

## תוכן העניינים

- 1 הגדרות
- 2 משפטיים

## 1 הגדרות

### הגדרה 1: שלם שמחוק שלם

יהיו  $a, b$  מספרים שלמים. אומרים כי  $b$  מחלק את  $a$  אם קיים מספר שלם  $q$  כך ש-  
 $a = qb$ .

כלומר  $\frac{a}{b}$  שווה למספר שלם  $q$ . הסימון  $b \mid a$  אומר כי  $b$  מחלק את  $a$ .

### הגדרה 2: יחס שקולות בין $a$ ו- $b$

נניח כי  $a, b \in \mathbb{Z}$  מספרים שלמים ו-  $m$  מספר שלם חיובי. היחס  
 $a \equiv b \pmod{m}$   
אומר כי  $m$  מחלק את ההפרש  $a - b$ , כלומר  $.m \mid a - b$ .

התנאים הבאים שקולים:

$$a \equiv b \pmod{m} \iff m \mid a - b \iff \exists q, r : a = qm + r$$

אומרים גם כי " $a$  שקול ל-  $b$  מודולו  $m$ ".

### הגדרה 3: השארית

נתונים שניים שלמים  $a, b \in \mathbb{Z}$ , היחס

$$a \bmod b$$

מציאן את השארית בחלוקת  $a$  ב-  $b$ .

### הגדרה 4: המחלק המשותף הגדול ביותר gcd

נתונים שניים שלמים  $a, b > 0$ . המחלק המשותף הגדל ביותר של  $a$  ו-  $b$  מסומן gcd( $a, b$ ) (greatest common divisor) ומודגר להיות המספר שלם הגדל ביותר שמחוק גם  $a$  וגם  $b$ .

### הגדרה 5: כפולה משותפת קטנה ביותר lcm

נתונים שניים שלמים  $a, b > 0$ . הכפולה המשותפת הקטנה ביותר מוסומן lcm( $a, b$ ) (lowest common multiple) ומודגר להיות המספר השלם החויבי הקטן ביותר ש-  $a$  ו-  $b$  מחלקים אותו.

### הגדרה 6: מספרים זרים

נניח כי  $1 < a \leq b$  מספרים שלמים. אומרים כי  $a$  ו-  $b$  **מספרים זרים** אם  $\gcd(a, b) = 1$ .

במילים פשוטות, שני מספרים שלמים נקראים **מספרים זרים** אם המחלק המשותף המקסימלי שלהם הוא 1, כלומר, אין אף מספר גדול ממהלך את שניהם.

### הגדרה 7: פונקציית אוילר

יהי  $m$  מספר שלם. הפונקציית אוילר מסומנת ב-  $\phi(m)$  ומוגדרת להיות השלמים שקטנים ממש מ-  $m$  וזרים ביחס ל-  $m$ .  
 $\phi(m) := \{a \in \mathbb{N} \mid \gcd(a, m) = 1, a < m\}$ .

### הגדרה 8: צופן ההזזה

יהי  $0 \leq k \leq 25$ . עברו  $P = C = K = \mathbb{Z}_{26}$   
 $e_k(x) = (x + k) \pmod{26}, \quad x \in \mathbb{Z}_{26}$   
 $d_k(y) = (y - k) \pmod{26}, \quad y \in \mathbb{Z}_{26}$ .

צופן ההזזה מוגדר מעל

### הגדרה 9: צופן החלפה (substitution cypher) צופן החלפה

בצופן החלפה,  $P = C = \mathbb{Z}_{26}$   
 $K$  מורכב מכל החלפות האפשריות של ה- 26 סמלים  $0, 1, 2, \dots, 25$ .  
עבור כל החלפה  $K \in \pi$  נגידר כל מיפוי

$$e_\pi(x) = \pi(x)$$

ונגידר כל פעולה

$$d_\pi(x) = \pi^{-1}(x),$$

כאשר  $\pi^{-1}$  החלפה ההפוכה של  $\pi$ .

### הגדרה 10: צופן אפייני

יהי  $P = C = \mathbb{Z}_{26}$  ויהי  
 $K = \{a, b \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}$ .  
עבור  $x \in \mathbb{Z}_{26}$  גידר כל המיפוי  
 $e_k(x) = (ax + b) \pmod{26},$   
עבור  $y \in \mathbb{Z}_{26}$  גידר כל המיפוי  
 $d_k(y) = a^{-1}(y - b) \pmod{26}.$

### הגדורה 15: צופן RSA

יהי  $n = pq$  כאשר  $p, q$  מספרים ראשוניים שונים. תהי הקבוצת טקסט גלי  $P = \mathbb{Z}_n^*$ , והקבוצות טקסט מוצפן  $C = \mathbb{Z}_n^*$ . נגידר קבוצת המפתחות

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

לכל  $(n, p, q, a, b) \in K$  נגידר כל מצפין

$$e_k(x) = x^b \pmod{n},$$

ונגידר כל מפענה

$$d_k(x) = x^a \pmod{n}.$$

הערכים של  $n$  ו-  $b$  הם ערכים ציבוריים בעוד  $p, q, a$  ערכים סודיים.

### הגדורה 16: רשת פיסטל (Feistel)

נתון טקסט גלי  $x = \{0, 1\}^{2n}$  כרץ סיביות.

$$R_0 : x = \underbrace{x_1 \dots x_n}_{L_0} \quad \underbrace{x_{n+1} \dots x_{2n}}_{R_0}$$

מחלקים את  $x$  לשני חצאים שנסמנו  $L_0$  ו-  $R_0$ :

- מספר שלם  $N$  אשר קובע את המספר של שלבים בתהליך הצפנה.
- מפתח התחלתי  $k$ .

• מערכת של  $N$  תות-מפתחות  $(k_1, \dots, k_N)$ , אחד לכל שלב של התהליך הצפנה.

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$$

$$R_0 = x_n \dots x_{2n}, L_0 = x_1 \dots x_n$$

$$(1 \leq i \leq N) : L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

$$y = R_N L_N$$

(2) בשלב ה-  $i$  יה  $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

(3) בשלב ה-  $N$  קיבל את הטקסט מוצפן לפי

### הגדורה 17: משוואות פיסטל

משוואות פיסטל להצפנה:

$$x = L_0 R_0 : 1 \leq i \leq N$$

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i), \quad y = R_N L_N$$

משוואות פיסטל לפענוח:

$$y = R_N L_N : 1 \leq i \leq N$$

$$R_i = L_{i+1}, \quad L_i = R_{i+1} \oplus f(R_i, k_{i+1}), \quad x = L_0 R_0$$

### הגדורה 11: צופן ויז'ניר (Vigenere Cipher)

יהי  $m$  מספר שלם חיובי.

$$P = C = K = \mathbb{Z}_{26}^m$$

ונגידר  $k = (k_1, k_2, \dots, k_m)$  נגידר כל מצפין

$$e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, \dots, x_m + k_m) \pmod{26}$$

ונגידר כל מפענה

$$d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, y_3 - k_3, \dots, y_m - k_m) \pmod{26},$$

כאשר כל הפעולות נקבעות ב-  $\mathbb{Z}_{26}$ .

### הגדורה 12: צופן הייל

נניח כי  $m \geq 2$  מספרשלם.

$$P = C = \mathbb{Z}_{26}^m$$

$$k = \mathbb{Z}_{26}^{m \times m}$$

מטריצה בחוג  $\mathbb{Z}_{26}^m$  מסדר  $m \times m$ .

עבור מפתח  $k \in K$  נגידר כל מצפין

$$e_k(x) = x \cdot k \pmod{26},$$

ונגידר כל מפענה

$$d_k(y) = y \cdot k^{-1} \pmod{26},$$

כאשר כל פעולות נקבעות ב-  $\mathbb{Z}_{26}$ .

### הגדורה 13: המטריצה של קופקטורים

תהי  $A \in \mathbb{R}^{n \times n}$

הקובקטור ה-  $(i, j)$  של  $A$  מוגדר להיות הדטרמיננטה של המטריצה המתקבלת מ-  $A$ - $i,j$  מחקיקת שורה  $i$  ועומודה  $j$ , כפול  $(-1)^{i+j}$ .

המטריצה של קופקטורים של המטריצה  $A$  מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר  $C_{ij}$  הקובקטור ה-  $(i, j)$  של  $A$ .

