

תוכן העניינים

1	1	1. הגדרות
1	1.1	שלם שמחלקשלם .
1	1.2	יחס שקלות מודולרי .
2	1.3	השארית .
2	1.4	הצפנים הבסיסיים .
6	2	2. משפטים
6	2.1	חוויים .
13	2.2	הפונקציה אילר .
14	2.3	משפט הקטן של פרמה .

1 הגדרות

1.1 שלם שמחלקשלם

הגדרה 1: שלם שמחלקשלם

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 . הסימן $a | b$ אומר כי b מחלק את a .

1.2יחס שקלות מודולרי

הגדרה 2:יחס שקלות בין a ל- b

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

אומרים כי m מחלק את ההפרש $a - b$, כלומר $m | a - b$.

התנאים הבאים שקולים:

$$a \equiv b \pmod{m} \iff m | a - b \iff \exists q, r : a = qm + r \quad \text{אומרים גם כי } a \pmod{m} \text{ שקול ל- } b \pmod{m}.$$

הגדרה 3: השארית

נתונים מספרים שלמים $a, b \in \mathbb{Z}$, היחס
 $a \pmod{b}$
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 (greatest common divisor) gcd(a, b) ומוגדר להיות המספר
שלם הגדל ביותר שמחולק גם a וגם b .

הגדרה 5:כפולת משותפת קטנה ביותר

נתונים שני מספרים שלמים $a, b > 0$.
הכפולת המשותפת הקטנה ביותר מסומן (lowest common multiple) lcm(a, b) ומוגדר להיות המספר השלם
החייב הקlein ביותר ש- a ו- b מחולקים אליו.

הגדרה 6:מספרים זרים

נניח כי $1 < a \leq b \geq 2$ 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 מכך שמחולק את שניהם.

הגדרה 7: פונקציית אוילר

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

1.4 הצפנים הבסיסיים

הגדרה 8: צופן ההזאה

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

צופן ההזאה מוגדר מעל

הגדה 9: צופן החלפה (substitution cypher) צופן החלפה

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

.0, 1, 2, ..., 25 סמלים מרכיב מכל החלפות האפשריות של - 26 סמלים

עבור כל החלפה $K \in \pi$ נגידר ככל מיפוי

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

ונגידר ככל פעולה

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

כאשר π^{-1} החלפה ההפוכה של π .

הגדה 10: צופן אפיני

$$\text{יהי } P = C = \mathbb{Z}_{26} \text{ ויהי}$$

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

עבור $x \in \mathbb{Z}_{26}$ ועבור $k = (a, b) \in K$ נגידר ככל מיפוי

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

עבור $y \in \mathbb{Z}_{26}$ נגידר ככל פעולה

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

הגדה 11: צופן ויינר (Vigenere Cipher)

יהי m מספר של חיובי.

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

ונגידר $k = (k_1, k_2, \dots, k_m)$ נגידר ככל מיפוי

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

ונגידר ככל פעולה

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

כasher כל הפעולות נמצאות ב- \mathbb{Z}_{26}

הגדה 12: צופן הייל

נניח כי $2 \leq m$ מספרשלם.

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

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

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

עבור מפתח $k \in K$ נגידר ככל מיפוי

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

ונגידר ככל פעולה

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

כasher כל הפעולות נמצאות ב- \mathbb{Z}_{26}

הגדה 13: המטריצה של קופקטורים

$$A \in \mathbb{R}^{n \times n}$$

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

המטריצה של קופקטורים של המטריצה A מוגדרת

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

כasher C_{ij} הקופקטור ה- (i, j) של A .

הגדה 14: המטריצה המצורפת

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

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

כasher C המטריצה של קופקטורים של A .

הגדה 15: צופן RSA

יהי $n = pq$ מספרים ראשוניים שונים. תהי הקבוצת טקסט גלי $P = \mathbb{Z}_n$ והקבוצת טקסט מוצפן $C = \mathbb{Z}_n$. נגידר קבוצת המפתחות

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

לכל $k \in K$ ו $y \in C$ ו $x \in P$ וכל מיפוי

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

ונגידר ככל פעולה

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

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

הגדה 16: רשת פיסטל (Feistel)

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

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

מחלקים את x לשני חצאים שנסמן L_0 ו- R_0 :

ברשת פיסטל יש 4 מרכיבים:

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

- מפתח התחלתי k .

