שיעור 6
צופן RSA

6.1 אלגוריתם RSA

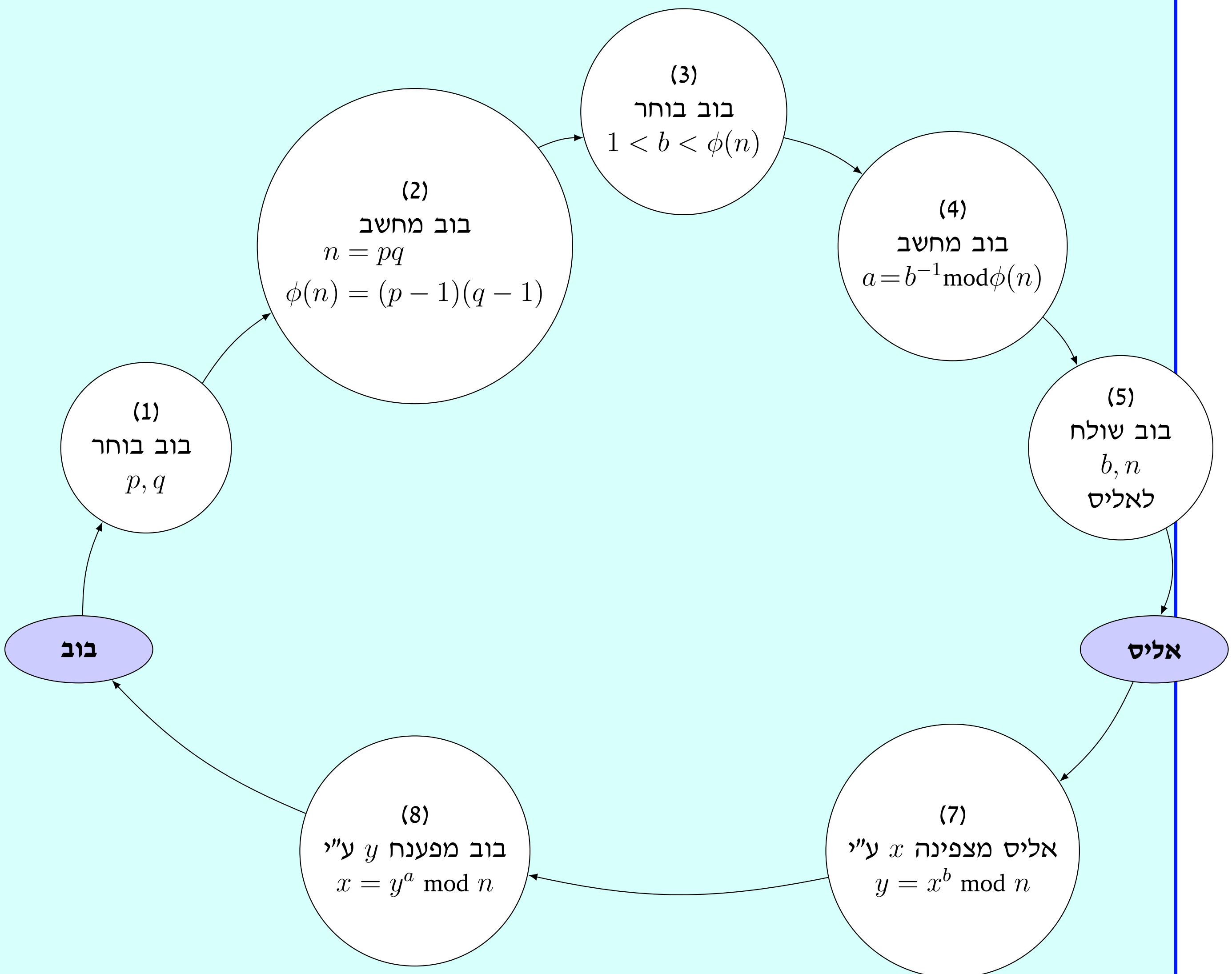
צופן RSA הומצא בשנה 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman .

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.

<u>שלב הפענוח</u>

[8] בוב מפענח את הטקסט מוצפן עם המתתח הסודי באמצעות הכלל מפענח $x = y^a \bmod n$.

