שאלה 16 נתון הטקסט גלוי

mynameisbond

והטקסט מוצפן

KAANAEMKWVVC

המתקבל באמצעות צופן היל. מצאו את המפתח של הצופן.

$x \in P$	m	y	n	a	m	e	i	s	b	o	n	d
$x \in \mathbb{Z}_{26}$	12	24	13	0	12	4	8	18	1	14	13	3
$y \in C$	K	A	A	N	A	E	M	K	W	V	V	C
$y \in \mathbb{Z}_{26}$	10	0	0	13	0	4	12	10	22	21	21	2

$x_1 = 12 \quad x_2 = 24$

$x_3 = 13 \quad x_4 = 0$

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 12 & 24 \\ 13 & 0 \end{pmatrix}$$

$$|X| = -24(13) = -312 \bmod 26$$

$$= 0$$

X הפיכה אם ורק אם $|X| \neq 0$ ו-$\gcd(|X|, 26) = 1$.

$$a+b>0 \quad i \quad a-b>0$$

$$\Longrightarrow \quad (a-b)(c-d)>0$$

$$\Longrightarrow \quad ac-bc-ad+bd>0$$

$$\Longrightarrow \quad ac+bd>ad+bc$$

$$ac+bd \;\; ? \;\; ad+bc$$

$$a-b>0 \quad \Longrightarrow \quad a>b$$

$$c-d>0 \quad \Longrightarrow \quad c>d$$

$$ac+bd>ad+bc$$

$$\overline{a}\overline{c}+\tilde{b}\overline{r}>ad+bc \quad \text{ולכן} \quad a>b \quad i \quad c>d \quad \text{כיוון}$$

$$\text{נתון:}$$

$$\text{הוכח:}$$

$$\text{הוכחה:}$$

$$\text{נתון:}$$

$$\text{הוכח:}$$

$$\text{הוכחה:}$$

(1) נתון: $p_1 \geq p_2 \geq \cdots \geq p_k$ כך ש

$1' \cdot 1$ מספרים ראשוניים כך ש

p מספר ראשוני.

$$n_1 \leq n_2 \leq \cdots \leq n_k .$$

פתרון: $X = \{x_1, x_2, x_3\}$

$P_1 = \frac{1}{2}$, $P_2 = \frac{3}{8}$, $P_3 = \frac{1}{8}$

$P_1 \geq P_2 \geq P_3$

$$\left.\begin{array}{ll} \gamma(x_1) = 0 & n_1 = 1 \\ \gamma(x_2) = 10 & n_2 = 2 \\ \gamma(x_3) = 100 & n_3 = 3 \end{array}\right\} \Rightarrow \Longrightarrow \quad n_1 \leq n_2 \leq n_3$$

פתרון: $X = \{x_1, x_2, \ldots, x_k\}$

$\gamma(x_1) = 0000$ $\Longrightarrow$ $n_1 = 4$

$\gamma(x_2) = 10$ $\Longrightarrow$ $n_2 = 2$

$P_X(x_1) = p_1$, ... , $P_X(x_k) = p_k$

$P_X(x_i) = p_i$ $\quad 0 \leq p_i \leq 1$ $\quad i = 1, \ldots, k$

$\gamma_X(x_i)$: X של i-ית המילה הבינארית של x_i, $1 \leq i \leq k$

γ הוא קוד קומפקטי עבור X.

פתרון: $X = \{a, b, \ldots, g\}$

$X = \{x_1, \ldots, x_k\}$ נניח בה"כ ש

$E_0 = \lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_k P_k$

$\lambda_1 \le \lambda_2 \le \cdots \le \lambda_k$ כך ש $P_1, P_2, \cdots, P_k$

תרגיל 3

פתרון:

$E_0 = \lambda_1' P_1 + \lambda_2' P_2 + \lambda_3' P_3 = 2\left(\frac{1}{2}\right) + 1\left(\frac{2}{8}\right) + 3\left(\frac{1}{8}\right) = \frac{13}{8}$

$E = \lambda_1' P_1 + \lambda_2' P_2 + \lambda_3' P_3 = 2\left(\frac{1}{2}\right) + 1\left(\frac{2}{8}\right) + 3\left(\frac{1}{8}\right) = \frac{15}{8}$

