$$d_{k'}\left(e_{k'}(x)\right) = x \,. \qquad \text{(משל RSA)}$$

$d_k(y)$ הוא ההופכי של $e_k(x)$ מודולו n. אלגוריתם זה נקרא

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

כלומר: x מוצפן ל $y = x^b \bmod n$.

(אם n ידוע אך לא $\varphi(n)$)

$$k = \left(n, p, q, a, b \;\middle|\; ab \equiv 1 \bmod \varphi(n)\right) .$$

a,b מספרים טבעיים p,q ראשוניים

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

RSA	אל גמל	דיפי-הלמן
(RSA וגם אל גמל)		

: אלגוריתם X מוגדר על ידי (e, d, n) כאשר n מכפלת שני מספרים ראשוניים גדולים, e מספר טבעי כלשהו, ו d הוא ההופכי של e מודולו $\varphi(n)$.

תרגיל בית 1

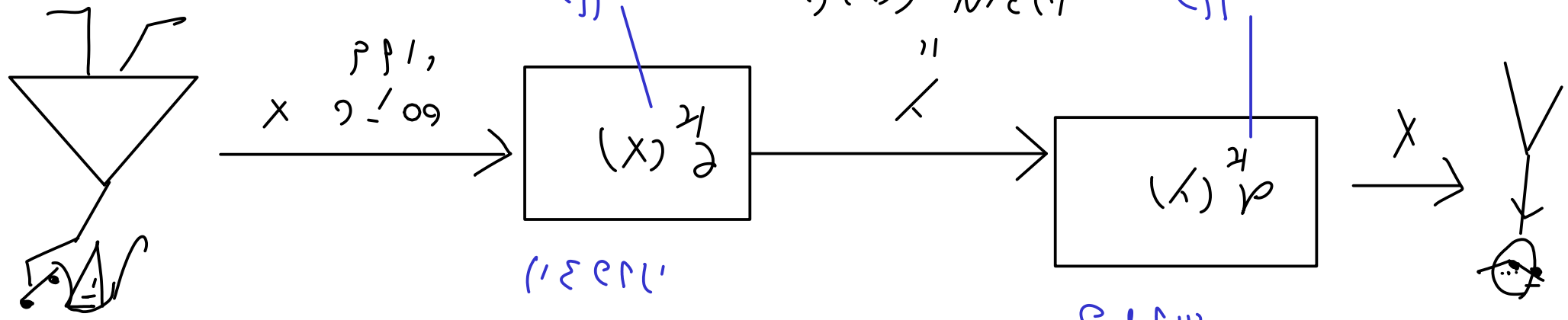
שאלה 1 (20 נק') — יהיו p, q שני מספרים ראשוניים שונים זה מזה.

(1) הוכיחו כי $\varphi(p^k) = p^{k-1}(p-1)$ לכל $k \geq 1$.

(2) הוכיחו כי $\varphi(pq) = (p-1)(q-1)$.

(3) הוכיחו כי $\varphi(n) = \varphi(p)\varphi(q)$ לכל n טבעי שמקיים $n = pq$.

(4) יהיו a, b שני מספרים טבעיים זרים זה לזה. הוכיחו כי $a^{\varphi(b)} \equiv 1 \pmod{b}$.



שאלה 2 (20 נק') — יהי n מספר טבעי. נגדיר $\varphi(n)$ להיות מספר המספרים הטבעיים הקטנים מ-n ושזרים ל-n.

(1) חשבו את $\varphi(1)$, $\varphi(2)$, $\varphi(3)$, $\varphi(4)$, $\varphi(5)$, $\varphi(6)$.

(2) הוכיחו כי $\varphi(n) \leq n-1$ לכל $n \geq 2$.

(3) הוכיחו כי $\varphi(n) = n-1$ אם ורק אם n ראשוני.

שאלה 3 (20 נק') — יהי p מספר ראשוני אי-זוגי. נגדיר $a_n = \varphi(p^n)$ לכל $n \geq 1$.

(1) הוכיחו כי a_n סדרה הנדסית מעל $\mathbb{Q}$.

(2) הוכיחו כי a_n סדרה הנדסית מעל $\mathbb{Z}/m\mathbb{Z}$ לכל $m \geq 2$.

שאלה 4 (20 נק') — יהי p מספר ראשוני אי-זוגי. נגדיר $a_n = \varphi(p^n)$ לכל $n \geq 1$.

