

1	הגדרות	1
5	משפטים	2

1 הגדרות

הגדרה 1: שלם שמחלק 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 שקילות בין a ל- 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 מספרים שלמים $a, b \in \mathbb{Z}$, היחס

$$a \bmod b$$

מציין את השארית בחלוקת a ב- b .

הגדרה 4: המחלק המשותף הגדול ביותר gcd

נתונים שני מספרים שלמים $a, b > 0$. המחלק המשותף הגדול ביותר של a ו- b מסומן $\gcd(a, b)$ (greatest common divisor) ומוגדר להיות המספר שלם הגדול ביותר שמחלק גם a וגם b .

הגדרה 5: כפולה משותפת קטנה ביותר

נתונים שני מספרים שלמים $a, b > 0$. הכפולה המשותפת הקטנה ביותר מסומן $\text{lcm}(a, b)$ (lowest common multiple) ומוגדר להיות המספר השלם החיובי הקטן ביותר ש- a ו- b מחלקים אותו.

הגדרה 6: מספרים זרים

נניח כי $a \geq 1$ ו- $b \geq 2$ 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 מאחת שמחלק את שניהם.

הגדרה 7: פונקציית אוילר

יהי m מספר שלם. הפונקציית אוילר מסומנת ב- $\phi(m)$ ומוגדרת להיות השלמים שקטנים ממש m זרים ביחס ל- m .

$$\phi(m) := \{a \in \mathbb{N} \mid \gcd(a, m) = 1, a < m\}.$$

הגדרה 8: צופן ההזזה

יהיו $P = C = K = \mathbb{Z}_{26}$. עבור $0 \leq k \leq 25$ נגדיר

$$e_k(x) = (x + k) \bmod 26, \quad x \in \mathbb{Z}_{26}$$

ו-

$$d_k(y) = (y - k) \bmod 26, \quad y \in \mathbb{Z}_{26}.$$

צופן ההזזה מוגדר מעל

הגדרה 9: (substitution cypher) צופן ההחלפה

בצופן ההחלפה, $P = C = \mathbb{Z}_{26}$.
 K מורכב מכל ההחלפות האפשריות של ה-26 סמלים $0, 1, 2, \dots, 25$.

עבור כל החלפה $\pi \in K$ נגדיר כלל מצפין

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

ונגדיר כלל מפענח

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

כאשר π^{-1} ההחלפה ההופכית של π .

הגדרה 10: צופן אפיני

יהי $P = C = \mathbb{Z}_{26}$ ויהי

$$K = \{a, b \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}.$$

עבור $k = (a, b) \in K$ ועבור $x \in \mathbb{Z}_{26}$ נגדיר כלל המצפין

$$e_k(x) = (ax + b) \bmod 26,$$

ועבור $y \in \mathbb{Z}_{26}$ נגדיר כלל המענח

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

הגדרה 15: 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

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

לכל $k = (n, p, q, a, b) \in K$, וכל $x \in P$ ו- $y \in C$ נגדיר כלל מצפין $e_k(x) = x^b \pmod{n}$,

ונגדיר כלל מפענח

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

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

הגדרה 16: רשת פייסטל (Feistel)

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

מחלקים את x לשני חצאים שנסמן L_0 ו- R_0 :

ברשת פייסטל יש 4 מרכיבים:

- מספר שלם N אשר קובע את המספר השלבים בתהליך הצפנה.

- מפתח התחלתי k .

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

- פונקציית ליבה $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$.

(1) מגדירים $R_0 = x_n \dots x_{2n}$, $L_0 = x_1 \dots x_n$.

(2) בשלב ה- i ית $(1 \leq i \leq N)$:

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

(3) בשלב ה- N נקבל את הטקסט מוצפן לפי

$$y = R_N L_N$$

הגדרה 17: משוואות פייסטל

משוואות פייסטל להצפנה:

נתון טקסט גלוי $x = L_0 R_0$ לכל $1 \leq i \leq N$:

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

משוואות פייסטל לפענוח:

נתון טקסט גלוי $y = R_N L_N$ לכל $1 \leq i \leq N$:

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

הגדרה 11: צופן ויז'נר (Vigenere Cipher)

יהי m מספר שלם חיובי.

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

עבור מפתח $k = (k_1, k_2, \dots, k_m)$ נגדיר כלל מצפין

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

ונגדיר כלל מפענח

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

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

הגדרה 12: צופן היל

נניח כי $m \geq 2$ מספר שלם.

יהי $P = C = \mathbb{Z}_{26}^m$ ויהי

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

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

עבור מפתח $k \in K$ נגדיר כלל מצפין

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

ונגדיר כלל מפענח

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

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

הגדרה 13: המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$.

