שאלה 1 (25 נקודות)

הוכיחו כי פונקצית ההצפנה ופונקצית הפענוח של צופן ה-RSA הן פונקציות הופכיות.

כתרגיל

צריך להוכיח:

$$d_k(e_k(x)) = x \qquad e_k(d_k(x)) = x$$

כאן מצפינה — כאן מפענח

להוכיח: (קשה נוסחאית)

(p, q, b, a)

$p \cdot q$ (פיינלים) p, q

$p \cdot q = n$:סיכום

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

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

כך מצפין את RSA :

" :כך מפענח

$ab \equiv 1 \bmod \varphi(n)$.

$n = pq$.

צריך להוכיח:

$$d_k(e_k(x)) = x \iff d_k(x^b \bmod n) = x \iff (x^b \bmod n)^a \bmod n = x \quad \text{---------} \textcircled{0}$$

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

$ed - 1 = k(p-1)(q-1)$ ——— (3)

לפי (3) ו- $ed \equiv 1 \pmod{\phi(n)}$ אז ed הוא מהצורה $1 + k\phi(n)$ עבור k שלם.

$ed - 1 = k(p-1)(q-1)$ ——— (3)

לפי (3) ו- $ed \equiv 1 \pmod{(p-1)(q-1)}$ אז ed הוא מהצורה $1 + k(p-1)(q-1)$ עבור k שלם.

$ed \equiv 1 \pmod{\phi(n)} \Rightarrow ed \equiv 1 \pmod{(p-1)(q-1)}$ ——— (2)

ed הוא מהצורה $1 + k(p-1)(q-1)$ ו- (2) נובע ש- $ed - 1$ מתחלק ב- $(p-1)(q-1)$.

$ed \equiv 1 \pmod{\phi(n)}$ אז ed הוא מהצורה $1 + k\phi(n)$ עבור k שלם.

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

$\phi(n)$: פונקציית אוילר

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

פונקציית אוילר $\phi(n)$ מחזירה את מספר המספרים הטבעיים הקטנים מ- n ושזרים ל- n.

(1) נכון כי: ישנם pq מספרים טבעיים הקטנים מ- pq.

$x^{ed-1} \mod p = (x^{k(q-1)})^{p-1} \mod p \equiv 1 \mod p$ — (5)

$x^{ed-1} \mod p \equiv 1 \mod p$ נכון עבור כל x שלם.

$\Rightarrow$

$x^{ed-1} = \left(x^{k(q-1)}\right)^{p-1}$ ——— (4)

x^{ed-1} מתחלק ב- p עבור כל x שלם.

$x^{ed-1} \overset{(3)}{=} x^{k(p-1)(q-1)}$

$x^{ed-1} \overset{\text{משפט פרמה}}{=} x$

לפי (3) ו- $ed - 1 = k(p-1)(q-1)$ עבור k שלם, אז ed הוא מהצורה $1 + k(p-1)(q-1)$.

$ed - 1$ הוא מכפלה של $(p-1)(q-1)$ ו- (2) נובע ש- $ed - 1$ הוא מכפלה של $(p-1)(q-1)$.

ed הוא מהצורה $1 + k(p-1)(q-1)$ עבור k שלם.

$ed \equiv 1 \pmod{\phi(n)}$ ——— (2)

$ed \equiv 1 \pmod{(p-1)(q-1)}$

$ed \equiv 1 \pmod{\phi(n)}$ אז ed הוא מהצורה $1 + k\phi(n)$ עבור k שלם.

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

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

$\phi(n)$: פונקציית אוילר

משפט השאריות הסיני: יהיו $m_1, m_2, \ldots, m_k$ מספרים שלמים חיוביים זרים זה לזה בזוגות, ויהיו $a_1, a_2, \ldots, a_k$ מספרים שלמים כלשהם. אזי למערכת הקונגרואנציות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

קיים פתרון יחיד x מודולו $m_1 m_2 \cdots m_k$.