### הגדורה 14: המטריצה המכורעת

תהי  $A \in \mathbb{R}^{n \times n}$ . המטריצה המכורעת של  $A$  היא מטריצה מסדר  $n \times n$  שמסומנת  $\text{adj}(A)$  ומוגדרת

$$\text{adj}(A) = C^t$$

כאשר  $C$  המטריצה של קופקטורים של  $A$ .

$a \mid n$

#### הגדה 18: סודיות מושלמת

אומרים כי לкриיפטו-מערכת יש סודיות מושלמת אם

$$P(X = x | Y = y) = P(X = x)$$

לכל  $y \in Y, x \in X$ .

ז"א ההסתברות כי הטקסט גלי  $x$ , בידיעה כי הטקסט מוצפן  $y$  שווה רק להסתברות כי הטקסט גלי הוא  $x$  והבחירה של המפתח שבאמצעותו מתkowski הטקסט מוצפן  $y$  לא משנה על ההסתברות כי הטקסט גלי  $x$ .

#### הגדה 19: מידע של מאורע (שאנון)

נתנו משתנה מקרי  $X$ . המידע של ערך מסוים של  $X$  מסומן  $I_X(x)$  ומוגדר להיות

$$I(X = x) = \log_2 \left( \frac{1}{P_X(x)} \right) = -\log_2(P_X(x))$$

כאשר  $P_X(x)$  פונקציית ההסתברות של המשתנה מקרי  $X$ .

#### הגדה 20: הצפנת האפמן

נתנו משתנה מקרי  $X$ . נגדיר הצפנת האפמן של  $X$  להיות הפונקציה (כלל מיפוי)

$$f : X \rightarrow \{0, 1\}^*$$

כאשר  $\{0, 1\}^*$  קבוצת רצפים של סיביות סופיים.

נתנו רצף מאורעות  $x_1, \dots, x_n$ . נגדיר

$$f(x_1 \dots x_n) = f(x_1) || \dots || f(x_n)$$

כאשר " $||$ " מסמן שרשור (concatenation).

#### הגדה 21: תוחלת האורך של הצפנת האפמן

נתונה הצפנת האפמן  $f$ . תוחלת האורך של ההצפנה מוגדרת:

$$l(f) = \sum_{x \in X} P(X = x) |f(x)| .$$

## 2 משפטיים

#### משפט 1:

יהו  $a, b, n$  מספרים שלמים.

אם השלושה תנאים הבאים מתקיימים:

$$, b \mid a \quad (1)$$

$$, a \mid n \quad (2)$$

$$, b \mid n \quad (3)$$

הוכחה:

$$a \mid n , \quad b \mid n$$

לכן קיימים שלמים  $k$  ו-  $l$  כך ש-

$$n = ak , \quad n = bl .$$

$$\therefore a = bl$$

$$. b \mid ak$$

$$. k = bq \text{ וכן } \gcd(a, b) = 1 .$$

$$. n = ak = abq$$

#### משפט 2: תכונות של gcd

$$\gcd(ma, mb) = m \gcd(a, b) .$$

$$. \gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m} \text{ וא } m \mid b \rightarrow m \mid a \text{ ואם } m > 0 .$$

$$. \text{המספרים } \frac{b}{\gcd(a, b)} \rightarrow \frac{a}{\gcd(a, b)} \text{ הם זרים.}$$

$$. \text{אם } ab \text{ ו- } c \mid ab \text{ אז } c \mid a \text{ ו- } c \mid b .$$

$$. \text{אם } a, c \text{ זרים ו- } b, c \text{ זרים אז } ab \text{ ו- } ac \text{ זרים.}$$

$$. \gcd(a, b) = \gcd(a + cb, b) .$$

הוכחה:

$$1. \text{ יהיו } d = \gcd(a, b) \text{ ו- } s, t \text{ שלמים עוברים}$$

$$sa + tb = d .$$

מכאן

$$msa + mtb = md \Rightarrow s(msa) + t(mb) = md .$$

$$. \gcd(msa, mb) = md = m \gcd(a, b)$$

$$. \text{יהי } d = \gcd(a, b) \text{ ו- } s, t \text{ שלמים כך ש-}$$

$$sa + tb = d .$$

(\*)

נחלק (\*) ב-  $m$  ונקבל

$$s \frac{a}{m} + t \frac{b}{m} = \frac{d}{m} .$$

(\*\*)

$$. \text{נשים לב } \frac{a}{m} \text{ ו- } \frac{b}{m} \text{ שלמים. לכן } \frac{a}{m} \mid b \text{ ו- } m \mid a .$$

(\*\*\*)

$$\text{לכן } \frac{d}{m} = \gcd\left(\frac{a}{m}, \frac{b}{m}\right). \text{ לכן } \frac{d}{m} \text{ בהכרח שלם ולפי משפט בז'ו } \gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m}.$$

.3

4. אם  $a, b$  שלמים שכן קיימים שלמים  $s, t, d$  עוברים  $sa + tb = d$

$$\text{כasher } d = \gcd(a, b)$$

מכאן

$$s\left(\frac{a}{d}\right) + t\left(\frac{b}{d}\right) = 1.$$

נשים לב ש-  $d = \gcd(a, b)$  שכן בהכרח  $\frac{a}{d}$  ו-  $\frac{b}{d}$  שלמים. לכן קיבלונו שלמים  $s, t$  עוברים

$$s\left(\frac{a}{\gcd(a, b)}\right) + t\left(\frac{b}{\gcd(a, b)}\right) = 1.$$

$$\text{לכן השלמים } \frac{b}{\gcd(a, b)} \text{ ו- } \frac{a}{\gcd(a, b)} \text{ זרים.}$$

5. אם  $a, c$  מספרים זרים ו-  $a$  ו-  $c$  מספרים זרים אז  $ab$  מספרים זרים.

6. אם  $a, b$  זרים אז קיימים  $s$  ו-  $t$  שלמים עוברים  $sa + tc = 1$ .

7. אם  $a, b, c$  זרים אז קיימים  $\bar{s}$  ו-  $\bar{t}$  שלמים עוברים  $\bar{s}b + \bar{t}c = 1$ .

לכן

$$(sa + tc)(\bar{s}b + \bar{t}c) = 1$$

$$\Rightarrow s\bar{s}(ab) + (t\bar{s}b + \bar{t}c + \bar{s}t)c = 1$$

ז"א קיימים שלמים  $x, y$  עוברים  $x(ab) + yc = 1$  שכן  $x(ab) + yc = 1$  ו-  $x, y$  זרים.

8. אם  $a, b$  שלמים אז קיימים שלמים  $s$  ו-  $t$  עוברים  $sa + tb = d = \gcd(a, b)$ . מכאן

$$sa + tb = d$$

$$s(a + cb) + tb = d + scb$$

$$s(a + cb) + tb - scb = d$$

$$s(a + cb) + (t - sc)b = d$$

לכן קיימים שלמים  $y = t - cb$  ו-  $x = s$  עוברים  $x(a + cb) + yb = d$

$$\text{ולכן } \gcd(a + cb, b) = d = \gcd(a, b)$$

■

**משפט 3: תנאי לקיום איבר הופכי של חוג**

היה  $a \in \mathbb{Z}_m$ . קיים איבר הופכי  $a^{-1} \in \mathbb{Z}_m$  אם ורק אם  $\gcd(a, m) = 1$ .

הוכחה: יש להוכיח שקיים האיבר הופכי  $a^{-1}$  של  $a$  ב-  $\mathbb{Z}_m$  אם ורק אם  $\gcd(a, m) = 1$ .

כיוון ⇔

אם  $\gcd(a, m) = 1$  אז לפי משפט בז'ו קיימים שלמים  $s, t, d$  כך ש-  $sa + tm = d$  וגם  $d = \gcd(a, m)$  ו-  $sa + tm = 1$  אז קיימים שלמים  $s, t$  עוברים  $\gcd(a, m) = 1$

לפיכך קיימים שלמים  $s$  אשר הוא האיבר הופכי של  $a$  ב-  $\mathbb{Z}_m$ .

כיוון ⇔

אם קיימים איבר הופכי  $a^{-1} \in \mathbb{Z}_m$  אז  $\gcd(a, m) = 1$  (mod  $m$ ). ז"א קיימים שלמים  $q$  כך ש-  $a^{-1}a = 1 + qm$  ⇒  $a^{-1}a + (-q)m = 1$ .

