שיעור 6
צופן RSA

6.1 אלגוריתם RSA

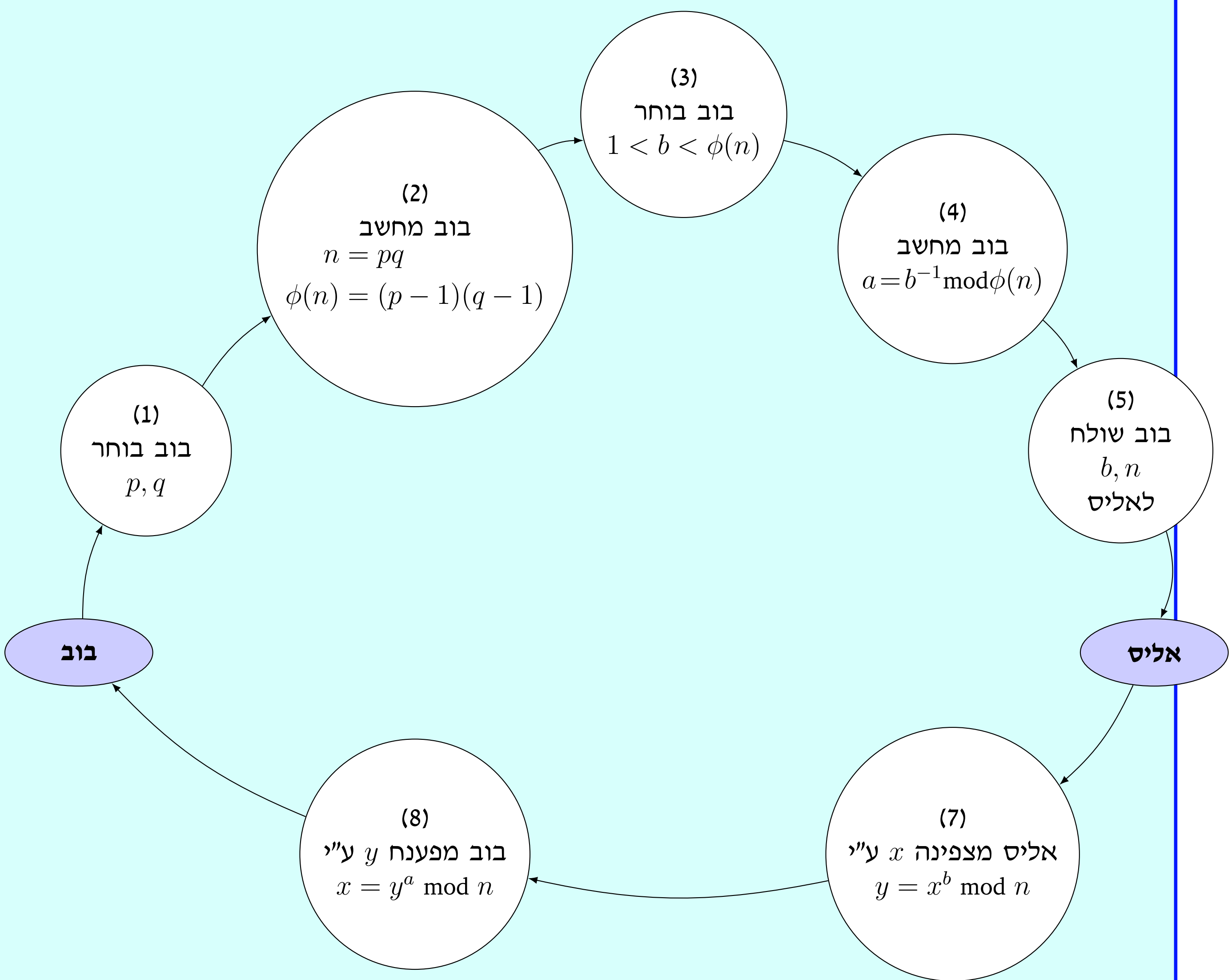
צופן RSA הומצא בשנה 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman .

הגדרה 6.1 צופן RSA

- יהיו p, q מספרים ראשוניים שונים ($p \neq q$).
- יהי $n = pq$.
- יהי b שלם כך ש: $1 < b < \phi(n)$ כאשר $\phi(n)$ הפונקצית אוילר של n.
- נגדיר $a \equiv b^{-1} \pmod{\phi(n)}$.
- אזי
  * המפתח הציבורי של צופן RSA הוא הקבוצה (b, n),
  * המפתח הסודי של צופן RSA הוא הקבוצה (a, p, q).
- יהי $x \in \mathbb{Z}^+$ שלם אי-שלילי.
  * הכלל מצפין מוגדר
$$e_k(x) = x^b \mod n ,$$
  * והכלל מפענח מוגדר
$$d_k(x) = y^a \mod n .$$

עכשיו שנתנו הגדרה מתמטית של הצופן RSA אנחנו נסביר את הסדר של הפעולות של הבניית המפתח, ההצפנה והפענוח באלגוריתם הבא.

הגדרה 6.2 אלגוריתם RSA



נניח שאליס (A) שולחת הודעה לבוב (B).

<u>שלב הבניית המפתח</u>

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

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

[3] B בוחר מספר שלם b באקראי כך שהשני תנאים הבאים מתקיימים:

- $1 < b < \phi(n)$
- $\gcd(b, \phi(n)) = 1$.

[4] B מחשב a לפי $a = b^{-1} \mod \phi(n)$ בעזרת האלגוריתם של אוקלידס (ראו כלל 1.12).

[5] B שולח את המפתח ציבורי (b, n) לאליס, אך בוב לא מגלה את המפתח הסודי (a, p, q) לאליס.

בניית מפתח עשוי פעם אחת.

<u>שלב הצפנה</u>

[6] אליס (A) מקבלת את המפתי הציבורי (b,n) מבוב, ומצפינה את הטקסט הגלוי x עם המחתח ציבורי באמצעות הכלל מצפין
$$y = x^b \bmod n \ .$$

[7] A שולחת את טקסט מוצפן ל- B.

שלב הפענוח

[8] בוב מפענח את הטקסט מוצפן עם המתחת הסודי באמצעות הכלל מפענח $x = y^a \bmod n$ לפי האלגוריתם הבא:
$$x_1 = \left[(y \bmod p)^{a \bmod (p-1)} \right] \bmod p \ ,$$
$$x_2 = \left[(y \bmod q)^{a \bmod (q-1)} \right] \bmod q \ .$$
ואז פוטרים את המערכת הבאה בעזרת המשפט השאריות הסיני:
$$x = x_1 \bmod p \ ,$$
$$x = x_2 \bmod q \ .$$

דוגמה 6.1 (הצפנה ע"י RSA)

בוב בוחר בפרמטרים הבאים כדי לבנות מפתח של צופן RSA:
$(b = 47, p = 127, q = 191)$.

א) חשבו את המפתח הציבורי והמפתח הסודי.

ב) אליס קוראת את המפתח ציבורי ומשתמשת בה כדי להצפין את המספר `2468`.
הוכיחו כי הטקסט מוצפן הוא `10642`.

פתרון:

סעיף א) המפתח הציבורי הוא (b,n). הפרמטר b כבר נתון בשאלה אז נשאר רק לחשב את n:
$$n = pq = 191 \times 127 = 24257 \ .$$
לכן המפתח הציבורי הוא
$$(b,n) = (47, 24257) \ .$$
כעת נחשב את המפתח הסודי (a,p,q). הראשוניים p,q נתונים בשאלה אז נשאר רק לחשב את a לפי הנוסחה $a = b^{-1} \pmod{\phi(n)}$, כאשר $\phi(n)$ הוא הפונקצית אוילר:
$$\phi(n) = \phi(pq) = (p-1)(q-1) = 190 \times 126 = 23940 \ .$$
לפיכך $a = 47^{-1} \mod 23940$.
נחשב את $47^{-1} \mod 23940$ בעזרת האלגוריתם לאיבר ההופכי (ראו משפט 2.9):

