

הגדרה 1:

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 $m \mid a - b$.

בנסוח שקול, $a \equiv b \pmod{m}$ אם קיים שלם q כך ש- $a = qm + b$.

לעתים אומרים כי " a שקול ל- b מודולו m ".

הגדרה 3: השארית

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

$$a \% b$$

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: 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 8: 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 9: צופן ההזזה

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

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

ו-

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

צופן ההזזה מוגדר מעל

הגדרה 10: צופן ההחלפה (substitution cypher)

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 11: צופן האפיני

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 12: 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

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

ונגדיר כלל מפענח

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

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

הגדרה 13: 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

$$e_k(x) = x \cdot k ,$$

ונגדיר כלל מפענח

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

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

הגדרה 14: 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

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

כאשר C_{ij} הקופקטור ה- (i, j) של A .

הגדרה 15: המטריצה המצורפת

תהי $A \in \mathbb{R}^{n \times n}$. המטריצה המצורפת 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 .

הגדרה 16: צופן RSA

יהי $n = pq$ כאשר p, q מספרים ראשוניים שונים. תהי הקבוצת טקסט גלוי $P = \mathbb{Z}_n$, והקבוצת טקסט מוצפן $C = \mathbb{Z}_n$. נגדיר קבוצת המפתחות

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

לכל $k = (n, p, q, a, b) \in K$, ולכל $x \in P$ ו- $y \in C$ נגדיר כלל מצפין

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

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 17: רשת פייסטל (Feistel)

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

מחלקים את x לשני חצאים שנשמך L_0 ו- R_0 :

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

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

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

(3) בשלב ה- N נקבל את הטקסט מוצפן לפי $y = R_N L_N$.

הגדרה 18: 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 $1 \leq i \leq N$:

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

הגדרה 19: סודיות מושלמת

אומרים כי לקריפטו-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 גלוי $X = x$, בידיעה כי הטקסט מוצפן $Y = y$ שווה רק להסתברות כי הטקסט גלוי הוא $X = x$ והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן y לא משפיע על ההסתברות כי הטקסט גלוי $X = x$.

הגדרה 20: מידע של מאורע (שאנון)

נתון 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 .

הגדרה 21: הצפנת האפמן

נתון משתנה מקרי X . נגדיר הצפנת האפמן של X להיות הפונקציה (כלל מצפין)

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

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

נתון 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)".

הגדרה 22: תוחלת האורך של הצפנת האפמן

נתונה הצפנת האפמן f . תוחלת האורך של ההצפנה מוגדרת

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

משפט 1: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.

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

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

לפי משפט הפירוק לראשוניים (ראו משפט 3 למעלה או משפט 12 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.

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

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

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

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

משפט 2: 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 3: 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 4: 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 5: 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 6: 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 7:

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

הוכחה:

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



משפט 8: 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.
- שימו לב: $r = a \% b$.

משפט 9: האלגוריתם של אוקליד

יהיו a, b משפרים שלמים חיוביים ($a, b \in \mathbb{Z}, a > 0, b > 0$). קיים אלגוריתם אשר נותן את $d = \gcd(a, b)$. האלגוריתם הינו מתואר להלן. נגדיר

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

לפי משפט החילוק 8 קיימים שלמים q_1 ו- $0 \leq r_2 < |b|$ עבורם $a = bq_1 + r_2$ כלומר

$$r_0 = r_1q_1 + r_2.$$

באותה מידה, לפי משפט החילוק קיימים שלמים q_2 ו- $0 \leq r_3 < |r_2|$ עבורם

$$r_1 = r_2q_2 + r_3.$$

התהליך ממשיך עד שנקבל $r_{n+1} = 0$ בשלב ה- n ית.

$$\text{שלב } k = 1: \quad a = bq_1 + r_2 \quad 0 \leq r_2 < |b|$$

$$\text{שלב } k = 2: \quad b = r_2q_2 + r_3 \quad 0 \leq r_3 < |r_2|$$

$$\text{שלב } k = 3: \quad r_2 = r_3q_3 + r_4 \quad 0 \leq r_4 < |r_3|$$

\vdots

$$\text{שלב } k = n - 1: \quad r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 \leq r_n < |r_{n-1}|$$

$$\text{שלב } k = n: \quad r_{n-1} = r_nq_n \quad r_{n+1} = 0$$

התהליך מסתיים בשלב ה- n ית אם $r_{n+1} = 0$ ואז

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

משפט 10: 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 11: האלגוריתם של אוקליד המוכלל (שיטה 1)

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

$$d = sa + tb$$

כאשר $d = \gcd(a, b)$, כמפורט להלן.

