

תוחם 16

טענה: $x \leq p < 2x$ \exists p ק \exists $N > x$ מספר של p בין x ל- $2x$

הוכחה: מספר של p בין x ל- $2x$ הוא $\pi(2x) - \pi(x)$

נראה כי קיים $N > x$: $\pi(2x) - \pi(x) > 0$

$$\left(\frac{\pi(2x)}{\pi(x)} - 1 \right) \pi(x) > 0$$

$$\frac{\pi(2x)}{\pi(x)} - 1 > \frac{1}{100}$$

מספר זכרון שזכור $x > N$

$$\lim_{x \rightarrow \infty} \frac{\pi(2x)}{\pi(x)} = 2$$

וכי כן

$$\lim_{x \rightarrow \infty} \frac{\pi(2x)}{\pi(x)} = \lim_{x \rightarrow \infty} \frac{\frac{\pi(2x)}{2x / \log 2x}}{\frac{\pi(x)}{x / \log x}} = \lim_{x \rightarrow \infty} \frac{2x / \log 2x}{x / \log x} = \lim_{x \rightarrow \infty} \frac{2 \log x}{\log 2x} = 2$$

(זמן Prime Number Theory)

סיכומים

טענה: נניח כי יבנה $n = pq$, p, q ראשוניים. אז נצטא $q-1$ כי n סדר

השקנה נצטא $\psi(n)$

המספר מהיחוד זמן הנח ψ הישירים בזמן פונקציונלי.

$$\psi(n) = \frac{n}{2} - 1$$

הוכחה: אם n זוגי כח $q = \frac{n}{2}$, $p = 2$

$$\psi(n) = (p-1)(q-1) = \frac{n}{2} - 1 - (p+q)$$

נניח n אי זוגי. אם יוצרים p, q אז

$$n - \psi(n) + 1 = p + q$$

$$pq = n$$

כיוון שני: אם אנו יוצרים $\psi(n)$ אז

אם $p+q = 2b$ אז p, q הישירים

$$x^2 - 2bx + n = 0$$

$$x = b \pm \sqrt{b^2 - n}$$

הישירים הישירים $(\log n)^3$ [השיעור בית]

מערכות הצפנה פשוטות

Bob
מקבל
Ciphertext

Cathrine

Alice
שולח
Plaintext

$$f: \mathcal{P} \rightarrow \mathcal{C}$$

plaintext ciphertext

טרנספורמציה הצפנה

$$f^{-1}: \mathcal{C} \rightarrow \mathcal{P}$$

f חזרה ויש טרנספורמציה פועלה

צטא

OMG ← זו היא נעמה (הצפנה) של יוליוס קיסר

$$f(p) = p + 3 \pmod{26}$$

{ A - Z }
f { 0 - 25 }

האותיות
(קוד 33)

$$f(p) = p + b \pmod{N}$$

יותר כפי N איותות, $b \in \mathbb{Z}/N/\mathbb{Z}$

$$f^{-1}(c) = c - b \pmod{N}$$

אלו יוצרים קיסר $N=26, b=3$

כמון ב - מפתח הצפנה
הקודם לזה של ב - מפתח הפענוח

k איותות האלפביתיות N איותות: $b \in (\mathbb{Z}/N\mathbb{Z})^k, p \in (\mathbb{Z}/N\mathbb{Z})^k$

$$C = AP + b \quad f \in \text{Mat}_k(\mathbb{Z}/N\mathbb{Z}) \text{ הפניה טרנספורמציה הצפנה תהיה:}$$

$$P = A^{-1}(C - b) = A^{-1}C - A^{-1}b$$

הקודם של כולל את מפתח הצפנה יוצר את מפתח הפענוח

RSA - ציפוף אנטי סימטרי
Ron Rivest, Adi Shamir, Leonard Adleman

בחרים שני ראשוניים שונים p, q (כמון) $n = pq$

כאשר $n = pq$ מנסים את $\phi(n)$ כמון p, q שונים

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

A מוחמ p, q תבולות, e_A - מספר $(p-1)(q-1)$

$$d_A := e_A^{-1} \pmod{\phi(n)} \quad n_A = p_A \cdot q_A$$

$$d_A \cdot e_A \equiv 1 \pmod{\phi(n)}$$

היא מפרמט את מפתח הצפנה $(n_A, e_A) = KE_A$ ומפתח את

מפתח הפענוח $(n_A, d_A) = KP_A$

$$f: \mathbb{Z}/n_A\mathbb{Z} \rightarrow \mathbb{Z}/n_A\mathbb{Z}$$

$$f(p) = p^{e_A} \pmod{n_A}$$

$$f^{-1}: \mathbb{Z}/n_A\mathbb{Z} \rightarrow \mathbb{Z}/n_A\mathbb{Z}$$

$$f^{-1}(c) = c^{d_A} \pmod{n_A}$$

$$(f^{-1} \circ f)(p) = p \pmod{n_A}$$

נבדוק שאכן f^{-1}

$$d_A e_A = k \cdot \phi(n_A) + 1$$

$$d_A e_A = 1 \pmod{\phi(n_A)}$$

$$p^{d_A e_A} = p^{(k \cdot \phi(n_A) + 1)} \equiv p \pmod{n_A}$$

כלומר p - מספר ראשוני

$$f^{-1} \circ f(x) = x$$

$$O((\log n_A)^3)$$

כמון חישובי - RSA

אלו p_A, q_A

הוכחת תוצאה 16

Primality testing

לבחון ראשוניות:

n גודל איזוס.

מבחן טולטון: בודקים אם מתחלק בטולטונים עד \sqrt{n} .

מטו, חיבה של $\frac{1}{2} \log n = e^{\frac{1}{2} \log n} \leftarrow$ אקספוננציאלי ב- $\log n$.

מבחן פולני: אם n טולטון אז כל b קטן ל- $\gcd(b, n) = 1$ מתקיים $b^{n-1} \equiv 1 \pmod{n}$.
אם $b^{n-1} \not\equiv 1 \pmod{n}$, אז n אינו ראשוני. (הוא עדיין ראשוני אם $b^{n-1} \equiv 1 \pmod{n}$, אז n ראשוני או Carmichael).

הצורה: מספר אי-הוא מספר Carmichael אם כל $a < n$ נכבד $a^{n-1} \equiv 1 \pmod{n}$.

דוגמה: $561 = 3 \cdot 11 \cdot 17$

טענה: אם a זוגי הוא אינו קרטיקל.

אם a מתחלק בריבוע, הוא אינו מס' קרטיקל.

אם a לא מתחלק בריבוע, אז a הוא מס' קרטיקל $\Leftrightarrow (a-1) | (n-1)$ כל n.

אם a הוא מס' קרטיקל אז הוא מרשה שיותר מ-2 טולטונים.

$b^{n-1} = (-1)^{n-1} = -1 \not\equiv 1 \pmod{n}$ (אם n אי-זוגי)

הוכחה: ניה n זוגי. נוק. ק. $b = -1$.

אם -1 הוא עפ' ל-2 אינו קרטיקל. \checkmark

אם לא