Algorithm 4 האלגוריתם לאיבר ההופכי

```
Input: Integers A, B .
r_0 ← A
r_1 ← B
t_0 ← 0
t_1 ← 1
n ← 1
while r_n ≠ 0 do
    q_n ← ⌊ r_{n-1} / r_n ⌋
    r_{n+1} ← r_{n-1} − q_n r_n
    t_{n+1} ← t_{n-1} − q_n t_n
    n ← n + 1
end while
n ← n − 1
if r_n ≠ 1 then
    B has no inverse modulo A
else
    return: t_n                                ▷ t_n = B^{-1} (mod A)
end if
```

נשים $A = 23940, B = 47$. נאתחל את המשתנים של האלגוריתם:

$$r_0 = A = 23940 \ , \qquad r_1 = B = 47 \ ,$$
$$t_0 = 0 \ , \qquad t_1 = 1 \ .$$

אזי האיטרציות של האלגוריתם הם כמפורט למטה:

$q_1 = 509$	$r_2 = 23940 - 509 \cdot 47 = 17$	$t_2 = 0 - 509 \cdot 1 = -509$	שלב $n = 1$:
$q_2 = 2$	$r_3 = 47 - 2 \cdot 17 = 13$	$t_3 = 1 - 2 \cdot (-509) = 1019$	שלב $n = 2$:
$q_3 = 1$	$r_4 = 17 - 1 \cdot 13 = 4$	$t_4 = -509 - 1 \cdot (1019) = -1528$	שלב $n = 3$:
$q_4 = 3$	$r_5 = 13 - 3 \cdot 4 = 1$	$t_5 = 1019 - 3 \cdot (-1528) = 5603$	שלב $n = 4$:
$q_5 = 4$	$r_6 = 4 - 4 \cdot 1 = 0$	$t_6 = -1528 - 4 \cdot (5603) = -23940$	שלב $n = 5$:

לפיכך $47^{-1} \equiv 5603 \pmod{23940}$. לכן התשובה הסופית בשביל a היא:

$$a = 5603 \ .$$

סעיף ב) אליס שולחת את ההודעה כטקסט מוצפן

$$y = x^b \bmod n = 2468^{47} \mod 24257 \ .$$

כדי לחשב את יחס מודולרי של חזקה הזה נשתמש בשיטת הריבועים שעובדת באופן הבא. בהינתן

$$x^b \bmod n \ .$$

רושמים b כצירוף לינארי של חזקות של 2:

$$b=\sum_{i=0}^{k} b_i 2^i \ ,$$

כאשר $b_i=0$ או 1. בעצם $b_k b_{k-1}\cdots b_1 b_0$ הוא הייצוג בינארי של b. אחרי זה אנחנו משחבים את $x^b \bmod n$ באמצעות האלגוריתם הבא:

Algorithm 5 האלגוריתם לשיטת הריבועים

```
Input: Integers x, b_0, ..., b_k, n .
i ← 1
z_0 ← x
while i ≤ k do
    z_i ← z_{i-1}^2 mod n
end while
i ← 1
y ← x
while i ≤ k do
    if b_i = 1 then
        y ← z_i y mod n
    end if
end while
return: y                                   ▷ y = x^b mod n
```

שלב 1) בדוגמה שלנו החזקה היא

$$b=47=32+8+4+2+1=1\left(2^5\right)+0\left(2^4\right)+1\left(2^3\right)+1\left(2^2\right)+1\left(2^1\right)+1\left(2^0\right) \ .$$

אזי הייצוג בינארי של b הוא

$$b=b_5b_4b_3b_2b_1b_0=101111 \ .$$

שלב 2) נאתחל: $z_0=x=2468$.

$$\begin{aligned}
z_1=z_0^2 \bmod n \quad &=(2468)^2 \bmod 24257=2517 \ ,\\
z_2=z_1^2 \bmod n \quad &=(2517)^2 \bmod 24257=4212 \ ,\\
z_3=z_2^2 \bmod n \quad &=(4212)^2 \bmod 24257=9077 \ ,\\
z_4=z_3^2 \bmod n \quad &=(9077)^2 \bmod 24257=15157 \ ,\\
z_5=z_4^2 \bmod n \quad &=(15157)^2 \bmod 24257=20859.
\end{aligned}$$

שלב 3) נאתחל: $y=x=2468$.

