3-2-25

קריפטוגרפיה (המשך)

סעיף כג יהיו a,b שלמים.

הוכיחו: $\frac{a}{gcd(a,b)}$ ו- $\frac{b}{gcd(a,b)}$ זרים.

נזכור לפי משפט אוקלידס לכל a,b שלמים $\exists$ שלמים s,t,d:

$$sa+tb=d=gcd(a,b) \text{ ——— } (*)$$

$gcd(a,b)$ הוא שלם, ובגלל שהוא ה-gcd של שני שלמים אז הוא שונה מ-0. לכן נחלק את $(*)$ ב-$gcd(a,b)$:

$$\frac{sa}{gcd(a,b)}+\frac{tb}{gcd(a,b)}=1 \text{ ——— } (\#)$$

$$\Longrightarrow s\left(\frac{a}{gcd(a,b)}\right)+t\left(\frac{b}{gcd(a,b)}\right)=1$$

לכן, בגלל שלפי משפט אוקלידס, והשלם 1 [illegible] מינ' הוא ה-gcd של $\frac{a}{gcd(a,b)}$ ו- $\frac{b}{gcd(a,b)}$, אז

$$gcd\left(\frac{a}{gcd(a,b)},\frac{b}{gcd(a,b)}\right)=1$$

מש"ל.

הוכחה: a,b שלמים לכן $\exists$ שלמים s,t,d

$$sa+tb=d=gcd(a,b)$$

$d\neq 0$ שלם. נחלק ב-d:

$$s\left(\frac{a}{d}\right)+t\left(\frac{b}{d}\right)=1$$

כנ"ל, הוכחנו, ובגלל שה-1 [illegible] מינ' [illegible] שלם, ובגלל ש-s ו-t שלמים, אז $\frac{a}{d}$ ו- $\frac{b}{d}$ הם שלמים.

__סעיף 3)__ אם $c|ab$ ואם c-b זרים אז $c|a$.

__נתון:__ $c|ab \Leftarrow \exists$ שלם q כך ש- $ab=cq$.

c-b זרים $\Leftarrow c\nmid b$.

__צריך להוכיח:__ $c|a$.

__הוכחה:__ $c|ab \Leftarrow \exists$ שלם q כך ש- $ab=cq$

$\Leftarrow$ $q=\frac{ab}{c}$.

q שלם, לכן $\frac{ab}{c}$ שלם.

ז"א $\frac{a}{c}$ שלם או $\frac{b}{c}$ שלם.

נתון ש- $c\nmid b$, ז"א $\frac{b}{c}$ לא שלם.

לכן $\frac{a}{c}$ שלם.

לכן $c|a$.

מש"ל.

<u>תרגיל:</u> יהיו a,m שלמים זרים. הוכיחו:

$ab\equiv ac \mod m$ אם"ם $b\equiv c \mod m$.

<u>הוכחה</u>

<u>$\Leftarrow$</u>

נניח כי $ab\equiv ac \mod m$.

ע"כ $\exists$ שלם q כך ש-

$$ab=ac+qm \Rightarrow \underbrace{a(b-c)=qm}_{(*)} \Longrightarrow a\mid qm.$$

נתון ש- a,m שלמים זרים $\Leftarrow a\nmid m$

אזי בהכרח $a\mid q \Leftarrow \exists$ שלם k כך ש- $q=ak$.

נציב זאת ב-(*):

$$a(b-c)=akm$$

$$\Longrightarrow b-c=km$$

$$\Longrightarrow b=km+c$$

$$\Longrightarrow b\equiv c \mod m.$$

<u>$\Longrightarrow$</u>

נניח כי $b\equiv c \mod m$. ו- a,m זרים.

נוכיח ש- $ab\equiv ac \mod m$.

$b \equiv c \bmod m$ אז $\exists$ שלם q כך ש-

$$b = qm + c \quad \Rightarrow \quad ab = aqm + ac$$

$$\Rightarrow ab = Qm + ac$$

לכן $\exists$ שלם $Q(=aq)$ כך ש- $ab = Qm + ac$

אז $ab \equiv ac \bmod m$.