לכן קיימים שלמים  $s$  ו-  $t = -q$  כך ש-  $sa + tm = 1$

ולכן לפי משפט בז'ו  $\gcd(a, m) = 1$ .

**משפט 4:**

יהיו  $a, b, c$  שלמים חיוביים. אם  $a, b$  לא זרים אז לא קיימים  $c$  עוברו  $(ac \equiv 1 \pmod{b})$

הוכחה: נניח בשילhouette כי  $a, b$  זרים ו-  $c$  עוברו  $(ac \equiv 1 \pmod{b})$ . ז"א קיימים שלמים  $q$ :

$$ac = qb + 1 \Rightarrow ac - qb = 1.$$

לכן קיימים שלמים  $c = s$  ו-  $t = -q$  עוברים  $sa + tb = 1$ . לפיכך משפט בז'ו  $a$  ו-  $b$  זרים, בסתיו  $ac \equiv 1 \pmod{b}$  לא זרים.

■

**משפט 5: חיסור של שרירות**

אם  $m$  מספרים שלמים חיוביים אז

$$((a + b) \pmod{m} - b) \pmod{m} = a \pmod{m}.$$

הוכחה: לפי משפט החילוק של אוקלידס קיימים שלמים  $q_1, r_1$  כך ש-  $a + b = q_1m + r_1$ ,  $0 \leq r_1 < m$ ,

$$\text{כאשר } r_1 = (a + b) \pmod{m} \text{ וגם } q_1 = \left\lfloor \frac{a + b}{m} \right\rfloor$$

$$((a + b) \pmod{m} - b) = r_1 - b = a - q_1m.$$

■

7

8

#### משפט 8: נסחת קיילי המילטון

נניח כי  $A \in \mathbb{R}^{n \times n}$  מטריצה ריבועית. אם  $A$  הפיכה, כלומר אם  $|A| \neq 0$  אז המטריצה ההפוכה נתונה ע"י:

$$A^{-1} = \frac{1}{|A|} \text{adj}(A) ,$$

כאשר  $\text{adj}(A)$  המטריצה המצורפת של  $A$ .

#### משפט 9: משפט הפירוק לראשוניים

המשפט היסודי של האריתמטיקה או משפט הפירוק לראשוניים קובע כי כל מספר טבעי ניתן לרשום כמכפלה ייחוד של מספרים ראשוניים. איזה  $a \in \mathbb{N}$  ניתן לרשום כמכפלה ייחוד של מספרים ראשוניים.

$$a = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_n^{e_n} .$$

כאשר  $p_1, p_2, \dots, p_n$  מספרים ראשוניים ו-  $e_1, e_2, \dots, e_n \in \mathbb{N}$ , והפירוק הזה ייחיד.

#### משפט 10: הפירוק לראשוניים של פונקציית אוילר

$$\text{נתון} \quad m. \quad \text{נניח כי הפירוק למספרים ראשוניים שלו הוא} \\ m = \prod_{i=1}^n p_i^{e_i} ,$$

כאשר  $p_i$  מספרים ראשוניים שונים ו-  $e_i > 0$  מספרים שלמים ו-  $1 \leq i \leq n$ . אז

$$\phi(m) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1}) .$$

#### משפט 11: שיטה לחישוב $\gcd$

נתונים השלמים  $a, b$  כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

וללא הגבלה כלליות נניח כי  $n \leq k$ . אז  $\gcd(a, b)$  נתו על ידי

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$

#### משפט 12: שיטה לחישוב $\text{lcm}$

נתונים השלמים  $a, b$  כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

וללא הגבלה כלליות נניח כי  $n \leq k$ . אז  $\text{lcm}(a, b)$  נתו על ידי

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

#### משפט 13:

$$\gcd(a, b) \text{lcm}(a, b) = ab .$$

"א' קיים שלם  $-q = Q$  כך ש:

$$((a+b) \bmod m) - b = Qm + a$$

ולכן

$$((a+b) \bmod m) - b \equiv a \pmod{m}$$

ולפי כן, מכיוון שהשני שלמים  $b$  ו-  $a$  שקיימים מודולריים ביחס ל-  $m$ , אז בהכרח יש להם אותן שאריות בחלוקת ב-  $m$ :

$$[((a+b) \bmod m) - b] \bmod m = a \bmod m .$$

#### משפט 6: צופן אפיני נתן לפענו

יהי  $e_k(x)$  הכלל מצפין של צופן אפיני ויהי  $d_k(y)$  הכלל מפענה של צופן אפיני. אז:

$$d_k(e_k(x)) = x \bmod 26$$

כל  $x \in \mathbb{Z}_{26}$ . כמובן, צופן אפיני נתן לפענו.

הוכחה: נסמן  $y = e_k(x)$

$$d_k(e_k(x)) = d_k(y)$$

$$= a^{-1}(y - b) \bmod 26$$

$$= a^{-1}([(ax + b) \bmod 26] - b) \bmod 26$$

$$\stackrel{\text{ככל הכפל}}{=} (a^{-1} \bmod 26) (([(ax + b) \bmod 26] - b) \bmod 26) \bmod 26$$

$$\stackrel{\text{משפט 5}}{=} (a^{-1} \bmod 26) (ax \bmod 26) \bmod 26$$

$$\stackrel{\text{ככל הכפל}}{=} (a^{-1}ax \bmod 26) \bmod 26$$

$$= x \bmod 26 .$$

#### משפט 7: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך דריך השילחה.

נניח כי  $\{p_1, \dots, p_n\}$  הוא הקבוצה של כל הראשוניים שקיים וקובוצה זו נוצרת סופי.

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

לפי המשפט הפירוק לראשוניים (ראו משפט 9 למעלה או משפט 18 למטה)  $M$  הוא מספר ראשוני או שווה למינימום של ראשוניים.

$M$  לא מסhor ראשוני בגלל ש-  $p_i > M$  לכל  $i \leq n$ .

אם לא קיים מסhor ראשוני  $p_i$  אשר מחלק את  $M$ . הרי

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

הגענו לסתירה של המשפט הפירוק לראשוניים, שכן קיימים אינסוף מספרים ראשוניים.

הוכחה:

$$\min(a, b) + \max(a, b) = a + b .$$

#### משפט 14: משפט חילוק של אוקלידס

יהיו  $a, b$  מספרים שלמים  $0 \neq b$ . קיימים מספרים שלמים  $q, r$  ייחדים כך ש-

$$a = qb + r$$

$$0 \leq r < |b|$$

- נקרא  $b$  מודולו,
- נקראת  $r$  המנה
- ואילו  $r$  נקרא השארית.

$$r = a \bmod b \quad \text{אזי } a, b > 0$$

#### משפט 15: האלגוריתם של אוקלידס

יהיו  $a, b$  מספרים שלמים חיוביים. קיים אלגוריתם אשר נותן את  $d = \gcd(a, b)$  כלהלן. ראשית מתחילהים:

$$r_0 = a , \quad r_1 = b .$$

אם  $r_1 = b \neq 0$  אז מתחילה את הלולאה. בשלב  $i = 1$  מוחسبים את  $q_1$  ו-  $r_2$  כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor , \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1 .$$

אם  $0 \neq r_2 = 2$  ממשיכים לשלב  $i = 2$  שבו מוחسبים את  $q_2$  ו-  $r_3$  כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor , \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2 .$$

התהליך ממשיך עד שנקבל  $0 = r_{n+1}$  בשלב ה-  $n$ -ית. כל השלבים של התהליך הם כדלקמן:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1 \quad : i = 1 \quad \text{שלב}$$

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2 \quad : i = 2 \quad \text{שלב}$$

$$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor \quad r_4 = r_2 - q_3 r_3 = r_2 - \left\lfloor \frac{r_2}{r_3} \right\rfloor r_3 \quad : i = 3 \quad \text{שלב}$$

$\vdots$

$$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor \quad r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor r_{n-1} \quad : i = n-1 \quad \text{שלב}$$

$$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor \quad r_{n+1} = 0 \quad : i = n \quad \text{שלב}$$

התהליך מסתיים בשלב ה-  $n$ -ית אם  $0 = r_{n+1}$ . ואז הפלט של האלגוריתם הוא  $d = \gcd(a, b)$ .

רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

#### האלגוריתם של אוקלידס

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $n \leftarrow 1$ 
5: while  $r_n \neq 0$  do
6:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
7:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
8:    $n \leftarrow n + 1$ 
9: end while
10:  $n \leftarrow n - 1$ 
11: Output:  $r_n = \gcd(a, b)$ 
```

#### משפט 16: משפט בז' (Bezout's identity)

יהיו  $a, b$  שלמים וכי  $d = \gcd(a, b)$  שניים  $s, t$  שקיימים לינאריים של  $a$  ו-  $b$ :

$$sa + tb = d .$$

#### משפט 17: האלגוריתם המוכבל של אוקלידס

יהיו  $a, b$  שלמים חיוביים. קיים אלגוריתם אשר נותן שלמים  $s, t, d$  עבורם  $d = sa + tb$  כלהלן.

כאשר  $d = \gcd(a, b)$ ,  $Cd$  קלוקמן. ראשית מתחילהים:

$$r_0 = a , \quad r_1 = b , \quad s_0 = 1 , \quad s_1 = 0 , \quad t_0 = 0 , \quad t_1 = 1 .$$

אם  $r_1 = b \neq 0$  אז מבצעים האיטרציה הראשונה של הלולאה. בשלב  $i = 1$  מוחسبים את  $q_1, r_2, s_2, t_2$  כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor , \quad r_2 = r_0 - q_1 r_1 , \quad s_2 = s_0 - q_1 s_1 , \quad t_2 = t_0 - q_1 t_1 .$$

אם  $0 \neq r_2 = 2$  עורבים לאיטריצה  $i = 2$  שבו מוחسبים את  $q_2, r_3, s_3, t_3$  כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor , \quad r_3 = r_1 - q_2 r_2 , \quad s_3 = s_1 - q_2 s_2 , \quad t_3 = t_1 - q_2 t_2 .$$

התהליך ממשיך עד שהשלב ה-  $n$  שבו מקבלים  $r_{n+1} = 0$ , והוא  $d = \gcd(a, b)$ . כל השלבים של האלגוריתם הם כדלקמן:

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$	:1 שלב
$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$	:2 שלב
				⋮
$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$	$r_{i+1} = t_{i-1} - q_i t_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i r_i$	:i שלב
				⋮
$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = t_{n-2} - q_{n-1} t_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} r_{n-1}$	:n-1 שלב
$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = t_{n-1} - q_n t_n$	$s_{n+1} = s_{n-1} - q_n s_n$	$t_{n+1} = t_{n-1} - q_n r_n$	:n שלב

$$d = \gcd(a, b) = r_n , \quad s = s_n , \quad t = t_n .$$

למטה רשות ייצוג פסאודו-קוד של האלגוריתם:

### Algorithm 2 האלגוריתם המוכלל של אוקלידס

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $s_0 \leftarrow 1$ 
5:  $s_1 \leftarrow 0$ 
6:  $t_0 \leftarrow 0$ 
7:  $t_1 \leftarrow 1$ 
8:  $n \leftarrow 1$ 
9: while  $r_n \neq 0$  do
10:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
11:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
12:    $s_{n+1} \leftarrow s_{n-1} - q_n s_n$ 
13:    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$ 
14:    $n \leftarrow n + 1$ 
15: end while
16:  $n \leftarrow n - 1$ 
17: Output:  $r_n, s_n, t_n$             $\triangleright d = r_n = \gcd(a, b)$  and  $d = sa + tb$  where  $s = s_n, t = t_n.$ 

```

### משפט 18: משפט הפירוק לראשוניים

(ראו משפט 9) 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 19: נוסחת לפונקציית אוילר

(ראו משפט 10) 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

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

### משפט 20: נוסחת השארית

נתונים  $a, b > 0$  מספר שלמים.

$$. a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor \quad (\text{א})$$

$$. (-a) \bmod b = b - (a \bmod b) = b \left\lceil \frac{a}{b} \right\rceil - a \quad (\text{ב})$$

הוכחה:

א) לפי משפט החילוק של אוקלידס 14, קיימים שלמים  $r, q$  כך ש-

$$a = qb + r \quad (*1)$$

כאשר  $b - r$  נחלק ב-  $b$ .  $r = a \bmod b \rightarrow 0 \leq r < b$  ונקבל

$$\frac{a}{b} = q + \frac{r}{b} \quad (*2)$$

נשים לב כי  $\frac{r}{b} < 1$ , לכן לפי (\*2)

$$\left\lfloor \frac{a}{b} \right\rfloor = q .$$

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r \Rightarrow r = a - b \left\lfloor \frac{a}{b} \right\rfloor . \quad (*3)$$

ב) לפי משפט החילוק של אוקלידס 14, קיימים שלמים  $q', r'$  כך ש-

$$-a = q'b + r'$$

נזכיר זה ב- (\*1) ונקבל

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r \Rightarrow r = a - b \left\lfloor \frac{a}{b} \right\rfloor .$$

נשים לב כי  $0 \leq r' < b$ .

אבל לפי (\*1)  $r = a \bmod b$   $a = qb + r$  (\*1)  $\rightarrow r$  ייחיד. לכן

$$r = b - r' \Rightarrow r' = b - r \stackrel{\text{משמעות (*3)}}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor = b - \left( a - b \left\lfloor \frac{a}{b} \right\rfloor \right) = b - (a \bmod b) . \quad (*5)$$

לכן  $r' = (-a) \bmod b = b - (a \bmod b)$

זהות החני מנווע מ- (\*5).

$$r = b - r' \Rightarrow r' = b - r \stackrel{\text{משמעות (*3)}}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor - a + \left\lceil \frac{a}{b} \right\rceil .$$

$$. r' = (-a) \bmod b = -a + \left\lceil \frac{a}{b} \right\rceil \quad \text{לכן}$$

### משפט 21: זהויות של הפונקציה אוילר

1 אם  $p$  מספר ראשוני אז  $\phi(p) = p - 1$

2 אם  $p$  מספר ראשוני אז  $\phi(p^n) = p^n - p^{n-1}$

3 אם  $s, t$  שלמים זרים (כלומר  $\gcd(s, t) = 1$ ) אז  $\phi(s \cdot t) = \phi(s) \cdot \phi(t)$

4 אם  $p$  ו-  $q$  מספרים ראשוניים שונים אז  $\phi(p \cdot q) = (p - 1)(q - 1)$

### משפט 22: משפט עזר למשפט הקטן של פרמה

אם  $p$  מספר ראשוני אז

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

הוכחה:

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

מכיוון ש-  $p \mid p!$  אז  $\binom{p}{k} \equiv 0 \pmod{p}$

מכיוון ש-  $p$  מספר ראשוני אז  $p \nmid k!(p-k)!$  לכן בהכרח:

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

### משפט 23: המשפט הקטן של פרמה

אם  $p$  מספר ראשוני ו-  $a \in \mathbb{Z}_p$ . אז התנאים הבאים מתקיימים:

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

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

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

הוכחה:

טענה 1. נוכיח באינדוקציה.

שלב הבסיס:

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

שלב המעבר:

נניח כי הטענה מתקיימת עבור  $a$  (זהות ההנחה האינדוקציה).

nocich ci hiya motkiyimot gam ubor 1 a + ubor a bofan haava.

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

לכל  $k \geq 1$  טבבי לפि משפט 22:  $\binom{p}{k} \mid p$  ולכן

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

על פי ההנחה האינדוקציה:  $a^p \equiv a \pmod{p}$  ולכן

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

כנדרש.

טענה 2. לכל מספר ראשוני ושלם  $a$  מתקיים  $\gcd(a, p) = 1$  לפיכך קיים איבר הופכי

ככפוף את היחס שקיים ב-  $a^p \equiv 1 \pmod{p}$  (שהוכיחנו בסעיף הקודם) ב-

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

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 24: משפט אוילר

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

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

$$a^{-1} \equiv a^{\phi(n)-1} \pmod{n} \quad (2)$$

### משפט 25: 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 שקיימים

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

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

⋮

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

קיים פתרון יחיד מודולו  $M = m_1m_2 \cdots m_r$  שנitin על ידי

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

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

טענה 26: משפט השאריות הסיני

יהיו  $a, b, m$  שלמים. אז

$$(a \pmod{m})(b \pmod{m}) \equiv ab \pmod{m}.$$

**הוכחה:** לפי משפט החלוק של אטקליזס קיימים שלמים  $r_1, r_2$  כך ש:  $a = q_1m + r_1$  וכך  $a \mod m = a - q_1m$ .  
 $a \mod m = b - q_2m$  וכך  $r_2 = b \mod m = q_2m + r_2$  וכך  $b = q_2m + r_2$ .  
באותה מידה  $(a \mod m) (b \mod m) = (a - q_1m)(b - q_2m) = ab + (-aq_2 - bq_1 + q_1q_2m) \equiv ab \pmod{m}$ .