(1) הוכיחו כי a_n סדרה הנדסית מעל $\mathbb{Q}$.

(2) הוכיחו כי a_n סדרה הנדסית מעל $\mathbb{Z}/m\mathbb{Z}$ לכל $m \geq 2$.

(6) נמצא כי $(a,b)=(3,5)$ הוא פתרון יחיד של המשוואה $3x+5y=1$ בקבוצה $\{0,1,2,3,4,5\}\times\{0,1,2,3,4,5\}$.

(7) $\mathbb{Z}_{11}$ הוא שדה, ולכן לכל $a\neq 0$ קיים a^{-1} יחיד ב-$\mathbb{Z}_{11}$ כך ש-$a\cdot a^{-1}\equiv 1 \pmod{11}$.

(8) $\mathbb{Z}_6$ אינו שדה, שכן $2\cdot 3=0$ ב-$\mathbb{Z}_6$, למרות ש-$2\neq 0$ ו-$3\neq 0$.

(9) $\mathbb{Z}_{15}$ אינו שדה, שכן $3\cdot 5=0$ ב-$\mathbb{Z}_{15}$, למרות ש-$3\neq 0$ ו-$5\neq 0$.

---

(5) $a\equiv b^{-1} \pmod{\varphi(n)}$ הוא הפתרון היחיד של המשוואה $ax\equiv b \pmod{n}$ בקבוצה $\{0,1,2,\ldots,n-1\}$, כאשר a ו-n זרים זה לזה.

(6) $(a,b)=(3,5)$ הוא הפתרון היחיד של המשוואה $3x+5y=1$ בקבוצה $\{0,1,2,3,4,5\}\times\{0,1,2,3,4,5\}$.

(7) $\mathbb{Z}_{11}$ הוא שדה, ולכן לכל $a\neq 0$ קיים a^{-1} יחיד ב-$\mathbb{Z}_{11}$ כך ש-$a\cdot a^{-1}\equiv 1 \pmod{11}$.

(8) $\mathbb{Z}_6$ אינו שדה, שכן $2\cdot 3=0$ ב-$\mathbb{Z}_6$, למרות ש-$2\neq 0$ ו-$3\neq 0$.

(9) $\mathbb{Z}_{15}$ אינו שדה, שכן $3\cdot 5=0$ ב-$\mathbb{Z}_{15}$, למרות ש-$3\neq 0$ ו-$5\neq 0$.

$\mathbb{Z}_9$ אינו שדה, שכן $3\cdot 3=0$ ב-$\mathbb{Z}_9$, למרות ש-$3\neq 0$.

$\mathbb{Z}_9$ אינו שדה, שכן $3\cdot 3=0$ ב-$\mathbb{Z}_9$, למרות ש-$3\neq 0$.

$$\mathbb{Z}_9=\{0,1,2,3,4,5,6,7,8\}$$

$$\mathbb{Z}_9=\{\underbrace{0,1,2,3,4,5,6,7,8}_{\text{כל האיברים של } \mathbb{Z}_9}\}$$

$$\mathbb{Z}_9=\{\underbrace{0,1,2,3,4,5,6,7,8}_{\text{כל האיברים של } \mathbb{Z}_9}\mid \underbrace{a,b,c,d,e,f,g,h,i}_{\text{כל האיברים של } \mathbb{Z}_9}\}$$

$$\mathbb{Z}_9=\{0,1,2,3,4,5,6,7,8\}$$

$$\mathbb{Z}_9=\{\underbrace{0,1,2,3,4,5,6,7,8}_{\text{כל האיברים של } \mathbb{Z}_9}\}$$

$$\mathbb{Z}_9=\{\underbrace{0,1,2,3,4,5,6,7,8}_{\text{כל האיברים של } \mathbb{Z}_9}\mid \underbrace{a,b,c,d,e,f,g,h,i}_{\text{כל האיברים של } \mathbb{Z}_9}\}$$

(א) כמה מספרים שונים יש בקבוצה $\{1,2,3,\dots,1000\}$ שמתחלקים ב-3 או ב-5?

(ב) כמה מספרים שונים יש בקבוצה $\{1,2,3,\dots,1000\}$ שמתחלקים ב-3 אבל לא ב-5?