<u>תרגיל</u>: יהי p ראשוני ו- n שלם חיובי. הוכיחו:

אם $p | n$ אז $\phi(pn) = p\phi(n)$

(כלומר p מחלק את n)

פתרון

$p | n$. לכן הראשוני p מופיע בפירוק לראשוניים של n:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{———} \quad (*1)$$

$$pn = \underbrace{p \cdot p_1^{e_1}}_{p_1^{e_1+1}} p_2^{e_2} \cdots p_k^{e_k}$$

לכן, הפירוק לראשוניים של השלם np הוא:

$$np = p_1^{e_1+1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{———} \quad (*2)$$

.

הוכחה:

$$n = p_1^{e_1}\cdots p_k^{e_k} \Longrightarrow \phi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)$$

$(*1) \Longleftarrow$

$$\phi(n) = \left(p^{e_1} - p^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)$$

$(*2) \Longleftarrow$

$$\phi(np) = \underbrace{\left(p^{e_1+1} - p^{e_1}\right)}_{\text{הוצאת גורם משותף } p}\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)$$

$$= p\left(p^{e_1} - p^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)$$

$$= p\cdot\phi(n).$$

מש"ל.

תרגיל: יהיו p ראשוני ו- n טבעי כלשהו. הוכיחו:

אם $p \nmid n$ אז $\phi(pn) = (p-1)\phi(n)$

פתרון: $p\nmid n$ ו- p ראשוני לכן p,n זרים
לכן $\phi(pn)=(p-1)\phi(n)$.

תרגיל: נתון כלל מצפין $e_K(x)=xK$ של צופן היל כאשר $x\in\mathbb{Z}_{26}^{n}$ ו- $K\in\mathbb{Z}_{26}^{n\times n}$.

הוכיחו:
אם $gcd(|K|,26)=1$ אז קיים כלל מפענח.

אם ה-gcd של הדטרמיננטה של K עם 26 שווה 1

פתרון. הכלל מפענח של צופן היל הוא:

$$d_K(y)=yK^{-1} \bmod 26$$

כאשר $y\in\mathbb{Z}_{26}^{n}$ טקסט מוצפן ו- K^{-1} המטריצה ההופכית של K שנמצאת ע"י נוסחת קרמר:

$$K^{-1} \overset{\text{נוסחאות}}{=} |K|^{-1}C^{t} \bmod 26$$

כאשר C המטריצה של הקופקטורים ו- $|K|^{-1}$ ההופכי של הדטרמיננטה של K.

$\exists$ ההופכי של $|K|$ אם ורק אם $gcd(|K|,26)=1$.
$\Leftarrow$ $\exists$ המטריצה ההופכית K^{-1} אם"ם $gcd(|K|,26)=1$

לכן הכלל מפענח קיים אם"ם $\gcd(|k|,26)=1$.
מש"ל.

<u>תרגיל:</u>

הוכיחו כי כלל מצפין וכלל מפענח של RSA הן
פונקציות הופכיות.

<u>פתרון:</u>

<u>נתון:</u> לפי דף הנוסחאות, צופן RSA הוא:

$$\left.\begin{array}{ll} \text{כלל מצפין:} & e_k(x)=x^b \bmod n \\ \text{כלל מפענח:} & d_k(y)=y^a \bmod n \end{array}\right\} \quad \begin{array}{l} n=pq \\ ab\equiv 1 \bmod \phi(n) \end{array}$$

מפתח: $k=(p,q,a,b)$

p,q ראשוניים, ו- a,b שלמים.

<u>צ"ל להוכיח:</u> $d_k(e_k(x))=x \bmod n$

כלומר, אנו רוצים להראות ש-

$$(x^b)^a \bmod n \equiv x \bmod n \qquad (*)$$

<u>הוכחה:</u> $n=pq$ ו- p,q שלמים לכן

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

נתון כי $ab\equiv 1 \bmod \phi(n)$

נתון ב- RSA ש- $ab\equiv 1 \bmod \phi(n)$
ו: $\phi(n)=\phi(pq)=(p-1)(q-1)$.

