תוכן העניינים

1 הגדרות 1

2 משפטים 5

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 $a \mid b$ 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 $m|a - b$.

התנאים הבאים שקולים:

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

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 dividor) 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 $\mathrm{lcm}(a, b)$ (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.
הפונקצית אוילר מסומנת ב- $\phi(m)$ ומוגדרת להיות השלמים שקטנים ממש מ- m וזרים ביחס ל- m.
$$\phi(m) := \left\{ a \in \mathbb{N} \,\middle|\, \gcd(a,m)=1,\ a<m \right\} \ .$$

הגדרה 8: צופן ההזזה

יהיו $P=C=K=\mathbb{Z}_{26}$. עבור $0 \leq k \leq 25$ נגדיר
$$e_k(x)=(x+k) \bmod 26 \ , \qquad x \in \mathbb{Z}_{26}$$
ו-
$$d_k(y)=(y-k) \bmod 26 \ , \qquad y \in \mathbb{Z}_{26} \ .$$

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 $0,1,2,\ldots,25$.

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
$$K=\left\{ a,b \in \mathbb{Z}_{26} \,\middle|\, \gcd(a,26)=1 \right\} \ .$$
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 11: צופן ויז'נר (Vigenere Cipher)

יהי m מספר שלם חיובי.
נגדיר $P = C = K = \mathbb{Z}_{26}^m$.
עבור מפתח $k = (k_1, k_2, \ldots, k_m)$ נגדיר כלל מצפין

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, \ldots, x_m + k_m) \bmod 26$$

ונגדיר כלל מפענח

$$d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, y_3 - k_3, \ldots, y_m - k_m) \bmod 26 \ ,$$

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

$$e_k(x) = x \cdot k \bmod 26 \ ,$$

ונגדיר כלל מפענח

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

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

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

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 $n \times n$ שמסומנת $\text{adj}(A)$ ומוגדרת

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

כאשר C המטריצה של קופקטורים של A.

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

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

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

$$e_k(x) = x^b \bmod n \ ,$$

ונגדיר כלל מפענח

$$d_k(x) = y^a \bmod n \ .$$

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

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 $f : \{0,1\}^n \to \{0,1\}^n$.

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

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

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

הגדרה 17: משוואות פייסטל

<u>משוואות פייסטל להצפנה:</u>

נתון טקסטט גלוי $x = L_0 R_0$. לכל $1 \le i \le N$:

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

<u>משוואות פייסטל לפענוח:</u>

נתון טקסטט גלוי $y = R_N L_N$. לכל $1 \le i \le N$:

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

הגדרה 18: סודיות מושלמת

אומרים כי לקריפטו-מערכת יש סודיות מושלמת אם
$$P(X=x|Y=y)=P(X=x)$$
לכל $x\in X$, $y\in Y$.
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 19: מידע של מאורע (שאנון)

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

הגדרה 20: הצפנת האפמן

נתון משתנה מקרי X. נגדיר הצפנת האפמן של X להיות הפונקציה (כלל מצפין)
$$f:X\to\{0,1\}^*$$
כאשר $\{0,1\}^*$ קבוצת רצפים של סיביות סופיים.

נתון רצף מאורעות $x_1,\ldots,x_n$. נגדיר
$$f(x_1\ldots x_n)=f(x_1)||\ldots||f(x_n)$$
כאשר "$||$" מסמן שרשור (concatenation).

הגדרה 21: תוחלת האורך של הצפנת האפמן

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

2 משפטים

משפט 1:

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

1) a ו- b זרים,
2) $a\mid n$,
3) $b\mid n$,

אז $ab \mid n$.

הוכחה:

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

לכן קיימים שלמים k ו- l כך ש-

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

ז"א $n = ak = bl$.
מכאן $b \mid ak$.
נתון כי $\gcd(a,b) = 1$, לכן $b \mid k$. לכן $k = bq$.
לכן $n = ak = abq$. ■

משפט 2: תכונות של ה- gcd

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

הוכחה:

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

$$sa + tb = d \ .$$

מכאן

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

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

2. יהי $d = \gcd(a,b)$.