דוגמה 6.1

בוב בוחר בפרמטרים הבאים כדי לבנות מפתח של צופן RSA:

$$(b = 47, p = 127, q = 191)$$

א)

ב) אליס קוראת את המפתח ציבורי ומשתמשת בה כדי להצפין את המסר 2468. מהי הטקסט מוצפן שהיא שולחת לבוב?

ג) כעת בוב מפענח את הטקסט מוצפן שהוא קיבל מאליס בעזרת המפתח הסודי שלו. בדקו כי הפענוח של הטקסט מוצפן מסעיף ב' הוא זהה לטקסט הגלוי המקורי שאליס שלחה אליו.

פתרון:

סעיף א)

$$n = pq = 191 \times 127 = 24257$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 190 \times 126 = 23940 \ .$$

$a = 47^{-1} \mod 23940$. נשתמש באלגוריתם של אוקליד:

<u>שיטה 1</u>

$a = 23940, b = 47$.

$$\begin{aligned} r_0 &= a = 23940 \ , & r_1 &= b = 47 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $k=1$:	$r_2 = 23940 - 509 \cdot 47 = 17$	$s_2 = 1 - 509 \cdot 0 = 1$	$t_2 = 0 - 509 \cdot 1 = -509$	$q_1 = 509$
שלב $k=2$:	$r_3 = 47 - 2 \cdot 17 = 13$	$s_3 = 0 - 2 \cdot 1 = -2$	$t_3 = 1 - 2 \cdot (-509) = 1019$	$q_2 = 2$
שלב $k=3$:	$r_4 = 17 - 1 \cdot 13 = 4$	$s_4 = 1 - 1 \cdot (-2) = 3$	$t_4 = -509 - 1 \cdot (1019) = -1528$	$q_3 = 1$
שלב $k=4$:	$r_5 = 13 - 3 \cdot 4 = 1$	$s_5 = -2 - 3 \cdot (3) = -11$	$t_5 = 1019 - 3 \cdot (-1528) = 5603$	$q_4 = 3$
שלב $k=5$:	$r_6 = 4 - 4 \cdot 1 = 0$	$s_6 = 3 - 4 \cdot (-11) = 47$	$t_6 = -1528 - 4 \cdot (5603) = -23940$	$q_5 = 4$

$$\gcd(a,b) = r_5 = 1 \ , \qquad x = s_5 = -11 \ , \qquad y = t_5 = 5603 \ .$$

$$sa + tb = -11(23940) + 5603(47) = 1 \ .$$

מכאן

$$5603(47) = 1 + 11(23940) \quad \Rightarrow \quad 5603(47) = 1 \mod 23940 \quad \Rightarrow \quad 47^{-1} = 5603 \mod 23940 \ .$$

<u>שיטה 2</u>

$$\begin{aligned} 23940 =& 509(47) + 17 \\ 47 =& 2(17) + 13 \\ 17 =& 13 + 4 \\ 13 =& 3(4) + 1 \\ 4 =& 4(1) + 0 \ . \end{aligned}$$

$$\begin{aligned} 1 =& 13-3(4) \\ =& 13-3(17-13) \\ =& 4(13)-3(17) \\ =& 4(47-2(17))-3(17) \\ =& 4(47)-11(17) \\ =& 4(47)-11(23940-509(47)) \\ =& 5603(47)-11(23940) \end{aligned}$$

לכן $a^{-1} = 5603$.

סעיף ב) אליס שולחת את ההודעה $2468^{47} \mod 24257$. כדי לחשב זה נשתמש בשיטת ריבועים:
$47 = 32 + 8 + 4 + 2 + 1$.

$$\begin{aligned} (2468)^2 & & = 2517 \mod 24257 \\ (2468)^4 =& (2517)^2 & = 4212 \mod 24257 \\ (2468)^8 =& (4212)^2 & = 9077 \mod 24257 \\ (2468)^{16} =& (9077)^2 & = 15157 \mod 24257 \\ (2468)^{32} =& (15157)^2 & = 20859 \mod 24257 \end{aligned}$$

לכן

$$\begin{aligned}246847 =& (2468)^{32} \times (2468)^{8} \times (2468)^{4} \times (2468)^{2} \times 2468 \mod 24257\\ =& 20859 \times 9077 \times 4212 \times 2517 \times 2468 \mod 24257\\ =& 10642 \mod 24257\ .\end{aligned}$$

לכן הטקסט מוצפן הוא $y = 10642$.

