

שיעור 6

צופן RSA

6.1 אלגוריתם RSA

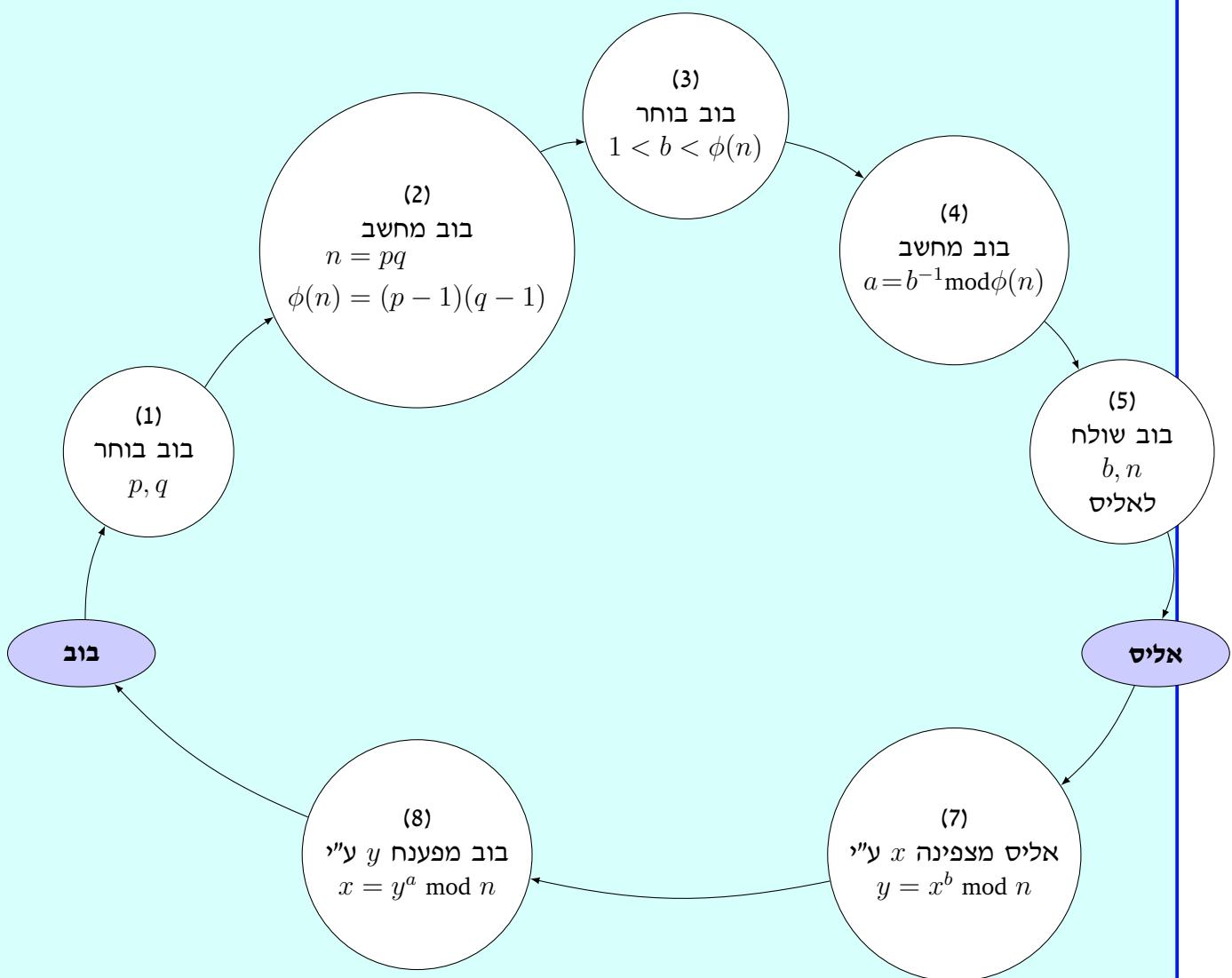
צופן RSA הומצא בשנת 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman.

