שיעור 5
צופן RSA

5.1 משפטים של מספרים ראשוניים

משפט 5.1 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.
נניח כי $\{p_1,\ldots,p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.
נגדיר השלם $M=(p_1\cdot p_2\cdot\ldots\cdot p_n)+1$.
לפי משפט הפירוק לראשוניים (ראו משפט 1.3 למעלה או משפט 5.2 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.
M לא מספר ראשוני בגלל ש- $M>p_i$ לכל $1\leq i\leq n$.
גם לא קיים מספפ ראשוני p_i אשר מחלק את M. הרי

$$M \,\%\, p_i = 1 \quad\Rightarrow\quad p_i \nmid M\ .$$

הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים. ■

משפט 5.2 משפט הפירוק לראשוניים

(ראו משפט 1.3) לכל מספר שלם n קיימים שלמים e_i וראשוניים p_i כך ש-

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

הוכחה: אינדוקציה. ■

משפט 5.3 נוסחה לפונקצית אוילר

(ראו משפט 1.4) לכל מספר שלם n בעל פירוק לראשוניים

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

פונקציית אוילר ניתנת על ידי

$$\phi(n)=\prod_{i=1}^{k}\left(p_i^{e_i}-p_i^{e_i-1}\right)=\left(p_1^{e_1}-p_1^{e_1-1}\right)\left(p_2^{e_2}-p_2^{e_2-1}\right)\ldots\left(p_k^{e_k}-p_k^{e_k-1}\right)$$

דוגמה 5.1

חשבו את $\phi(24)$

פתרון:

$$24 = 2^3 3^1 \ .$$

לכן

$$\phi(24) = (2^3 - 2^2)(3^1 - 3^0) = (8-4)(3-1) = 8 \ .$$

■

משפט 5.4

אם p מספר ראשוני אז

$$\phi(p) = p - 1 \ .$$

הוכחה: תרגיל בית. ■

משפט 5.5

אם p מספר ראשוני אז

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

הוכחה: תרגיל בית. ■

משפט 5.6

אם s,t שלמים זרים (כלומר $\gcd(s,t)=1$) אז

$$\phi\left(s \cdot t\right) = \phi(s) \cdot \phi(t) \ .$$

הוכחה: תרגיל בית. ■

משפט 5.7

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p \cdot q) = (p-1)(q-1) \ .$$

הוכחה: תרגיל בית. ■

משפט 5.8 המשפט הקטן של פרמה

אם p מספר ראשוני ו- $a \in \mathbb{Z}_p$. אז התנאים הבאים מתקיימים:

.1 $a^p \equiv a \mod p$

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

.3 $a^{-1} \equiv a^{p-2} \mod p$

הוכחה:

טענה 1. נוכיח באינדוקציה.

<u>בסיס:</u>

עבור $a=0$ הטענה $0^p \equiv 0 \mod p$ מתקיימת.

<u>מעבר:</u>

נניח כי הטענה מתקיימת עבור a.

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

ההנחת האינדוקציה אומרת ש- $a^p \equiv a \mod p$ לכן

$$(a+1)^p \mod p \equiv a^p + 1 \mod p \equiv (a+1) \mod p$$

כנדרש.

טענה 2. $\gcd(a,p)=1$ לפיכך קיים איבר הופכי $a^{-1} \in \mathbb{Z}_p$. נכפיל $a^p \equiv 1 \mod p$ ב- a^{-1} אשר הוכחנו בסעיף הקודם:

$$a^{-1}a^p \equiv a^{-1} \cdot a \mod p \qquad \Rightarrow \qquad a^{p-1} \equiv 1 \mod p \ .$$

טענה 3.

$$a^{p-1} \equiv 1 \mod p \qquad \Leftrightarrow \qquad 1 \equiv a^{p-1} \mod p \quad \Rightarrow \quad a^{-1} \equiv a^{p-2} \mod p \ .$$

■

משפט 5.9 משפט אוילר

אם a,n שלמים ו- $\gcd(a,n)=1$ אז

$$a^{\phi(n)} \equiv 1 \mod n \ .$$

משפט 5.10

אם a,n שלמים ו- $\gcd(a,n)=1$ אז

$$a^{-1} \equiv a^{\phi(n)-1} \mod n \ .$$

דוגמה 5.2

חשבו את האיבר ההופכי ל- 5 ב- $\mathbb{Z}_{11}$.

פתרון:

לפי משפט פרמט 5.8:

$$5^{-1} = 5^{11-2} \mod 11 = 5^9 \mod 11 \ .$$

לפי הנוסחת לשארית 1.2 :

$$5^9 \ \% \ 11 = 5^9 - 11 \left\lfloor \frac{5^9}{11} \right\rfloor = 9$$

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$.