$b_1=1$	$y=z_1y \bmod n=(2517)(2468) \bmod 24257=2164$
$b_2=1$	$y=z_2y \bmod n=(4212)(2164) \bmod 24257=18393$
$b_3=1$	$y=z_3y \bmod n=(9077)(2468) \bmod 24257=16587$
$b_4=0$	
$b_5=1$	$y=z_5y \bmod n=(20859)(2468) \bmod 24257=10642$

לכן

לכן השתובה סופיל להטקסט מוצפן הוא:

$$y = 10642 \ .$$

■

לפני לעשות דוגמה של טקסט שהוצפן ע"י RSA אנחנו צריכים ללמוד כלי עזר שמאפשר לנו לפתור את הכלל מפענח: משפט השאריות הסיני.

6.2 משפט השאריות הסיני

משפט השאריות הסיני הוא כלי עזר שמאפשר לנו לפתור את הכלל מפענח של צופן RSA.

משפט 6.1 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

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

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 6.2 (משפט השאריות הסיני)

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

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

פתרון:

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

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

$$y_1 = M_1^{-1} \mod m_1 = 113^{-1} \mod 101 \ , y_2 = M_2^{-1} \mod m_2 = 101^{-1} \mod 113 \ .$$

כדי לחשב את האיברים ההופכיים נשתמש בהאלגוריתם המוכלל של אוקלידס (אלגוריתם 2 למעלה).

נסמן $A = 113, B = 101$.

$$\begin{aligned} r_0 =& A = 113 \ , \qquad & r_1 = B = 101 \ , \\ s_0 =& 1 \ , & s_1 = 0 \ , \\ t_0 =& 0 \ , & t_1 = 1 \ . \end{aligned}$$

שלב $k=1$:	$r_2 = 113 - 1\cdot 101 = 12$	$s_2 = 1 - 1\cdot 0 = 1$	$t_2 = 0 - 1\cdot 1 = -1$	$q_1 = 1$
שלב $k=2$:	$r_3 = 101 - 8\cdot 12 = 5$	$s_3 = 0 - 8\cdot 1 = -8$	$t_3 = 1 - 8\cdot(-1) = 9$	$q_2 = 4$
שלב $k=3$:	$r_4 = 12 - 2\cdot 5 = 2$	$s_4 = 1 - 2\cdot(-8) = 17$	$t_4 = -1 - 2\cdot(9) = -19$	$q_3 = 2$
שלב $k=4$:	$r_5 = 5 - 2\cdot 2 = 1$	$s_5 = -8 - 2\cdot 17 = -42$	$t_5 = 9 - 2\cdot(-19) = 47$	$q_4 = 2$
שלב $k=5$:	$r_6 = 2 - 2\cdot 1 = 0$	$s_6 = 17 - 2\cdot(-42) = 101$	$t_6 = -19 - 2\cdot(47) = -113$	$q_5 = 2$

לכן הפירוק אוקלידס של $A=113$ ו- $B=101$ הוא

$$sA + tB = d$$

כאשר

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

מכאן

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

ו-

$$113^{-1} \equiv -42 \mod 101 \equiv 59 \mod 101\ .$$

לכן

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

ו-

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

נציב אותם לנוסחה $x = a_1M_1y_1 + a_2M_2y_2 \mod M$ ונקבל את התשובה הסופית הבאה:

$$\begin{aligned} x =& a_1M_1y_1 + a_2M_2y_2 \mod M \\ =& 22\cdot 113\cdot 59 + 104\cdot 111\cdot 47 \mod 11413 \\ =& 640362 \mod 11413 \\ =& 1234\ . \end{aligned}$$

■

דוגמה 6.3 (פענוח של צופן RSA)

הדוגמה הזאת היא ההמשך של דוגמה 6.1.