$\exists$ שלמים s,t כך ש-

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

נחלק (1*) ב- m ונקבל

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

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

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

$$sa+tb=d$$

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

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

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

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

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 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 $\gcd(a,m)=1$.

<u>כיוון $\Leftarrow$</u>

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

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

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

<u>כיוון $\Rightarrow$</u>

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:

$$a^{-1}a=1+qm \quad\Rightarrow\quad a^{-1}a+(-q)m=1\ .$$

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:

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

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

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

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

$$a+b=q_1m+r_1\ ,\qquad 0\leq r_1<m\ ,$$

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

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

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 מפענח של צופן אפיני. אזי
$$d_k\left(e_k(x)\right)=x \bmod 26$$
לכל $x\in\mathbb{Z}_{26}$. כלומר, צופן אפיני ניתן לפענות.

הוכחה: נסמן $y=e_k(x)$.
$$\begin{aligned}
d_k\left(e_k(x)\right) =& d_k(y)\\
=& a^{-1}(y-b) \bmod 26\\
=& a^{-1}([(ax+b) \bmod 26]-b) \bmod 26\\
\stackrel{\text{כלל הכפל}}{=}&\left(a^{-1} \bmod 26\right)\left(([(ax+b) \bmod 26]-b) \bmod 26\right) \bmod 26\\
\stackrel{\text{משפט 5}}{=}&\left(a^{-1} \bmod 26\right)(ax \bmod 26) \bmod 26\\
\stackrel{\text{כלל הכפל}}{=}&\left(a^{-1}ax \bmod 26\right) \bmod 26\\
=& x \bmod 26\ .
\end{aligned}$$
■

משפט 7: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.
נניח כי $\{p_1,\ldots,p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.
נגדיר השלם $M=(p_1\cdot p_2\cdot\ldots\cdot p_n)+1$.
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- $M>p_i$ לכל $1\leq i\leq n$.
גם לא קיים מספק ראשוני p_i אשר מחלק את M. הרי
$$M \bmod p_i=1 \quad\Rightarrow\quad p_i\nmid M\ .$$
הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים. ■

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

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

כאשר $p_1, \ldots, p_n$ מספרים ראשוניים ו- $e_1 \ldots e_n \in \mathbb{N}$, 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 שלמיים ו- $1 \leq i \leq n$. אז

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

משפט 11: שיטה לחישוב gcd

נתונים השלמים a, b כך שהפירוק לראשוניים שלהם הם:

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

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

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

משפט 12: שיטה לחישוב lcm

נתונים השלמים a, b כך שהפירוק לראשוניים שלהם הם:

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

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

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

משפט 13:

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

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 ה**מנה**
- ואילו r נקרא ה**שארית**.
- במקרה ש- $a,b>0$ אזי $r=a \bmod b$.

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:

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

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

$$q_1=\left\lfloor\frac{r_0}{r_1}\right\rfloor\ ,\qquad r_2=r_0-q_1r_1=r_0-\left\lfloor\frac{r_0}{r_1}\right\rfloor\ .$$

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

$$q_2=\left\lfloor\frac{r_1}{r_2}\right\rfloor\ ,\qquad r_3=r_1-q_2r_2=r_1-\left\lfloor\frac{r_1}{r_2}\right\rfloor\ .$$

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

שלב $i=1$: $\quad r_2=r_0-q_1r_1=r_0-\left\lfloor\frac{r_0}{r_1}\right\rfloor r_1 \qquad q_1=\left\lfloor\frac{r_0}{r_1}\right\rfloor$

שלב $i=2$: $\quad r_3=r_1-q_2r_2=r_1-\left\lfloor\frac{r_1}{r_2}\right\rfloor r_2 \qquad q_2=\left\lfloor\frac{r_1}{r_2}\right\rfloor$

שלב $i=3$: $\quad r_4=r_2-q_3r_3=r_2-\left\lfloor\frac{r_2}{r_3}\right\rfloor r_3 \qquad q_3=\left\lfloor\frac{r_2}{r_3}\right\rfloor$