הקופקטור ה- (i, j) של A מוגדר להיות הדטרמיננטה של המטריצה המתקבלת מ- A ע"י מחיקת שורה i ועמודה j , כפול $(-1)^{i+j}$.

המטריצה של קופקטורים של המטריצה A מוגדרת

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

כאשר C_{ij} הקופקטור ה- (i, j) של A .

הגדרה 14: המטריצה המצורפת

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

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

כאשר C המטריצה של קופקטורים של A .

$$ab \mid n$$

הוכחה:

$$\begin{aligned} a \mid n, \quad b \mid n \\ \text{לכן קיימים שלמים } k \text{ ו- } l \text{ כך ש-} \\ n = ak, \quad n = bl. \\ \text{ז"א } n = ak = bl \\ \text{מכאן } b \mid ak \\ \text{נתון כי } \gcd(a, b) = 1, \text{ לכן } b \mid k, \text{ לכן } k = bq \\ \text{לכן } n = ak = abq \end{aligned}$$

משפט 2: תכונות של ה- \gcd

$$\begin{aligned} 1. \gcd(ma, mb) &= m \gcd(a, b) \\ 2. \text{ אם } m > 0 \text{ ואם } m \mid a \text{ ו- } m \mid b \text{ אז } \gcd\left(\frac{a}{m}, \frac{b}{m}\right) &= \frac{\gcd(a, b)}{m} \\ 3. \text{ המספרים } \frac{a}{\gcd(a, b)} \text{ ו- } \frac{b}{\gcd(a, b)} &\text{ מספרים זרים.} \\ 4. \text{ אם } c \mid ab \text{ ו- } c \text{ זר ביחס ל- } b \text{ אז } c \mid a. \\ 5. \text{ אם } a, c \text{ מספרים זרים ואם } b, c \text{ מספרים זרים אז } c \mid ab &\text{ מספרים זרים.} \\ 6. \gcd(a, b) = \gcd(a + cb, b) \end{aligned}$$

הוכחה:

$$\begin{aligned} 1. \text{ יהי } d = \gcd(a, b). \text{ אז קיימים שלמים } s, t \text{ עבורם} \\ sa + tb = d. \\ \text{מכאן} \\ msa + mtb = md \Rightarrow s(ma) + t(mb) = md. \\ \text{לכן } \gcd(ma, mb) = md = m \gcd(a, b) \\ 2. \text{ יהי } d = \gcd(a, b) \\ \exists \text{ שלמים } s, t \text{ כך ש-} \\ sa + tb = d. \quad (*) \\ \text{נחלק } (1*) \text{ ב- } m \text{ ונקבל} \\ s \frac{a}{m} + t \frac{b}{m} = \frac{d}{m}. \quad (**) \\ \text{נשים לב } a \mid m \text{ ו- } b \mid m. \text{ לכן } \frac{a}{m} \text{ שלם ו- } \frac{b}{m} \text{ שלם.} \end{aligned}$$

הגדרה 18: סודיות מושלמת

$$\begin{aligned} \text{אומרים כי לקריפטו-מערכת יש סודיות מושלמת אם} \\ P(X = x | Y = y) = P(X = x) \\ \text{לכל } y \in Y, x \in X \\ \text{ז"א ההסתברות כי הטקסט גלוי } X = x, \text{ בידעה כי הטקסט מוצפן } Y = y \text{ שווה רק להסתברות כי הטקסט} \\ \text{גלוי הוא } X = x \text{ והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן } y \text{ לא משפיע על ההסתברות כי} \\ \text{הטקסט גלוי } X = x. \end{aligned}$$

הגדרה 19: מידע של מאורע (שאנון)

$$\begin{aligned} \text{נתון משתנה מקרי } X. \text{ המידע של ערך מסוים של } X \text{ מסומן } I_X(x) \text{ ומוגדר להיות} \\ I(X = x) = \log_2 \left(\frac{1}{P_X(x)} \right) = -\log_2(P_X(x)) \\ \text{כאשר } P_X(x) \text{ פונקציה ההסתברות של המשתנה מקרי } X. \end{aligned}$$

הגדרה 20: הצפנת האפמן

$$\begin{aligned} \text{נתון משתנה מקרי } X. \text{ נגדיר הצפנת האפמן של } X \text{ להיות הפונקציה (כלל מצפין)} \\ f: X \rightarrow \{0, 1\}^* \\ \text{כאשר } \{0, 1\}^* \text{ קבוצת רצפים של סיביות סופיים.} \\ \text{נתון רצף מאורעות } x_1, \dots, x_n. \text{ נגדיר} \\ f(x_1 \dots x_n) = f(x_1) || \dots || f(x_n) \\ \text{כאשר "||" מסמן שרשור (concatenation).} \end{aligned}$$