■

5.2 משפט השאריות הסיני

משפט 5.11 משפט השאריות הסיני

יהיו $m_1, m_2, \ldots, m_r$ שלמים אשר זרים בזוגות ויהיו $a_1, a_2, \ldots, a_r$ שלמים. למערכת של יחסים שקילות

$$\begin{aligned} x =& a_1 \mod m_1 \ , \\ x =& a_2 \mod m_2 \ , \\ &\vdots \\ x =& a_r \mod m_r \ , \end{aligned}$$

קיים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ שניתן על ידי

$$x = \sum_{i=1}^{r} a_i M_i y_i \mod M$$

כאשר $M_i = \dfrac{M}{m_i}$ ו- $y_i = M_i^{-1} \mod m_i$ לכל $1 \leq i \leq r$.

דוגמה 5.3

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

$$\begin{aligned} x =& 22 \mod 101 \ , \\ x =& 104 \mod 113 \ . \end{aligned}$$

פתרון:

$$a_1 = 22 \ , \qquad a_2 = 104 \ , \qquad m_1 = 101 \ , \qquad m_2 = 113 \ .$$

$$M = m_1 m_2 = 11413 \ , \qquad M_1 = \frac{M}{m_1} = 113 \ , \qquad M_2 = \frac{M}{m_2} = 101 \ .$$

בעזרת הקוד-פיתון `modularinverse.py`

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

$$x = 22 \cdot \left(\frac{101 \cdot 113}{101}\right) \cdot$$

ו-

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

$$\begin{aligned} x =& a_1 M_1 y_1 + a_2 M_2 y_2 \mod M \\ =& 22 \cdot 113 \cdot 59 + 104 \cdot 111 \cdot 47 \mod 11413 \\ =& 640362 \mod 11413 \\ =& 1234 \ . \end{aligned}$$

■

5.3 אלגוריתם RSA

צופן RSA הומצא בשנה 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman .

הגדרה 5.1 צופן RSA

יהי $n = pq$ כאשר p, q מספרים ראשוניים שונים. תהי הקבוצת טקסט גלוי $P = \mathbb{Z}_n$, והקבוצת טקסט מוצפן $C = \mathbb{Z}_n$. נגדיר קבוצת המפתחות

$$K = \left\{ (n, p, q, a, b) \middle| ab = 1 \mod \phi(n) \right\}$$

לכל $k = (n, p, q, a, b) \in K$, ולכל $x \in P$ ו- $y \in C$ נגדיר כלל מצפין

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

ונגדיר כלל מפענח

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

הערכים של n ו- b הם ערכים ציבוריים בעוד p, q, a ערכים סודיים.

משפט 5.12 קריפטו-מערכת RSA ניתן לפענוח

יהי $n = pq$ מספרים ראשוניים שונים, $a, b \in \mathbb{Z}$ שלמים חיובים כך ש- $ab = 1 \mod \phi(n)$.
אם $x \in \mathbb{Z}_n$ אז

$$\left(x^b\right)^a = x \mod n \ .$$

הוכחה: נתון כי $ab = 1 \mod \phi(n)$.
לפי משפט 5.7, $\phi(n) = \phi(pq) = (p-1)(q-1)$.
ז"א

$$ab = 1 \mod \phi(n) = 1 \mod (p-1)(q-1)$$

לכן קיים $t \in \mathbb{Z}$ כך ש-

$$ab - 1 = t(p-1)(q-1) \ .$$

לכל $z \neq 0 \in \mathbb{Z}$ לפי משפט 5.8, $z^{p-1} = 1 \mod p$. בפרט

$$x^{ab-1} = x^{t(p-1)(q-1)} = \left(x^{t(q-1)}\right)^{p-1} = y^{p-1}$$

כאשר $y = x^{t(q-1)}$. מכאן $x^{ab-1} = 1 \mod p$..

משיקולות של סיימטריה באותה מידה $x^{ab-1} = 1 \mod q$..

לכן $x^{ab-1} - 1 = 0 \mod p$ ו- $x^{ab-1} - 1 = 0 \mod q$..

מכיוון ש- p ו- q זרים אז

$$x^{ab-1} - 1 = 0 \mod (pq) \ .$$

לפיכך

$$x^{ab-1} = 1 \mod (pq) \ .$$

נכפיל ב- x ונקבל

$$(x^a)^b = x \mod (pq) \ .$$

ז"א הוכחנו כי לכל טקסט גלוי x, אם נצפין אותו ואז אחר כך נפענח את הטקסט מוצפן המתקבל מאלגוריתם RSA, נקבל אותו טקסט גלוי המקורי בחזרה. ■

הגדרה 5.2 אלגוריתם RSA

<u>שלב הרכבת המפתח</u>

נניח שאליס (A) שולחת הודעה לבוב (B).