$\vdots$

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

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

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

רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

Algorithm 1 האלגוריתם של אוקלידס

Input: Integers a, b .
$r_0 \leftarrow a$
$r_1 \leftarrow b$
$n \leftarrow 1$
while $r_n \neq 0$ **do**
  $q_n \leftarrow \left\lfloor \dfrac{r_{n-1}}{r_n} \right\rfloor$
  $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
  $n \leftarrow n + 1$
end while
$n \leftarrow n - 1$
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:

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

אם $r_2 \neq 0$ אז עוברים לאיטרציה $i = 2$ שבה מחשבים את q_2, r_3, s_3, t_3 כך:

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

התהליך ממשיך עד השלב ה- n שבו מקבלים r_{n+1}, ואז פולטים $d = r_n = \gcd(a, b), s = s_n, t = t_n$. כל השלבים של האלגוריתם הם כדלקמן:

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

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

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

Algorithm 2 האלגוריתם המוכלל של אוקלידס

Input: Integers a, b .
$r_0 \leftarrow a$
$r_1 \leftarrow b$
$s_0 \leftarrow 1$
$s_1 \leftarrow 0$
$t_0 \leftarrow 0$
$t_1 \leftarrow 1$
$n \leftarrow 1$
while $r_n \neq 0$ **do**
    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$
    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
    $s_{n+1} \leftarrow s_{n-1} - q_n s_n$
    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$
    $n \leftarrow n + 1$
end while
$n \leftarrow n - 1$
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: נוסחה לפונקצית 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

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

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-

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

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

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

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

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

נציב זה ב- (*1) ונקבל

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

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

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

כאשר $r' = (-a) \bmod b$. מכאן

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

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

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

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

הזהות השני מנובע מ- (*5):

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

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

■

משפט 21: זהויות של הפונקציית אוילר

1) אם p מספר ראשוני אז $\phi(p)=p-1$.

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

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

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:

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

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 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.

<u>שלב הבסיס:</u>

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

<u>שלב המעבר:</u>

נניח כי הטענה מתקיימת עבור a (שזה ההנחת האינדוקציה).

נוכיח כי היא מתקיימת גם עבור $a+1$ באופן הבא.

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

לכל $k \geq 1$ טבבעי 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}:

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

טענה 3.

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

■

משפט 24: משפט אוילר

אם a,n שלמים ו- $\gcd(a,n)=1$ אזי:

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

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

משפט 25: משפט השאריות הסיני

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

$$\begin{aligned} x =& a_1 \mod m_1 \ , \\ x =& a_2 \mod m_2 \ , \\ &\vdots \\ x =& a_r \mod m_r \ , \end{aligned}$$

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

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

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

משפט 26:

יהיו a,b,m שלמים. אזי

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

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

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

■

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:

$$a\equiv b \pmod{m} \quad \Longleftrightarrow \quad b\equiv a \pmod{m} \quad \Longleftrightarrow \quad a \bmod m = b \bmod m \ .$$

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

$a\equiv b \pmod{m} \Leftarrow$ קיים שלם q כך ש- $a=qm+b$. ז"א

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

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

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

כנדרש.

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

$a\equiv b \pmod{m}$ 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 $a=qm+b$:

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

■

משפט 29:

יהיו a, m שלמים. אזי
$$(a \bmod m)^{-1} \bmod m = a^{-1} \bmod m$$

הוכחה:
נסמן $x \equiv (a \bmod m)^{-1} \pmod m$. ז"א, מכיוון ש- x הוא האיבר ההופכי של $a \bmod m$ מודולו m אזי
$$(a \bmod m)\, x \equiv 1 \pmod m)\ .$$
מכאן קיים שלם q_1 כך ש: $(a \bmod m)x = q_1 m + 1$. נציב $a \bmod m = a - q_2 m$ ונקבל $(a - q_2 m)x = q_1 m + 1$.
לכן $ax = (q_2 x + q_1)m + 1$ ולכן
$$ax \equiv 1 \pmod m$$
ולכן
$$x \equiv a^{-1} \pmod m \quad \Rightarrow \quad (a \bmod m)^{-1} \bmod m = a^{-1} \bmod m\ .$$
■