הוכחה: נוכיח תחילה את היחידות. נניח ש-x_1 ו-x_2 שניהם פתרונות. אזי לכל i מתקיים $x_1 \equiv a_i \equiv x_2 \pmod{m_i}$, כלומר $m_i \mid (x_1 - x_2)$. מכיוון שהמספרים $m_1, \ldots, m_k$ זרים זה לזה בזוגות, נובע ש-$m_1 m_2 \cdots m_k \mid (x_1 - x_2)$, כלומר $x_1 \equiv x_2 \pmod{m_1 m_2 \cdots m_k}$.

נוכיח כעת את הקיום. נסמן $M = m_1 m_2 \cdots m_k$ ו-$M_i = M / m_i$ לכל i. מכיוון ש-$\gcd(M_i, m_i) = 1$, קיים מספר שלם y_i כך ש-$M_i y_i \equiv 1 \pmod{m_i}$. נגדיר

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k.$$

לכל $j \neq i$ מתקיים $m_i \mid M_j$, ולכן $a_j M_j y_j \equiv 0 \pmod{m_i}$. לכן

$$x \equiv a_i M_i y_i \equiv a_i \cdot 1 \equiv a_i \pmod{m_i}$$

לכל i, כלומר x הוא פתרון המערכת. $\square$

דוגמה: נמצא את כל המספרים הטבעיים x שמקיימים $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ ו-$x \equiv 2 \pmod{7}$.

כאן $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $M = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$. נחשב y_1 כך ש-$35 y_1 \equiv 1 \pmod{3}$, כלומר $2 y_1 \equiv 1 \pmod{3}$, ולכן $y_1 = 2$. נחשב y_2 כך ש-$21 y_2 \equiv 1 \pmod{5}$, כלומר $y_2 \equiv 1 \pmod{5}$, ולכן $y_2 = 1$. נחשב y_3 כך ש-$15 y_3 \equiv 1 \pmod{7}$, כלומר $y_3 \equiv 1 \pmod{7}$, ולכן $y_3 = 1$. אזי

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233.$$

המספר הקטן ביותר הוא $233 - 2 \cdot 105 = 23$, וכל הפתרונות הם $x \equiv 23 \pmod{105}$.

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

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

הוכחה: נסמן ב-$r_1, r_2, \ldots, r_{\varphi(n)}$ את המספרים הטבעיים הקטנים מ-n וזרים ל-n. נתבונן במספרים $ar_1, ar_2, \ldots, ar_{\varphi(n)}$. מכיוון ש-$\gcd(a, n) = 1$ ו-$\gcd(r_i, n) = 1$, נובע ש-$\gcd(ar_i, n) = 1$ לכל i. כמו כן, המספרים $ar_1, \ldots, ar_{\varphi(n)}$ שונים זה מזה מודולו n: אם $ar_i \equiv ar_j \pmod{n}$ אז $r_i \equiv r_j \pmod{n}$ (כי a הפיך מודולו n), ולכן $i = j$.

לכן $ar_1, \ldots, ar_{\varphi(n)}$ הם $\varphi(n)$ מספרים שונים זה מזה מודולו n, וכל אחד מהם זר ל-n. מכאן שהם שקולים מודולו n לאיברי $r_1, \ldots, r_{\varphi(n)}$ בסדר כלשהו. נכפיל את כל הקונגרואנציות:

$$ar_1 \cdot ar_2 \cdots ar_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$$

$$a^{\varphi(n)} \cdot r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$$

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

כאשר המעבר האחרון נובע מכך שהמכפלה $r_1 r_2 \cdots r_{\varphi(n)}$ זרה ל-n ולכן ניתן לצמצם בה. $\square$

משפט פרמה הקטן: יהי p מספר ראשוני ויהי a מספר שלם כך ש-$p \nmid a$. אזי

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

הוכחה: זהו מקרה פרטי של משפט אוילר, שכן $\varphi(p) = p - 1$ כאשר p ראשוני. $\square$

מסקנה: לכל מספר שלם a ולכל מספר ראשוני p מתקיים $a^p \equiv a \pmod{p}$.