(ג) כמה מספרים שונים יש בקבוצה $\{1,2,3,\dots,1000\}$ שמתחלקים ב-3 או ב-5 אבל לא בשניהם?

(ד) $\{1,2,3,\dots,1000\}$ מתוך הקבוצה $\frac{1}{3}$ כמה מספרים יש בקבוצה $\frac{1}{5}$ אבל לא $\frac{1}{15}$?

(ה) $\{1,2,3,\dots,1000\}$ מתוך הקבוצה $\frac{1}{3}$ כמה מספרים יש בקבוצה $\frac{1}{5}$ אבל לא $\frac{1}{15}$?

(15) מספרים טבעיים שאינם מתחלקים לא ב-3 ולא ב-5 נקראים מספרים טובים.

$X = \{1,2,3,\dots,1000\}$ מתוך A.

$A = \{x \in X \mid x \text{ מתחלק ב-3}\}$: תזכורת

$B = \{x \in X \mid x \text{ מתחלק ב-5}\}$.

$P(A \cup B)$ מהי העוצמה של

$|A| = 333$, $|B| = 200$.

$|A \cap B| = 66$.

1	2	3	4
5	6	7	8

(א) $|A \cup B| = 333 + 200 - 66 = 467$

$|A| = 333$, $|B| = 200$

1	2	3	4
5	6	7	8

(ב) $|A \setminus B| = 333 - 66 = 267$

(ג) $|A \triangle B| = 333 + 200 - 2 \cdot 66 = 401$.

(ד) $|A \setminus B| = 267$ מתוך $|A| = 333$

$\frac{267}{333}$ מתוך $\frac{1}{3}$

(ה) $|A \setminus B| = 267$ מתוך $|X| = 1000$

$\frac{267}{1000}$ מתוך $\frac{1}{5}$

$$r_0 = A = 2390 \qquad r_1 = B = 47$$
$$s_0 = 1 \qquad s_1 = 0$$
$$t_0 = 0 \qquad t_1 = 1$$

$$r_{k+1} = r_{k-1} - q_k r_k$$
$$s_{k+1} = s_{k-1} - q_k s_k$$
$$t_{k+1} = t_{k-1} - q_k t_k$$

$r_2 = r_0 - q_1 r_1$
$= 2390 - (50)47$
$= 18$

$s_2 = s_0 - q_1 s_1$
$= 1 - q_1 \cdot 0$
$= 1$

$t_2 = t_0 - q_1 t_1$
$= 0 - (50)(1)$
$= -50$

$k=1$
$q_1 = 50$

משפט (קיום הופכי כפלי מודולו n)
יהי n טבעי ו-$\phi(n)$ פונקציית אוילר. אם a ו-n זרים, אז a הפיך מודולו n, כלומר קיים b כך ש-$ab \equiv 1 \pmod{n}$.

הוכחה: נסמן $b = a^{\phi(n)-1} \bmod n$. אז $ab = a^{\phi(n)} \bmod n$. לפי משפט אוילר, $a^{\phi(n)} \equiv 1 \pmod{n}$, ולכן $ab \equiv 1 \pmod{n}$. $\square$

דוגמה: נמצא את ההופכי של 47 מודולו 2390.

$\phi(2390) = \phi(2 \cdot 5 \cdot 239) = (2-1)(5-1)(239-1) = 1 \cdot 4 \cdot 238 = 952$

$47^{952} \bmod 2390 = 1$ (ניתן לחשב בקלות בעזרת חזקות מהירות).

לכן $47^{951} \bmod 2390$ הוא ההופכי של 47 מודולו 2390.

$47^{951} \bmod 2390 = 1033$

בדיקה: $47 \cdot 1033 = 48551 = 20 \cdot 2390 + 1 \equiv 1 \pmod{2390}$. $\checkmark$

דוגמה: נמצא את ההופכי של 7 מודולו 26.

$\phi(26) = \phi(2 \cdot 13) = (2-1)(13-1) = 12$

$7^{12} \bmod 26 = 1$

לכן $7^{11} \bmod 26$ הוא ההופכי של 7 מודולו 26.

$7^{11} \bmod 26 = 15$

בדיקה: $7 \cdot 15 = 105 = 4 \cdot 26 + 1 \equiv 1 \pmod{26}$. $\checkmark$

משפט (קיום הופכי כפלי מודולו p)
יהי p ראשוני ו-a טבעי. אם a ו-p זרים, אז a הפיך מודולו p, כלומר קיים b כך ש-$ab \equiv 1 \pmod{p}$.