סעיף ג) $y = 10642$.

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

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>

$a = 191, b = 127$.

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

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

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

■

6.2 משפט השאריות הסיני

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

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

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 6.2

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 אוקליד.

נסמן $a = 113, b = 101$.

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

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 $k = 5$:	$r_6 = 2 - 2 \cdot 1 = 0$	$s_6 = 17 - 2 \cdot (-42) = 101$	$t_6 = -19 - 2 \cdot (47) = -113$	$q_5 = 2$

$$\gcd(a,b) = r_5 = 1 \ , \qquad s = s_5 = -42 \ , \qquad t = t_5 = 47 \ .$$

$$ta + sb = -42(113) + 47(101) = 1 \ .$$

מכאן

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

ו-

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

לכן

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

ו-

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

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

■

6.3 משפטים של מספרים ראשוניים

משפט 6.2 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 1.4 למעלה או משפט 6.3 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 מספק 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 6.3 משפט הפירוק לראשוניים

(ראו משפט 1.4) 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 6.4

אם a,b שלמים זרים (כלומר $\gcd(a,b)=1$) אז

$$\phi\left(m\cdot n\right)=\phi(m)\cdot\phi(n)\ .$$

הוכחה: **(להעשרה בלבד)**

■

משפט 6.5

אם p מספר ראשוני אז

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

הוכחה: נתבונן על $\gcd\left(p^n,m\right)$ כאשר m שלם ו- p ראשוני.

האפשרויות היחידות של המחלק המשותף הגדול ביותר $\gcd\left(p^n,m\right)$ הן $1,p,p^2,\ldots,p^n$. בסה"כ יש p^n אפשרויות.

$\gcd\left(p^n,m\right)>1$ רק אם $m\in\{p,2p,3p,\ldots,p^{n-1}p\}$, כלומר רק אם m שווה לכפולה של p.

מכאן קיימים p^n-p^{n-1} שלמים עבורם $\gcd\left(p^n,m\right)=1$.

■

משפט 6.6 נוסחה לפונקצית אוילר

(ראו משפט ??) 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

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

הוכחה: משפט 6.4 ו- 6.5. ■

דוגמה 6.3

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 6.7

אם p מספר ראשוני אז

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

הוכחה: משפט 6.4 ו- 6.5. ■

משפט 6.8

אם p ו- q מספרים ראשוניים שונים אז

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

הוכחה: תרגיל בית. ■

משפט 6.9 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 6.10 משפט אוילר

אם a,n שלמים ו- $\gcd(a,n)=1$ אז

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

משפט 6.11

אם a,n שלמים ו- $\gcd(a,n)=1$ אז

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

דוגמה 6.4

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

פתרון:

לפי משפט פרמט 6.9:

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

לפי הנוסחת לשארית **??** :

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

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$. ■

6.4 הוכחה שצופן RSA ניתן לפענוח

משפט 6.12 קריפטו-מערכת RSA ניתן לפענוח

יהי $n=pq$ מספרים ראשוניים שונים, $a,b\in\mathbb{Z}$ שלמים חיוביים 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 6.8, $\phi(n)=\phi(pq)=(p-1)(q-1)$.
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 6.9, $z^{p-1}=1 \mod p$. 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. ■

6.5 צופן RSA המוכלל

משפט 6.13

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-

$$p-1=p'd \quad\Leftrightarrow\quad \frac{p-1}{d}=p' \quad\Leftrightarrow\quad d=\frac{p-1}{p'}\ . \qquad \text{(\#1)}$$

באותה מידה קיים q' שלם כך ש-

$$q-1=q'd \quad\Leftrightarrow\quad \frac{q-1}{d}=q' \quad\Leftrightarrow\quad d=\frac{q-1}{q'}\ . \qquad \text{(\#2)}$$

שלב 3)

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

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

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

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

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

לכן

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

מכאן

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

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-

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

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

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

לפיכך

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

כנדרש.

■