הגדרה 21: תוחלת האורך של הצפנת האפמן

$$\begin{aligned} \text{נתונה הצפנת האפמן } f. \text{ תוחלת האורך של ההצפנה מוגדרת} \\ l(f) = \sum_{x \in X} P(X = x) |f(x)|. \end{aligned}$$

2 משפטים

משפט 1:

יהיו a, b, n מספרים שלמים.
אם השלושה תנאים הבאים מתקיימים:

$$\begin{aligned} (1) \quad a \text{ ו- } b \text{ זרים,} \\ (2) \quad a \mid n, \\ (3) \quad b \mid n \end{aligned}$$

משפט 3: תנאי לקיום איבר הופכי של חוג

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

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

כיוון \Leftarrow

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

$$sa + tm = 1 \Rightarrow sa = 1 - tm \Rightarrow sa \equiv 1 \pmod{m}.$$

לפיכך קיים שלם s אשר הוא האיבר ההופכי של a ב- \mathbb{Z}_m .

כיוון \Rightarrow

אם קיים איבר הופכי a^{-1} של a ב- \mathbb{Z}_m אז $a^{-1}a \equiv 1 \pmod{m}$. ז"א קיים שלם q כך ש:
 $a^{-1}a = 1 + qm \Rightarrow a^{-1}a + (-q)m = 1$.

לכן קיימים שלמים $s = a^{-1}$ 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 קיים c עבורו $ac \equiv 1 \pmod{b}$.

הוכחה: נניח בשלילה כי a, b זרים וקיים c עבורו $ac \equiv 1 \pmod{b}$.

ז"א קיים שלם q :

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

לכן קיימים שלמים $s = c$ ו- $t = -q$ עבורם $sa + tb = 1$. לפיכך ממשפט בז'ו a ו- b זרים, בסתירה לכך ש- a ו- b לא זרים.

משפט 5: חיסור של שאריות

אם a, b, m מספרים שלמים חיוביים אז

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

הוכחה: לפי משפט החילוק של אוקלידס קיימים שלמים q_1, r_1 כך ש:

$$a + b = q_1 m + r_1, \quad 0 \leq r_1 < m,$$

כאשר $q_1 = \left\lfloor \frac{a+b}{m} \right\rfloor$ וגם $r_1 = (a+b) \bmod m$. מכאן:

$$((a + b) \bmod m) - b = r_1 - b = a - q_1 m.$$

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

3.

4. a, b שלמים לכן קיימים שלמים s, t, d עבורם

$$sa + tb = d$$

$$d = \gcd(a, b)$$

מכאן

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

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

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

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

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

a ו- c זרים אז קיימים s ו- t שלמים עבורם

$$sa + tc = 1.$$

b ו- c זרים אז קיימים \bar{s} ו- \bar{t} שלמים עבורם

$$\bar{s}b + \bar{t}c = 1.$$

לכן

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

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

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

6. אם a, b שלמים אז קיימים שלמים s ו- t עבורם $sa + tb = d$ כאשר $d = \gcd(a, b)$. 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 $x = s$ ו- $y = t - cb$ עבורם

$$x(a + cb) + yb = d$$

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

משפט 8: נוסחת קיילי המילטון

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

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

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 יחידה של מספרים ראשוניים.

ז"א, יהי $a \in \mathbb{N}$ כל מספר טבעי. אז

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

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

משפט 10: הפירוק לראשוניים של פונקציית אוילר

נתון מספר טבעי m . 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:

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

וללא הגבלה כלליות נניח כי $k \leq n$. אז ה- \gcd נתון על ידי

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

משפט 12: שיטה לחישוב lcm

נתונים השלמים a, b כך שהפירוק לראשוניים שלהם הם:

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

וללא הגבלה כלליות נניח כי $k \leq n$. אז ה- lcm נתון על ידי

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

משפט 13:

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

ז"א קיים שלם $Q = -q_1$ כך ש:

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

ולכן

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

ולפיכך, מכיוון שהשני שלמים $((a+b) \bmod m) - b$ ו- a שקולים מודולריים ביחס ל- m , אז בהכרח יש להם אותה שארית בחלוקה ב- m :

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

משפט 6: צופן אפיני ניתן לפענוח

יהי $e_k(x)$ הכלל מצפין של צופן אפיני ויהי $d_k(y)$ הכלל מופענח של צופן אפיני. אזי

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

כלל $x \in \mathbb{Z}_{26}$. כלומר, צופן אפיני ניתן לפענוח.

הוכחה: נסמן $y = e_k(x)$.

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

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

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

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

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

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

$$= x \bmod 26 .$$

משפט 7: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.

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

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

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

M לא מספר ראשוני בגלל ש- $p_i > M$ לכל $1 \leq i \leq n$.

