאל
9)

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$$

משפט השאריות הסיני: יהיו $m_1, m_2, \ldots, m_k$ מספרים שלמים חיוביים זרים זה לזה, כלומר $\gcd(m_i, m_j) = 1$ לכל $i \neq j$.

יהיו $a_1, \ldots, a_k$ מספרים שלמים כלשהם.

אזי למערכת הקונגרואנציות לעיל קיים פתרון יחיד x מודולו $M = m_1 \cdot m_2 \cdots m_k$.

$$x = \sum_{i=1}^{k} a_i M_i y_i \bmod M$$

כאשר $M_i = \frac{M}{m_i}$ ו־$y_i = M_i^{-1} \bmod m_i$.

$$X = \sum_{i=1}^{k=2} a_i M_i x_i \pmod{M}$$

$$M = (101)(113)$$

$$a_1 = 22 \qquad m_1 = 101$$

$$a_2 = 104 \qquad m_2 = 113 \qquad M_1 = \frac{M}{m_1} = 113 \qquad M_2 = \frac{M}{m_2} = 101$$

$$X = a_1 \bmod m_1 = 22 \bmod 101$$

$$X = a_2 \bmod M_2 = 104 \bmod 113$$

$$X = 104 \bmod 113$$

$$X = 22 \bmod 101$$

$$\gcd(101, 113) = 1$$

Chinese Remainder Theorem

$$113\,s + 101\,t = 1 \quad \Longrightarrow \quad 113\,s = 1 - (101)\,t \equiv 1 \bmod 101$$

$$113\,s \equiv 1 \bmod 101$$

$$s = 113^{-1} \bmod 101$$

$$\Rightarrow \quad 101\,t = 1 - 113\,s \equiv 1 \bmod 113$$

$$101\,t \equiv 1 \bmod 113$$

$$t = 101^{-1} \bmod 113$$

שאלה 2 סעיף א' (3 נק'): מצאו את $101^{-1} \bmod 113$ בעזרת האלגוריתם המורחב של אוקלידס.

$r_0 = \alpha = 113$ $\quad r_1 = b = 101$

$s_0 = 1$ $\quad s_1 = 0$

$t_0 = 0$ $\quad t_1 = 1$

$$\gcd(113, 101) = 1$$

$$\alpha \cdot b = \beta \qquad \text{נתון כי } \beta \text{ שארית חיובית}$$

$$\beta = 12\alpha + 1\beta$$

$$\Rightarrow \quad \exists \; 113^{-1} \bmod 101 \quad \Leftarrow \quad \gcd(101, 113) = 1$$

$$113^{-1} \bmod 101 = 57$$

$$\chi = a_1 M_1 \gamma_1 + a_2 M_2 \gamma_2 \qquad \Longrightarrow$$

$$\gamma_1 = M_1^{-1} \bmod m_1 = 113^{-1} \bmod 101$$

$$\gamma_2 = M_2^{-1} \bmod m_2 = 101^{-1} \bmod 113 .$$

סוף שאלה 2

$$r_{k+1} = r_{k-1} - q_k r_k$$
$$s_{k+1} = s_{k-1} - q_k s_k$$
$$t_{k+1} = t_{k-1} - q_k t_k$$