**משפט 29:**

יהיו  $a, m$  שלמים. אז

$$(a \mod m)^{-1} \mod m = a^{-1} \mod m$$

**משפט 27:**  
 $\text{יהיו } a, b, m \text{ שלמים. אז}$   
 $(a \mod m)(b \mod m) \mod m = ab \mod m$ .

**הוכחה:**

**משפט 28:**  
 $\text{אם } a, b, m \text{ שלמים חיובים אז:}$   
 $a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff a \mod m = b \mod m$ .

**הוכחה:**

נניח ש-  $b \equiv a \pmod{m}$ . נוכיח כי  $a \equiv b \pmod{m}$ .

$$\begin{aligned} a &= qm + b \Rightarrow b = -qm + a \Rightarrow b = Qm + b, \\ \text{ולכן } b &= Qm + a \text{ כ"א קיים שלם } Q = -q \text{ וכך } b \equiv a \pmod{m}. \end{aligned}$$

כנדרש.

נניח ש-  $a \equiv b \pmod{m}$ . נוכיח כי  $b \equiv a \pmod{m}$ .

$$\begin{aligned} a &= qm + b \text{ או קיים שלם } q \text{ כך ש: } a \equiv b \pmod{m} \\ \text{על פי ההגדרה של השארית:} \\ a \mod m &= a - \left\lfloor \frac{a}{m} \right\rfloor m. \end{aligned}$$

נזכיר:  $a = qm + b$

$$\begin{aligned} a \mod m &= qm + b - \left\lfloor \frac{qm + b}{m} \right\rfloor m \\ &= qm + b - \left\lfloor q + \frac{b}{m} \right\rfloor m \\ &= qm + b - qm - \left\lfloor \frac{b}{m} \right\rfloor m \\ &= b - \left\lfloor \frac{b}{m} \right\rfloor m \\ &= b \mod m. \end{aligned}$$

**הוכחה:**  
 $\text{נסמן } x \text{ מכיוון ש- } x \text{ הוא האיבר ההפכי של } a \mod m \text{ מודולר } m \text{ אז}$   
 $(a \mod m)x \equiv 1 \pmod{m}$ .  
 $\text{מכך קיימים שלם } q_1 \text{ כך ש: } (a \mod m)x = q_1m + 1 \text{ ונקבל}$   
 $(a - q_2m)x = q_1m + 1 \text{ וכך } a \mod m = a - q_2m$ .  
 $\text{ולכן } ax = (q_2x + q_1)m + 1 \text{ וכך}$   
 $ax \equiv 1 \pmod{m}$

ולכן

$$x \equiv a^{-1} \pmod{m} \Rightarrow (a \mod m)^{-1} \mod m = a^{-1} \mod m.$$

**משפט 30:**

$$d_k(e_k(x)) = x \mod p.$$

**הוכחה:**

$$\begin{aligned} \text{לפי ההגדרה של צופן El-Gamal, הכלל מצפינו הוא} \\ e_k(x) = (y_1, y_2) \quad y_1 \alpha^d \mod p, \quad y_2 = \beta^d x \mod p, \\ \text{כאשר } p \text{ ראשוני ו- } d \text{ שלם, והכלל מעונן הוא} \\ d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \mod p. \end{aligned}$$

**לפיכך:**

$$\begin{aligned} d_k(e_k(x)) &= d_k(y_1, y_2) \\ &= (y_1^a)^{-1} y_2 \mod p \\ &= [(\alpha^d \mod p)^a]^{-1} (x \beta^d \mod p) \mod p \\ &= (\alpha^{da} \mod p)^{-1} (x \beta^d \mod p) \mod p \\ &= ((\alpha^{da})^{-1} \mod p) (x \beta^d \mod p) \mod p \quad (\text{משפט 29}) \\ &= (\alpha^{da})^{-1} (x \beta^d) \mod p \quad (\text{משפט 27}) \\ &= (\alpha^{da})^{-1} (x (\alpha^a)^d) \mod p \quad (\text{El-Gamal}) \\ &= (\alpha^{da})^{-1} (x \alpha^{ad}) \mod p \\ &= (\alpha^{da})^{-1} \alpha^{ad} x \mod p \\ &= x \mod p. \end{aligned}$$

### משפט 31

יהיו  $a, b, c, d$  מספרים ממשיים כך ש-  $a \geq b \Rightarrow a - b \geq 0$  ו-  $c \geq d \Rightarrow c - d \geq 0$   
 $ac + bd \geq ad + bc$ .

הוכחה:

$$a \geq b \Rightarrow (a - b) \geq 0$$

$$c \geq d \Rightarrow (c - d) \geq 0.$$

לכן

$$(a - b)(c - d) \geq 0 \Rightarrow ac + bd - bc - ad \geq 0 \Rightarrow ac + bd \geq bc + ad.$$

### משפט 32

יהי  $X = \{x_1, x_2, \dots, x_k\}$  קבוצת אובייקטים בעלי פונקציית ההסתברות  $p_i = P_X(x_i)$  כך ש-

$$p_1 \geq p_2 \geq \dots \geq p_k$$

ונתונה הצפנה בינהarity  $f : X \rightarrow \{0, 1\}$ .

כלומר, אורך ההצעה ובינהarity של  $x_i$  בambil אורות, אותן  $x_i$  מוצפן ע"י  $n_i$  ספרות בינהarity.

$$n_1 \leq n_2 \leq \dots \leq n_k.$$

הוכחה: נניח בשלילה שקיימות תמורה  $\{n_1, \dots, n_k\}$  של  $\{n_{i_1}, \dots, n_{i_k}\}$  כך שהתוחלת

$$E = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_{i_j}p_j + \dots + n_{i_k}p_k.$$

ולא הגבלת הכלליות נניח כי  $n_1 = n_{i_j}$  וא'

$$E = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_{i_j}p_j + \dots + n_{i_k}p_k.$$

$n_{i_{j-1}} \geq n_1$  אז בהכרח  $n_1 = \min(n_1, \dots, n_k)$

$p_{j-1} \geq p_j$  לכן  $p_1 \geq p_2 \geq \dots \geq p_k$

כלומר לפי משפט 31

$$n_{i_{j-1}}p_{j-1} + n_{i_j}p_j \geq n_1p_{j-1} + n_{i_{j-1}}p_j. \quad (1*)$$

לכן אם נחליף  $n_1$  עם  $n_{i_{j-1}}$  ב-  $E$  נקבל את התוחלת החדשה

$$E' = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_{i_{j-1}}p_j + \dots + n_{i_k}p_k$$

כך שלפי (1\*)

$$E' = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_{i_{j-1}}p_j + \dots + n_{i_k}p_k \leq n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_1p_j + \dots + n_{i_k}p_k = E$$

ו"א  $E' \leq E$  בסתיו לכך  $E'$  כהוותת המינימלית.