גם לא קיים מספק ראשוני p_i אשר מחלק את M . הרי

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

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

רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

Algorithm 1 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 בזו (Bezout's identity)

יהיו a, b שלמים ויהי $d = \gcd(a, b)$. קיימים שלמים s, t כך שניתן לרשום ה- $\gcd(a, b)$ כצירוף לינארי של a ו- b :

$$sa + tb = d.$$

משפט 17: האלגוריתם המוכלל של אוקלידס

יהיו a, b שלמים חיוביים. קיים אלגוריתם אשר נותן שלמים s, t, d עבורם

$$d = sa + tb$$

כאשר $d = \gcd(a, b)$, כדלקמן. ראשית מאתחלים:

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

אם $r_1 = b \neq 0$ אז מבצעים האיטרציה הראשונה של הלולאה. בשלב $i = 1$ מחשבים 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 $r_2 \neq 0$ אז עוברים לאיטרציה $i = 2$ שבה מחשבים 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 השלב ה- n שבו מקבלים r_{n+1} , ואז פולטים $s = s_n, t = t_n, d = r_n = \gcd(a, b)$. כל השלבים של האלגוריתם הם כדלקמן:

הוכחה:

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

משפט 14: משפט החילוק של אוקלידס

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

$$a = qb + r$$

כאשר $0 \leq r < |b|$.

• b נקרא ה מודולו,

• q נקראת המנה

• ואילו r נקרא השארית.

• במקרה ש- $a, b > 0$ אזי $a \bmod b = r$.

משפט 15: האלגוריתם של אוקלידס

יהיו a, b מספרים שלמים חיוביים. קיים אלגוריתם אשר נותן את $d = \gcd(a, b)$ כדלקמן. ראשית מאתחלים r_0 ו- r_1 :

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

אם $r_1 = b \neq 0$ אז מתחילים את הלולאה. בשלב $i = 1$ מחשבים 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 $r_2 \neq 0$ ממשיכים לשלב $i = 2$ שבו מחשבים 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 $r_{n+1} = 0$ בשלב ה- n . ית. כל השלבים של התהליך הם כדלקמן:

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

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

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

⋮

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

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

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

הוכחה: אינדוקציה.

משפט 19: נוסחה 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.

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

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

הוכחה:

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

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

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

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

נשים לב כי $0 < \frac{r}{b} < 1$, לכן לפי (*)2

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

נציב זה ב- (*)1 ונקבל

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

(ב) לפי משפט החילוק של אוקלידס 14, קיימים שלמים $q', 0 \leq r' < b$ כך ש-

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

כאשר $r' = (-a) \bmod b$ מכאן

$$a = -q'b - r' = -q'b - b + b - r' = -(q' + 1)b + (b - r'). \quad (*)4$$

נשים לב כי $b - r' \geq 0$. אבל לפי (*)1 $a = qb + r$ כאשר $r = a \bmod b$ ו- r יחיד. לכן

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

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

זהות השני מנובע מ- (*)5:

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

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

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

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

למטה רשום 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-

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$



■

משפט 21: זהויות של הפונקציות 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 ($\gcd(s, t) = 1$ כלומר) אז $\phi(st) = \phi(s) \cdot \phi(t)$.**(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 אזי

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

הוכחה:

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

מכיוון ש- $p \mid p!$ אזי $p \mid k!(p-k)! \binom{p}{k}$.
מכיוון ש: p מספר ראשוני אזי $p \nmid k!(p-k)!$ לכן בהכרח:

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

■

משפט 23: המשפט הקטן של פרמהאם p מספר ראשוני ו- $a \in \mathbb{Z}_p$ אז התנאים הבאים מתקיימים:

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

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

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

הוכחה:**טענה 1.** נוכיח באינדוקציה.שלב הבסיס:עבור $a = 0$ הטענה $0^p \equiv 0 \pmod{p}$ מתקיימת.שלב המעבר:נניח כי הטענה מתקיימת עבור a (שזה ההנחת האינדוקציה).נוכיח כי היא מתקיימת גם עבור $a + 1$ באופן הבא.

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

לכל $k \geq 1$ טבעי לפי משפט 22: $p \mid \binom{p}{k}$ ולכן

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

על פי ההנחת האינדוקציה: $a^p \equiv a \pmod{p}$ לכן

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

כנדרש.

טענה 2. לכל מספר ראשוני ושלם a מתקיים $\gcd(a, p) = 1$ לפיכך קיים איבר הופכי $a^{-1} \in \mathbb{Z}_p$.נכפיל את היחס שקילות $a^p \equiv 1 \pmod{p}$ (שהוכחנו בסעיף הקודם) ב- a^{-1} :

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

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

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

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

משפט 25: משפט השאריות הסינייהיו m_1, m_2, \dots, m_r שלמים אשר זרים בזוגות ויהיו a_1, a_2, \dots, a_r שלמים. למערכת של יחסים שקילות

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

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

⋮

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

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

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

כאשר $M_i = \frac{M}{m_i}$ ו- $y_i \equiv M_i^{-1} \pmod{m_i}$ לכל $1 \leq i \leq r$.**משפט 26:**יהיו a, b, m שלמים. אזי

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

משפט 29:

יהיו a, m שלמים. אזי

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

הוכחה:

נסמן $(a \bmod m)^{-1} \bmod m \equiv x$. אז, מכיוון ש- x הוא האיבר ההופכי של $a \bmod m$ מודולר m אזי $(a \bmod m)x \equiv 1 \bmod m$.