הוכחה: אם $p \mid a$ אז $a \equiv 0 \pmod{p}$ ו-$a^p \equiv 0 \pmod{p}$, ולכן הקונגרואנציה מתקיימת. אם $p \nmid a$ אז לפי משפט פרמה הקטן $a^{p-1} \equiv 1 \pmod{p}$, ומכפילים ב-$a$ מקבלים $a^p \equiv a \pmod{p}$. $\square$

דוגמה: נחשב את $2^{100} \bmod 7$. מכיוון ש-7 ראשוני ו-$7 \nmid 2$, לפי משפט פרמה הקטן $2^6 \equiv 1 \pmod{7}$. נכתוב $100 = 6 \cdot 16 + 4$, ולכן

$$2^{100} = (2^6)^{16} \cdot 2^4 \equiv 1^{16} \cdot 16 \equiv 16 \equiv 2 \pmod{7}.$$

דוגמה: נחשב את $3^{1000} \bmod 11$. מכיוון ש-11 ראשוני ו-$11 \nmid 3$, לפי משפט פרמה הקטן $3^{10} \equiv 1 \pmod{11}$. נכתוב $1000 = 10 \cdot 100$, ולכן

$$3^{1000} = (3^{10})^{100} \equiv 1^{100} \equiv 1 \pmod{11}.$$

נכפיל ⑧ ב-x ולפי כלל זה כפל (כלל I) נקבל

$$(x^{ab-1})x \equiv (1)(x) \bmod n$$

$$x^{ab} \equiv x \bmod n$$

$$(x^b)^a \equiv x \bmod n \text{ ——— } ⑦$$

לפי כלל אסוציאטיביות של מודולרי, כל [illegible]:

$$x \bmod m \equiv y \bmod m \iff x \bmod m \equiv y \iff x \equiv y \bmod m$$

אז

$$(x^b)^a \bmod n \equiv x.$$

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

מש"ל.

אסוציאטיביות:

נוכיח $x \equiv y \bmod m \Rightarrow y \equiv x \bmod m$

נניח $x \equiv y \bmod m$.

ז"א קיים שלם q כך ש $x = qm + y$. $\Rightarrow y = (-q)m + x$

$\Rightarrow y = q'm + x$ כאשר $q' = -q$.

לכן $y \equiv x \bmod m$.

$\square$

$\square$

$x \bmod m = 2m+1 \iff x \bmod m \equiv 1 \bmod m$.

ש"ג

$x \bmod m = 2.m+1 - 2m = (2,-2)m+1 = 2m+1$

ולכן $2=2.-2$

$x = 2.m+1$.

ולכן $x \equiv 1 \bmod m$ עבור $m \in \mathbb{N}^+$ כלשהו. ראינו בתרגול 3 כי:

(#) $\iff$ יש s כך ש $x = 2.m+1$

$x = 2m+5$ ——— (*)

$x \bmod m = 5$ עבור $m > 5$.

(*) $\Rightarrow$ סתירה לתכונה 3 בתרגול 2

$x = 2m-2$ ——— (#)

$x \bmod m = x-2m \iff 2 = x-2m$

$x \equiv 1 \bmod m$:1 תרגיל

$x \equiv 1 \bmod m \iff x \bmod m \equiv m \bmod m$

שאלה 3 **(25 נקודות)** תהי $X = \{\mathtt{s}, \mathtt{t}, \mathtt{u}\}$ קבוצת טקסט גלוי בעלת פונקצית הסתברות

$$P_X(\mathtt{s}) = \frac{1}{6}\,, \qquad P_X(\mathtt{t}) = \frac{1}{4}\,, \qquad P_X(\mathtt{u}) = \frac{7}{12}\,.$$

תהי $K = \{k_1, k_2, k_3, k_4\}$ קבוצת מפתחות בעלי הסתברות שווה.
תהי $Y = \{\mathtt{A}, \mathtt{B}, \mathtt{C}\}$ קבוצת טקסט מוצפן. יהי

$$e_{k_i}(x) = 2x + i \mod 3$$

כלל מצפין לכל $x \in \mathbb{Z}_{26}$ ולכל $i \in \{1, 2, 3, 4\}$.

א) (20 נקודות)
מצאו את הפונקצית הסתברות של הטקסט מוצפן.

ב) (5 נקודות)
הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.