[1] B יוצר שני מספרים ראשוניים גדולים שונים, p ו- q בסדר גודל של 100 ספרות דצמליות.

[2] B מחשב $n = pq$ ו- $\phi(n) = (p-1)(q-1)$.

[3] B בוחר במספר שלם באופן מקרי $(0 \leq b \leq \phi(n))$ כך ש- $\gcd(b, \phi(n)) = 1$.

[4] B מחשב a כך ש- $a = b^{-1} \mod \phi(n)$ בעזרת האלגוריתם של אוקלידס, (ראו כלל 1.10) ולכן $0 \leq a < \phi(n)$.

[5] B שומר את המפתח ציבורי (b, n) בכתובת קובץ ציבורי, ושומר על המפתח פענוח הפרטי (a, p, q) סודי.

בניית מפתח עשוי פעם אחת.

<u>שלב הצפנה</u>

[6] אליס (A) קוראת את המפתח הצפנה (הציבורי) $k = (b, n)$ מכתובת קובץ הציבורי.

[7] בכדי להצפין הודעה x, $(0 \leq x < n)$ אליס (A) מחשבת $y = x^b \mod n$.

[8] A שולחת טקסט מוצפן ל- B.

[9] בכדי לפענח את הטקסט מוצפן y, בוב (B) משמש במפתח הפרטי שלו $k^{-1} = (a, p, q)$ ומחשב $x = y^a \mod n$.

דוגמה 5.4

בוב בוחר ב- $p = 101, q = 113$.
אז $n = 11413$.
לפי משפט 5.7

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 100 \cdot 112 = 11200 \ .$$

בוב בוחר באופן מקרי את $b = 569$.
שימו לב: $\gcd(b, \phi(n)) = \gcd(569, 11200) = 1$.

מכאן המפתח פענוח סודי של בוב יהיה a כך ש-

$$\begin{aligned} ab &= 1 \mod \phi(n) \\ &= 1 \mod 11200 \end{aligned}$$

לכן

$$a = b^{-1} \mod 11200 = 1929 \ .$$

כעת בוב שומר את $n = 11413$ ו- $b = 569$ בכתובת ציבורית.

בזמן שאליס רוצה להעביר את הטקסט גלוי $x = 1234$ לבוב, היא צריכה לחשב

$$y = e_k(x) = x^b \mod n = 1234^{569} \mod 11413 = 1932 \ .$$

על קבלת הטקסט מוצפן $y = 1932$ הוא מפענח את זה בעזרת המפתח פענוח סודי שלו a:

$$y^a \mod n = 1932^{1929} \mod 11413 = 1234 \ .$$

דוגמה 5.5

חשבו את $1234^{569} \mod 11413$.

פתרון:

נסמן $x = 1234$ ו- $n = 11413$. כדי לחשב x^{569}, נרשום 569 כסכום של חזקות של 2:

$$569 = 512 + 32 + 16 + 8 + 1 = 2^9 + 2^5 + 2^4 + 2^3 + 2^0 \ .$$

כעת נחשב

$$x^2 \mod n \ , \quad x^4 \mod n \ , \quad x^8 \mod n \ , \quad x^{16} \mod n \ , \quad x^{32} \mod n \ , \quad x^{512} \mod n \ .$$

בעזרת הנוסחה

$$a \mod m = a - m \left\lfloor \frac{a}{m} \right\rfloor$$

והנוסחה

$$ab \mod m = (a \mod m)(b \mod m) \mod m$$

:

$$
\begin{aligned}
(1234)^2 &\mod 11413 && = 4827 \ . \\
(1234)^4 &\mod 11413 = (4827)^2 \mod 11413 && = 5996 \ . \\
(1234)^8 &\mod 11413 = (5996)^2 \mod 11413 && = 1066 \ . \\
(1234)^{16} &\mod 11413 = (1066)^2 \mod 11413 && = 6469 \ . \\
(1234)^{32} &\mod 11413 = (6469)^2 \mod 11413 && = 7903 \ . \\
(1234)^{64} &\mod 11413 = (7903)^2 \mod 11413 && = 5473 \ . \\
(1234)^{128} &\mod 11413 = (5473)^2 \mod 11413 && = 6017 \ . \\
(1234)^{256} &\mod 11413 = (6017)^2 \mod 11413 && = 2253 \ . \\
(1234)^{512} &\mod 11413 = (2253)^2 \mod 11413 && = 8637 \ .
\end{aligned}
$$

לפיכך

$$\begin{aligned} x^{569} =& x^{512}x^{32}x^{16}x^{8}x^{1} \mod n \\ =&(8637\cdot 7903\cdot 6469\cdot 1066\cdot 1234) \mod 11413 \\ =&(8471\cdot 6469\cdot 1066\cdot 1234) \mod 11413 \\ =&(5086\cdot 1066\cdot 1234) \mod 11413 \\ =&(501\cdot 1234) \mod 11413 \\ =&1932 \ . \end{aligned}$$

