

## שיעור 6

### צופן RSA

#### 6.1 אלגוריתם RSA

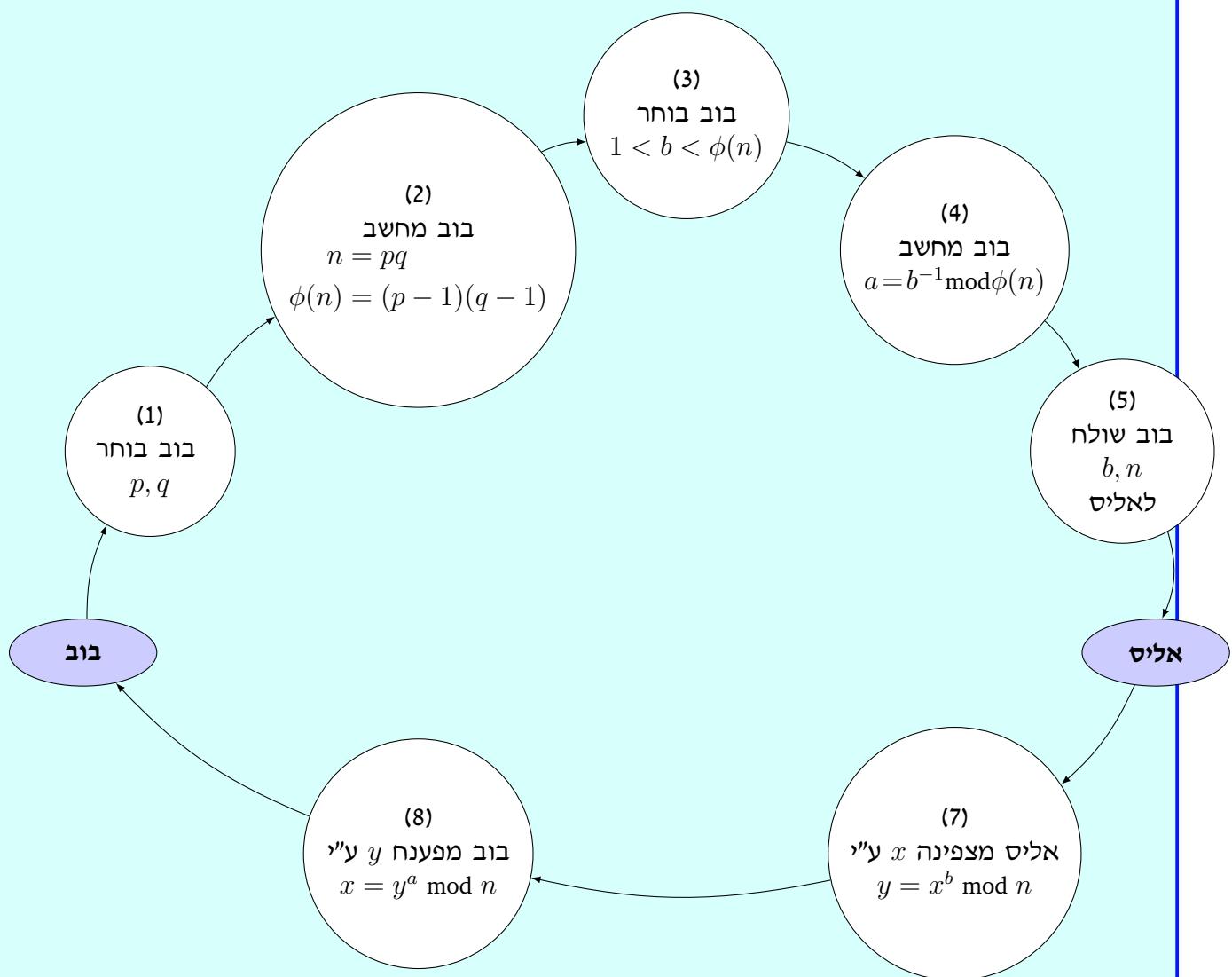
צופן RSA הומצא בשנת 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman.

##### 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

$$y = x^b \pmod{n}.$$

[7] A שולחת את טקסט מוצפן ל- B.