הוכחה: נסמן $b = a^{p-2} \bmod p$. אז $ab = a^{p-1} \bmod p$. לפי משפט פרמה הקטן, $a^{p-1} \equiv 1 \pmod{p}$, ולכן $ab \equiv 1 \pmod{p}$. $\square$

דוגמה: נמצא את ההופכי של 47 מודולו 2389.

$47^{2389} \bmod 2389 = 1$

לכן $47^{2388} \bmod 2389$ הוא ההופכי של 47 מודולו 2389.

$47^{2388} \bmod 2389 = 1033$

בדיקה: $47 \cdot 1033 = 48551 = 20 \cdot 2389 + 1 \equiv 1 \pmod{2389}$. $\checkmark$

דוגמה: נמצא את ההופכי של 7 מודולו 13.

$7^{12} \bmod 13 = 1$

לכן $7^{11} \bmod 13$ הוא ההופכי של 7 מודולו 13.

$7^{11} \bmod 13 = 2$

בדיקה: $7 \cdot 2 = 14 = 1 \cdot 13 + 1 \equiv 1 \pmod{13}$. $\checkmark$

$r_3 = r_1 - q_2 r_2$

$= 47 - 2 \cdot 17$

$= 13$

$s_3 = s_1 - q_2 s_2$

$= 0 - 2 \cdot (1)$

$= -2$

$t_3 = t_1 - q_2 t_2$

$= 1 - 2(-509)$

$= 1019$

$k = 2$

$q_2 = 2$

$r_4 = r_2 - q_3 r_3$

$= 17 - (1)13$

$= 4$

$s_4 = s_2 - q_3 s_3$

$= 1 - 1(-2)$

$= 3$

$t_4 = t_2 - q_3 t_3$

$= -509 - 1(1019)$

$= -1528$

$q_3 = 1$

$r_5 = r_3 - q_4 r_4$

$= 13 - 3(4)$

$= 1$

$s_5 = s_3 - q_4 s_4$

$= -2 - 3(3)$

$= -11$

$t_5 = t_3 - q_4 t_4$

$= 1019 - 3(-1528)$

$= 5603$

$q_4 = 3$

$r_6 = r_4 - q_5 r_5$

$= 4 - (4) \cdot 1$

$= 0$

23940 ↓ 47 ↙

$sA + tB = d = \gcd(A, B)$

$s = s_5 = -11$

$t = t_5 = 5603$

$d = r_5 = 1$

$q_5 = 4$

$-11(23940) + 5603(47) = 1$

משפט ההופכיים המודולריים:

$sA + tB = 1$	אם
$A^{-1} \equiv s \bmod B$	אז
$B^{-1} \equiv t \bmod A$	

משפט ההופכיים מודולריים

$$-11(23940) + 5603(47) = 1 \Longrightarrow \begin{cases} 47^{-1} \equiv 5603 \bmod 23940 \\ 23940^{-1} \equiv -11 \bmod 47 \equiv 36 \bmod 47 \end{cases}$$

לכן $a = b^{-1} \bmod \phi(n) = 47^{-1} \bmod 23940 = 5603.$

מכאן והתאכה. סודית למתמה והסודי הינה $(a=5603, p=127, q=191)$

והמפתח ציבורי (אשר כל אחד יודע) $(b=47, n=pq=24257)$

סעיף ב) אליס מצפינה את ההודעה לבוב

באמצעות ולכן מצפין עם

המפתח הציבורי:

נ"ל כי $p \equiv 5 \pmod 8$ אז 2 הוא שארית ריבועית מודולו p.

$$q^7 = 32 + 8 + q + 2 + 1$$

$$2q^6 \equiv 2q^5 7 \pmod{2q^6 8}$$

$$(2q^6 8)^2 \equiv 2q^5 7 \pmod{2q^6 8}$$

$$(2q^6 8)^4 \equiv 1 \pmod{(2q^6 8)^2}$$

$$= (2q^6 8)^2 \equiv 1 \pmod{2q^5 7}$$

$$= q^2 12$$

2 היא שארית ריבועית מודולו p אם ורק אם $p \equiv 1$ או $p \equiv 7 \pmod 8$.