### משפט 33: קריפטו-מערכת RSA ניתן לפענוח

יהי  $n = pq$  מספרים ראשוניים שונים,  $a, b \in \mathbb{Z}$  שלמים חיוביים כך ש-  $(a, b) = 1 \pmod{\phi(n)}$

אם  $x \in \mathbb{Z}_n$

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

### שיטת 2

לפי ההגדירה של צופן El-Gamal, הכלל מצפין הוא

$$e_k(x) = (y_1, y_2) \quad y_1 = \alpha^d \pmod{p}, \quad y_2 = \beta^d x \pmod{p},$$

כאשר  $p$  ראשוני ו-  $d$  שלם, והכלל מעפנח הוא

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \pmod{p}.$$

לפיכך:

$$d_k(e_k(x)) = d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \pmod{p} = [(\alpha^d \pmod{p})^a]^{-1} (\beta^d x \pmod{p}) \pmod{p}. \quad (*1)$$

זהות הbhava מתקיימת. אם  $z, m, n$  שלמים חיוביים אז

$$(z \pmod{m})^n \equiv z^n \pmod{m}. \quad (*2)$$

הוכחה: לפי משפט החלוק של אטקלידס קיימים שלמים  $q, r$  כך ש-  $z = qm + r$ . מכיוון  $r = z \pmod{m}$ ,  $z = qm + r$  ו-  $z = qm + r - qm = r$ . לכן

ממשוואת (\*2), לכל  $y, z, m, n$  שלמים חיוביים:  $y(z \pmod{m})^n \equiv yz^n \pmod{m}$  ולכן  $y(z \pmod{m})^n \pmod{m} = yz^n \pmod{m}$ .  $(*)3$

בנוסף להזאות הbhava מתקיימת. לכל שלמים חיוביים  $b, c, m$

$$b \equiv c \pmod{m} \Rightarrow b^{-1} \equiv c^{-1} \pmod{m}. \quad (*)4$$

הוכחה: נניח  $cb^{-1} \equiv bb^{-1} \pmod{m}$   $\equiv 1 \pmod{m}$  ו-  $bb^{-1} \equiv 1 \pmod{m}$ . מכיוון  $b \equiv c \pmod{m}$  ו-  $b^{-1} \equiv c^{-1} \pmod{m}$

מן (\*2) ו- (\*4), לכל  $z, m, n$  שלמים חיוביים:  $[(z \pmod{m})^n]^{-1} \equiv z^{-n} \pmod{m}$ .  $(*)5$

מכאן, לכל  $y$  שלם:

$$[(z \pmod{m})^n]^{-1} \equiv z^{-n} \pmod{m} \Rightarrow [(z \pmod{m})^n]^{-1} y \equiv z^{-n}y \pmod{m}. \quad (*)6$$

ולכן

$$[(z \pmod{m})^n]^{-1} y \pmod{m} = z^{-n}y \pmod{m}. \quad (*)7$$

לפי משוואת (\*7), אם נציב  $y = x\beta^d \pmod{p}$ ,  $m = p$ ,  $z = \alpha^d \pmod{p}$ ,  $\beta = \alpha^a \pmod{p}$  נקבל:

$$[(\alpha^d \pmod{p})^a]^{-1} (\beta^d \pmod{p}) \pmod{p} = \alpha^{-ad} (\beta^d \pmod{p}) \pmod{p}, \quad (*)8$$

ולכן לפי משוואת (\*1):

$$d_k(e_k(x)) = \alpha^{-ad} (\beta^d \pmod{p}) \pmod{p}. \quad (*)9$$

לכל שלמים  $b, c, m$  מתקיימים:

$$b(c \pmod{m}) \pmod{m} = bc \pmod{m} \quad (*)10$$

ולכן

$$d_k(e_k(x)) = \alpha^{-ad} x \beta^d \pmod{p}. \quad (*)11$$

נציב את ההגדירה של  $p$  ו-  $\beta = \alpha^a \pmod{p}$

$$d_k(e_k(x)) = \alpha^{-ad} x (\alpha^a \pmod{p})^d \pmod{p}.$$

ואז לפי משוואת (\*8) אנחנו נקבל ש:

$$d_k(e_k(x)) = \alpha^{-ad} x \alpha^{ad} \pmod{p} = x \pmod{p}.$$

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**

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

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

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

**שלב 4** (נתון) לכן  $t$  קיים שלם כך ש-  $ab \equiv 1 \pmod{\lambda(n)}$

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

$$\text{לכן } ab - 1 = t(p - 1)q' .$$

מכאן

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

כאשר  $y = x^{tp'}$  והשוויין השני מתקיים בגלל ש-  $p$  מספר ראשוני. לפיכך  $x^{ab-1} \equiv 1 \pmod{p}$ .

**שלב 5** (נתון) לכן  $t$  קיים שלם כך ש-  $ab \equiv 1 \pmod{\lambda(n)}$

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

לכן

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

מכאן

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

כאשר  $z = x^{tp'}$  והשוויין 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.

**הוכחה:**

**שלב 1** רושמים את הצלופן:

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

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

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

**משפט 35**

$$a \equiv b \pmod{m} \text{ ו } a \pmod{m} = b \pmod{m}$$

מכאן הפונקציית אוילר של  $np$  היא

$$\begin{aligned}\phi(np) &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_i^{e_{i-1}-1}) (p_i^{e_i+1} - p_i^{e_i}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_i^{e_{i-1}-1}) p(p_i^{e_i} - p_i^{e_i-1}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p(p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_i^{e_{i-1}-1}) (p_i^{e_i} - p_i^{e_i-1}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p\phi(n).\end{aligned}$$

■

### משפט 37:

יהיו  $a$  ו-  $b$  מספרים ראשוניים.

$$\phi(a) = a - 1 . \mathbf{1}$$

$$\phi(ab) = (a - 1)(b - 1) . \mathbf{2}$$

הוכחה:

1. ראשוני לכן הפירוק לראשוניים שלו הוא  $p_1^{e_1}$  כאשר  $e_1 = 1$  ו-  $p_1 = a$ .

לכן הפונקציית אוילר של  $a$  הינה

$$\phi(a) = (p_1^{e_1} - p_1^{e_1-1}) = a - 1.$$

2. ראשוני ו-  $b$  ראשוני לכן הפירוק לראשוניים של  $ab$  הוא  $p_1^{e_1}p_2^{e_2}$  כאשר  $e_1 = 1, e_2 = 1$ ,  $p_1 = a, p_2 = b$ .

לכן הפונקציית אוילר של  $ab$  הינה

$$\phi(ab) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) = (a - 1)(b - 1).$$

■

### משפט 38:

יהיו  $a, b$  מספרים שלמים.

אם קיימים שלמים  $s, t$  כך ש-  $sa + tb = 1$  אז  $a$  ו-  $b$  זרים.

הוכחה: יהי  $d$  וה-  $a$  של  $\gcd(a, b) = 1$ . אם  $d \mid a$  ו-  $d \mid b$  אז  $d$  מחלק  $sa + tb = 1$ .

■

### משפט 39:

יהיו  $a, b, n$  שלמים חיוביים. אז  $\gcd(a^n, b^n) = \gcd(a, b)^n$ .

הוכחה: יהי  $d \mid a$  ו-  $d \mid b$ . לכן קיימים שלמים  $q_1, q_2$  עבורם  $a = q_1d$ ,  $b = q_2d$ .

מכאן

$$\gcd(q_1, q_2) = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) \stackrel{\text{טעמ}}{=} 1$$

"א"א  $q_1, q_2$  לא חולקים גורמים משותפים (לפי פירוק לגרורותים הראשונים) ולכן גם  $\gcd(q_1^n, q_2^n) = 1$ .

נשים לב:

$$\begin{aligned} \gcd(a^n, b^n) &= \gcd(q_1^n d^n, q_2^n d^n) \\ &= d^n \gcd(q_1^n, q_2^n) \\ &= d^n \\ &= \gcd(a, b)^n. \end{aligned}$$

#### משפט 40:

יהיו  $a, b$  שלמים.

$c | d \wedge b \mid a \Rightarrow d = \gcd(a, b)$

הוכחה:  
כיוון  $\Leftarrow$

יהי  $b = cb' \wedge a = ca'$ . נניח כי  $c | a$  וגם  $c | b$ . אזי קיימים שלמים  $s, t$  עבורם  $a = sca' + tcb' = c(sa' + tb')$ .

לכן לכל מחלק משותף  $c$  של  $a$  ו- $b$  מתקיים  $c | d$ .

כיוון  $\Rightarrow$

נניח שעבור כל מחלק משותף  $c$  של  $a$  ו- $b$  מתקיים  $c | d'$ .

$$d' \leq c \Leftrightarrow d' = qc \Leftrightarrow$$

מכיוון ש-  $c | a$  ו-  $c | b$  אזי  $c | \gcd(a, b)$  בפרט  $c \leq \gcd(a, b)$ .

$$d' \leq \gcd(a, b) \Leftrightarrow d' \leq c \leq \gcd(a, b) \Leftrightarrow$$

מצד שני, הוא עצמו מחלק משותף של  $a$  ו- $b$ , לכן לפי ההנחה התחתית,  $\gcd(a, b) \leq d' \Leftrightarrow d' = Q \gcd(a, b)$  עבורו  $Q$

"א"א קיבלנו ש-  $\gcd(a, b) \leq d'$  וגם  $d' \leq \gcd(a, b)$  לכן בחרך (ב)

#### משפט 41: האלגוריתם של אוקלידיס

אם  $a, b$  שלמים ווגם  $b \neq 0$  אז  $\gcd(a, b) = \gcd(b, a \bmod b)$

הוכחה:

$$\gcd(a, b) \mid \gcd(b, a \bmod b)$$

לפי המשפט החילוק של אוקלידיס (משפט קיימים שלמים  $q, r$  עבורם  $a = qb + r$   $\Rightarrow a \bmod b = a - \lfloor \frac{a}{b} \rfloor b$ ).