### שלב הפענוח

[8] בוב מפענח את הטקסט מוצפן עם המפתח הסודי באמצעות הכלל מפענח  $n$   $x$  לפי  
האלגוריתם הבא:

$$x_1 = \left[ (y \pmod{p})^{a \pmod{(p-1)}} \right] \pmod{p},$$

$$x_2 = \left[ (y \pmod{q})^{a \pmod{(q-1)}} \right] \pmod{q}.$$

אז פוטרים את המערכת הבאה בעזרת המשפט השARING השני:

$$x = x_1 \pmod{p},$$

$$x = x_2 \pmod{q}.$$

### 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 הציבורי ומשתמשת בה כדי להצפין את המספר 2468.  
הוכינו כי הטקסט מוצפן הוא 10642.

**פתרונות:**

**סעיף א)** המפתח הציבורי הוא  $(b, n)$ . הפרמטר  $b$  כבר נתון בשאלת א' נשאר רק לחשב את  $n$ :

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

לכן המפתח הציבורי הוא  
 $(b, n) = (47, 24257)$ .

כעת נחשב את המפתח הסודי  $(a, p, q)$ . הרשוניים  $p, q$  נתונים בשאלת א' נשאר רק לחשב את  $a$  לפי  
הנוסחה  $\phi(n) \pmod{\phi(n)}$  והוא הפונקציית אוילר:

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

$$\text{לפיכך } a = 47^{-1} \pmod{23940}.$$

נחשב את  $47^{-1} \pmod{23940}$  בעזרת האלגוריתם לאיבר ההופכי (ראו משפט 2.9):

**Algorithm 4 האלגוריתם לאיבר ההופכי**


---

```

1: Input: Integers  $A, B$  .
2:  $r_0 \leftarrow A$ 
3:  $r_1 \leftarrow B$ 
4:  $t_0 \leftarrow 0$ 
5:  $t_1 \leftarrow 1$ 
6:  $n \leftarrow 1$ 
7: while  $r_n \neq 0$  do
8:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
9:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
10:   $t_{n+1} \leftarrow t_{n-1} - q_n t_n$ 
11:   $n \leftarrow n + 1$ 
12: end while
13:  $n \leftarrow n - 1$ 
14: if  $r_n \neq 1$  then
15:    $B$  has no inverse modulo  $A$ 
16: else
17:   return:  $t_n$   $\triangleright t_n = B^{-1} \pmod{A}$ 
18: end if

```

---

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

$$\begin{aligned} r_0 &= A = 23940 , & r_1 &= B = 47 , \\ t_0 &= 0 , & t_1 &= 1 . \end{aligned}$$

אזי האיטרציות של האלגוריתם הם כמפורט למטה:

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

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

$$a = 5603 .$$

**סעיף ב)** אליס שולחת את הודעה בטקסט מוצפן

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

כדי לחשב את יחס מודולרי של חזקה זהה משתמש בשיטת הריבועים שעובדת באופן הבא. בהינתן

$$x^b \pmod{n} .$$

רשותם  $b$  כצירוף לינארי של חזקות של 2:

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

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

---

### האלגוריתם לשיטת הריבועים 5

---

```

1: Input: Integers  $x, b_0, \dots, b_k, n$  .
2:  $i \leftarrow 1$ 
3:  $z_0 \leftarrow x$ 
4: while  $i \leq k$  do
5:    $z_i \leftarrow z_{i-1}^2 \bmod n$ 
6: end while
7:  $i \leftarrow 1$ 
8:  $y \leftarrow x$ 
9: while  $i \leq k$  do
10:  if  $b_i = 1$  then
11:     $y \leftarrow z_i y \bmod n$ 
12:  end if
13: end while
14: return:  $y$                                  $\triangleright y = x^b \bmod n$ 
```

---

**שלב 1)** בדוגמה שלנו החזקה היא

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

אזי הייצוג הבינארי של  $b$  הוא

$$b = b_5 b_4 b_3 b_2 b_1 b_0 = 101111 .$$

**שלב 2)** נתחל:  $.z_0 = x = 2468$

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

**שלב 3)** נתחל:  $.y = x = 2468$

$b_1 = 1$	$y = z_1 y \bmod n = (2517)(2468) \bmod 24257 = 2164$
$b_2 = 1$	$y = z_2 y \bmod n = (4212)(2164) \bmod 24257 = 18393$
$b_3 = 1$	$y = z_3 y \bmod n = (9077)(2468) \bmod 24257 = 16587$
$b_4 = 0$	
$b_5 = 1$	$y = z_5 y \bmod n = (20859)(2468) \bmod 24257 = 10642$

לכן השתובה סופיל להtekסט מוצפן הוא:

$$y = 10642 .$$

לפנינו לעשות דוגמה של טקסט שהוצפן ע"י RSA אנחנו צריכים למדוד כל עזר שמאפשר לנו לפתור את הכלל מפענה: משפט השאריות הסיני.