מכאן קיים שלם q_1 כך ש: $(a \bmod m)x = q_1m + 1$. נציב $a \bmod m = a - q_2m$ ונקבל $(a - q_2m)x = q_1m + 1$ ולכן $ax = (q_2x + q_1)m + 1$ ולכן

$$ax \equiv 1 \bmod m$$

ולכן

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

משפט 30:

צופן El-Gamal ניתן לפענוח. כלומר

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

הוכחה:

שיטה 1

לפי ההגדרה של צופן El-Gamal, הכלל מצפיון הוא

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

כאשר p ראשוני ו- d שלם, והכלל מעפנח הוא

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

לפיכך:

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

הוכחה: לפי משפט החילוק של אטקלידס קיימים שלמים q_1, r_1 כך ש: $a = q_1m + r_1$ כאשר $r_1 = a \bmod m$ לכן $a \bmod m = a - q_1m$.

באותה מידה q_2, r_2 כך ש: $b = q_2m + r_2$ כאשר $b \bmod m = b - q_2m$ לכן $b \bmod m = b - q_2m$. לפיכך:

$$(a \bmod m)(b \bmod m) = (a - q_1m)(b - q_2m) = ab + (-aq_2 - bq_1 + q_1q_2m)m \equiv ab \bmod m .$$

משפט 27:

יהיו a, b, m שלמים. אזי

$$(a \bmod m)(b \bmod m) \bmod m = ab \bmod m .$$

הוכחה:

משפט 28:

אם a, b, m שלמים חיוביים אז:

$$a \equiv b \bmod m \iff b \equiv a \bmod m \iff a \bmod m = b \bmod m .$$

הוכחה:

נניח ש- $a \equiv b \bmod m$. נוכיח כי $b \equiv a \bmod m$ באופן הבא.

אז"א $a \equiv b \bmod m \Leftarrow$ קיים שלם q כך ש- $a = qm + b$.

$$a = qm + b \Rightarrow b = -qm + a \Rightarrow b = Qm + b ,$$

אז"א קיים שלם $Q = -q$ כך ש- $b = Qm + a$ ולכן

$$b \equiv a \bmod m$$

כנדרש.

נניח ש- $a \equiv b \bmod m$. נוכיח כי $b \bmod m = a \bmod m$ באופן הבא.

$a \equiv b \bmod m$ אז קיים שלם q כך ש: $a = qm + b$.

על פי ההגדרה של השארית:

$$a \bmod m = a - \left\lfloor \frac{a}{m} \right\rfloor m .$$

נציב $a = qm + b$:

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

$$= qm + b - \left\lfloor q + \frac{b}{m} \right\rfloor m$$

$$= qm + b - qm - \left\lfloor \frac{b}{m} \right\rfloor m$$

$$= b - \left\lfloor \frac{b}{m} \right\rfloor m$$

$$= b \bmod m .$$

משפט 31:

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

הוכחה:

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

ו-

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

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 אותיות בעלת פונקציית ההסתברות $p_i = P_X(x_i)$ כך ש-

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

ונתונה הצפנה בינארית $f: X \rightarrow \{0, 1\}^*$ כך ש- $|f(x_i)| = n_i$. במילים אחרות, האות x_i מוצפן ע"י n_i ספרות בינאריות. כלומר, אורך ההצפנה הבינארית של x_i הוא n_i . אזי התוחלת המינימלית מתקבלת על ידי ההצפנה שמקיימת

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

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

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

היא מינימלית.

ללא הגבלת הכלליות נניח כי $n_1 = n_{i_j}$. אזי

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

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

$$\text{בנוסף } p_1 \geq p_2 \geq \dots \geq p_k \text{ לכן } p_1 \geq p_j \text{ ו- } p_{j-1} \geq p_j.$$

לכן לפי משפט 31:

$$(1^*) \quad n_{i_{j-1}}p_{j-1} + n_1p_j \geq n_1p_{j-1} + n_{i_{j-1}}p_j.$$

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

$$E' = n_{i_1}p_1 + \dots + n_1p_{j-1} + n_{i_{j-1}}p_j + \dots + n_{i_k}p_k$$

כך שלפי (1*):

$$E' = n_{i_1}p_1 + \dots + n_1p_{j-1} + n_{i_{j-1}}p_j + \dots + n_{i_k}p_k \leq n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_1p_j + \dots + n_{i_k}p_k = E$$