משפט 30:

צופן El-Gamal ניתן לפענות. כלומר
$$d_k\left(e_k(x)\right) = x \bmod p\ .$$

הוכחה:

<u>**שיטה 1**</u>

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

שיטה 2

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:

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

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

$$(z \bmod m)^n \equiv z^n \pmod m \ . \qquad (*2)$$

הוכחה: לפי משפט החילוק של אטקלידס קיימים שלמים q, r כך ש- $z = qm + r$ כאשר $r = z \bmod m$, לכן $z \bmod m = z - qm$ ולכן: $(z \bmod m)^n = z^n + \sum\limits_{k=1}^{n} \binom{n}{k} (-qm)^k z^{n-k} \equiv z^n \pmod m$.

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

$$y\left(z \bmod m\right)^n \bmod m = yz^n \bmod m \ . \qquad (*3)$$

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

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

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

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

$$\left[(z \bmod m)^n\right]^{-1} \equiv z^{-n} \pmod m \ . \qquad (*5)$$

מכאן, לכל y שלם:

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

ולכן

$$\left[(z \bmod m)^n\right]^{-1} y \bmod m = z^{-n} y \bmod m \ . \qquad (*7)$$

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

$$\left[\left(\alpha^d \bmod p\right)^a\right]^{-1} \left(x\beta^d \bmod p\right) \bmod p = \alpha^{-ad} \left(x\beta^d \bmod p\right) \bmod p \ , \qquad (*8)$$

ולכן לפי משוואה (1*):

$$d_k\left(e_k(x)\right) = \alpha^{-ad} \left(x\beta^d \bmod p\right) \bmod p \ . \qquad (*9)$$

לכל שלמים b, c, m מתקיים:

$$b\left(c \bmod m\right) \bmod m = bc \bmod m \qquad (*10)$$

ולכן

$$d_k\left(e_k(x)\right) = \alpha^{-ad} x\beta^d \bmod p \ . \qquad (*11)$$

נציב את ההגדרה של $\beta = \alpha^a \bmod p$:

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

ואז לפי משוואה (8*) אנחנו נקבל ש:

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

■

משפט 31:

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

הוכחה:
$$a\geq b\quad\Rightarrow\quad(a-b)\geq 0$$
ו-
$$c\geq d\quad\Rightarrow\quad(c-d)\geq 0\ .$$
לכן
$$(a-b)(c-d)\geq 0\quad\Rightarrow\quad ac+bd-bc-ad\geq 0\quad\Rightarrow\quad ac+bd\geq bc+ad\ .$$
■

משפט 32:

יהי $X=\{x_1,x_2,\ldots,x_k\}$ קבוצת אותיות בעלת פונקצית ההסתברות $p_i=P_X\left(x_i\right)$ כך ש-
$$p_1\geq p_2\geq\cdots\geq p_k$$
ונתונה הצפנה בינארית $f:X\to\{0,1\}^*$ 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 ביניאריות.
אזי התוחלת המינימלית מתקבלת על ידי ההצפנה שמקיימת
$$n_1\leq n_2\leq\ldots\leq n_k\ .$$