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

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

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

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

2) בשלב ה- i ית $(1 \leq i \leq N)$

3) בשלב ה- N נקלט הטקסט מוצפן לפי

$$y = R_N L_N$$

הגדה 17: משוואות פיסטל

משוואות פיסטל להצפנה:

נתון טקסט גלי $x = L_0 R_0$. 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 פיסטל לפענו:

נתון טקסט גלי $y = R_N L_N$. לכל $1 \leq i \leq N$.

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

הגדה 18: סודיות מושלמות

אומרים כי לкриיפטו-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 גלי x , $X = y$, בידעה כי הטקסט מוצפן y שווה רק להסתברות כי גלי הוו $X = x$ והבחירה של המפתח שבאמצעותו מתיקבל הטקסט מוצפן y לא משנה על ההסתברות כי הטקסט גלי x .

הגדה 19: 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 .

הגדה 20: הצפנה האפמן

נתון משתנה מקרי X . נגדיר הצפנה האפמן של X להיות הפונקציה (כלל מיפוי)

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

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

נתון רצף מאורעות x_1, \dots, x_n . נגדיר

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

כasher "||" מסמן שרשור (concatenation).

הגדה 21: תוחלת האורך של הצפנה האפמן

נתונה הצפנה האפמן f . תוחלת האורך של הצפנה מוגדרת

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

2 משפטים

2.1 חוגים

משפט 1: תנאי לקיום איבר הופכי של חוג

יהי $a \in \mathbb{Z}_m$. קיים איבר הופכי של a אם ורק אם

הוכחה: יש להוכיח שקיים האיבר הופכי של a^{-1} של a ב- \mathbb{Z}_m אם ורק אם

כיוון \Leftarrow

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

או קיימים שלמים s, t עבורם $\gcd(a, m) = 1$

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

\mathbb{Z}_m

לפיכך קיימים שלם s אשר הוא האיבר הופכי של a ב-

כיוון \Rightarrow

אם קיים איבר הופכי a^{-1} של a ב- \mathbb{Z}_m א.ז"א קיימים שלם q כך ש-:

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

לכן קיימים שלמים s ו- $t = a^{-1}$ כך ש-:

$$sa + tm = 1$$

ולכן לפי משפט בז'ו $\gcd(a, m) = 1$

משפט 2:

יהיו שלמים a, b, c שליליים. אם b, a זרים אז לא קיימים c עבורו $ac \equiv 1 \pmod{b}$

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

וא.ז"א קיימים שלם q :

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

משפט 5: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

משפט 3: חישוב של שאריותאם a, b, m מספרים שלמים חיוביים אז

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

הוכחה: לפי משפט החלוק של אוקלידס קיימים שלמים r_1, r_2 כך ש: $a + b = q_1m + r_1$, $0 \leq r_1 < m$,

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

וא"א קיים שלם $q_1 = -Q$ כך ש:

$$((a+b) \text{ mod } m) - b = Qm + a$$

ולכן

$((a+b) \text{ mod } m) - b \equiv a \pmod{m}$
לפיכך, מכיוון שהשני שלמים $b - a$ ו- $((a+b) \text{ mod } m) - b$ שקולים מודולריים ביחס ל- m , אז בהכרח יש להם אותה שארית בחלוקת ב- m :

$$[((a+b) \text{ mod } m) - b] \text{ mod } m = a \text{ mod } m .$$

משפט 4: צופן אפיני נתן לפענוווחיהי $e_k(x)$ הצלל מצפין של צופן אפיני ויהי $d_k(y)$ הצלל מפענה של צופן אפיני. אז $d_k(e_k(x)) = x \text{ mod } 26$ כל $x \in \mathbb{Z}_{26}$.**הוכחה:** נסמן $y = e_k(x)$

$$\begin{aligned} d_k(e_k(x)) &= d_k(y) \\ &= a^{-1}(y - b) \text{ mod } 26 \\ &= a^{-1}([(ax + b) \text{ mod } 26] - b) \text{ mod } 26 \\ &\stackrel{\text{ככל הכלל}}{=} (a^{-1} \text{ mod } 26) (([(ax + b) \text{ mod } 26] - b) \text{ mod } 26) \text{ mod } 26 \\ &\stackrel{\text{משפט 3}}{=} (a^{-1} \text{ mod } 26) (ax \text{ mod } 26) \text{ mod } 26 \\ &\stackrel{\text{ככל הכלל}}{=} (a^{-1}ax \text{ mod } 26) \text{ mod } 26 \\ &= x \text{ mod } 26 . \end{aligned}$$