ז"א $E' \leq E$ בסתירה לכך כי E התוחלת המינימלית. ■

משפט 33: קריפטו-מערכת RSA ניתן לפענוח

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

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

שיטה 2

לפי ההגדרה של צופן El-Gamal, הכלל מצפיון 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:

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

הזהות הבאה מתקיימת. אם z, m, n שלמים חיוביים אז

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

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

$$(z \pmod{m})^n = z^n + \sum_{k=1}^n \binom{n}{k} (-qm)^k z^{n-k} \equiv z^n \pmod{m}.$$

ולכן $z \pmod{m} = z - qm$

ממשוואה (2*), לכל y, z, m, n שלמים חיוביים: $y(z \pmod{m})^n \equiv yz^n \pmod{m}$ לכן

$$(3^*) \quad y(z \pmod{m})^n \pmod{m} = yz^n \pmod{m}.$$

בנוסף הזהות הבאה מתקיימת. לכל שלמים חיוביים b, c, m :

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

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

$$b^{-1} \equiv c^{-1} \pmod{m}.$$

מ- (2*) ו- (4*), לכל z, m, n שלמים חיוביים:

$$(5^*) \quad [(z \pmod{m})^n]^{-1} \equiv z^{-n} \pmod{m}.$$

מכאן, לכל y שלם:

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

ולכן

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

לפי משוואה (7*), אם נציב $z = \alpha^d, m = p, y = x\beta^d$ נקבל:

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

ולכן לפי משוואה (1*):

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

לכל שלמים b, c, m מתקיים:

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

ולכן

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

נציב את ההגדרה של $\beta = \alpha^a \pmod{p}$:

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

ואז לפי משוואה (8*) אנחנו נקבל ש:

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

■

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

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

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

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

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

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

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

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

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. ■

משפט 35:

$$a \equiv b \pmod{m} \text{ אם ורק אם } a \equiv b \pmod{m}$$

הוכחה: נתון כי $ab \equiv 1 \pmod{\phi(n)}$.
 לפי משפט 21: $\phi(n) = \phi(pq) = (p-1)(q-1)$.
 ז"א

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

לכן קיים $t \in \mathbb{Z}$ כך ש-

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

לכל $z \neq 0 \in \mathbb{Z}$ לפי משפט 23, $z^{p-1} \equiv 1 \pmod{p}$. **בפרט**

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

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

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

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

מכיוון ש- p ו- q זרים אז

$$x^{ab-1} - 1 \equiv 0 \pmod{pq} .$$

לפיכך

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

נכפיל ב- x ונקבל

$$(x^a)^b \equiv x \pmod{pq} ,$$

ולכן

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

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. ■

משפט 34:

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- $ab \equiv 1 \pmod{\lambda(n)}$. אזי הקריפטו-מערכת ניתן לפענח.

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

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

מכאן הפונקציית אוילר של np היא

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

משפט 37:

יהיו a ו- b מספרים ראשוניים.

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

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

הוכחה:

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

לכן הפונקציית אוילר של a הינה

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

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

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 ה- \gcd של a ו- b . אם $sa + tb = 1$ אז בהכרח d מחלק 1. לכן $d = 1$ לכן $\gcd(a, b) = 1$.

משפט 39:

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

הוכחה: יהי $d = \gcd(a, b)$. אז $d \mid a$ וגם $d \mid b$. לכן קיימים שלמים q_1, q_2 עבורם $a = q_1 d$, $b = q_2 d$.

הוכחה: נניח כי $a \bmod m = b \bmod m$.

נסמן $r = a \bmod m = b \bmod m$ אז

$$a = mq_1 + r, \quad b = mq_2 + r$$

כאשר q_1, q_2 מספרים שלמים. אז

$$a - b = mq_1 - mq_2 = m(q_1 - q_2) .$$

$q_1 - q_2$ מספר שלם לכן $m \mid a - b$ לכן $a \equiv b \bmod m$ כנדרש.

כעת נניח כי $a \equiv b \bmod m$.

ז"א $m \mid a - b$ קיים q שלם כך ש-

$$a - b = mq$$

נסמן $r = a \bmod m$. קיים מספר שלם q_1 כך ש-

$$a = q_1 m + r .$$

מכאן

$$b = a - qm = q_1 m + r - qm = (q_1 - q)m + r .$$

ז"א $b \bmod m = r$.

כנדרש.