Q' מצב עירור ראשון של המערכת, Q מצב היסוד של המערכת

$\lambda_1' = 2 \quad \lambda_2' = 1 \quad \lambda_3' = 3$

$f(x_1) = 10$
$f(x_2) = 0$
$f(x_3) = 10$

$\lambda_1' \le \lambda_2' \le \lambda_3'$

$E_0 < E_Q$, (1)

$$\begin{cases} \lambda_{j-1} \geq \lambda_j \\ p_{j-1} \geq p_j \end{cases} \Rightarrow \boxed{p_{j-1} n_{j-1} + \lambda_j p_j \geq p_j n_j + \lambda_j p_{j-1}} \quad (*)$$

$$p_{j-1} \geq p_j \geq \cdots \geq p_k > 0 \Rightarrow$$

$$\Rightarrow \lambda_{j-1} \geq \lambda_j = \min(\lambda_1, \ldots, \lambda_k) \quad \lambda_j = \min(\lambda_1, \ldots, \lambda_k) \Leftarrow$$

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k > 0 \quad \text{כך ש-} \quad \lambda_j = \lambda_1$$

$$E = \lambda_1 p_1 + \cdots + \lambda_k p_k$$

$$\lambda_1 p_2 + \cdots$$

$\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ הוא רצף יורד של מספרים חיוביים, נקרא

λ_1 הוא הערך העצמי הגדול ביותר של A.

λ_k הוא הערך העצמי הקטן ביותר של A.

λ_2 הוא הערך העצמי השני בגודלו של A.

λ_{k-1} הוא הערך העצמי השני בקטנותו של A.

λ_j הוא הערך העצמי ה-j בגודלו של A.

משפט אוילר: יהיו p,q מספרים ראשוניים שונים זה מזה. אזי

$$\varphi(n)=\varphi(pq)=(p-1)(q-1)=pq-p-q+1.$$

הוכחה: נסמן ב-A את קבוצת המספרים הטבעיים הקטנים או שווים ל-n שאינם זרים ל-n. כלומר,

$$A=\{1\le x\le n \mid x \text{ מתחלק ב-} p \text{ או ב-} q\}.$$

ברור ש-$|A|=n-\varphi(n)$. נשים לב כי

$$A=\{p,2p,\dots,(q-1)p\}\cup\{q,2q,\dots,(p-1)q\}$$

ולכן $|A|=(q-1)+(p-1)=p+q-2$. מכאן נובע כי

$$\varphi(n)=n-|A|=pq-(p+q-2)=pq-p-q+1.$$

□

דוגמה: נחשב את $\varphi(100)$. נפרק $100=2^2\cdot 5^2$, ולכן $p=2$, $q=5$, $n=100$. נקבל

$$\varphi(100)=100-50-20+10=40.$$

משפט אוילר: יהיו a,n מספרים שלמים כך ש-$\gcd(a,n)=1$ ו-$n>1$. אזי

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

בפרט, אם p ראשוני ו-a אינו מתחלק ב-p, אזי

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

משפט RSA: יהיו p,q מספרים ראשוניים שונים זה מזה, ויהי $n=pq$. נגדיר

$$E_k(x)=x^k \bmod n$$
$$d_k(y)=y^e \bmod n$$

כאשר $k=1,2,\dots,\varphi(n)$. אזי $e=k^{-1} \bmod \varphi(n)$ קיים אם ורק אם $\gcd(k,\varphi(n))=1$. במקרה זה E_k ו-d_k הן פונקציות הפוכות זו לזו.

הוכחה: נניח ש-k זר ל-$\varphi(n)$. אזי קיים $e=k^{-1} \bmod \varphi(n)$, כלומר $ek\equiv 1 \pmod{\varphi(n)}$. נסמן $ek=1+t\varphi(n)$ עבור $t\in\mathbb{Z}$. נקבל

$$d_k(E_k(x))=x^{ek}=x^{1+t\varphi(n)}=x\cdot(x^{\varphi(n)})^t.$$

אם x זר ל-n אז $x^{\varphi(n)}\equiv 1 \pmod n$ לפי משפט אוילר, ולכן $d_k(E_k(x))\equiv x \pmod n$. אם x אינו זר ל-n (כלומר $x=0$ או x מתחלק ב-p או ב-q) אפשר להראות באופן ישיר שהשוויון עדיין מתקיים.