הוכחה: נניח בשלילה שקיימת תמורה $\{n_{i_1},\ldots,n_{i_k}\}$ של $\{n_1,\ldots,n_k\}$. כך שהתוחלת
$$E=n_{i_1}p_1+\ldots+n_{i_{j-1}}p_{j-1}+n_{i_j}p_j+\ldots+n_{i_k}p_k\ .$$
היא מינימלית.
ללא הגבלת הכלליות נניח כי $n_1=n_{i_j}$. אזי
$$E=n_{i_1}p_1+\ldots+n_{i_{j-1}}p_{j-1}+n_1p_j+\ldots+n_{i_k}p_k\ .$$
$n_1=\min(n_1,\ldots,n_k)$ אז בהכרח $n_{i_{j-1}}\geq n_1$.
בנוסף $p_1\geq p_2\geq\cdots\geq p_k$ לכן $p_{j-1}\geq p_j$.
לכן לפי משפט 31:
$$n_{i_{j-1}}p_{j-1}+n_1p_j\geq n_1p_{j-1}+n_{i_{j-1}}p_j\ .\qquad(1*)$$
לכן אם נחליף n_1 עם $n_{i_{j-1}}$ ב- E נקבל את התוחלת החדשה
$$E'=n_{i_1}p_1+\ldots+n_1p_{j-1}+n_{i_{j-1}}p_j+\ldots+n_{i_k}p_k$$
כך שלפי (1*):
$$E'=n_{i_1}p_1+\ldots+n_1p_{j-1}+n_{i_{j-1}}p_j+\ldots+n_{i_k}p_k\leq n_{i_1}p_1+\ldots+n_{i_{j-1}}p_{j-1}+n_1p_j+\ldots+n_{i_k}p_k=E$$
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- $ab=1\mod\phi(n)$.
אם $x\in\mathbb{Z}_n$ אז
$$\left(x^b\right)^a=x\bmod n\ .$$

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, $z^{p-1} = 1 \mod p$. 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 $x^{ab-1} \equiv 1 \pmod{p}$.

באותה מידה אפשר להראות כי $x^{ab-1} \equiv 1 \pmod{q}$.

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

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

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

ולכן

$$(x^a)^b = x \bmod (pq) = x \bmod n \ .$$

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:

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

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

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

באותה מידה קיים q' שלכם כך ש-

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

שלב 3)

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

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

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

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

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

לכן

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

מכאן

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

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 שלכם כך ש-

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

לכן

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

מכאן

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

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

$$\left.\begin{aligned} x^{ab-1} &\equiv 1 \pmod{q} \\ x^{ab-1} &\equiv 1 \pmod{q} \end{aligned}\right\} \quad \Rightarrow \quad x^{ab-1}\equiv 1 \pmod{pq}$$

לפיכך

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

כנדרש.

■

משפט 35:

$a \bmod m = b \bmod m$ אם ורק אם $a\equiv b \mod m$.

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

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

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 $a \equiv b \mod m$ כנדרש.

כעת נניח כי $a \equiv b \mod m$.
ז"א $m \mid a - b \Leftarrow$ 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

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

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

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

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

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

מכאן הפונקציית אוילר עבור pn היא

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

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

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

■

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 הפונקצית אוילר של a הינה

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

.2 a ראשוני 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 הפונקצית אוילר של ab הינה

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

■

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 $\gcd\left(a^n, b^n\right) = \gcd\left(a, b\right)^n$.

הוכחה: יהי $d = \gcd\left(a, b\right)$. ז"א $a \mid d$ וגם $b \mid d$. לכן קיימים שלמים q_1, q_2 עבורם

$$a = q_1 d\ , \quad b = q_2 d\ .$$

מכאן

$$\gcd\left(q_1,q_2\right)=\gcd\left(\frac{a}{d},\frac{b}{d}\right)\overset{2 \text{ משפט}}{=}1$$

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

$$\gcd\left(q_1^n,q_2^n\right)=1\ .$$

נשים לב:

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

■

משפט 40:

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

הוכחה:

כיוון $\Leftarrow$

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

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

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 $c|d'$.

$\Leftarrow$ $d'=qc$ $\Leftarrow$ $d'\leq c$.

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

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

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

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

■

משפט 41: האלגוריתם של אוקלידס

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

הוכחה:

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

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

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

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

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 אוקלידיס קיימים שלמים q,r עבורם

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

לכו $d \mid a$. ז"א $d \mid a$ וגם $d \mid b \Leftarrow d \mid \gcd(a,b)$.

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

הוכחה:

<u>כיוון $\Leftarrow$</u>

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

$$a = qm + b \ .$$

לפי משפט החילוק של אוקלידס,

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

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:

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

ז"א $a \bmod m = r_1 = b \bmod m$.