בדוגמה 6.1 קיבלנו את הפרמטרים $b=47$, $p=127$, $q=191$ וחישבנו $n=24257$, $\phi(n)=23940$ ו- $a=b^{-1} \mod n = 5603$. בעזרת המפתח הציבורי $(b,n)=(47,24257)$ אנחנו חישבנו את הטקסט מוצפן של $x=2468$ על פי הכלל מצפין וקיבלנו את התשובה $y=x^b \mod n = 10642$. כעת נקח את הטקסט מוצפן $y=10642$ והמפתח הסודי $(a,p,q)=(5603,127,191)$ ונוכיח כי הטקסט הגלוי, על פי הכלל מפענח $x=x^a \mod n$, הוא $x=2468$.

פתרון:

$$y \mod p = 10642 \mod 127 = 101\ , \qquad a \mod (p-1) = 5603 \mod 126 = 59\ .$$

לכן
$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p = 101^{59} \mod 127 = 55$$
(ניתן לחשב זה לפי $101 \times 101^2 \times 101^8 \times 101^{16} \times 101^{32}$.)

$$\begin{aligned}
(101)^2 & & \equiv 41 \mod 127\\
(101)^4 &\equiv (41)^2 \mod 127 & \equiv 30 \mod 127\\
(101)^8 &\equiv (30)^2 \mod 127 & \equiv 11 \mod 127\\
(101)^{16} &\equiv (11)^2 \mod 127 & \equiv 121 \mod 127\\
(101)^{32} &\equiv (121)^2 \mod 127 & \equiv 36 \mod 127
\end{aligned}$$

לכן
$$101^{59} \mod 127 = (101)(41)(11)(121)(36) \mod 127 = 55 \ .$$

$$y \mod q = 10642 \mod 191 = 137 \ , \qquad a \mod (p-1) = 5603 \mod 190 = 93 \ .$$

לכן
$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q = 137^{93} \mod 191 = 176$$
(ניתן לחשב זה לפי $137 \times 137^4 \times 137^8 \times 137^{16} \times 137^{64}$.)

$$\begin{aligned}
(137)^2 & & \equiv 51 \mod 191\\
(137)^4 &\equiv (51)^2 \mod 191 & \equiv 118 \mod 191\\
(137)^8 &\equiv (118)^2 \mod 191 & \equiv 172 \mod 191\\
(137)^{16} &\equiv (172)^2 \mod 191 & \equiv 170 \mod 191\\
(137)^{32} &\equiv (170)^2 \mod 191 & \equiv 59 \mod 191\\
(137)^{64} &\equiv (59)^2 \mod 191 & \equiv 43 \mod 191
\end{aligned}$$

לכן
$$137^{93} \mod 191 = (137)(118)(172)(170)(43) \mod 191 = 176 \ .$$

בנוסף
$$y \mod q = 9625 \mod 127 = 100 \ , \qquad a \mod (q-1) = 5603 \mod 126 = 59 \ .$$

לכן
$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q = 100^{59} \mod 127 = 87$$

לכן עלינו לפתור את המערכת
$$\begin{aligned}
x &= x_1 \mod p = 55 \mod 127\\
x &= x_2 \mod q = 176 \mod 191
\end{aligned}$$
בעזרת המשפט השאריות הסיני. נסמן $a_1 = 55$, $m_1 = 127$, $a_2 = 176$, $m_2 = 191$.
$$M = m_1 m_2 = (191)(127) = 24257 \ , \qquad M_1 = \frac{M}{m_1} = 191 \ , \qquad M_2 = \frac{M}{m_2} = 127 \ .$$
כעת נחשב $y_1 = M_1^{-1} \mod m_1 = 191^{-1} \mod 127$ ו- $y_2 = M_2^{-1} \mod m_2 = 127^{-1} \mod 191$.

<u>שיטה 1</u>

$a=191, b=127$.

$$\begin{aligned} r_0 =& a=191\ , & r_1 &= b = 127\ ,\\ s_0 =& 1\ , & s_1 &= 0\ ,\\ t_0 =& 0\ , & t_1 &= 1\ . \end{aligned}$$