לכן אם  $d \mid \gcd(b, a \bmod b) \Leftrightarrow d \mid (a \bmod b) \Leftrightarrow d \mid b \wedge d \mid a$  אזי  $d = \gcd(a, b)$ .

ובת נוכחות כי  $\gcd(b, a \bmod b) \mid \gcd(a, b)$ .

נסמן  $q, r$  עבורם  $a = qb + r$ . לפי המשפט החילוק של אוקלידיס קיימים שלמים  $r$  עבורם  $a \bmod b = a - \lfloor \frac{a}{b} \rfloor b$ .

לכו א"מ  $d \mid a \bmod b \wedge d \mid b \Rightarrow d \mid a$  וגם  $d \mid a$ .

הוכחנו כי  $\gcd(a, b) \mid \gcd(b, a \bmod b) \wedge \gcd(b, a \bmod b) \mid \gcd(a, b)$  ולכן  $\gcd(a, b) = \gcd(b, a \bmod b)$ .

#### משפט 42: הקשר בין יחס שקולות מודולרי והשארית

יהיו  $a, b, m$  שלמים חיוביים.

הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:  
 $a \bmod m = b \bmod m \Rightarrow a \equiv b \pmod{m}$

הוכחה:

כיוון  $\Leftarrow$

נניח ש-  $a \equiv b \pmod{m}$ . אזי קיים שלם  $Q$  כך ש:

$$a = qm + b.$$

לפי משפט החילוק של אוקלידיס,

$$b = \bar{q}m = r_1, \quad r_1 = b \bmod m.$$

לכן

$$a = (q + \bar{q})m + r_1 = Qm + r_1$$

כאשר  $Q = q + \bar{q}$  שלם ו-  $0 \leq r_1 < b$  הוא השארית. מכאן נובע:

$$a \bmod m = a - m \left\lfloor \frac{a}{m} \right\rfloor = Qm + r_1 - Qm = r_1$$

$a \bmod m = r_1 = b \bmod m$  נ"ז

כיוון  $\Rightarrow$

לכן

$$a - m \left\lfloor \frac{a}{m} \right\rfloor = b - m \left\lfloor \frac{b}{m} \right\rfloor \Rightarrow a = \left( \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor \right) m + b \Rightarrow a = qm + b$$

נניח ש  $a \bmod m = b \bmod m$  אז  
כלומר קיים שלם  $q = \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor$

**משפט 43:**

$b \equiv c \pmod{m}$  אם ורק אם  $ab \equiv ac \pmod{m}$ .  
יהי  $a, m$  מספרים זרים.

הוכחה:

ביוון ⇔

נניח כי  $ab \equiv ac \pmod{m}$

$$ab \equiv ac \pmod{m} \Rightarrow ab = ac + qm \Rightarrow ab - ac = qm \Rightarrow a(b - c) = qm.$$

מכאן  $a \mid qm$ .

$q = ak$  זרים שכן  $a \nmid m$  ולכן  $k \exists$  ש  $a \nmid k$  שכן  $a, m$  זרים.

$$a(b - c) = qm \Rightarrow a(b - c) = akm \Rightarrow b - c = km \Rightarrow b = c + km \Rightarrow b \equiv c \pmod{m}.$$

ביוון ⇒

נניח כי  $b \equiv c \pmod{m}$

$$b = qm + c \Rightarrow ab = aqm + ac \Rightarrow ab \equiv ac \pmod{m}.$$

**משפט 44:**

יהי  $a, m$  מספרים (לא בהכרח זרים).

$$. b \equiv c \pmod{\frac{m}{\gcd(a, m)}} \text{ אם ורק אם } ab \equiv ac \pmod{m}$$

הוכחה:

ביוון ⇔

נניח כי  $ab \equiv ac \pmod{m}$  אז

$$ab = ac + qm \Rightarrow ab - ac = qm \Rightarrow m \mid a(b - c) \Rightarrow \frac{m}{\gcd(a, m)} \mid \frac{a}{\gcd(a, m)}(b - c).$$

מכיוון ש  $\frac{a}{\gcd(a, m)}$  זרים, אז

$$\frac{m}{\gcd(a, m)} \mid (b - c).$$

$$b \equiv c \pmod{\left(\frac{m}{\gcd(a, m)}\right)}.$$

**משפט 45:**

יהיו  $a, b, c$  שלמים.

$a^n \equiv b^n \pmod{c}$  אם ורק אם  $a \equiv b \pmod{c}$  ו  $n > 1$ .

הוכחה: אם  $a \equiv b \pmod{c}$  אז קיים שלם  $q$  כך ש:  $a = qc + b$ .

לכן

$$a^n = (qc + b)^n = \left( \sum_{k=1}^n \binom{n}{k} q^k c^{k-1} b^{n-k} \right) c + b^n = Qc + b^n$$

כאשר  $Q$  שלם. לכן קיים שלם  $Q$  כך ש:  $a^n = Qc + b^n \Rightarrow a^n \equiv b^n \pmod{c}$ .

**משפט 46: מחזור בחזקת האורך שלו הוא תמורה הזותות**

תהי  $\pi : \Sigma \rightarrow \Sigma$  תמורה מעלהalfavit. אם  $\pi$  היא מחזור של אורך  $k$  אז

הוכחה: נניח כי  $\pi : \Sigma \rightarrow \Sigma$  מחזור באורך  $k$ . ז"א הוכיח למחוזרים של  $\pi$  והוא:

$$\pi = (a_1 \ a_2 \ \dots \ a_{k-1} \ a_k),$$

או, כפונקציה מעלה  $\Sigma$ :

$$\pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1.$$

אפשר לרשום את זה בביטוי יחיד:

$$\pi(a_i) = a_{(i \bmod k)+1}.$$

עבור  $\pi^2$ 

$$\pi^2(a_1) = a_3, \quad \pi^2(a_2) = a_4, \quad \dots \quad \pi^2(a_{k-2}) = a_k, \quad \pi^2(a_{k-1}) = a_1, \quad \pi^2(a_k) = a_2.$$

ובאותה מידה אפשר לרשום  $\pi^j$  בביטוי יחיד:

$$\pi^j(a_i) = a_{((i+1) \bmod k)+1}.$$

באופן כללי לכל  $j \geq 0$  טבעי:

$$\pi^j(a_i) = a_{((i+j-1) \bmod k)+1}.$$

מכיון נציג  $k$   $j = k$   $i < k$ .

$$\pi^k(a_i) = a_{((i+k-1) \bmod k)+1} = a_{((i-1) \bmod k)+1} = \begin{cases} a_i & : i < k \\ a_k & : i = k \end{cases}.$$

ז"א לכל  $1 \leq i \leq k$ 

$$\pi^k(a_i) = a_i \Rightarrow \pi^k = \text{id}$$

ז"א לצופן קיסר יש סודיות מושלמת.  
במילים פשוטות צופן קיסר אינו ניתן לפענה בתנאי שימושים ב מפתחות מקרי חדש כל פעם שמצפים אותם אחד של טקסט גלי.

#### משפט 47: תנאי לסודיות מושלמת של צופן קיסר

אם לכל מפתח  $K \in K$  בצופן קיסר יש הסתברות שווה, כלומר  
 $P(K = k) = \frac{1}{26}$ .

אז לצופן קיסר יש סודיות מושלמת.

**הוכחה:** תחילה נחשב את ההסתברות  $P(Y = y)$  באמצעות (??). הקבוצת מפתחות בצופן קיסר היא  $K = \{0, 1, \dots, 25\} = \mathbb{Z}_{26}$ .

לכן

$$P(Y = y) = \sum_{k \in \mathbb{Z}_{26}} P(K = k)P(X = d_k(y)) .$$

אם ההסתברות של כל מפתח שווה אז  $P(K = k) = \frac{1}{26}$  ולפיכך  $P(K = k) = \frac{1}{26}$ .