הוכחה: נניח הטענה דרכ' השילילה.
נניח כי $\{p_1, \dots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקובוצה זו נוצרת סופי.
נדיר השלים $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$.
לפי משפט הפירוק לראשוניים (ראה משפט 7 למעלה או משפט 16 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $p_i < M$ לכל $i \leq n$ אשר מחלק את M . הרוי

$$M \text{ mod } p_i = 1 \Rightarrow p_i \nmid M .$$

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

משפט 6: נוסחת קיילי המילטוןנניח כי $A \in \mathbb{R}^{n \times n}$ מטריצה ריבועית. אם A הפיכה, כלומר $\det(A) \neq 0$ אז המטריצה ההופכית נתונה ע"י
נוסחת קיילי המילטון:

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

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

משפט 7: משפט הפירוק לראשוניים
המשפט היסודי של האריתמטיקה או משפט הפירוק לראשוניים קובע כי כל מספר טבעי ניתן לרשום כמכפלה ייחידה של מספרים ראשוניים. אז "א", $a \in \mathbb{N}$ ניתן לרשום כמכפלה ייחידה של מספרים ראשוניים.

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

כאשר $p_1, p_2, \dots, p_n \in \mathbb{N}$ ו- $e_1, \dots, e_n \in \mathbb{N}$, והפירוק הזה ייחיד.**משפט 8: 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 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 9: שיטה לחישוב gcdנתונים 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 כלויות נניח כי $n \leq k$. אז ה- $\gcd(a, b)$ נתון על ידי

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

משפט 10: שיטה לחישוב lcm

נתונים השלמים a, b כך שהפירוק לגורמים שלהם הם:
 $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$
 וללא הגבלה כלויות נניח כי $n \leq k$. אז ה- $\text{lcm}(a, b)$ נתון על ידי

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

משפט 11:

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

תוכחה:

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

משפט 12: משפט החלוק של אוקלידס

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

$$a = qb + r$$

כאשר $0 \leq r < |b|$

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

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

משפט 13: האלגוריתם של אוקלידס

יהיו a, b מספרים שלמים חיוביים. קיים אלגוריתם אשר נותן את (gcd) כלהלן: $r_1 \leftarrow r_0$

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

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

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

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

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

התהיליך ממשיך עד שנתקבל 0 בשלב ה- n -ית. כל השלבים של התהיליך הם כדלקמן:

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

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

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

⋮

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

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

התהיליך מסתיים בשלב ה- n -ית אם $r_{n+1} = 0$. אז הפלט של האלגוריתם הוא $r_n = \gcd(a, b)$ למטה
רשום יציג 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 14: משפט בז' (Bezout's identity)

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

$$sa + tb = d .$$

משפט 15: האלגוריתם המוכל של אוקלידס

יהיו שלמים חיוביים. קיים אלגוריתם אשר נתנו שלמים s, t, d עבורם
 $d = sa + tb$

כאשר $d = \gcd(a, b)$, כלהלן. 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:

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

התהlik ממשיך עד השלב n שבו מקבלים r_n , ו s_n, t_n פולטים, ועוד פולטים הם כלהלן. כל השלבים של האלגוריתם הם כלהלן:

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

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

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

האלגוריתם המוכל של אוקלידס 2

```

Algorithm 2: Integers  $a, b$  .
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:  $r_n, s_n, t_n$   $d = r_n = \gcd(a, b)$  and  $d = sa + tb$  where  $s = s_n, t = t_n$ .

```

משפט 16: משפט הפירוק לראשוניים

(ראו משפט 7) לכל מספר טבעי 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 17: נוסחה לפונקציית אוילר

(ראו משפט 8) לכל מספר טבעי 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 18: נוסחת השארית

נתונים $a, b > 0$ מספרים שלמים.

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

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

a) לפי משפט החלוק של אוקלידס 12, קיימים שלמים r, q כך ש-

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

כאשר $0 \leq r < b$. נחלק ב- b ונקבל

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

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

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

נזכיר זה ב- $(*)$ ונקבל

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

b) לפי משפט החלוק של אוקלידס 12, קיימים שלמים $0, q', r'$ כך ש- $-a = q'b + r'$

כאשר $b \mid (-a) \text{ mod } b = r'$. מכאן

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

נשים לב כי $0 \leq r' < b$. אבל לפי $(*)$ $a = qb + r$ כאמור. לכן $r = r'$.

$$r = b - r' \Rightarrow r' = b - r \stackrel{(4)}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor = b - \left(a - b \left\lfloor \frac{a}{b} \right\rfloor \right) = b - (a \text{ mod } b). \quad (5)$$

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

זהות השני מנובע מ- $(*)$:

$$r = b - r' \Rightarrow r' = b - r \stackrel{(4)}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor - a + \left\lceil \frac{a}{b} \right\rceil. \\ r' = (-a) \text{ mod } b = -a + \left\lceil \frac{a}{b} \right\rceil \text{ לכן}$$

