

## שיעור 6

### צופן RSA

#### 6.1 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 שקילות

$$x = a_1 \pmod{m_1},$$

$$x = a_2 \pmod{m_2},$$

$$\vdots$$

$$x = a_r \pmod{m_r},$$

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

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

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

##### דוגמה 6.1

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

$$x = 22 \pmod{101},$$

$$x = 104 \pmod{113}.$$

##### 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 בהאלגוריתם המוכלל של אוקליד.

נסמן  $a = 113, b = 101$ .

$$r_0 = a = 113, \quad r_1 = b = 101,$$

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

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

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

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

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

מכאן

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

ו-

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

לכן

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

ו-

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

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



## 6.2 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 וקבוצה זו נוצרת סופי.

נגדיר השלם  $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$ .

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

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

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.

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

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 ו- 6.5.

## דוגמה 6.2

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:

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

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

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

הוכחה:

טענה 1. נוכיח באינדוקציה.

בסיס:עבור  $a = 0$  הטענה  $0^p \equiv 0 \pmod{p}$  מתקיימת.מעבר:נניח כי הטענה מתקיימת עבור  $a$ .

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

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

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

כנדרש.

**טענה 2.**  $\gcd(a, p) = 1$  לפיכך קיים איבר הופכי  $a^{-1} \in \mathbb{Z}_p$ . נכפיל ב-  $a^{-1}$  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-  $\gcd(a, n) = 1$  אז

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

### משפט 6.11

אם  $a, n$  שלמים ו-  $\gcd(a, n) = 1$  אז

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

### דוגמה 6.3

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

**פתרון:**

לפי משפט פרמט 6.9:

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

לפי הנוסחת לשארית ?? :

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

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

■

## 6.3 אלגוריתם RSA

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

### הגדרה 6.1 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

$$K = \left\{ (n, p, q, a, b) \mid ab = 1 \pmod{\phi(n)} \right\}$$

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 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

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

**הוכחה:** נתון כי  $ab = 1 \mod \phi(n)$

לפי משפט 6.8,  $\phi(n) = \phi(pq) = (p-1)(q-1)$ ,  $\phi(n) = \phi(pq)$  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

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

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 6.2 אלגוריתם RSA

### שלב הרכבת המפתח

נניח שאלים  $(A)$  שולחת הודעה לבוב  $(B)$ .

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

[4] מחשב  $a$  כך ש-  $a = b^{-1} \mod \phi(n)$  בעזרת האלגוריתם של אוקלידס, (ראו כלל 1.12) ולכן  $0 \leq a < \phi(n)$ .

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

בניית מפתח עשוי פעם אחת.

#### שלב הצפנה

[6] אליס  $(A)$  קוראת את המפתח הצפנה (הציבורי)  $(b, n)$   $k = (b, n)$  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 6.4

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

(א) חשבו את  $n$ ,  $\phi(n)$  ו-  $a$ .

(ב) אליס קוראת את המפתח ציבורי  $(b, n)$  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  $(a, p, q)$ . בדקו כי הפענוח של הטקסט מוצפן מסעיף ב' זהה לטקסט גלוי אשר אליס שלחה.

## פתרון:

סעיף א)

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

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

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

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

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

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

מכאן

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

שיטה 2

$$23940 = 509(47) + 17$$

$$47 = 2(17) + 13$$

$$17 = 13 + 4$$

$$13 = 3(4) + 1$$

$$4 = 4(1) + 0.$$

$$1 = 13 - 3(4)$$

$$= 13 - 3(17 - 13)$$

$$= 4(13) - 3(17)$$

$$= 4(47 - 2(17)) - 3(17)$$

$$= 4(47) - 11(17)$$

$$= 4(47) - 11(23940 - 509(47))$$

$$= 5603(47) - 11(23940)$$

$$.a^{-1} = 5603 \text{ לכן}$$

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

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

$$(2468)^2 = 2517 \pmod{24257}$$

$$(2468)^4 = (2517)^2 = 4212 \pmod{24257}$$

$$(2468)^8 = (4212)^2 = 9077 \pmod{24257}$$

$$(2468)^{16} = (9077)^2 = 15157 \pmod{24257}$$

$$(2468)^{32} = (15157)^2 = 20859 \pmod{24257}$$



לכן

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

לכן הטקסט מוצפן הוא  $y = 10642$ .סעיף ג)  $y = 10642$ 

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

לכן

$$\begin{aligned}
 x_1 &= (y \pmod{p})^{a \pmod{(p-1)}} \pmod{p} = 101^{59} \pmod{127} = 55 \\
 &\quad (\text{ניתן לחשב זה לפי } 101^{32} \times 101^{16} \times 101^8 \times 101^2 \times 101)
 \end{aligned}$$

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

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

$$\begin{aligned}
 x_2 &= (y \pmod{q})^{a \pmod{(q-1)}} \pmod{q} = 137^{93} \pmod{191} = 176 \\
 &\quad (\text{ניתן לחשב זה לפי } 137^{64} \times 137^{16} \times 137^8 \times 137^4 \times 137)
 \end{aligned}$$

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

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 עלינו לפתור את המערכת

$$x = x_1 \mod p = 55 \mod 127$$

$$x = x_2 \mod q = 176 \mod 191$$

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

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

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

### שיטה 1

$$a = 191, b = 127$$

$$r_0 = a = 191, \quad r_1 = b = 127,$$

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

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

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

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

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

לכן

$$191^{-1} \equiv 2 \mod 127$$

$$127^{-1} \equiv (-3) \mod 191 \equiv 188 \mod 191.$$

### שיטה 2

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

$$191 = 127 \cdot 1 + 64$$

$$127 = 64 \cdot 1 + 63$$

$$64 = 63 \cdot 1 + 1$$

$$63 = 1 \cdot 63 + 0.$$

$$\gcd(191, 127) = 1 \text{ לכן}$$

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

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

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

לכן

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

### 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:

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

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

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

באותה מידה קיים  $q'$  שלם כך ש-

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

(שלב 3)

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

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

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

**שלב 4**  $ab \equiv 1 \pmod{\lambda(n)}$  (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

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

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

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

**שלב 5**  $ab \equiv 1 \pmod{\lambda(n)}$  (נתון) לכן קיים  $t$  שלם 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  $z = x^{tp'}$  והשוויון השני מתקיים בגלל ש- $q$  מספר ראשוני. לפיכך

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

**שלב 6** מכיוון ש- $p, q$  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.