משפט 36:

אם p מספר ראשוני ו- n מספר שלם חיובי אז

$$\phi(pn) = \begin{cases} (p-1)\phi(n) , & p \nmid n \text{ אם} \\ p\phi(n) , & p \mid n \text{ אם} \end{cases} .$$

הוכחה: אם $p \nmid n$ אז p לא מופיע לפירוק לראשוניים של n . ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

אז $p \neq p_i$ לכל $1 \leq i \leq k$. לכן הפירוק לראשוניים של pn הוא

$$pn = p^1 p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} .$$

מכאן הפונקציית אוילר עבור pn היא

$$\phi(pn) = (p^1 - p^0) (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) .$$

אבל הפונקציית אוילר של p היא $\phi(p) = p - 1$ והפונקציית אוילר של n הוא $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$ לכן

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

אם $p \mid n$ אז p מופיע בפירוק לראשוניים של n . ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}$$

אז קיים i , $1 \leq i \leq k$ עבורו $p_i = p$. לכן

$$np = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p^{e_i+1} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k} .$$

הוכחה:

ראשית נוכיח כי $\gcd(a, b) \mid \gcd(b, a \bmod b)$.

לפי המשפט החילוק של אוקלידס (משפט קיימים שלמים q, r עבורם

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

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

כעת נוכיח כי $\gcd(b, a \bmod b) \mid \gcd(a, b)$.

נסמן $d = \gcd(b, a \bmod b)$. לכן $d \mid b$ ו- $d \mid (a \bmod b)$. לפי המשפט החילוק של אוקלידס קיימים שלמים q, r עבורם

$$a = qb + r = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b)$$

לכן $a \mid d$. אזי $d \mid a$ וגם $d \mid b$ $\Leftrightarrow d \mid \gcd(a, b)$.

הוכחנו כי $\gcd(a, b) \mid \gcd(b, a \bmod b)$ ו- $\gcd(b, a \bmod b) \mid \gcd(a, b)$ לפיכך :

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

■

משפט 42: הקשר בין יחס שקילות מודולרי והשארית

יהיו a, b, m שלמים חיוביים.

הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:

$$a \equiv b \pmod{m} \text{ אם ורק אם } a \bmod m = b \bmod m.$$

הוכחה:

כיוון \Leftarrow

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

$$a = Qm + b.$$

לפי משפט החילוק של אוקלידס,

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

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 $r_1 = b \bmod m$. מכאן נובע ש:

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

$$a \bmod m = r_1 = b \bmod m.$$

כיוון \Rightarrow

מכאן

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

ז"א q_1, q_2 לא חולקים גורמים משותפים (לפי פירוק לגורמים לראשוניים) 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.

$$d = \gcd(a, b) \text{ אם ורק אם לכל מחלק משותף } c \text{ של } a \text{ ו- } b: d \mid c.$$

הוכחה:

כיוון \Leftarrow

יהי $d = \gcd(a, b)$. נניח כי $c \mid a$ וגם $c \mid b$. אזי קיימים שלמים a' ו- b' עבורם $a = ca'$ ו- $b = cb'$. לפי משפט בז'ו קיימים שלמים s, t עבורם

$$d = sa + tb = sca' + tcb' = c(sa' + tb').$$

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

כיוון \Rightarrow

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

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

מכיוון ש- $c \mid a$ ו- $c \mid b$ אזי $c \leq \gcd(a, b)$, בגלל ש- $\gcd(a, b)$ הוא המחלק המשותף הגדול ביותר של a ו- b .

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

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

ז"א קיבלנו ש- $d' \leq \gcd(a, b)$ וגם $d' \leq \gcd(a, b)$ לכן בהכרח $d' = \gcd(a, b)$.

משפט 41: האלגוריתם של אוקלידס

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

לכן

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

משפט 45:

יהיו a, b, c שלמים.

אם $a \equiv b \pmod{c}$ אז לכל $n > 1$: $a^n \equiv b^n \pmod{c}$.

הוכחה: אם $a \equiv b \pmod{c}$ אז קיים שלם q :

$$a = qc + b.$$

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 בחזקה של האורך שלה הוא תמורת הזהות

תהי $\pi: \Sigma \rightarrow \Sigma$ תמורה מעל אלפבית Σ . אם π היא מחזור של אורך k אזי $\pi^k = \text{id}$.

הוכחה: נניח כי $\pi: \Sigma \rightarrow \Sigma$ מחזור באורך k . ז"א הפירוק למחזורים של π הוא:

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

או, כפונקציה מעל Σ :

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

אפשר לרשום את זה בביטוי יחיד:

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

עבור π^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 π^2 בביטוי יחיד:

$$\pi^2(a_i) = a_{((i+1) \bmod k) + 1}.$$

באופן כללי לכל $j \geq 0$ טבעי:

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

מכאן נציב $j = k$:

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

ז"א לכל $1 \leq i \leq k$:

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

נניח ש- $a \bmod m = b \bmod m$. אזי

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

כלומר קיים שלם $q = \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor$ עבורו $a = qn + b$ ולכן $a \equiv b \pmod{m}$.