■

כלל 5.1 פענוח של צופן RSA

המשוואת פענוח

$$x = y^a \mod n$$

ניתן לפתור באמצעות האלגוריתם הבא:

[1] מחשבים $y \mod p$ ו- $a \mod (p-1)$. ואז מחשבים

$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p \ .$$

[2] מחשבים $y \mod q$ ו- $a \mod (q-1)$. ואז מחשבים

$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q \ .$$

[3] בעזרת המשפט השאריות הסיני פותרים את המערכת

$$\begin{aligned} x =& x_1 \mod p \ , \\ x =& x_2 \mod q \ . \end{aligned}$$

דוגמה 5.6

חשבו את $1932^{1929} \mod 11413$ בעזרת המשפט השאריות הסיני.

פתרון:

נסמן $y = 1932$, $n = 11413 = pq$, $p = 101$, $q = 113$, $a = 1929$.

[1]

$$y \mod p = 1932 \mod 101 = 1932 - 101\left\lfloor \frac{1932}{101} \right\rfloor = 13 \ .$$

$$a \mod (p-1) = 1929 \mod 100 = 1929 - 100\left\lfloor \frac{1929}{100} \right\rfloor = 29 \ .$$

$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p = 13^{29} \mod 101 \ .$$

$$29 = 16 + 8 + 4 + 1 = 2^4 + 2^3 + 2^2 + 2^0 \ .$$

$$\begin{aligned}
(13)^2 \mod 101 &= 169 \mod 101 &&= 68 \ . \\
(13)^4 \mod 101 &= (68)^2 \mod 101 = 4624 \mod 101 &&= 79 \ . \\
(13)^8 \mod 101 &= (79)^2 \mod 101 &&= 80 \ . \\
(13)^{16} \mod 101 &= (80)^2 \mod 101 &&= 37 \ .
\end{aligned}$$

לפיכך

$$\begin{aligned}
y^{29} \mod p =& y^{16} y^8 y^4 y^1 \mod p \\
=& (37 \cdot 80 \cdot 79 \cdot 13) \mod 101 \\
=& (31 \cdot 79 \cdot 13 \mod 101) \\
=& (25 \cdot 13) \mod 101 \\
=& 22 \mod 101 \\
=& 22 \ .
\end{aligned}$$

לכן $13^{29} \mod 101 = 22$.

[2]

$$y \mod q = 1932 \mod 113 = 1932 - 113 \left\lfloor \frac{1932}{113} \right\rfloor = 11 \ .$$

$$a \mod (q-1) = 1929 \mod 112 = 1929 - 112 \left\lfloor \frac{1929}{112} \right\rfloor = 25 \ .$$

$$x_1 = (y \mod q)^{a \mod (q-1)} \mod q = 11^{25} \mod 113 \ .$$

$$25 = 16 + 8 + 1 = 2^4 + 2^3 + 2^1 \ .$$

$$\begin{aligned}
(11)^2 \mod 113 &= 121 \mod 113 &&= 8 \ . \\
(11)^4 \mod 113 &= (8)^2 \mod 113 = 64 \mod 113 &&= 64 \ . \\
(11)^8 \mod 113 &= (64)^2 \mod 113 = 4096 \mod 113 &&= 28 \ . \\
(11)^{16} \mod 113 &= (28)^2 \mod 101 &&= 106 \ .
\end{aligned}$$

לפיכך

$$\begin{aligned} y^{25} \mod q =& y^{16}y^8y^1 \mod q \\ =& (106\cdot 28\cdot 11) \mod 113 \\ =& (30\cdot 11) \mod 113 \\ =& 104 \ . \end{aligned}$$

לכן $11^{25} \mod 113 = 104$.

[3] נפתור את המערכת הבאה בעזרת המשפט השאריות הסיני:

$$\begin{aligned} x =& x_1 \mod p = 22 \mod 101 \ , \\ x =& x_2 \mod q = 104 \mod 113 \ . \end{aligned}$$

$$a_1 = 22, \quad a_2 = 104 \ , \quad m_1 = 101 \ , \quad m_2 = 113 \ .$$

$$M = m_1m_2 = 11413 \ , \quad M_1 = \frac{M}{m_1} = 113 \ , \qquad M_2 = \frac{M}{m_2} = 101 \ .$$

$$y_1 = M_1^{-1} \mod m_1 = (113)^{-1} \mod 101 = 59 \ , \qquad y_2 = M_2^{-1} \mod m_2 = (101)^{-1} \mod 113 = 47 \ .$$

$$y = a_1M_1y_1 + a_2M_2y_2 = 640362 \ .$$

$$x \mod n = 640362 \mod 11413 = 1234 \ .$$

■