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = d_k(y)) .$$

הכלל מצפין והכלל מפענץ של צופן קיסר מוגדרים  $e_k(x) = x + k \pmod{26}$ ,  $d_k(y) = y - k \pmod{26}$ .

כאשר לפיכך  $P(X = d_k(y)) = P(X = y - k \pmod{26})$ .  $k \in \mathbb{Z}_{26}$

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = y - k \pmod{26}) .$$

הסכום בצד הימין הוא רק סכום של  $P(X = k)$  מעל כל האיברים  $k \in \mathbb{Z}_{26}$ . לכן

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = k) = \frac{1}{26} \cdot 1 = \frac{1}{26} .$$

כאשר בשווין השני השתמשנו בתכונת הנרמול של הפונקציית הסתברות של המ"מ  $X$ .

מצד שני, לפי (??),

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k)$$

האילוץ על הסכום  $x = d_k(y)$  אומר ש-

$$x = k - y \pmod{26} \Rightarrow k = x + y \pmod{26} .$$

כל  $x \in X$  וכל  $y \in Y$  קיים רק מפתח אחד אשר מקיים תנאי זה. ז"א רק איבר אחד של הסכום נושא ולפיכך

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k) = P(K = y - x \pmod{26}) .$$

אם ההסתברות של כל מפתח שווה, כאמור אם  $P_K(k) = \frac{1}{26}$  לכל  $k \in K$  אז

$$P(Y = y|X = x) = P(K = y - x \pmod{26}) = \frac{1}{26} .$$

לכן

$$P(Y = y) = \frac{1}{26} = P(Y = y|X = x)$$

■  
במילים פשוטות צופן קיסר אינו ניתן לפענה בתנאי שימושים ב מפתחות מקרי חדש כל פעם שמצפים אותם אחד של טקסט גלי.

#### משפט 48: תנאי חילופי לסודיות מושלמת

לפי נוסחת בייס אם לкриpto-מערכת יש סודיות מושלמת אז מתקאים גם (1)

$$P(Y = y|X = x) = P(Y = y) .$$

#### משפט 49

נתונה קריpto-מערכת בעלת סודיות מושלמת.

אם  $P(Y = y) > 0$  אז

(1) קיימים לפחות מפתח אחד  $k \in K$  כך ש-  $e_k(x) = y$

(2)  $|K| \geq |Y|$

**הוכחה:**

(1) לפי (1)

$$P(Y = y|X = x) = P(Y = y) > 0 \quad (\#1)$$

נambil (??) בצד שמאל ונקבל

$$\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) = P(Y = y) > 0 \quad (\#2)$$

נ"ז

$$\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) > 0 \quad (\#3)$$

לכן קיימים לפחות מפתח אחד,  $k$  עבורו  $x = d_k(y)$

ז"א קיימים לפחות מפתח אחד,  $k$  עבורו  $y = e_k(x)$

(2) לפי (#1) ו- (#3), לכל  $y \in Y$  קיים לפחות מפתח אחד,  $k$  עבורו  $y = e_k(x)$ , לכן בהכרח  $|K| \geq |Y|$ . (#4)

#### משפט 50: משפט שאנו

נתונה קריpto-מערכת  $(X, Y, K, E, D)$  כך ש-  $|X| = |Y| = |K|$  ומתקיים גם

למערכת יש סודיות מושלמת אם ורק אם

(1) לכל  $x \in X$  ולכל  $y \in Y$  קיים מפתח  $k$  ייחיד עבורו  $y = e_k(x)$

**2)** לכל מפתח יש הסתברות שווה, כלומר  $P(K = k) = \frac{1}{|K|}$

הוכחה:

$$1) \text{ נניח כי } |Y| = |K|. \text{ כלומר}$$

$$|\{e_k(x) | x \in X\}| = |K|.$$

ז"א לא קיימים שני מפתחות  $k_1 \neq k_2$  כך ש-

לכן לכל  $x \in X$  וכל  $y \in Y$  קיים מפתח  $k$  ייחד עבורו  $y$

2) נסמן אורך של קבועות מפתחות ב-  $n = |K|$ . נרשים את הקבוצת טקסטים גלויים כ-

$$X = \{x_i | 1 \leq i \leq n\}$$

נתון  $y \in Y$  קבוע. מספר את המפתחות כ-  $k_1, k_2, \dots, k_n$  כך ש-  $e_{k_i}(x_i) = y$ . לפי נוסחת ביס'

$$P(X = x_i | Y = y) = \frac{P(Y = y | X = x_i) P(X = x_i)}{P(Y = y)}$$

$$\stackrel{\text{טענה}}{=} \frac{P(K = k_i) P(X = x_i)}{P(Y = y)}$$

אם לمعרכת יש סודיות מושלמת אז  $P(X = x_i | Y = y) = P(X = x_i)$  כלומר

$$P(X = x_i) = \frac{P(K = k_i) P(X = x_i)}{P(Y = y)} \Rightarrow P(K = k_i) = P(Y = y)$$

לכל  $n \geq i \geq 1$ . ז"א לכל מפתח יש הסתברות שווה

$$P(K = k_i) = \frac{1}{|K|}.$$

### משפט 51: אנטרופיה של שניו

נתון משתנה מקרי  $X$  בעל פונקציית ההסתברות  $P_X(x)$ . התוחלת המינימלית של אורך ההצפנה של  $X$  מסומן ב-  $H[X]$  ונתונה על ידי הנוסחה

$$H[X] = - \sum_{x \in X} P_X(x) \log_2 P_X(x).$$

נקרא האנטרופיה של  $X$ .

הוכחה: נניח כי  $X = Y \cap Z$ , כאשר  $Y, Z$  משתנים מקרים בלתי תלויים. לפי משווה (??):

$$\ell_Q(x) = f(p_x).$$

$$H[X] = \sum p_x \ell_Q(x) = \sum p_x f(p_x).$$

תהיינה  $P_Y(y)$  ו-  $P_Z(z)$  פונקציות ההסתברות של  $Y$  ושל  $Z$  בהתאמה.  
נסמן  $p_z = P_Z(z)$  ו-  $p_y = P_Y(y)$

מכיוון ש-  $Y$  ו-  $Z$  משתנים בלתי תלויים אז

$$P(X = Y \cap Z) = P_Y(y)P_Z(z) = p_y p_z.$$

נשים לב שידיעה של  $Y$  לא נותנת שום מידע על הערך של  $Z$ , לכן  $\ell_Q[Y \cap Z] = \ell_Q[Y] + \ell_Q[Z]$ .

לפיכך

$$H[X] = \sum p_x \ell_Q(x) = \sum p_y p_z [\ell_Q(y) + \ell_Q(z)]$$

$$H[X] = \sum p_y p_z f(p_y p_z) = \sum p_y p_z [f(p_y) + f(p_z)]$$

$$f(p_y p_z) = f(p_y) + f(p_z).$$

$$. f(p) = C \log(p) \text{ נ"א}$$

כעת נניח כי יש לנו משתנה מקרי  $X = \{a, b\}$  בעל פונקציית ההסתברות  $P_X(a) = \frac{1}{2}, P_X(b) = \frac{1}{2}$ . ההצפנה של  $X$  צריכה ספרה אחת, לכן  $f(\frac{1}{2}) = 1$  ונקבל  $f(Q^*(a)) = \ell_{Q^*}(a) = 1$  ו-  $f(Q^*(b)) = \ell_{Q^*}(b) = 1$ .

■

### משפט 52:

נתון מ"מ בדיד  $X$  אשר מקבל  $N$  ערכים שונים  $X = \{x_1, \dots, x_N\}$  בהסתברות שווה, כלומר

$$P(X = x_i) = \frac{1}{N}$$

از האנתרופיה מקבלת ערך מקסימלי שניתנת על ידי  $H_{\max}(X) = \log_2 N$ .

ערך זה הוא הערך המקסימלי האפשרי של האנתרופיה.

### משפט 53: אי שוויון האפמן

נתון קבועות אחרות של טקסט גלי  $X$  והצפנה האפמן  $f$ . נניח כי  $l(f)$  תוחלת האורך של ההצפנה ו-  $H(X)$  האנתרופיה של הטקסט גלי. מתקיים

$$H(X) \leq l(f) \leq H(X) + 1.$$