שלב $k=1$:	$r_2=191-1\cdot 127=64$	$s_2=1-1\cdot 0=1$	$t_2=0-1\cdot 1=-1$	$q_1=1$
שלב $k=2$:	$r_3=127-1\cdot 64=63$	$s_3=0-1\cdot 1=-1$	$t_3=1-1\cdot(-1)=2$	$q_2=1$
שלב $k=3$:	$r_4=64-1\cdot 63=1$	$s_4=1-1\cdot(-1)=2$	$t_4=-1-1\cdot(2)=-3$	$q_3=1$
שלב $k=4$:	$r_5=63-63\cdot 1=0$	$s_5=-1-63\cdot(2)=-127$	$t_5=2-63\cdot(-3)=191$	$q_4=63$

$$\gcd(a,b)=r_4=1\ , \qquad s=s_4=2\ , \qquad t=t_4=-3\ .$$

$$sa+tb=2(191)-3(127)=1\ .$$

לכן

$$\begin{aligned} &191^{-1}\equiv 2 \mod 127\\ &127^{-1}\equiv(-3) \mod 191 \equiv 188 \mod 191\ . \end{aligned}$$

<u>שיטה 2</u>

נחשב $y_1=191^{-1} \mod 127$ ו- $y_2=127^{-1} \mod 191$ בעזרת האלגוריתם של אוקליד:

$$\begin{aligned} 191 =& 127\cdot 1+64\\ 127 =& 64\cdot 1+63\\ 64 =& 63\cdot 1+1\\ 63 =& 1\cdot 63+0\ . \end{aligned}$$

לכן $\gcd(191,127)=1$.

$$\begin{aligned} 1 =& 64-63\cdot 1\\ =& 64-(127-64\cdot 1)\\ =& 64\cdot 2-127\cdot 1\\ =& (191-127\cdot 1)\cdot 2-127\\ =& 191\cdot 2+127\cdot(-3)\ . \end{aligned}$$

לכן

$$\begin{aligned} y_1 &= M_1^{-1} \mod m_1 &= 127^{-1} \mod 191 &\equiv 188 \mod 191\\ y_2 &= M_2^{-1} \mod m_2 &= 191^{-1} \mod 127 &\equiv 2 \mod 127\ . \end{aligned}$$

נחשב

$$y_1=M_1^{-1} \mod m_1=127^{-1} \mod 191=188\ , \qquad y_2=M_2^{-1} \mod m_2=191^{-1} \mod 127=2\ .$$

לכן

$$\begin{aligned} y =& a_1 M_1 y_1 + a_2 M_2 y_2 \\ =& 55(191)(2) + 176(127)(188) \mod 24257 \\ =& 4223186 \mod 24257 \\ =& 2468 \ . \end{aligned}$$

■

6.3 המשפט הקטן של פרמה

משפט 6.2 משפט עזר 1

אם p ו- k ראשוני עבורו $1<k<p$ אז

$$p \mid \binom{p}{k}$$

כאשר $\binom{p}{k}$ המקדם הבינומי.

הוכחה: ראשית נרשום את הביטוי המפורש של $\binom{p}{k}$:

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} \ .$$

מכאן:

$$k!\binom{p}{k} = \frac{p!}{(p-k)!} = p(p-1)(p-2)\cdots(p-k+1) \ .$$

ברור ש-

$$p \mid p(p-1)(p-2)\cdots(p-k+1) = k!\binom{p}{k}$$

לכן $p \mid k!\binom{p}{k}$. מכיוון ש- p מספר ראשוני ו- $1<k<p$ אז $p \nmid k!$. לכן בהכרח:

$$p \mid \binom{p}{k} \ .$$

■

משפט 6.3 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 את טענה **1.** דרך אינדוקציה.

<u>שלב הבסיס:</u>

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

<u>שלב מעבר:</u>

נניח כי הטענה מתקיימת עבור השלם a, כלומר: $a^p \equiv a \bmod p$. זה מהווה את ההנחת האינדוקציה שלנו. נוכיח בעזרת ההנחת האינדוקציה הזו כי $(a+1)^p \equiv (a+1) \bmod p$ באופן הבא:

ראשית נפתח את $(a+1)^p$ לפי הטור בינומי:

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

מכאן:

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

ממשפט עזר 1 לכל $1 < k < p$ מתקיים $a^{p-k}\binom{p}{k} \equiv 0 \bmod p$ לפיכך:

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

כעת נציב את ההנחת האינדוקציה שאומרת: $a^p \equiv a \bmod p$ ואז נקבל כי:

$$(a+1)^p \bmod p \equiv a \bmod p + 1 \bmod p \equiv (a+1) \bmod p \ .$$

טענה 2. מכיוון ש- p ראשוני אז לכל שלם a מתקיים $\gcd(a,p)=1$. לפיכך מובטח לנו שהאיבר הופכי $a^{-1} \in \mathbb{Z}_p$ קיים. נכפיל את היחס $a^p \equiv a \mod p$ 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.