$$X = 2q^6 8 \text{ ו-} 1$$

$$X^b \equiv 1 \pmod n$$

$$b = q^7 \cdot \quad n = 2q^2 5 7.$$

$$X \equiv 1 \pmod n$$

$$2q^6 8 \equiv 1 \pmod{2q^2 5 7}$$

$$(2468)^8 \bmod n = \left((2468)^4\right)^2 \bmod n$$

$$= (4212)^2 \bmod 24257$$

$$= 9077$$

$$(2468)^{16} \bmod n = \left((2468)^8\right)^2 \bmod n$$

$$= (9077)^2 \bmod n$$

$$= 15157$$

$$(2468)^{32} \bmod n = \left((2468)^{16}\right)^2 \bmod n$$

$$= (15157)^2 \bmod 24257$$

$$= 20859$$

$$(2468)^{47} = (2468)^{32}\,(2468)^{8}\,(2468)^{4}\,(2468)^{2}\,(2468) \bmod n$$

$$= (20859)(9077)(4212)(2514)(2468) \bmod 24257$$

$$= 10642 \bmod 24257$$

$$\therefore y = 10642.$$

$$X \equiv X_2 \bmod q \qquad X \equiv X_1 \bmod p$$

משפט השאריות הסיני

$$X_2 = \left[(Y \bmod q)^{a \bmod (q-1)} \right] \bmod q$$

$$a \bmod (q-1)$$

$$Y \bmod q$$

$$X_1 = \left[(Y \bmod p)^{a \bmod (p-1)} \right] \bmod p$$

$$a \bmod (p-1)$$

$$Y \bmod p$$

משפט פרמה הקטן: p ראשוני ו-a זר ל-p אז $a^{p-1} \equiv 1 \pmod p$

משפט אוילר: a זר ל-n אז $a^{\varphi(n)} \equiv 1 \pmod n$

$\varphi(n)$ = מספר המספרים הטבעיים הקטנים מ-n וזרים ל-n

$\varphi(p) = p-1$ עבור p ראשוני

$\varphi(pq) = (p-1)(q-1)$ עבור p, q ראשוניים

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

$\varphi(ab) = \varphi(a)\varphi(b)$ אם a, b זרים

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

$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 1000 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$

$\varphi(1001) = \varphi(7 \cdot 11 \cdot 13) = 6 \cdot 10 \cdot 12 = 720$

$\varphi(p) = p - 1$ עבור p ראשוני

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

$\varphi(ab) = \varphi(a)\varphi(b)$ אם a, b זרים

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

$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 1000 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$

$\varphi(1001) = \varphi(7 \cdot 11 \cdot 13) = 6 \cdot 10 \cdot 12 = 720$

$X = 2468.$

$Y = 10642$, $q = 1009$ (ראשוני), $p = 1013$ (ראשוני), $N = pq = 1022117$

$\varphi(N) = (p-1)(q-1) = 1020096$

$e = 17$ (זר ל-$\varphi(N)$)

$d = e^{-1} \bmod \varphi(N) = 960113$

$C = X^e \bmod N = 2468^{17} \bmod 1022117 = 1018852$

$X_1 = C^{d \bmod (p-1)} \bmod p = 1018852^{113} \bmod 1013 = 2468$

$X_2 = C^{d \bmod (q-1)} \bmod q = 1018852^{881} \bmod 1009 = 2468$

$X = 2468$ (לפי משפט השאריות הסיני)

$X_1 = (y \bmod p) \bmod p$

(Find $59^{13} \bmod 127$)