$k=1$

$r_2 = r_0 - q_1 r_1 = 113 - 1 \cdot 101 = 12$ $\quad q_1 = 1$

$0 \le r_2 < r_1$

$s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1$

$t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1$

$k=2$

$r_3 = r_1 - q_2 r_2 = 101 - 8 \cdot 12 = 5$ $\quad q_2 = 8$

$0 \le r_3 < r_2$

$s_3 = s_1 - q_2 s_2 = 0 - 8 \cdot (1) = -8$

$t_3 = t_1 - q_2 t_2 = 1 - 8(-1) = 9$

$k=3$

$r_4 = r_2 - q_3 r_3 = 12 - q_3 \cdot 5 = 2$

$s_4 = s_2 - q_3 s_3 = 17$

$t_4 = t_2 - q_3 t_3 = -19.$

$k=4$

$r_5 = r_3 - q_4 r_4 = 5 - q_4 \cdot 2 = 1$ $\quad q_4 = 2$

$s_5 = s_3 - q_4 s_4 = -42$

$t_5 = t_3 - q_4 t_4 = 47$

! אין צורך

$k=5$

$r_6 = r_4 - q_5 r_5 = 2 - q_5 \cdot 1 = 0$ $\quad q_5 = 2$

אלגוריתם עוצר

$\therefore$ סיימנו

$t = t_5 = 47$, $d = r_5 = 1$, $s = s_5 = -42$

$$sa + tb = d$$

$$-42(13) + 47(101) = 1$$

$$-42(113) = 1 - 47(101)$$

$$\Rightarrow (-42)(113) \equiv 1 \mod 101$$

$$113^{-1} \equiv (-42) \mod 101 = 59 \mod 101$$

$$47(101) = 1 + 42(113)$$

$$47(101) \equiv 1 \mod 113$$

$$101^{-1} \equiv 47 \mod 113$$

$$113^{-1} \equiv 59 \mod 101$$

$$101^{-1} \equiv 47 \mod 113$$

$$X = a_1 M_1 y_1 + a_2 M_2 y_2$$

$$y_1 = M_1^{-1} \mod m_1 = 113^{-1} \mod 101 = 59$$

$$y_2 = M_2^{-1} \mod m_2 = 101^{-1} \mod 113 = 47$$

$M = (101)(113)$

$$X = 22(113)(59) + (104)(101)(47) \mod 11413$$

$$= 640362 \mod 11413$$

$$= 1234$$

$$X = a_1 \mod m_1 = 22 \mod 101$$

$$X = a_2 \mod m_2 = 104 \mod 113$$

$$1234 \equiv 22 \mod 101$$

$$1234 \equiv 104 \mod 113$$

$$\phi(a) = \{ m \mid gcd(a,m) = 1 \}$$

gcd(1,3) = 1

gcd(2,3) = 1

$\phi(3) = 2 \iff \{1,2\}$: 3 - عدد صحيح موجب N.

التالي:

$\{1,3,5,7,9,11,15,17,19,21,23,25\}$: 26 - عدد صحيح موجب N.

gcd(19,26) = 1

gcd(9,26) = 1

$\phi(26) = 12 \iff$

$\phi(3) = 2 \quad \phi(26) = 12$

$gcd(3,12) = 3 \neq 1$.

$\phi(3 \cdot 12) \neq \phi(12)\phi(3)$

مبرهنة 8 - لتكن ϕ دالة أويلر. عندئذ

لكل عددين صحيحين موجبين a, b أوليين فيما بينهما

$\phi(ab) = \phi(a) \cdot \phi(b)$

(*) $\alpha = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ ——— $p_1, p_2, \ldots, p_k$ أعداد أولية موجبة مختلفة مثنى مثنى و $e_i \geq 1$.

توجد أعداد أولية موجبة وحيدة

α على الأقل.

برهان - نبرهن أولا وجود أعداد أولية موجبة وحيدة على الأقل تحقق (*)

لكل $a \geq 1$ (عدد صحيح موجب) نبرهن بالتدريج على a

$\Rightarrow \quad 4^9 \bmod 7 = (2)(4) \bmod 7 = 8 \bmod 7 = 1 \bmod 7$

$(4^3)^2 \bmod 7 = 1936 \bmod 7 = 1936 - 7\left\lfloor \frac{1936}{7} \right\rfloor = 1936 - 7(276) = 4$

$(4^3) \bmod 7 = \overline{4 \cdot 4} \bmod 7 = 2$

$4^9 \bmod 7 = (4^3)^2 (4^3) \bmod 7$

$4^9 \bmod 7$

$(31^5)(31) \bmod 5 = (1)(1) \bmod 5 = 1 \bmod 5 \quad \therefore 1 > 5$

$31^6 \bmod 5 = (31^5)(31) \bmod 5$

$31^5 \bmod 5 = 31^{\text{מספר זוגי}} \bmod 5 = \overline{-1} \bmod 5$

$\therefore$ מספר זוגי $p = 5$ ו α יוצר של $\mathbb{Z}_p^*$ אזי α^{p-1} הוא שורש יחידה מסדר p.