הגדרה 6.1 צופן RSA

- יהיו p, q מספרים ראשוניים שונים ($p \neq q$).
- יהיה $n = pq$.
- יהיה b שלם כךže: $1 < b < \phi(n)$ הפונקציה 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) .
- יהיה $x \in \mathbb{Z}^+$ שלם אי-שלילי.
 - * הכלל מצפין מוגדר $e_k(x) = x^b \pmod{n}$,
 - * והכלל מפענח מוגדר $d_k(x) = y^a \pmod{n}$.

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

הגדלה 6.2 אלגוריתם RSA



נניח שאليس (A) שלחת הודעה לבוב (B).

שלב הבניית המפתח

[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 מספרשלם b באקראי כך שהשני תנאים הבאים מתקיימים:

$$\begin{aligned} 1 < b < \phi(n) &\bullet \\ \gcd(b, \phi(n)) = 1 &\bullet \end{aligned}$$

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

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

בנייה מפתח עשויה פעם אחת.

שלב הצפנה

[6] אליס (A) מקבלת את המפתח הציבורי (n, b) מבוב, ומצפינה את הטקסט הגרפי x עם המפתח הציבורי
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 המפתח הסודי באמצעות הכלל מפענח $y^a \bmod n$.

דוגמה 6.1

בוב בונה צופן RSA עם המפתח הציבורי $(b = 47, p = 127, q = 191)$.

a) חשבו את n ו- a .

b) אליס קוראת את המפתח הציבורי (n, b) ומשתמש בה כדי להצפין את המסר 2468. מהי הטקסט מוצפן שהיא שולחת לבוב?

c) כעת בוב מפענח את הטקסט מוצפן שהוא קיבל מלאיס בעזרת המפתח (a, p, q) . בדקו כי הפענוח של הטקסט מוצפן מסעיף ב' זהה לטקסט גלי אשר אליס שלחנה.

פתרונות:

סעיף a)

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

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

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

שיטת 1

$$a = 23940, b = 47$$

$$r_0 = a = 23940 , \quad r_1 = b = 47 ,$$

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

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

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

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

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

מכאן

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

שיטת 2

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

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

$$\text{לכן } a^{-1} = 5603$$

סעיף ב) אליס שולחת את הודעה $2468^{47} \pmod{24257}$. כדי לחשב זה משתמש בשיטת ריבועים:

$$.47 = 32 + 8 + 4 + 2 + 1$$

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

לכן

$$\begin{aligned} 2468^{47} &= (2468)^{32} \times (2468)^8 \times (2468)^4 \times (2468)^2 \times 2468 \pmod{24257} \\ &= 20859 \times 9077 \times 4212 \times 2517 \times 2468 \pmod{24257} \\ &= 10642 \pmod{24257} . \end{aligned}$$

$$\text{לכן הtekסט מוצפן הוא } y = 10642$$

$$\text{סעיף ג) } y = 10642$$

$$y \pmod{p} = 10642 \pmod{127} = 101 , \quad a \pmod{p-1} = 5603 \pmod{126} = 59 .$$

לכן

$$x_1 = (y \pmod{p})^{a \pmod{(p-1)}} \pmod{p} = 101^{59} \pmod{127} = 55$$

(ניתן לחשב זה לפי $.101^{32} \times 101^{16} \times 101^8 \times 101^2 \times 101$)

$$(101)^2 \equiv 41 \pmod{127}$$

$$(101)^4 \equiv (41)^2 \pmod{127} \equiv 30 \pmod{127}$$

$$(101)^8 \equiv (30)^2 \pmod{127} \equiv 11 \pmod{127}$$

$$(101)^{16} \equiv (11)^2 \pmod{127} \equiv 121 \pmod{127}$$

$$(101)^{32} \equiv (121)^2 \pmod{127} \equiv 36 \pmod{127}$$

לכן

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

$$y \pmod{q} = 10642 \pmod{191} = 137 , \quad a \pmod{(p-1)} = 5603 \pmod{190} = 93 .$$