$y \bmod p = 106^{42} \bmod 127 = 101$

$\alpha \bmod (p-1) = 5603 \bmod 126 = 59$

$y \bmod q = 106^{42} \bmod 191 = 137$

$\alpha \bmod (q-1) = 5603 \bmod 190 = 93$

$X_2 = (y \bmod q) \bmod q$

$= 137^{93} \bmod 191$

$= (137)^{64} (137)^{16} (137)^{8} (137)^{4} (137)^{1} \bmod 191$

$= 176$

$= (101)^{32} (101)^{16} (101)^{8} (101)^{2} (101)^{1} \bmod 127$

$= 55$

Find $K = 55^{59} \bmod 191$

$$= 2468$$

$$= \left((55)(2)(191) + (176)(881)(121) \right) \bmod 24257$$

$$X = \left(a_1 y_1 M_1 + a_2 y_2 M_2 \right) \bmod M$$

$$y_2 = M_2^{-1} \bmod m_2 = 127^{-1} \bmod 191 = 1881$$

$$y_1 = M_1^{-1} \bmod m_1 = 191^{-1} \bmod 127 = 2$$

$$M_1 = \frac{M}{m_1} = 191 \qquad M_2 = \frac{M}{m_2} = 127$$

$$M = m_1 m_2 = 24257$$

$$m_2 = 191 \quad , m_1 = 127 \quad , a_2 = 176 \quad , a_1 = 55$$

$$\begin{cases} X = 55 \bmod 127 \\ X = 176 \bmod 191 \end{cases}$$

משפט השאריות הסיני:

$$X = x_1 \bmod p$$

$$X = x_2 \bmod q$$

$$\gcd(p, q) = 1$$

RSA التشفير باستخدام

مثال: لنفرض أن $p=7$ و $q=11$ عددان أوليان.

$$n = p \cdot q = 77$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 60$$

(حيث ϕ هي دالة أويلر)

نختار e بحيث $1 < e < \phi(n)$ و e و $\phi(n)$ أوليان فيما بينهما.

لنختر $e = 13$

نحسب d بحيث $de \equiv 1 \pmod{\phi(n)}$

$$de = k\phi(n) + 1 \Rightarrow de = k(p-1)(q-1) + 1$$

$$\Rightarrow de - 1 = k(p-1)(q-1)$$

$$de - 1 = X^{k(p-1)(q-1)} = X^{\phi(n)}$$

$$d_k(e_k(x)) = x \pmod{n}$$

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

$$d_k(y) = y^d \pmod{n}$$

$$de = 1 \pmod{\phi(n)}$$

$$n = p \cdot q$$

حيث (p, e) هو المفتاح العام

$$de \equiv 1 \pmod{\phi(n)}$$

حيث d هو المفتاح الخاص

$$de = k\phi(n) + 1 \Rightarrow de = k(p-1)(q-1) + 1$$

$$\Rightarrow de - 1 = k(p-1)(q-1)$$

$$de - 1 = X^{k(p-1)(q-1)} = X$$

$$X^{ab-1} \equiv 1 \bmod 17 \Leftarrow$$

$$X^{ab-1} \equiv 1 \bmod pq \Leftarrow$$

$$X^{ab-1} - 1 = \Gamma pq \Rightarrow X^{ab-1} = 1 + \Gamma pq$$

$$\text{-e } ?^{\text{?}} \Gamma \text{ ?de } \exists \text{ ?}^{5}$$

$$pq \mid (X^{ab-1} - 1) \qquad \text{?}^{5} \text{ ?.?ieve ?.?oN pq}$$

$$X^{ab-1} - 1 = sq \Rightarrow q \mid (X^{ab-1} - 1)$$

$$X^{ab-1} - 1 = tp \Rightarrow p \mid (X^{ab-1} - 1)$$

$$X^{ab-1} = \left(X^{t(q-1)}\right)^{q-1} \equiv 1 \bmod q \Rightarrow X^{ab-1} - 1 \equiv 0 \bmod q$$

$$X^{ab-1} = \left(X^{t(q-1)}\right)^{p-1} \equiv 1 \bmod p \Rightarrow X^{ab-1} - 1 \equiv 0 \bmod p$$

.?ieve ? ?de $a^{p-1} \equiv 1 \bmod p$?ni? e ?n? ?oeN ?

$$\text{?ne?i?i ?ni?e ?.?? 2 -? } X^{t(p-1)(q-1)} \text{ ?e ?? ?}^{\text{?}}$$

$$\Rightarrow \quad \rho^{21} \left(e_2(x) \right) \equiv x \,.$$

$$\Leftarrow \quad \left(e_2(x) \right)^2 \bmod n \equiv x$$

$$\Rightarrow \quad \left(e_2(x) \right)^\alpha \equiv x \bmod n$$

$$\left(x^b \bmod n \right)^\alpha \equiv x \bmod n$$

ρd | כלומר $\left(x^b \right)^\alpha \equiv x \bmod n$ וכ"ש

$x^{ab} \equiv x \bmod n$ - ב לפחות אחד $x - a$ לפי הנחה ו) וזה בדיוק מה שצריך