2.2 הפונקציה אוילר

משפט 19: זהות של הפונקציה אוילר

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

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

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

$\phi(s \cdot t) = \phi(s) \cdot \phi(t)$ (gcd(s, t) = 1)

4 אם p ו- q מספרים ראשוניים שונים אז

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

משפט 20: משפט עזר למשפט הקטן של פרמה

אם p מספר ראשוני איי

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

הוכחה:

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

מכיוון ש- $p \mid p!$ אז $p \mid k!(p-k)!$

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

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

משפט 21: המשפט הקטן של פרמה

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

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

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

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

הוכחה:

טענה 1. נוכיח באינדוקציה.

שלב הבסיס:

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

שלב המעבר:

נניח כי הטענה מותקינה עבור a (זויה ההנחה האינדוקציה).

נוכיח כי היא מותקינה 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 $1 \leq k \leq p$ טבבי למשפט 20: $\binom{p}{k} \mid p$ ולכן

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

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

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

משפט 25:

יהיו a, b, m שלמים. אז

$$(a \text{ mod } m)(b \text{ mod } m) \text{ mod } m = ab \text{ mod } m .$$

הוכחה:

משפט 26:

אם a, b, m שלמים חיביים אז:

$$a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff a \text{ mod } m = b \text{ mod } m .$$

הוכחה:

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

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

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

$$\text{א"א קיימים שלם } q \text{ כך ש- } b = Qm + a \text{ ולכן } b \equiv a \pmod{m}$$

כנדרש.

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

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

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

:
מציב

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

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

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

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

$$=b \text{ mod } m .$$

משפט 27:

יהיו a, m שלמים. אז

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

כנדרש.

טענה 2: לכל מספר ראשוני ושלם a מתקיים $\gcd(a, p) = 1$ לפיכך קיים איבר הופכי a^{-1} ב- $(\mathbb{Z}/p\mathbb{Z})^\times$ שהוא שוכן במס' הקודם ב- a^{-1} נס饱יל את היחס שקיים $a^p \equiv 1 \pmod{p}$ (שהוכחנו במס' הקודם) ב- $a^{-1}a^p \equiv a^{-1} \cdot a \pmod{p}$ $\Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

טענה 3:

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

משפט 22: משפט אويلר

אם n שלמים ו- $\gcd(a, n) = 1$

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

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

משפט 23: משפט השאריות השני

יהיו m_1, m_2, \dots, m_r שלמים אשר זרים בזוגות ויהיו a_1, a_2, \dots, a_r שלמים. המערכת של חישום שקליות

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

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

⋮

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

קיים פתרון ייחיד מודולו $M = m_1m_2 \cdots m_r$ שניתן על ידי

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

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

משפט 24:

יהיו a, b, m שלמים. אז

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

הוכחה: לפי משפט החלוק של אטקלידי קיימים שלמים q_1, r_1 כך ש: $a = q_1m + r_1$ כאשר $m \mid r_1$ לכן $r_1 = a \text{ mod } m$ $a \text{ mod } m = a - q_1m$

באותה מידת $b = q_2m + r_2$ לכן $r_2 = b \text{ mod } m$ $b \text{ mod } m = b - q_2m$ $r_2 = b - q_2m$ $b = q_2m + r_2$ $b \equiv q_2m + r_2 \pmod{m}$ $b \equiv a - q_1m \pmod{m}$ $b \equiv q_2m + r_2 \pmod{m}$ $b \equiv a - q_1m + q_2m + r_2 \pmod{m}$ $b \equiv ab + (-aq_2 - bq_1 + q_1q_2m) \pmod{m}$ $b \equiv ab \pmod{m}$.

לפיכך:

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

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

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

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

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

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

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

בנוסף להזאות הבאה מתקיימות. לכל שלמים חיוביים b, c, m :

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

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

מ- $(*)$, לכל z, m, n שלמים חיוביים:

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

מכאן, לכל y שלם:

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

ולכן

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

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

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

ולכן לפי מושואה $(*)$:

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

לכל שלמים מתקיים: b, c, m

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

ולכן

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

נציב את ההגדרה של d_k ב- $\beta = \alpha^a \pmod{p}$

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

ואז לפי מושואה $(*)$ אנחנו נקבל ש:

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

משפט 29

זה a, b, c, d מספרים ממשיים כך ש- $a \geq b \wedge c \geq d$ אז $ac + bd \geq ad + bc$.