להפך, נניח ש-k אינו זר ל-$\varphi(n)$. אזי $\gcd(k,\varphi(n))=d>1$. נבחר x כך ש-$1<x<n$ ו-x זר ל-n (למשל $x=2$). נסמן $y=E_k(x)=x^k \bmod n$. אם E_k היתה הפיכה, היה קיים z יחיד עם $E_k(z)=y$, ומכיוון ש-$x^{\varphi(n)}\equiv 1$ נקבל $z=x^{k^{-1} \bmod \varphi(n)}$. אבל $x^{\varphi(n)/d}\equiv 1$ ולכן $x^{k\cdot\varphi(n)/d}\equiv 1$, כלומר $x^{\varphi(n)}\equiv 1$ גורר $x^{k\cdot\varphi(n)/d}\equiv 1$. מכאן שקיימים לפחות d ערכים שונים של z עם $E_k(z)=y$, ולכן E_k אינה חד-חד-ערכית. □

דוגמה: נבחר $p=11$, $q=13$, $n=143$, $\varphi(n)=120$. נבחר $k=7$ (זר ל-120). אזי $e=7^{-1} \bmod 120=103$ (כי $7\cdot 103=721=6\cdot 120+1$). נצפין את $x=2$:

$$E_7(2)=2^7 \bmod 143=128.$$

נפענח:

$$d_{103}(128)=128^{103} \bmod 143=2.$$

נבחר $k=8$ (לא זר ל-120). אזי $\gcd(8,120)=8$. נצפין את $x=2$:

$$E_8(2)=2^8 \bmod 143=256 \bmod 143=113.$$

נפענח:

$$d_{113}(113)=113^{113} \bmod 143=2.$$

שוב קיבלנו 2, אך E_8 אינה חד-חד-ערכית: $E_8(0)=0$ ו-$E_8(11)=11^8 \bmod 143=0$.

$$f_3 = f_1 - q_2 f_2 = 7 - (1)q = 3 \qquad 0 \le f_3 < f_2$$

$$s_3 = s_1 - q_2 s_2 = 0 - 1(1) = -1 \qquad q_2 = 1$$

$$t_3 = t_1 - q_2 t_2 = 1 - 1(-68) = 69$$

$$f_4 = f_2 - q_3 f_3 = 4 - (1)3 = 1 \qquad 0 \le f_4 < f_3$$

$$s_4 = s_2 - q_3 s_3 = 1 - 1(-1) = 2 \qquad q_3 = 1$$

$$t_4 = t_2 - q_3 t_3 = -68 - 1(69) = -137$$

$$f_5 = f_3 - q_4 f_4 = 3 - (3)1 = 0 \qquad q_4 = 0$$

$$f_0 = 480 \qquad f_1 = 7$$

$$s_0 = 1 \qquad s_1 = 0$$

$$t_0 = 0 \qquad t_1 = 1$$

$$f_{k+1} = f_{k-1} - q_k f_k$$

يتوقف عندما $f_{k+1} = 0$:

$$0 \le f_{k+1} < f_k$$

مثال:

$$480 + 74 = x$$

$$f_0 = 480 \qquad f_1 = 74$$

$$s_0 = 1 \qquad s_1 = 0$$

$$t_0 = 0 \qquad t_1 = 1$$

$$f_2 = f_0 - q_1 f_1 = 480 - (68)7 = 4 \qquad 0 \le f_2 < f_1$$

$$s_2 = s_0 - q_1 s_1 = 1 - 68(0) = 1$$

$$t_2 = t_0 - q_1 t_1 = 0 - 68(1) = -68 \qquad q_1 = 68$$

$$z^{10} + z^5 + z^2 + z + 1 = 0$$

ج: $\varphi(12) = 4$

$$a^4 \equiv 1 \pmod{12}$$

$$a^{-1} = a^3 \pmod{12}$$

$$5^{-1} = 5^3 \equiv 5 \pmod{12}$$

$$7^{-1} = -13 \equiv -1 \pmod{12}$$

$$-13 \cdot 7 \equiv 1 \pmod{12}$$

$$-13 \cdot 7 = 1 + 2 \cdot 12$$

$$1 = 7 \cdot 7 - 13 \cdot 4$$

$$7^{-1} \equiv 7 \pmod{12}$$

$$x = 7 \cdot 5 \pmod{12}$$

$$= 35 \pmod{12}$$

$$= 11$$

$$\varphi(n) = \varphi(12) = \varphi(2^2 \cdot 3) = 4$$

$$\varphi(n) = \varphi(p_1^{k_1} \cdots p_r^{k_r}) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1)$$