<u>כיוון $\Rightarrow$</u>

נניח ש- $a \bmod m = b \bmod m$. אזי

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

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 $ab \equiv ac \pmod{m}$.

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

מכאן $a \mid qm$.

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

לפיכך

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

כיוון $\Rightarrow$

נניח כי $b \equiv c \pmod{m}$. אז

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

■

משפט 44:

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:

כיוון $\Leftarrow$

נניח כי $ab \equiv ac \pmod{m}$. אז

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

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

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

לכן

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

■

משפט 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:

$$a^n = Qc + b^n \quad \Rightarrow \quad a^n \equiv b^n \pmod{c} .$$

■

משפט 46: מחזור בחזקה של האורך שלה הוא תמורת הזהות

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

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

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

או, כפונקציה מעל Σ:

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

אפשר לרשום את זה בביטוי יחיד:

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

עבור π^2:

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

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 $1 \leq i \leq k$:

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

■

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
$$K=\{0,1,\ldots,25\}=\mathbb{Z}_{26}\ .$$
לכן
$$P(Y=y)=\sum_{k\in\mathbb{Z}_{26}} P(K=k)P\left(X=d_k(y)\right)\ .$$
אם ההסתברות של כל מפתח שווה אז $P(K=k)=\frac{1}{26}$ ולכן
$$P(Y=y)=\frac{1}{26}\sum_{k\in\mathbb{Z}_{26}} P\left(X=d_k(y)\right)\ .$$
הכלל מצפין והכלל מפענח של צופן קיסר מוגדרים
$$e_k(x)=x+k \mod 26\ , \qquad d_k(y)=y-k \mod 26\ .$$
כאשר $k\in\mathbb{Z}_{26}$. לכן $P(X=d_k(y))=P(X=y-k \mod 26)$. לפיכך
$$P(Y=y)=\frac{1}{26}\sum_{k\in\mathbb{Z}_{26}} P\left(X=y-k \mod 26\right)\ .$$
הסכום בצד הימין הוא רק סכום של $P(X=k)$ מעל כל האיברים k ב- $\mathbb{Z}_{26}$. לכן
$$P(Y=y)=\frac{1}{26}\sum_{k\in\mathbb{Z}_{26}} P\left(X=k\right)=\frac{1}{26}\cdot 1=\frac{1}{26}\ .$$
כאשר בשוויון השני השתמשנו בתכונת הנרמול של הפונקצית 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-
$$x=k-y \mod 26 \qquad \Rightarrow \qquad k=x+y \mod 26\ .$$
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
$$P(Y=y)=\frac{1}{26}=P(Y=y|X=x)$$

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

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

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),

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

נציב (??) בצד שמאל ונקבל

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

ז"א

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

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

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

■

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 $y=e_k(x)$.

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

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- $n=|K|$. 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,

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

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

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

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

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 פונקצית 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 (**??**):

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

$$H[X]=\sum p_x\ell_Q(x)=\sum p_xf\left(p_x\right)\ .$$

תהיינה $P_Y(y)$ 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

$$P\left(X=Y\cap Z\right)=P_Y(y)P_Z(z)=p_yp_z\ .$$

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

$$H[X]=\sum p_x\ell_Q(x)=\sum p_yp_z\left[\ell_Q(y)+\ell_Q(z)\right]$$

מכאן

$$H[X]=\sum p_yp_zf\left(p_yp_z\right)=\sum p_yp_z\left[f\left(p_y\right)+f\left(p_z\right)\right]$$

לכל p_y ו- p_z. לכן

$$f\left(p_yp_z\right)=f\left(p_y\right)+f\left(p_z\right)\ .$$

ז"א $f(p)=C\log(p)$.

כעת נניח כי יש לנו משתנה מקרי $X=\{a,b\}$ בעל פונקצית 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 $f\left(\frac{1}{2}\right)=1$ ונקבל $f(p)=-\log_2(p)$.

■

משפט 52:

נתון מ"מ בדיד X אשר מקבל N ערכים שונים

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

בהסתברות שווה, כלומר

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

אז האנטרופיה מקבלת ערך מקסימלי שניתנת על ידי

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

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

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