הוכחה:

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

שיטת 2

לפי ההגדרה של צופן El-Gamal, הכלל מצפינו 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 מעפנה הוא

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

$$\begin{aligned} c \geq d &\Rightarrow (c-d) \geq 0 . \\ (a-b)(c-d) \geq 0 &\Rightarrow ac+bd-bc-ad \geq 0 \Rightarrow ac+bd \geq bc+ad . \end{aligned}$$

-1

לכן

משפט 30: קבוצת אוטיות בעלת פונקציית החסטבות $p_i = P_X(x_i)$ כך ש-
וינה הצפנה בינהירות $f(x_i) = n_i$. $f : X \rightarrow \{0, 1\}^*$ כך ש-
כלומר, אורך הצפנה הבינהירות של x_i הוא n_i . במילים אחרות, x_i מופגן ע"י n_i ספרות בינהירות.
אז התוחלת המינימלית מתקבלת על ידי הצפנה שמיימת
 $n_1 \leq n_2 \leq \dots \leq n_k$.

הוכחה: נניח בשלילה שקיימת תמורה E של $\{n_1, \dots, n_k\}$ כך שהותולות
 $E = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_{i_j}p_j + \dots + n_{i_k}p_k$.
היא מינימלית.
לא הגבלת הכלויות נניח כי $n_{i_j} = n_1$.
 $E = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_1p_j + \dots + n_{i_k}p_k$.
 $n_{i_{j-1}} \geq n_1 = \min(n_1, \dots, n_k)$
 $p_{j-1} \geq p_j$ $p_1 \geq p_2 \geq \dots \geq p_k$ לכן $n_{i_{j-1}} \geq p_{j-1}$
לכן לפי משפט 29:
 $n_{i_{j-1}}p_{j-1} + n_1p_j \geq n_1p_{j-1} + n_{i_{j-1}}p_j$.
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 (*):

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

א"א $E' \leq E$ וא"א בסתיו לכך E' מינימלית.

משפט 31: קרייפטו-מערכת RSA ניתנת לפענוח

שי-
היא $n = pq$ מספרים ראשוניים שונים, $a, b \in \mathbb{Z}$ שלמים חיוביים כך ש-
אם $x \in \mathbb{Z}_n$

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

הוכחה: נתון כי $ab \equiv 1 \pmod{\phi(n)}$
לפי משפט 19: $\phi(n) = \phi(pq) = (p-1)(q-1)$
א"א
 $ab \equiv 1 \pmod{\phi(n)} \equiv 1 \pmod{(p-1)(q-1)}$
 $ab - 1 = t(p-1)(q-1)$.

לכן קיימים $t \in \mathbb{Z}$ כך ש-

$$\begin{aligned} \text{לכל } z \neq 0 \in \mathbb{Z} \text{ לפי משפט 21 בפרט} \\ x^{ab-1} = x^{t(p-1)(q-1)} = (x^{t(q-1)})^{p-1} = y^{p-1} \\ \text{כאשר } y = x^{t(q-1)} \text{ מכאן} \\ x^{ab-1} \equiv 1 \pmod{p} \end{aligned}$$

באותה מידה אפשר להראות כי $(q-1) \mid x^{ab-1} - 1$

$$\text{לכן } (q-1) \mid x^{ab-1} - 1 \pmod{q} \text{ ו- } x^{ab-1} - 1 = 0$$

מכיוון ש- $p - q$ זרים אז

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

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

כפイル ב- x ונקבל

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

ולכן

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

"א הוכחנו כי לכל טקסט גלי x , אם צפין אותו ואז אחר כך נפענץ את הטקסט מופגן המתקבל מאלגוריתם RSA, קיבל אותו טקסט גלי המקורי בחזרה.

משפט 32:

היו p, q מספרים ראשוניים ויהי $n = pq$.
 $\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$.
נדיר צוף חדש זהה ל- RSA אלא $\phi(n)$ הוחלף עם $\lambda(n)$ כך ש- א"י הקרייפטו-
מערכת ניתן לפענוח.

הוכחה:

שלב 1) רושמים את הצופן:

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

$$\text{שלב 2) נתון כי } d = \gcd(p-1, q-1) . \text{ א"א שקיימים } p' \text{ שלם כך ש-} \\ p-1 = p'd \Leftrightarrow \frac{p-1}{d} = p' \Leftrightarrow d = \frac{p-1}{p'} . \quad (\#1)$$

באותה מידה קיימים q' שלם כך ש-

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

שלב 3)

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

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 שכן $m | a - b$ mod m שכן

כעת נניח כי $a \equiv b$ mod m

ז"א q שלים כך ש-

$$a - b = mq$$

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

$$a = q_1m + r .$$

מכאן

$$b = a - mq = q_1m + r - qm = (q_1 - q)m + r .$$

$b \mod m = r$ ז"א

כנדרש.