מגדירים את הפרמטרים ההתחלתיים:

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

אז מבצעים את השלבים הבאים:

$(0 \leq r_2 < r_1)$	$t_2 = t_0 - q_1 t_1$	$s_2 = s_0 - q_1 s_1$	$r_2 = r_0 - q_1 r_1$	שלב 1:
$(0 \leq r_3 < r_2)$	$t_3 = t_1 - q_2 t_2$	$s_3 = s_1 - q_2 s_2$	$r_3 = r_1 - q_2 r_2$	שלב 2:
				⋮
$(0 \leq r_{k+1} < r_k)$	$t_{k+1} = t_{k-1} - q_k t_k$	$s_{k+1} = s_{k-1} - q_k s_k$	$r_{k+1} = r_{k-1} - q_k r_k$	שלב k :
				⋮
$(0 \leq r_n < r_{n-1})$	$t_n = t_{n-2} - q_{n-1} t_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$r_n = r_{n-2} - q_{n-1} r_{n-1}$	שלב $n-1$:
			$r_{n+1} = 0$	שלב n :

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

משפט 12: משפט הפירוק הראשוניים

(ראו משפט 3) 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 13: נוסחה לפונקציה אוילר

(ראו משפט 4) 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 14: נוסחת השארית

נתונים $a, b > 0$ מספר שלמים.

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

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

הוכחה:

(א) לפי משפט החילוק של אוקלידס 8, קיימים שלמים q, r כך ש-

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

כאשר $0 \leq r < b$ ו- $r = a \% b$. 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 8, קיימים שלמים q', r' כך ש-

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

כאשר $r' = (-a) \% b$ 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 $r = a \% b$ ו- r יחיד. לכן

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

$$\text{לכן } r' = (-a) \% b = b - (a \% b)$$

הזהות השני מנובע מ- (*5):

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

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

משפט 15:

אם p מספר ראשוני אז

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

הוכחה: תרגיל בית.

משפט 16:

אם p מספר ראשוני אז

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

הוכחה: תרגיל בית.

משפט 17:

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

$$\phi(s \cdot t) = \phi(s) \cdot \phi(t).$$

הוכחה: תרגיל בית.

משפט 18:

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p \cdot q) = (p - 1)(q - 1).$$

הוכחה: תרגיל בית.

משפט 19: 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.

בסיס:

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

מעבר:

נניח כי הטענה מתקיימת עבור a .

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

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

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

כנדרש.

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

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

טענה 3.

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

משפט 20: משפט אוילר

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז

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

משפט 21:

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז

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

משפט 22: משפט השאריות הסיני

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

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

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

$$\vdots$$

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

קיים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ 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 23:

יהיו a, b, m שלמים. אזי

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

הוכחה: לכל a, m שלמים $\exists q_1, r_1$ כך ש-

$$a = q_1 m + r_1 \Rightarrow r_1 \equiv a \pmod{m}.$$

באותה מידה לכל b, m שלמים $\exists q_2, r_2$ כך ש-

$$b = q_2 m + r_2 \Rightarrow r_2 \equiv b \pmod{m}.$$

לכן

$$ab = (q_1 m + r_1)(q_2 m + r_2) = (q_1 q_2 m + r_1 q_2 + r_2 q_1)m + r_1 r_2 = Qm + r_1 r_2$$

לכן \exists שלם Q שך כ-

$$ab = Qm + r_1 r_2$$

ולכן

$$ab \equiv r_1 r_2 \pmod{m} \Rightarrow r_1 r_2 \equiv ab \pmod{m} \Rightarrow (a \pmod{m})(b \pmod{m}) \equiv ab \pmod{m}$$

■

משפט 24:

$$a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m} \Leftrightarrow a \pmod{m} \equiv b \pmod{m}.$$

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

\Leftarrow קיים שלם q כך ש- $a = qm + b$. ז"א

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

ז"א קיים שלם $Q = -q$ כך ש- $b = Qm + a$ לכן

$$b \equiv a \pmod{m}.$$

נניח ש- $a \equiv b \pmod{m}$. נוכיח כי $b \pmod{m} \equiv a \pmod{m}$. לכל שלמים a, m קיימים q_1, r_1 כך ש-
לפי משפט החילוק של אוקלידס,

$$a = q_1m + r_1,$$

כאשר $r_1 = a \pmod{m}$.