$e_{K_i}(x) = 2x + i \mod 3$

S: $i=1$: $e_{K_1}(18) = 2(18) + 1 \mod 3 = 37 \mod 3 = 1 \longrightarrow B$

$i=2$: $e_{K_2}(18) = 2(18) + 2 \mod 3 = 38 \mod 3 = 2 \longrightarrow C$

$i=3$: $e_{K_3}(18) = 2(18) + 3 \mod 3 = 39 \mod 3 = 0 \longrightarrow A$

$i=4$: $e_{K_4}(18) = 2(18) + 4 \mod 3 = 40 \mod 3 = 1 \longrightarrow B$

L: $i=1$: $e_{K_1}(19) = 2(19)+1 \bmod 3 = 39 \bmod 3 = 0 \longrightarrow A$

$i=2$: $e_{K_2}(19) = 2(19)+2 \bmod 3 = 40 \bmod 3 = 1 \longrightarrow B$

$i=3$: $e_{K_3}(19) = 2(19)+3 \bmod 3 = 41 \bmod 3 = 2 \longrightarrow C$

$i=4$: $e_{K_4}(19) = 2(19)+4 \bmod 3 = 42 \bmod 3 = 0 \longrightarrow A$

U: $i=1$: $e_{K_1}(20) = 2(20)+1 \bmod 3 = 41 \bmod 3 = 2 \longrightarrow C$

$i=2$: $e_{K_2}(20) = 2(20)+2 \bmod 3 = 42 \bmod 3 = 0 \longrightarrow A$

$i=3$: $e_{K_3}(20) = 2(20)+3 \bmod 3 = 43 \bmod 3 = 1 \longrightarrow B$

$i=4$: $e_{K_4}(20) = 2(20)+4 \bmod 3 = 44 \bmod 3 = 2 \longrightarrow C$

$$e_{K_i}(x) = 2x + i \bmod 3$$

$$e_{K_i}(x+1) = \left(e_{K_i}(x) + 2\right) \bmod 3$$

	S	L	U
k_1	B	A	C
k_2	C	B	A
k_3	A	C	B
k_4	B	A	C

$$P_X(S)=\frac{1}{6} \qquad P_X(L)=\frac{1}{4} \qquad P_X(U)=\frac{7}{12}$$

$$P_K(k_i)=\frac{1}{4} \qquad 1\le i\le 4$$

$$P(Y=y)=\sum_{k\in\{k_1,k_2,k_3,k_4\}} P(K=k)\,P(X=d_k(y))$$

$$P_Y(A)=P_K(k_1)P_X(d_{k_1}(A))+P_K(k_2)P_X(d_{k_2}(A))+P_K(k_3)P_X(d_{k_3}(A))+P_K(k_4)P_X(d_{k_4}(A))$$

$$=\frac{1}{4}\left(\frac{1}{4}\right)+\frac{1}{4}\left(\frac{7}{12}\right)+\frac{1}{4}\left(\frac{1}{6}\right)+\frac{1}{4}\left(\frac{1}{4}\right)=\frac{3+7+2+3}{48}=\frac{15}{48}=\frac{5}{16}.$$

$$P_Y(B)=P_K(k_1)P_X(d_{k_1}(B))+P_K(k_2)P_X(d_{k_2}(B))+P_K(k_3)P_X(d_{k_3}(B))+P_K(k_4)P_X(d_{k_4}(B))$$

$$=\frac{1}{4}\left(\frac{1}{6}\right)+\frac{1}{4}\left(\frac{1}{4}\right)+\frac{1}{4}\left(\frac{7}{12}\right)+\frac{1}{4}\left(\frac{1}{6}\right)=\frac{2+3+7+2}{48}=\frac{14}{48}=\frac{7}{24}.$$

$$P_Y(C)=1-P_Y(A)-P_Y(B)=1-\frac{15}{48}-\frac{14}{48}=\frac{19}{48}.$$

$$P(Y=y \mid X=x) = P(Y=y) \iff P(X=x \mid Y=y) = P(X=x)$$

$P(Y=A) = \frac{5}{16}$

$P(Y=A \mid X=5)$:

$$P(Y=A \mid X=5) = \sum_{\{k_1,k_2,k_3,k_4\}} P(k=k_i) \quad P(k=k_3) = \frac{1}{4}$$

$$5 = d_{k_i}(A)$$

$$P(Y=A \mid X=5) = \frac{1}{4} \neq \frac{5}{16} = P(Y=A)$$

$$P(X=E \mid Y=B) \overset{\text{בייס}}{=} \frac{P(Y=B \mid X=E) P(X=E)}{P(Y=B)}$$