משפט 34

אם p מספר ראשוני ו- n מספר שלם חיובי אז

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

הוכחה: אם $n \neq p$ או p לא מופיע לפירוק הראשוניים של n . ז"א אם הפירוק הראשוניים של n הוא

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

או $p_i \neq p$ לכל i ב- $1 \leq i \leq k$. לכן הפירוק הראשוניים 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 היה $\phi(p) = p-1$ 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 $n \neq p$ מופיע בפירוק הראשוניים של n . ז"א אם הפירוק הראשוניים של n הוא

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

או קיימים i, j ב- $1 \leq i \leq k, 1 \leq j \leq k$, כך

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

מכאן הפונקציית אוילר של np היא

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

משפט 33

$a \equiv b \mod m$ אם $a \mod m = b \mod m$

הוכחה: נניח כי $a \mod m = b \mod m$ ור' אם $a \mod m = b \mod m$

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

. $n = ak = bl$ **א'**

ב' $b \mid ak$

מכאן כי $\gcd(a, b) = 1$, כלומר $k = bq$, ולכן $b \mid k$.

ג' $n = ak = abq$

משפט 35:

יהיו a ו- b מספרים ראשוניים.

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

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

הוכחה:

1. ראשוני לכן הפירוק לזרים נושא $p_1^{e_1}$ כאשר $p_1 = a$ ו-

לכן הפונקציה אוילר של a הינה

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

2. ראשוני ו- b ראשוני לכן הפירוק לזרים נושא ab הוא ab כאשר b

$$e_1 = 1, e_2 = 1$$

לכן הפונקציה אוילר של ab הינה

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

משפט 38:

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

$$\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m} \quad \text{א' } m \mid b \text{ ו- } m \mid a \text{ ו- } m > 0 \quad .2$$

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

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

$$\text{5. אם } a, c \text{ זרים ו- } b, c \text{ זרים אז } ab \text{ ו- } bc \text{ זרים.}$$

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

הוכחה:

משפט 36:

יהיו a, b מספרים שלמים.

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

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

משפט 37:

יהיו a, b, n מספרים שלמים.

אם השלושה תנאים הבאים מתקיים:

$$(1) \quad a \mid b \text{ ו- } a \mid n$$

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

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

$$.ab \mid n \quad \text{א'}$$

הוכחה:

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

לכן קיימים שלמים k ו- l כך ש-

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

1. יהי $d = \gcd(a, b)$. א' קיימים שלמים s, t עבורם

$$sa + tb = d \quad .$$

מכאן

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

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

2. יהי $d = \gcd(a, b)$. א' קיימים שלמים s, t כך ש-

$$sa + tb = d \quad .$$

נניח (*) 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 בא' $\frac{d}{m} = \gcd\left(\frac{a}{m}, \frac{b}{m}\right)$. לכן

$$\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m} \quad .$$

3.

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

$$sa + tb = d \quad .$$

$$.d = \gcd(a, b) \quad \text{כasher } (a)$$

משפט 43:

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

הוכחה:

ביוון \Leftarrow

$$\begin{aligned} & \text{נניח כי } ab \equiv ac \pmod{m} \Rightarrow ab = ac + qm \Rightarrow ab - ac = qm \Rightarrow a(b - c) = qm. \\ & \text{מכאן } a | qm \text{ ור' } a | q \text{ לכן } m \nmid a \text{ ו } q \text{ שלם עבורו } a | q \text{ נ' א'}. \\ & \text{לפיכך } a(b - c) = qm \Rightarrow a(b - c) = akm \Rightarrow b - c = km \Rightarrow b = c + km \Rightarrow b \equiv c \pmod{m}. \\ & \text{כיוון} \Rightarrow \end{aligned}$$

$$\begin{aligned} & \text{נניח כי } b \equiv c \pmod{m} \text{ נ'}. \\ & b = qm + c \Rightarrow ab = aqm + ac \Rightarrow ab \equiv ac \pmod{m}. \end{aligned}$$

משפט 44:

יהיו a, m מספרים (לא בהכרח זרים).