$a \equiv b \pmod{m}$ לכן קיים שלם q_2 כך ש-

$$a = q_2m + b.$$

מכאן

$$q_1m + r_1 = q_2m + b \Rightarrow r_1 = (q_2 - q_1)m + b \Rightarrow r_1 = Qm + b$$

כאשר $Q = q_2 - q_1$ ו- $r_1 = a \% m$. ז"א קיים שלם Q כך ש-

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

משפט 25:

יהיו a, m שלמים. אזי

$$(a \pmod{m})^{-1} \pmod{m} \equiv a^{-1} \pmod{m}$$

הוכחה: נסמן $x = (a \pmod{m})^{-1} \pmod{m}$. ז"א, מכיון ש- x הוא האיבר ההופכי של $a \pmod{m}$ מודולר m אזי

$$(a \pmod{m})x \equiv 1 \pmod{m}.$$

מכאן מנובע

$$ax \equiv 1 \pmod{m}$$

ולכן

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

משפט 26:

צופן El-Gamal ניתן לפענוח. כלומר

$$d_k(e_k(x)) = x.$$

הוכחה: 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

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

לפיכך:

$$\begin{aligned} d_k(e_k(x)) &= d_k(y_1, y_2) \\ &= (y_1^a)^{-1} y_2 \mod p \\ &= [(\alpha^d \mod p)^a]^{-1} (x\beta^d \mod p) \mod p \\ &= (\alpha^{da} \mod p)^{-1} (x\beta^d \mod p) \mod p \quad (\text{כלל הכפל של יחסי מודולרים}) \\ &= ((\alpha^{da})^{-1} \mod p) (x\beta^d \mod p) \mod p \quad (\text{משפט 25}) \\ &= (\alpha^{da})^{-1} (x\beta^d) \mod p \quad (\text{משפט 23}) \\ &= (\alpha^{da})^{-1} (x(\alpha^a)^d) \mod p \quad (\text{הגדרה של צופן El-Gamal}) \\ &= (\alpha^{da})^{-1} (x\alpha^{ad}) \mod p \\ &= (\alpha^{da})^{-1} \alpha^{ad} x \mod p \\ &= x \mod p . \end{aligned}$$

משפט 27:

יהיו a, b, c, d מספרים ממשיים כך ש- $a \geq b$ ו- $c \geq d$. 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 28:

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- $|f(x_i)| = n_i$. כלומר, אורך ההצפנה הבינארית של x_i הוא n_i . במילים אחרות, האות x_i מוצפן ע"י n_i ספרות בינאריות. 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

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

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

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

לכן לפי משפט 27:

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

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

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

כך שלפי (*):

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

■

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

משפט 29: 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

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

הוכחה: נתון כי $ab \equiv 1 \pmod{\phi(n)}$

לפי משפט 18, $\phi(n) = \phi(pq) = (p-1)(q-1)$.

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 19, $z^{p-1} \equiv 1 \pmod{p}$ בפרט

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

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

משיקולות של סיימטריה באותה מידה $x^{ab-1} \equiv 1 \pmod{q}$

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

מכיוון ש- p ו- q זרים אז

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

לפיכך

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

נכפיל ב- x ונקבל

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

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

משפט 30:

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:

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

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

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

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-

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

לכן

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

מכאן

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

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

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

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

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

לכן

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

מכאן

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

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

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

שלב 6 מכיוון ש- p, q ראשוניים אז

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

לפיכך

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

כנדרש.

משפט 31:

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

הוכחה: נניח כי $a \% m = b \% m$.

נסמן $r = a \% m = b \% m$ אז

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

כאשר q_1, q_2 מספרים שלמים. ז"א

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

$q_1 - q_2$ מספר שלם לכן $m \mid a - b$ לכן $a \equiv b \pmod{m}$ כנדרש.

כעת נניח כי $a \equiv b \pmod{m}$.

ז"א $a - b \Leftarrow m \mid a - b$ קיים q שלם כך ש-

$$a - b = mq$$

נסמן $r = a \% m$. 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 $b \% m = r$.

כנדרש.

משפט 32:

אם p מספר ראשוני ו- n מספר שלם חיובי אז

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

הוכחה: אם $p \nmid n$ אז p לא מופיע בפירוק 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

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

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 33:

יהיו a ו- b מספרים ראשוניים.

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

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

הוכחה:

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

לכן הפונקציה אוילר של a הינה

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

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

לכן הפונקציה 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 34:

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 35:

יהיו a, b, n מספרים שלמים.