לכן

$$x_2 = (y \pmod{q})^{a \pmod{(q-1)}} \pmod{q} = 137^{93} \pmod{191} = 176$$

(ניתן לחשב זה לפי $.137^{64} \times 137^{16} \times 137^8 \times 137^4 \times 137$)

$$(137)^2 \equiv 51 \pmod{191}$$

$$(137)^4 \equiv (51)^2 \pmod{191} \equiv 118 \pmod{191}$$

$$(137)^8 \equiv (118)^2 \pmod{191} \equiv 172 \pmod{191}$$

$$(137)^{16} \equiv (172)^2 \pmod{191} \equiv 170 \pmod{191}$$

$$(137)^{32} \equiv (170)^2 \pmod{191} \equiv 59 \pmod{191}$$

$$(137)^{64} \equiv (59)^2 \pmod{191} \equiv 43 \pmod{191}$$

לכן

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

בנוסף

$$y \pmod{q} = 9625 \pmod{127} = 100 , \quad a \pmod{(q-1)} = 5603 \pmod{126} = 59 .$$

לכן

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

לכן עליינו לפתור את המערכת

$$x = x_1 \pmod{p} = 55 \pmod{127}$$

$$x = x_2 \pmod{q} = 176 \pmod{191}$$

בעזרת המשפט השאריות הסיני. נסמן $m_2 = 191 , a_2 = 176 , m_1 = 127 , a_1 = 55$

$$M = m_1 m_2 = (191)(127) = 24257 , \quad M_1 = \frac{M}{m_1} = 191 , \quad M_2 = \frac{M}{m_2} = 127 .$$

כעת נחשב $y_2 = M_2^{-1} \pmod{m_2} = 127^{-1} \pmod{191}$ ו- $y_1 = M_1^{-1} \pmod{m_1} = 191^{-1} \pmod{127}$

שיטת 1

$$a = 191, b = 127$$

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

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

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

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

לכן

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

שיטת 2

נחשב $191^{-1} \pmod{127}$ 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

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

נחשב

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

לכן

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

■

6.2 משפט השאריות הסיני

משפט 6.1 משפט השאריות הסיני

יהיו m_1, m_2, \dots, m_r שלמים אשר זרים בזוגות ויהיו a_1, a_2, \dots, a_r שלמים. למערכת של יחסים שקיים

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

קיימים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ שנייתן על ידי

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

כאשר $1 \leq i \leq r$ $y_i = M_i^{-1} \pmod{m_i}$ ו $M_i = \frac{M}{m_i}$

דוגמה 6.2

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

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

פתרון:

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

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

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

כדי לחשב את האיברים ההופכיים נשתמש באלגוריתם המוכפל של אוקlid.

נסמן $a = 113, b = 101$

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

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

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

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

מכאן

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

-1

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

לכז

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

-1

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

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

■

6.3 משפטים של מספרים ראשוניים

משפט 6.2 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.
נניח כי $\{p_1, \dots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקובוצת זו נוצרת סופית.

נגידר השלם $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$. לפי משפט הפירוק לראשוניים (ראו המשפט 1.4 לעילו או משפט 6.3 למטה) הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $p_i > M$ לכל i . גם לא קיים מספק ראשוני p_i אשר מחלק את M . הרי

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

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

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

הוכחה: (להעשרה בלבד)

משפט 6.5

אם p מספר ראשוני אז

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

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

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

בsek' רק אם $m \in \{p, 2p, 3p, \dots, p^{n-1}p\}$ רק $\gcd(p^n, m) > 1$.

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

משפט 6.6 נוסחה לפונקציית 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

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

הוכחה: משפט 6.4 - 1.

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 - 1.

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:

$$a^p \equiv a \pmod{p} . \quad \text{1}$$

$$a^{p-1} \equiv 1 \pmod{p} . \quad \text{2}$$

$$a^{-1} \equiv a^{p-2} \pmod{p} . \quad \text{3}$$

הוכחה:

טענה 1. נוכח באינדוקציה.