$$= \frac{P(Y=B \mid X=E)\left(\frac{1}{4}\right)}{\binom{14}{48}} = \left(\frac{12}{14}\right) P(Y=B \mid X=E)$$

$$\overset{\text{בייס}}{=} \left(\frac{12}{14}\right) \sum_{\{k_1,k_2,k_3,k_4\}} P_{k}(k_i) = \frac{12}{14} \cdot P(k=k_2)$$

$$d_{k_i}(B) = E$$

$= \left(\frac{12}{17}\right)\left(\frac{1}{4}\right) = \frac{3}{17}$.

שאלה 4 (25 נקודות)

אליס רוצה לשלוח הודעה לבוב. היא מבקשת להצפין את ההודעה באמצעות צופן אל-גמאל. למטרה הזאת בוב בוחר במפתח הציבורי הבא : $(p = 47, \alpha = 12, a = 10)$.
בוב צריך מפתח הסודי המתאים למפתח הציבורי הזה, כדי לפענח את הטקסט מוצפן אשר אליס שולחת.

א) (10 נקודות) חשבו את המפתח הסודי.

ב) (15 נקודות)
הטקסט המוצפן של ההודעה אשר בוב מקבל הוא $(3, 42)$.
מצאו את הטקסט הגלוי של ההודעה.

$\beta = \alpha^{a} \bmod p$

$= 12^{10} \bmod 47$

$10 = 8 + 2$.

$12^{2} \bmod 47 = 144 \bmod 47 = \underline{3}$

$12^{4} \bmod 47 = (12^{2})^{2} \bmod 47 = 3^{2} \bmod 47 = 9$

$12^{8} \bmod 47 = (12^{4})^{2} \bmod 47 = 9^{2} \bmod 47 = \underline{34}$.

$$\beta = 12^{10} \bmod 47 = (12^8)(12^2) \bmod 47 = (34)(5) \bmod 47$$

$$= 102 \bmod 47$$

$$= 8$$

$$\therefore \beta = 8 \not> 5$$

שאלה 3 נתון $y_1=3,\ y_2=42$ מעל $GF(47)$. פתור את המשוואה $y_1^a = y_2$

$$x = (y_1^a)^{-1} y_2 \bmod p = (3^{10})^{-1} \cdot 42 \bmod 47$$

$$= 3^{-10}(42) \bmod 47 = (3^{-10} \bmod 47)(42 \bmod 47) \quad \text{---} \quad (1)$$

משפט פרמה: $c^{p-1} \equiv 1 \bmod p$.

$$3^{47-1} \equiv 1 \bmod 47 \iff$$

נחשב $3^{-10} \bmod 47$ ע"י שימוש במשפט פרמה

$$3^{-10} \bmod 47 = 3^{-10}(1) \bmod 47$$

$$= (3^{-10} \bmod 47)(1 \bmod 47)$$

$$= (3^{-10} \bmod 47)(3^{47-1} \bmod 47)$$

$$= (3^{-10})(3^{47-1}) \bmod 47$$

$$= 3^{36} \bmod 47$$

$36 = 32 + 4$. נחשב $3^{36} \bmod 47$ ע"י שימוש בריבועים חוזרים

$3^2 \bmod 47 = 9$ $\quad 3^4 \bmod 47 = 9^2 \bmod 47 = 34$ $\quad 3^8 \bmod 47 = 34^2 \bmod 47 = 28$

$3^{16} \bmod 47 = 28^2 \bmod 47 = 32$

$3^{32} \bmod 47 = 32^2 \bmod 47$

$= 1024 \bmod 47$

$= 37$

$3^{36} \bmod 47 = 3^{32} \cdot 3^4 \bmod 47 = (37)(34) \bmod 47 = 1258 \bmod 47 = 26$

$$(y_1^a)^{-1} \bmod 47 = (3^{10})^{-1} \bmod 47 = 36$$

$$(y_1^a)^{-1} y_2 \bmod 47 = (36)(42) \bmod 47 = 1512 \bmod 47 = 8$$

$x = 8$ /25