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r})$$

$$\varphi(p^k) = p^k - p^{k-1}$$

$$\varphi(p) = p - 1$$

$$\varphi(1) = 1$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\varphi(n) = p_1^{k_1} \cdots p_r^{k_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\varphi(n) = p_1^{k_1 - 1}(p_1 - 1) \cdots p_r^{k_r - 1}(p_r - 1)$$

$$\varphi(n) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1)$$

$$\equiv 1 \pmod{527}$$

$$\Rightarrow 204^{t} \equiv 204^{1+2+4+\cdots+2^{t-1}} = (204)(204^{2})(204^{4})\cdots$$

$$204 \bmod 527 = 204$$

$$204^{2} \bmod 527 = (204)^{2} \bmod 527 = 289$$

$$204^{4} \bmod 527 = (289)^{2} \bmod 527 = 510$$

$$204^{8} \bmod 527 = (510)^{2} \bmod 527 = 1$$

$$\Rightarrow$$

$$(204)^{t} \bmod 527 = (204)(289)(510) \bmod 527$$

$$= 204 \bmod 527$$

$$= 204 .$$

$$x = 204 \quad (\because 1 \le x < 527)$$

$$\gcd(204, 527) = 1 \quad \text{و} \quad 204 \text{ عنصر في } \mathbb{Z}_{527}^{*}$$

$$\text{رتبة } 204 \text{ في } \mathbb{Z}_{527}^{*} \text{ هي } 1 .$$

$$3q_3 = 256 + 64q + 16 + 4q + 2 + 1$$

תרגיל: נתון מפתח ציבורי של צופן El-Gamal

$$K = (\alpha = 8,\ a = 25,\ p = 23,\ d = 2)$$

א) הצפן הטקסט גלוי $x = 10$.

פענח את הטקסט המוצפן.

ב) הוכיחו: הפענוח של $(y_1 = 18,\ y_2 = 15)$ הוא $x = 10$.

פתרון.

כלל מצפין של El-Gamal:

$$e_K(x, d) = (y_1, y_2)$$

$$y_1 = \alpha^d \bmod p$$

$$y_2 = \beta^d x \bmod p.$$

$$\beta = \alpha^a \bmod p.$$

$$\beta = 8^{25} \bmod 23 = 8^{3}\, 8^{22} \bmod 23$$

($p-1$ → 22; p → 23)

משפט פרמה: לכל ראשוני p ולכל x מתקיים

$$x^{p-1} \equiv 1 \bmod p$$

$y_2 = g^x \bmod p = 6^{10} \bmod 23$

$= 3650 \bmod 23$

$= 13$

$\Rightarrow e_{12}(x, k) = (18, 13)$.

: Ex-Comm, Alice and Bob did

$d_{12}(x_1, y_2) = (y_1^{\alpha})^{-1} y_2 \bmod p$.

: $(y_1^{\alpha})^{-1} \bmod p$ find

$y_1 = g^{\alpha} \bmod p = 9^3 \bmod 23$

$= 729 \bmod 23 = 16$

$e_k(x, \alpha) = (y_1, y_2)$

$= (6, 16)$

$K = (y_1^3 \bmod 23)(y_2^{22} \bmod 23)$

Inverse $(5^{12} \bmod 23)$ (1)

$$17 = 16 + 2 + 1 .$$

$$18 \bmod 23 = 18$$

$$18^2 \bmod 23 = 324 \bmod 23 = 2$$

$$18^4 \bmod 23 = 2^2 \bmod 23 = 4$$

$$18^8 \bmod 23 = 4^2 \bmod 23 = 16$$

$$18^{16} \bmod 23 = 16^2 \bmod 23 = 3$$

נשים לב כי $p = 23$ הוא ראשוני ו-$a = 18$ הוא שורש פרימיטיבי מודולו 23.

$$(18^{-1} \bmod 23)^{17} = 18^{-17} \bmod 23.$$

$$18^{-17} \bmod 23 = (18^{22})(18^{-39}) \bmod 23$$

$$= 18^{19} \bmod 23$$

$$= 18^{-3} \bmod 23.$$

$$18^{-17} \bmod 23 = (18^{22})(18^{-39}) \bmod 23$$

$$18^{22} \equiv 1 \bmod 23$$

נשים לב כי 18 הוא שורש פרימיטיבי מודולו 23, כלומר

$$(18^{-1} \bmod 23)^{17} = 18^{-17} \bmod 23.$$

$$18^{19} \bmod 23 = (2)(2)(18) \bmod 23$$

$$\equiv 108 \bmod 23$$

$$= 16.$$

$$(11)^{-1} \bmod 29 = 18^{-25} \bmod 23 \quad \text{and} \quad 18 \equiv 16 \bmod 23$$

$$(11^{-1})^{-1} \bmod 29 = (18^{-25} \bmod 23)(18 \bmod 23)$$

$$= (16 \times 18) \bmod 23$$

$$= 16.$$