## 6.2 משפט השאריות הסיני

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

### 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

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

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

 $\vdots$ 

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

קיים פתרון ייחיד מודולו  $M = m_1 m_2 \cdots m_r$  שנייתן על ידי

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

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

### דוגמה 6.2 (משפט השאריות הסיני)

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 באלגוריתם המוכפל של אוקלידס (אלגוריתם 2 למעלה).

$$\text{נסמן } A = 113, B = 101$$

$$r_0 = A = 113 , \quad r_1 = B = 101 ,$$

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

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

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

לכן הפירוק אוקלידי של 13 הוא  $B = 101$  ו-  $A = 113$

$$sA + tB = d$$

כאשר

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

מכאן

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

-1

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

לכן

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

-1

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

נציב אותם לנוסחה  $x = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod{M}$  ונקבל את התשובה הסופית הבאה:

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



### דוגמה 6.3 (פענוח של צופן RSA)

הדוגמה הזאת היא המשך של דוגמה 6.1.

בדוגמה 6.1 קיבלנו את הפרמטרים  $\phi(n) = 23940$ ,  $n = 24257$ ,  $p = 127$ ,  $b = 47$  ו-  $q = 191$ . בעזרת המפתח הציבורי  $(b, n) = (47, 24257)$  ו-  $a = b^{-1} \pmod{n} = 5603$  אנחנו חישבנו את הטקסט מוצפן של  $x = 2468$  על פי הכלל מצפין וקיבלו את התשובה  $y = x^b \pmod{n} = 10642$ . בעת נחח את הטקסט מוצפן  $y$  והמפתח הסודי  $(a, p, q) = (5603, 127, 191)$  ונוכח כי הטקסט המקורי, על פי הכלל מפענה  $x = 2468$ , הוא  $x = x^a \pmod{n}$ .

פתרונות:

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

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

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

בנוסח

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

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-  $y_1 = M_1^{-1} \pmod{m_1} = 191^{-1} \pmod{127}$

$$a = 191, b = 127$$

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

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

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

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

לכן

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

שיטת 2

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

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

$$\text{לכן } \gcd(191, 127) = 1$$

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

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

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



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

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

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

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

**הוכחה:**

**טענה 1.** נוכח באינדוקציה.

בסיס:

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

מעבר:

נניח כי הטענה מתקיימת עבור  $a$ .

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

ההנחה 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.** 1.  $\gcd(a, p) = 1$  לפיכך קיים איבר הופכי  $a^{-1} \in \mathbb{Z}_p$  ב-  $a^p \equiv 1 \pmod{p}$  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.**

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



## 6.4 משפט: צופן RSA ניתן לפענוח

### משפט 6.4 צופן RSA ניתן לפענוח

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

**הוכחה:** נתון כי  $.ab = 1 \pmod{\phi(n)}$  לפי משפט 2.5,  $\phi(n) = \phi(pq) = (p-1)(q-1)$  ו"

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

לכן קיים  $t \in \mathbb{Z}$  כך ש-

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

לכל  $z \in \mathbb{Z}$  לפי משפט 6.3  $z^{p-1} = 1 \pmod{p}$  . בפרט

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

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

משיקולות של סיימטריה באותה מידה

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

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

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

וז"א הוכחנו כי לכל טקסט גלי  $x$ , אם נצפין אותו ואז אחר כך נפענה את הטקסט מוצפן המתקיים RSA, נקבל אותו טקסט גלי המקורי בחזרה.  
■

## 6.5 צופן RSA המוכבל

### משפט 6.5

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

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

נגידר צופן חדש אשר זהה ל-RSA אלא  $\phi(n)$  הוחלף עם  $\lambda(n)$  וכך ש-  $ab \equiv 1 \pmod{\lambda(n)}$  אזי הקריפטו-מערכת ניתנת לפענה.

הוכחה:

**שלב 1** רושמים את הצופן:

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

**שלב 2** נתנו כי  $d = \gcd(p-1, q-1)$ . ז"אקיימים  $p'$  שלם כך ש-

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

באותה מידה 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**

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

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

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

**שלב 4)** נתון  $ab \equiv 1 \pmod{\lambda(n)}$  לכן קיים  $t$  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  $y = x^{tq'}$  והשווין השני מתקיים בגלל ש-  $p$  מספר ראשוני. לפיכך

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

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

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

**שלב 6)** מכיוון ש-  $q, p$  ראשוניים אז

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

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