בסיס:

עבור $0 = a$ הטענה $a^p \equiv 0 \pmod{p}$ מתקיימת.

מעבר:

נניח כי הטענה מתקיימת עבור a .

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

הנחה האינדוקציה אומרת ש- $a^p \equiv a \pmod{p}$ נכון

$$(a+1)^p \pmod{p} \equiv a^p + 1 \pmod{p} \equiv (a+1) \pmod{p}$$

כנדרש.

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

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

טענה 3.

$$a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow 1 \equiv a^{p-1} \pmod{p} \Rightarrow a^{-1} \equiv a^{p-2} \pmod{p}.$$

משפט 6.10 משפט אוילר

אם a, n שלמים ו- $\text{gcd}(a, n) = 1$ אז $a^{\phi(n)} \equiv 1 \pmod{n}$.

משפט 6.11

אם a, n שלמים ו- $\text{gcd}(a, n) = 1$ אז $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$.

דוגמה 6.4

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

פתרון:

לפי משפט פרימט 6.9:

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

לפי הנוסחת לשארית ?? :

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

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

6.4 הוכחה שצופן RSA ניתן לפענוח

משפט 6.12 קריפטו-מערכת RSA ניתן לפענוח

יהי p, q מספרים ראשוניים שונים, $a, b \in \mathbb{Z}$ שלמים חיוביים כך ש- $(ab)^{\phi(n)} \equiv 1 \pmod{\phi(n)}$ ו- $x \in \mathbb{Z}_n$ איזו

$$(x^b)^a \equiv x \pmod{n}.$$

הוכחה: נתון כי $.ab = 1 \pmod{\phi(n)}$ לפי משפט 6.8 .
 $\phi(n) = \phi(pq) = (p-1)(q-1)$

2

$$ab = 1 \pmod{\phi(n)} = 1 \pmod{(p-1)(q-1)}$$

לכן קיים $t \in \mathbb{Z}$ כך ש-

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

לכל $z \in \mathbb{Z}$ לפי משפט 6.9 $z^{p-1} = 1 \pmod{p}$. בפרט

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

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

משיקולות של סיימטריה באותה מידה.

$$x^{ab-1} - 1 = 0 \pmod{q} \text{ ו } x^{ab-1} - 1 = 0 \pmod{p}$$

מכיוון ש- p ו- q זרים אז

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

לפיכך

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

נכפיל ב- x ונקבל

$$(x^a)^b = x \pmod{(pq)} .$$

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

6.5 צופן RSA המובלל

משפט 6.13

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

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

נגידר צופן חדש אשר זהה ל- RSA אלא $\lambda(n)$ הוחלף עם $\phi(n)$ וכך לאzioni הקריפטו-מערכת ניתנת לפענה.

הוכחה:

שלב 1) רושמים את הצופן:

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

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

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

באותה מידת קיימים q' שלם כך ש-

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

שלב 3

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

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

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

שלב 4) מכיוון $ab \equiv 1 \pmod{\lambda(n)}$ ניתן למצוא t שולם כך ש-

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

לכן
 $ab - 1 = t(p-1)q'.$

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

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

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

שלב 5) מכיוון $ab \equiv 1 \pmod{\lambda(n)}$ ניתן למצוא t שולם כך ש-

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

לכן
 $ab - 1 = t(q-1)p'.$

מכאן
 $x^{ab-1}x^{tp'(q-1)} = z^{q-1} \stackrel{\text{פרמה}}{\equiv} 1 \pmod{q}$

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

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

שלב 6) מכיוון ש- q, p ראשוניים אז

$$\left. \begin{array}{l} x^{ab-1} \equiv 1 \pmod{q} \\ x^{ab-1} \equiv 1 \pmod{p} \end{array} \right\} \Rightarrow x^{ab-1} \equiv 1 \pmod{pq}$$

לפיכך
 $x^{ab-1} \equiv 1 \pmod{n} \Rightarrow (x^b)^a \equiv x \pmod{n}$
 כנדרש.