משפט 43:

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

הוכחה:

כיוון \Leftarrow

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 $a \mid qm$.

a, m זרים לכן $a \nmid m$ לכן $a \mid q$. ז"א $\exists k$ שלם עבורו $q = ak$.

לפיכך

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

כיוון \Rightarrow

נניח כי $b \equiv c \pmod{m}$. אז

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

משפט 44:

יהיו a, m מספרים (לא בהכרח זרים).

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

הוכחה:

כיוון \Leftarrow

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- $\frac{a}{\gcd(a, m)}$ ו- $\frac{m}{\gcd(a, m)}$ זרים, אז

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

ז"א לצופן קיסר יש סודיות מושלמת.
במילים פשוטות צופן קיסר אינו ניתן לפענח בתנאי שמשתמשים במפתח מקרי חדש כל פעם שמצפינים אות אחד של טקסט גלוי.

משפט 48: תנאי חילופי לסודיות מושלמת

לפי נוסחת בייס אם לקריפטו-מערכת יש סודיות מושלמת אז מתקיים גם
(1) $P(Y = y|X = x) = P(Y = y)$.

משפט 49:

נתונה קריפטו-מערכת בעלת סודיות מושלמת.

אם $P(Y = y) > 0$ אז

- (1) קיים לפחות מפתח אחד $k \in K$ כך ש- $e_k(x) = y$
(2) $|K| \geq |Y|$.

הוכחה:

- (1) לפי (1),
(#1) $P(Y = y|X = x) = P(Y = y) > 0$
נציב (??) בצד שמאל ונקבל
(#2) $\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) = P(Y = y) > 0$

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

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

ז"א קיים 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
(#4) $|K| \geq |Y|$.

משפט 50: משפט שאנון

נתונה קריפטו-מערכת (X, Y, K, E, D) כך ש- $|K| = |X| = |Y|$.
למערכת יש סודיות מושלמת אם ורק אם

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

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 $P(K = k) = \frac{1}{26}$ ולכן

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

הכלל מצפין והכלל מפענח של צופן קיסר מוגדרים

$$e_k(x) = x + k \mod 26, \quad d_k(y) = y - k \mod 26.$$

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

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

הסכום בצד הימין הוא רק סכום של $P(X = k)$ מעל כל האיברים k ב- \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 בשוויון 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-

$$x = k - y \mod 26 \Rightarrow k = x + y \mod 26.$$

לכל $x \in X$ ולכל $y \in Y$ קיים רק מפתח אחד אשר מקיים תנאי זה. ז"א רק איבר אחד של הסכום נשאר ולפיכך

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

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

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

לכן

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

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

לפיכך

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

מכאן

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

לכל p_y ו- p_z . לכן

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

ז"א $f(p) = C \log(p)$.

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 $\ell_{Q^*}(a) = \ell_{Q^*}(b) = 1$. לכן נשים $f(\frac{1}{2}) = 1$ ונקבל $f(p) = -\log_2(p)$.

משפט 52:

נתון מ"מ בדיד X אשר מקבל N ערכים שונים

$$X = \{x_1, \dots, x_N\}$$

בהסתברות שווה, כלומר

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

אז האנטרופיה מקבלת ערך מקסימלי שניתנת על ידי

$$H_{\max}(X) = \log_2 N.$$

ערך זה הוא הערך המקסימלי האפשרי של האנטרופיה.

משפט 53: אי שוויון האפמן

נתון קבוצת אותיות של טקסט גלוי X והצפנת האפמן f . נניח כי $l(f)$ תוחלת האורך של ההצפנה ו- $H(X)$ האנטרופיה של הטקסט גלוי. מתקיים

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

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

הוכחה:

(1) נניח כי $|Y| = |K|$. כלומר

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

ז"א לא קיימים שני מפתחות $k_1 \neq k_2$ כך ש- $e_{k_1}(x) = y = e_{k_2}(x)$.

לכן לכל $x \in X$ ולכל $y \in Y$ קיים מפתח k יחיד עבורו $e_k(x) = y$.

(2) נסמן אורך של קבוצת מפתחות ב- $|K| = n$. נרשום את הקבוצת טקסטים גלויים כ-

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

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

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

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

אם למערכת יש סודיות מושלמת אז $P(X = x_i) = P(X = x_i | Y = y)$ לכן

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

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

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

משפט 51: אנטרופיה של שאנון

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

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

$H[X]$ נקרא **האנטרופיה של X** .

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

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

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

תהייה $P_Y(y)$ ו- $P_Z(z)$ פונקציות ההסתברות של Y ושל Z בהתאמה.

נסמן $p_y = P_Y(y)$ ו- $p_z = P_Z(z)$.

מכיוון ש- Y ו- Z משתנים בלתי תלויים אז

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