$\alpha^{p-1} \equiv 1 \bmod p \quad (4)$

$\alpha^{-1} \equiv \alpha^{p-2} \bmod p \quad (3)$

$31 \bmod 5$ אזי הופכי של

$\alpha \equiv \alpha \bmod p \quad (1)$

$\alpha^p \equiv \alpha \bmod p \quad (2)$

$\therefore$ נתון α יוצר של $\mathbb{Z}_p^*$ ו p ראשוני אי זוגי

$\phi(60) = \phi(12 \cdot 5) = \phi(12)\phi(5)$

$g^{\phi(12 \cdot 5)} = 7^0$

$\phi(121) = 4 \quad \Longleftarrow \quad \{1, 5, 7, 11\} : 12 - 6 \text{ מספרים } 5 \text{ ו } 60 \text{ זרים}$

$\phi(5) = 4 \quad \Longleftarrow \quad \{1, 2, 3, 4\} : 5 - 6 \text{ מספרים } 5 \text{ ו } 60 \text{ זרים}$

$\phi(60) = \phi(12 \cdot 5) = \phi(12)\phi(5) = 4 \cdot 4 = 16$

$\alpha = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ הוא α יוצר של $\mathbb{Z}_n^*$ אם ורק אם:

$\phi(\alpha) = \left(p_1^{e_1} - p_1^{e_1 - 1}\right)\left(p_2^{e_2} - p_2^{e_2 - 1}\right) \cdots \left(p_n^{e_n} - p_n^{e_n - 1}\right)$. כאשר

הוכחה של משפט פרמה הקטן

__חלק ①__ נוכיח כי $a^p \equiv a \bmod p$.

נניח כי p מספר ראשוני.

נוכיח את הטענה בדרך אינדוקציה.

__שלב הבסיס__ $a=0$.

$$0^p \equiv 0 \bmod p$$

כלומר $0 \equiv 0 \bmod p$ מתקיים.

__שלב הצעד:__ נניח כי $a^p \equiv a \bmod p$ עבור a שלם.

לפי הנחת האינדוקציה.

נוכיח כי הטענה מתקיימת עבור $a+1$:

$$(a+1)^p = \sum_{k=0}^{p} a^{p-k} \binom{p}{k}$$

$$= a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a^1 + a^0$$

$$= a^p + p a^{p-2} + \frac{p(p-1)}{2} a^{p-1} + \cdots + pa + 1.$$

$$(a+1)^p \bmod p = \left(a^p + p a^{p-2} + \frac{p(p-1)}{2} a^{p-1} + \cdots + pa + 1.\right) \bmod p$$

כל הכפולות של p, מחולק p שווה ל-0, כלומר $kp \bmod p = 0$

$$(a+1)^p \bmod p = \left(a^p \bmod p\right) + \left(p a^{p-2} + \frac{p(p-1)}{2} a^{p-1} + \cdots + pa\right) \bmod p + 1 \bmod p$$

$$= a^p \bmod p + p\left(a^{p-2} + \frac{p-1}{2} a^{p-1} + \cdots + a\right) \bmod p + 1 \bmod p$$

$$\Rightarrow (a+1)^p \bmod p = (a^p + 1) \bmod p = a^p \bmod p + 1 \bmod p$$

לפי הנחת האינדוקציה: $a^p \bmod p = a \bmod p$.

$$(a+1)^p \bmod p = a \bmod p + 1 \bmod p = (a+1) \bmod p$$

כפי שצ״ל

② נוכיח כי $a^{p-1} \equiv 1 \mod p$.

① לפי $a^p \equiv a \mod p$ ——— (#)

$\gcd(a,p)=1$ כי p ראשוני $\Leftarrow$ $\exists\ a^{-1} \mod p$.