אם השלושה תנאים הבאים מתקיימים:

(1) a ו- b זרים,

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

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

$$.ab \mid n \text{ אז}$$

הוכחה:

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

לכן קיימים שלמים k ו- l כך ש-

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

$$.n = ak = bl \text{ ז"א}$$

$$.b \mid ak \text{ מכאן}$$

$$.k = bq \text{ לכן } b \mid k, \gcd(a, b) = 1 \text{ נתון כי}$$

$$.n = ak = abq \text{ לכן}$$

משפט 36:

$$.1. \gcd(ma, mb) = m \gcd(a, b)$$

$$.2. \text{ אם } m > 0 \text{ ואם } m \mid a \text{ ו- } m \mid b \text{ אז } \gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m}$$

$$.3. \text{ המספרים } \frac{a}{\gcd(a, b)} \text{ ו- } \frac{b}{\gcd(a, b)} \text{ מספרים זרים.}$$

$$.4. \text{ אם } c \mid ab \text{ ו- } c \text{ זר ביחס ל- } b \text{ אז } c \mid a.$$

$$.5. \text{ אם } a, c \text{ מספרים זרים ואם } b, c \text{ מספרים זרים אז } c \mid ab \text{ מספרים זרים.}$$

$$.6. \gcd(a, b) = \gcd(a + cb, b)$$

הוכחה:

$$.1. \text{ יהי } d = \gcd(a, b). \text{ אז קיימים שלמים } s, t \text{ עבורם}$$

$$sa + tb = d.$$

מכאן

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

$$. \gcd(ma, mb) = md = m \gcd(a, b) \text{ לכן}$$

$$.2. \text{ יהי } d = \gcd(a, b).$$

$$\exists \text{ שלמים } s, t \text{ כך ש-}$$

$$sa + tb = d. \quad (*)$$

נחלק (*) ב- m ונקבל

$$s \frac{a}{m} + t \frac{b}{m} = \frac{d}{m} . \quad (**)$$

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

לכן $\frac{d}{m}$ בהכרח שלם ולפי משפט בזו $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) \mid \frac{d}{m}$. 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

$$sa + tb = d$$

כאשר $d = \gcd(a, b)$.

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

$$\begin{aligned} (sa + tc)(\bar{s}b + \bar{t}c) &= 1 \\ \Rightarrow s\bar{s}(ab) + (t\bar{s}b + \bar{t}tc + s\bar{t}a)c &= 1 \end{aligned}$$

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

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

$$\begin{aligned} sa + tb &= d \\ s(a + cb) + tb &= d + scb \\ s(a + cb) + tb - scb &= d \\ s(a + cb) + (t - sc)b &= d \end{aligned}$$

לכן קיימים שלמים $x = s$ ו- $y = t - cb$ עבורם

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

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

משפט 37:

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

הוכחה: 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

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

נניח כי $b \equiv c \pmod{m}$. אז

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

משפט 38:

יהיו a, m מספרים (לא בהכרח זרים).
 $ab \equiv ac \pmod{m}$ אם ורק אם $b \equiv c \pmod{\frac{m}{\gcd(a, m)}}$.

הוכחה: 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

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

לכן

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

■

משפט 39: 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

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

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

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

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

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

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

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

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

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

לכן

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

■ 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 40: תנאי חילופי לסודיות מושלמת

לפי נוסחת בייס אם לקריפטו-מערכת יש סודיות מושלמת אז מתקיים גם

$$P(Y = y|X = x) = P(Y = y). \quad (1)$$

משפט 41:

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),

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

נציב (??) בצד שמאל ונקבל

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

ז"א

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

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

$$|K| \geq |Y|. \quad (\#4)$$

משפט 42: 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 $y = e_k(x)$.

(2) 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 $y = e_k(x)$.

(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,

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

$$\stackrel{\text{לפי (1)}}{=} \frac{P(K = k_i) P(X = x_i)}{P(Y = y)}$$

אם למערכת יש סודיות מושלמת אז $P(X = x_i | Y = y) = P(X = x_i)$ 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 43: אנטרופיה של שאנון

נתון משתנה מקרי X בעל פונקציה 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 (??):

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

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

תהינה $P_Y(y)$ 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

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

נשים לב שידעיה 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

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

$$f(p) = C \log(p) .$$

כעת נניח כי יש לנו משתנה מקרי $X = \{a, b\}$ בעל פונקציה 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 44:

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 45: 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

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