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

הוכחה:

ביוון \Leftarrow

$$\begin{aligned} & \text{נניח כי } ab \equiv ac \pmod{m} \text{ נ'}. \\ & ab = ac + qm \Rightarrow ab - ac = qm \Rightarrow m | a(b - c) \Rightarrow \frac{m}{\gcd(a, m)} | \frac{a}{\gcd(a, m)}(b - c). \\ & \text{מכיוון ש-} \frac{a}{\gcd(a, m)}, \frac{m}{\gcd(a, m)} \text{ ור' } \frac{m}{\gcd(a, m)} \text{ נ' } \frac{m}{\gcd(a, m)} | (b - c). \\ & \text{לכן} \end{aligned}$$

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

■

$$\begin{aligned} & \text{לפי המשפט החילוק של אוקלידי (משפט קיימים שלמים } q, r \text{ עבורם)} \\ & a = qb + r = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b) \Rightarrow a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b. \\ & \text{לכן אם } d | \gcd(b, a \bmod b) \Leftrightarrow d | (a \bmod b) \Leftrightarrow d | b \text{ ו-} d | a \text{ נ' } d = \gcd(a, b). \end{aligned}$$

$$\text{כעת נכח כי } . \gcd(b, a \bmod b) | \gcd(a, b)$$

$$\begin{aligned} & \text{נסמן } q, r \text{ עבורם}. \text{ לפי המשפט החילוק של אוקלידי (משפט קיימים שלמים } q, r \text{ עבורם)} \\ & a = qb + r = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b) \end{aligned}$$

$$\begin{aligned} & \text{לכו } d | \gcd(a, b) \Leftrightarrow d | b \text{ ו-} d | a \text{ נ' } d | a \bmod b. \\ & \text{הוכחנו כי } \gcd(a, b) | \gcd(b, a \bmod b) \text{ ו-} \gcd(b, a \bmod b) | \gcd(a, b) \text{ לפיכך } \gcd(a, b) = \gcd(b, a \bmod b). \end{aligned}$$

משפט 42: הקשר בין יחס שיקילות מודולרי והשארית

יהיו a, b, m שלמים חיוביים.
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
. $a \bmod m = b \bmod m$ אם ורק אם $a \equiv b \pmod{m}$

הוכחה:

ביוון \Leftarrow

$$\begin{aligned} & \text{נניח ש-} a \equiv b \pmod{m} \text{ נ'}. \text{ אי קיים שלם } Q \text{ כך ש:} \\ & a = qm + b. \end{aligned}$$

לפי משפט החילוק של אוקלידי,

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

לכן

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

כאשר $r_1 = b \bmod m$ ו- $0 \leq r_1 < b$ זה הוא השארית. מכאן נובע

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

$$. a \bmod m = r_1 = b \bmod m \text{ נ'}$$

ביוון \Rightarrow

$$\begin{aligned} & \text{נניח ש-} a \bmod m = b \bmod m \text{ נ'}. \text{ אי קיים שלם } m \text{ כך ש-} a \bmod m = b \bmod m \\ & a - m \left\lfloor \frac{a}{m} \right\rfloor = b - m \left\lfloor \frac{b}{m} \right\rfloor \Rightarrow a = \left(\left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor \right)m + b \Rightarrow a = qm + b \end{aligned}$$

$$. a \equiv b \pmod{m} \text{ ולכן } a = qm + b \text{ עבורו } q = \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor \text{ קיימים שלם}$$

משפט 45:

$$\text{יהי } a, b, c \text{ שלמים.}$$

$$a^n \equiv b^n \pmod{c} \text{ אם ורק אם } a \equiv b \pmod{c}.$$

הוכחה: אם $a \equiv b \pmod{c}$ אז קיימים 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 קיימים שלם Q כך ש:

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

משפט 46: מבחן בחזקה של האורך של הואה תמורה זהות

תהי $\pi^k : \Sigma \rightarrow \Sigma$ תמורה מעלהalfavit. אם π היא מבחן של אורך k אז $\pi^k = \text{id}$

הוכחה: נניח כי $\Sigma \rightarrow \Sigma$ מבחן של אורך k . נ"א הפירוק למחוזרים של π הוא:

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

או, כפונקציה מעלה 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 מידת 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 $j = k$

וא"א לכל $i < k$

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

וא"א לכל $1 \leq i \leq k$

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

משפט 47: תנאי סודיות מושלמת של צופן קיסר

אם לכל מפתח $K \in K$ בצופן קיסר יש הסתברות שווה, כלומר

$$P(K = k) = \frac{1}{26}.$$

וא"ל צופן 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

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

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

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

הכל מנצח והכל מפענה של צופן קיסר מוגדרים

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

כאשר π בצד ימין הוא רק סכום של האיברים b ב- \mathbb{Z}_{26} . לכן $P(X = d_k(y)) = P(X = y - k \pmod{26})$.