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

■

6.4 משפט: צופן RSA ניתן לפענוח

משפט 6.4 צופן RSA ניתן לפענוח

יהיו p,q מספרים ראשוניים שונים ויהי $n=pq$. יהי (b,n) מפתח ציבורי של צופן RSA, כאשר $1<b<\phi(n)$, ויהי (a,p,q) מפתח סודי של צופן RSA כאשר $a \equiv b^{-1} \bmod \phi(n)$. אם

$$e(x) = x^b \bmod n$$

הוא הכלל מצפין של צופן RSA, כאשר x שלם, ואם

$$y(x) = y^a \bmod n$$

הוא הכלל מפענח של צופן RSA, כאשר y שלם, אז

$$d\left(e(x)\right) \equiv x \bmod n$$

לכל מספר שלם x.

הוכחה:
ראשית נציין כי
$$ab \equiv 1 \mod \phi(n) \quad \Rightarrow \quad ab-1 \equiv 0 \mod \phi(n) \ .$$
ז"א $\phi(n)$ מחלק את $ab-1$. לכן קיים שלם t כך ש:
$$ab-1 = t\phi(n) \ .$$
לפי משפט 2.5, בגלל ש- p,q הם מספרים ראשוניים אזי
$$\phi(n) = \phi(pq) = (p-1)(q-1) \ .$$
לכן
$$ab-1 = t(p-1)(q-1) \ . \tag{*1}$$
מכאן אפשר לרשום כי:
$$x^{ab-1} = x^{t(p-1)(q-1)} \ . \tag{*2}$$
בשלב הזה נגדיר $y \triangleq x^{t(q-1)}$ ואז אפשר לראשום את משוואה (*2) באופן הבא:
$$x^{ab-1} = y^{p-1} \ . \tag{*3}$$
באותה מידה אם נגדיר $z \triangleq z^{t(p-1)}$ ואז אפשר לראשום את משוואה (*2) באופן הבא:
$$z^{ab-1} = z^{q-1} \ . \tag{*4}$$
כעת נשתמש במשפט הקטו של פרמה. כלומר, מכיוון ש- p מספר ראשוני ו- y שלם, אזי
$$\begin{aligned} y^{p-1} \overset{\text{פרמה}}{\equiv} 1 \bmod p \quad &\xRightarrow{\text{משוואה (*3)}} \quad \left(x^{t(q-1)}\right)^{p-1} \equiv 1 \bmod p \quad \Rightarrow \quad x^{t(p-1)(q-1)} \equiv 1 \bmod p \\ &\xRightarrow{\text{משוואה (*1)}} \quad x^{ab-1} \equiv 1 \bmod p \end{aligned} \tag{*5}$$
באופן דומה מכיוון ש- q מספר ראשוני ו- z שלם, אזי
$$\begin{aligned} z^{q-1} \overset{\text{פרמה}}{\equiv} 1 \bmod q \quad &\xRightarrow{\text{משוואה (*3)}} \quad \left(x^{t(p-1)}\right)^{q-1} \equiv 1 \bmod q \quad \Rightarrow \quad x^{t(p-1)(q-1)} \equiv 1 \bmod q \\ &\xRightarrow{\text{משוואה (*1)}} \quad x^{ab-1} \equiv 1 \bmod q \end{aligned} \tag{*6}$$
מכיוון ש- p ו- q זרים אז
$$x^{ab-1} - 1 \equiv 0 \mod (pq)$$
ולכן בגלל ש- $n=pq$ אז
$$x^{ab-1} - 1 \equiv 0 \mod n \ .$$
נעביר אגפים:
$$x^{ab-1} \equiv 1 \mod n \ .$$
נכפיל ב- x:
$$x^{ab} \equiv x \mod n \ .$$
ולכן
$$(x^a)^b \equiv x \mod n \ .$$
ז"א הוכחנו כי לכל טקסט גלוי x, אם נצפין אותו ואז אחר כך נפענח את התשובה אנחנו נקבל את אותו טקסט הגלוי המקורי, x בחזרה. ■