נכפול את (#) ב a^{-1} ונקבל

$$a^p a^{-1} \equiv a a^{-1} \mod p$$

$$a^{p-1} \equiv 1 \mod p . \quad \text{———} \ (*)$$

③ באותה מידה: $\gcd(a,p)=1 \Leftarrow \exists\ a^{-1} \mod p$

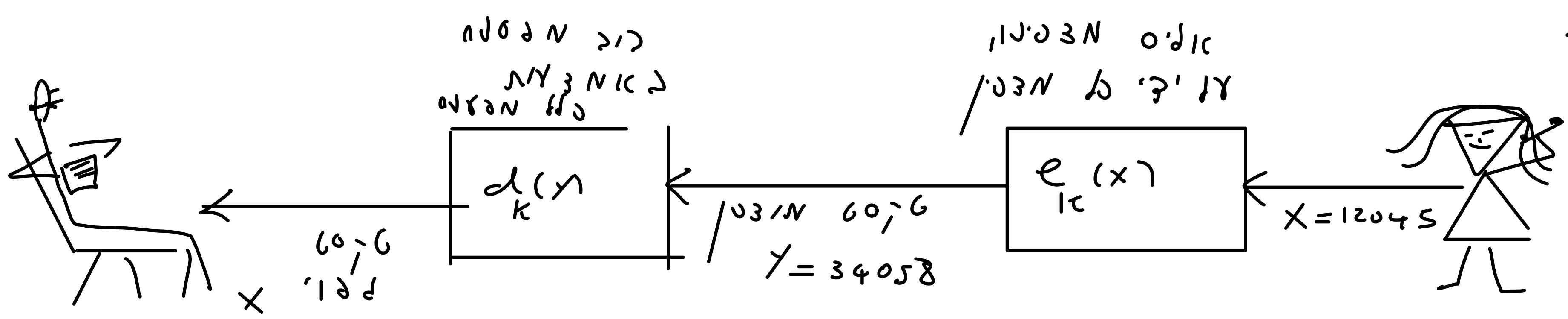
נכפול (*) ב- a^{-1}:

$$a^{-1} a^{p-1} \equiv a^{-1} \mod p$$

$$a^{p-2} \equiv a^{-1} \mod p .$$

צופן RSA

דוגמה:



$ab \equiv 1 \mod \phi(n) \Rightarrow a = b^{-1} \mod \phi(n)$

הגדרה של צופן RSA

יהיו p, q ראשוניים. $n=pq$.

נגדיר מערכת של RSA כדלקמן:

$K=(n, p, q, a, b)$ $\quad n=pq \quad$ $ab \equiv 1 \mod \phi(n)$

וכלל מצפין לכל מספר טבעי x נגדיר:

$$e_k(x) = x^b \mod n$$

וכלל מפענח נגדיר

$$d_k(y) = y^a \mod n .$$

(2)

$$\lambda = 17(19) = 323$$

$$\phi(n) = \phi(pq) = (p-1)(q-1)$$

$$= 16(18)$$

$$= 288$$

(3) כן ? b : מכיוון ש

$$b = 301 \qquad \gcd(b, \phi(n)) = \gcd(301, 288) = 1$$

$p = 17,\ q = 19.$ (1) כיוון ש : N נתון

---

(5)

$$d = b^{-1} \bmod \phi(n), \quad \alpha = b^{r}$$

$$N = p_1^{e_1} \cdots p_k^{e_k}$$

$$\Rightarrow \phi(N) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right)$$

$$N = p = \prod_{i=1}^{e_i = 1} p_i$$

$$\phi(p) = \left(p_1^{1} - p_1^{1-1}\right) = (p-1)$$

(6) נתון n מספר טבעי גדול. x נבחר באקראי כך ש $\gcd(x, n) = 1$. נגדיר $y = e(x)$ מעתיק זה (b, n).

---

(1) כיוון ש $p = 17,\ q = 19.$

$$\gcd(b, \phi(n)) = \gcd(301, 288) = 1$$

(2) $n = pq$ נתון (B) כיוון ש $\phi(n)$:

$$\phi(n) = \phi(pq) \overset{\text{נתון}}{=\!=} \phi(p)\,\phi(q) = (p-1)(q-1)$$

(3) כיוון ש b הוא מספר טבעי $\gcd(\phi(n), b) = 1$ (B) כיוון ש b הוא מספר טבעי $-$ מספר זה α הוא מספר טבעי כך ש :

(4)

(A) כיוון ש X הוא קבוצה סופית נתונה (B) כיוון ש P, Q הם מספרים ראשוניים גדולים זהים ב 100 ספרות. (1)

$a = b^{-1} \bmod \phi(n) = 3d1 \bmod 288$ (4)

(ג'ו ז'ור פה פ.מ.ומ קטנים)

ס'ורך /בזוא לס'כו'ן (b,n) מלוה ביה (5)

. a אוי מלוה ,, ך ביה ליה