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

הסכום בצד ימין הוא רק סכום של $P(X = k)$ מעל כל האיברים b 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 בשווין השני השתמשנו בתכונת הנורמל של הפונקציית הסתברות של המ"מ X .

מצד שני, לפי (??)

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

האליז על הסכום $x = d_k(y)$ אומר ש-

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

כל $X \in X$ וכל $y \in Y$ קיים רק מפתח אחד אשר מקיים תנאי זה. נ"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 $P_K(k) = \frac{1}{26}$ לכל $k \in K$, אז

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

לכן

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

וא"ל צופן קיסר יש סודיות מושלמת.

במילים פשוטות צוין קיסר איןנו ניתן לפענה בתנאי שימושים בפתח מקרי חדש כל פעם שימושים אותן אחד של טקסט גלי.

משפט 48: תנאי חילופי לסודיות מושלמת
לפי נוסחת בייס אם לкриיפטו-מערכת יש סודיות מושלמת אז מתקיים גם

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

משפט 49:
נתונה קרייפטו-מערכת בעלת סודיות מושלמת.
אם $P(Y = y) > 0$ אז

$$(1) \text{ קיים לפחות מפתח אחד } k \in K \text{ כך ש-} e_k(x) = y$$

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

הוכחה:

$$(1) \text{ לפי (1)} \quad (\#1)$$

$$\text{נניח (?) בצד שמאל ונוכיח} \quad (\#2)$$

$$P(Y = y|X = x) = P(Y = y) > 0$$

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

$$\text{לפניהם } (\#1) \text{ ו-} (\#2) \text{ נסsatן}$$

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

$$\text{לכן קיים לפחות מפתח אחד, } k \text{ עבורו } x = d_k(y)$$

$$\text{ז"א קיים לפחות מפתח אחד, } k \text{ עבורו } y = e_k(x)$$

$$(2) \text{ לפי (1) ו-} (\#3), \text{ לכל } y \in Y \text{ קיים לפחות מפתח אחד, } k \text{ עבורו } y = e_k(x), \text{ לכן בהכרח} \quad (\#4)$$

משפט 50: משפט שאנו
נתונה קרייפטו-מערכת (X, Y, K, E, D) כך ש-
למערכת יש סודיות מושלמת אם ורק אם

$$(1) \text{ לכל } x \in X \text{ ולכל } y \in Y \text{ קיים לפחות אחד } k \text{ עבורו } y = e_k(x)$$

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 $x \in X$ ו לכל $y \in Y$ קיים מפתח k יחיד עבורו y
 נסמן אורך של הקבוצת מפתחות ב- $|K| = n$. נרשום את הקבוצת טקטים 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,

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

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

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

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

 לכל $n \geq 1$ נסמן אורך של הסתברות שווה

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

משפט 51: אנטרופיה של שאנו

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

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

נקרא האנטרופיה של X .

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

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

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

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

מכיוון ש- Y ו- Z משתנים בלתי תלויים אז

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

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

$$\begin{aligned} H[X] &= \sum p_x \ell_Q(x) = \sum p_y p_z [\ell_Q(y) + \ell_Q(z)] && \text{לפיכך} \\ H[X] &= \sum p_y p_z f(p_y p_z) = \sum p_y p_z [f(p_y) + f(p_z)] && \text{מכאן} \\ f(p_y p_z) &= f(p_y) + f(p_z) \quad \text{לכל } p_y \text{ ו- } p_z. \text{ לכן} \\ .f(p) &= C \log(p) \text{ נ'''}. \end{aligned}$$

icut nenihi ci yish leno meshutana makihi $\{a, b\} = X$ beul ponkzit hahtsbarotot shel $P_X(a) = \frac{1}{2}$, $P_X(b) = \frac{1}{2}$. $f(p) = -\log_2(p)$ vinkbel $f(\frac{1}{2}) = 1$ vinkbel $f(Q^*(a)) = \ell_{Q^*}(a) = 1$ vinkbel $f(Q^*(b)) = \ell_{Q^*}(b) = 1$.

■

משפט 52:

נתנו 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 האנתרופיה מקבלת ערך מקסימלי שניתנת על ידי

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

ערך זה הוא הערך המקסימלי האפשרי של האנתרופיה.

משפט 53: אי שוויון האפמן

נתנו קבוצת אוטיות של טקסט גלי X והצפנת האפמן f . נניח כי $l(f)$ תוחלת האורך של ההצפנה ו- $H(X)$ האנתרופיה של הטקסט גלי. מתקיים

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