לכן $ab\equiv 1 \bmod (p-1)(q-1) \Longrightarrow ab=t(p-1)(q-1)+1$

כאשר t שלם.

$\Longrightarrow ab-1=t(p-1)(q-1)$

ג״א

$$ab \equiv 1 \bmod (p-1)(q-1)$$

$$\Rightarrow \quad ab = t(p-1)(q-1) + 1$$

$$\Rightarrow \quad ab-1 = t(p-1)(q-1).$$

$$\Rightarrow \quad x^{ab-1} = x^{t(p-1)(q-1)} \qquad \text{———} (\#)$$

משפט פרמה: לכל y שזר ל p ראשוני $y^{p-1} \equiv 1 \bmod p$

$$x^{ab-1} = \left(x^{t(p-1)}\right)^{(q-1)} \overset{\text{פרמה}}{\equiv} 1 \bmod q$$

$$x^{ab-1} = \left(x^{t(q-1)}\right)^{(p-1)} \overset{\text{פרמה}}{\equiv} 1 \bmod p$$

$$x^{ab-1} \equiv 1 \bmod pq \Longleftarrow \begin{cases} x^{ab-1} \equiv 1 \bmod p \\ x^{ab-1} \equiv 1 \bmod q \end{cases} \text{ אז}$$

לכל y שזר לראשוניים p-q.

$$y \equiv 1 \bmod pq \Longleftarrow \begin{cases} y \equiv 1 \bmod p \\ y \equiv 1 \bmod q \end{cases} \text{ אז}$$

מציבים $n=pq$ ואז נקבל ש-

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

נכפיל ב-x, ולפי כלל הכפל של מודולים:

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

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

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

לפי הכלל,

$$Z \bmod m \equiv Y \Longleftrightarrow Y \bmod m \equiv Z \bmod m \Longleftrightarrow Y \equiv Z \bmod m$$

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

$$\Rightarrow d_k(x^b) \equiv x \bmod n$$

$$\Rightarrow d_k(e_k(x)) \equiv x \bmod n.$$

מש"ל.

<u>הגדרה</u>: צופן אלגמל ניתן לפענוח.

<u>פתרון</u>: <u>נתון</u>:

כלל הצפנה: (עפ מפתח ציבורי)

$$e_k(x) = (y_1, y_2), \quad y_1 = \alpha^d \bmod p \quad y_2 = \beta^d x \bmod p$$

כלל פענוח: (עפ מפתח פרטי)

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

p ראשוני, α, a, d שלמים.

<u>צריך להוכיח</u>: e_k ו- d_k פונקציות הופכיות.

$$d_k(e_k(x)) = x \bmod p$$

<u>הוכחה</u>: $e_k(x) = (y_1, y_2)$ כאשר

$$y_1 = \alpha^d \bmod p \qquad y_2 = x\beta^d \bmod p$$

לכן,

$$d_k(e_k(x)) = (y_1^a)^{-1} y_2 \bmod p$$

$$= \left((\alpha^d \bmod p)^a \right)^{-1} \left(x\beta^d \bmod p \right) \bmod p$$

$$= \left(\left(\alpha^{da} \bmod p \right)^{-1} \left(x \beta^{d} \bmod p \right) \right) \bmod p$$

לפי המשפט:

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

נקבל

$$= \left(\left(\alpha^{da} \right)^{-1} \bmod p \right) \left(x \beta^{d} \bmod p \right) \bmod p$$

לפי המשפט:

$$(a \bmod m)(b \bmod m) = ab \bmod m$$

(הוכחנו בתרגיל של 16-1)

$$= \left(\alpha^{da} \right)^{-1} x \beta^{d} \bmod p .$$

בסוף, כיוון $\beta = \alpha^{a} \bmod p$ אז נקבל

$$d_k(e_k(x)) = \left(\alpha^{da} \right)^{-1} x \left(\alpha^{a} \bmod p \right)^{d} \bmod p$$

$$= \left(\alpha^{da} \right)^{-1} x \, \alpha^{ad} \bmod p$$

$$= x \bmod p$$

מש"ל.