6.5 צופן RSA המוכלל

משפט 6.5

יהיו p,q מספרים ראשוניים ויהי $n=pq$. יהי

$$\lambda(n)=\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}\ .$$

נגדיר צופן חדש אשר זהה ל- RSA אלא $\phi(n)$ הוחלף עם $\lambda(n)$ כך ש- $ab\equiv 1 \mod \lambda(n)$. אזי הקריפטו-מערכת ניתן לפענח.

הוכחה:

שלב 1) רושמים את הצופן:

$$\left.\begin{aligned} e_k(x)&=x^b \mod n\\ d_k(y)&=y^a \mod n\end{aligned}\right\}\qquad n=pq\ ,\qquad ab\equiv 1 \mod \lambda(n)\ .$$

שלב 2) נתון כי $d=\gcd(p-1,q-1)$. ז"א שקיים p' שלם כך ש-

$$p-1=p'd \quad\Leftrightarrow\quad \frac{p-1}{d}=p' \quad\Leftrightarrow\quad d=\frac{p-1}{p'}\ . \tag{\#1}$$

באותה מידה קיים q' שלם כך ש-

$$q-1=q'd \quad\Leftrightarrow\quad \frac{q-1}{d}=q' \quad\Leftrightarrow\quad d=\frac{q-1}{q'}\ . \tag{\#2}$$

שלב 3)

$$\lambda(n)=\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}=\frac{(p-1)(q-1)}{d}\ .$$

$$\lambda(n)\stackrel{(\#1)}{=}\frac{(p-1)(q-1)}{\left(\frac{p-1}{p'}\right)}=p'(q-1)\ .\quad\Leftrightarrow\quad d=\frac{p-1}{p'}\ . \tag{1*}$$

$$\lambda(n)\stackrel{(\#2)}{=}\frac{(p-1)(q-1)}{\left(\frac{q-1}{q'}\right)}=q'(p-1)\ .\quad\Leftrightarrow\quad d=\frac{p-1}{p'}\ . \tag{2*}$$

שלב 4) $ab\equiv 1 \mod \lambda(n)$ (נתון) לכן קיים t שלם כך ש-

$$ab=1+t\lambda(n)\stackrel{(2*)}{=}1+t(p-1)q'\ .$$

לכן

$$ab-1=t(p-1)q'\ .$$

מכאן

$$x^{ab-1}x^{tq'(p-1)}=y^{p-1}\stackrel{\text{פרמה}}{\equiv}1 \mod p$$

כאשר $y=x^{tq'}$ והשוויון השני מתקיים בגלל ש- p מספר ראשוני. לפיכך

$$x^{ab-1}\equiv 1 \mod p\ .$$

שלב 5) $ab \equiv 1 \mod \lambda(n)$ (נתון) לכן קיים t שלם כך ש-

$$ab = 1 + t\lambda(n) \overset{(1*)}{=} 1 + t(q-1)p' \ .$$

לכן

$$ab - 1 = t(q-1)p' \ .$$

מכאן

$$x^{ab-1} x^{tp'(q-1)} = z^{q-1} \overset{\text{פרמה}}{\equiv} 1 \mod q$$

כאשר $z = x^{tp'}$ והשוויון השני מתקיים בגלל ש- q מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \mod q \ .$$

שלב 6) מכיוון ש- p, q ראשוניים אז

$$\left.\begin{array}{ll} x^{ab-1} & \equiv 1 \mod q \\ x^{ab-1} & \equiv 1 \mod q \end{array}\right\} \quad \Rightarrow \quad x^{ab-1} \equiv 1 \mod pq$$

לפיכך

$$x^{ab-1} \equiv 1 \mod n \quad \Rightarrow \quad \left(x^b\right)^a \equiv x \mod n$$

כנדרש.

■