Szerkesztette :
Sándor András

Titkosírás

Biztos, hogy titkos?

Szabó István előadása

Az életben sok helyen használunk titkosítást (mobil, internet, jelszavak...)

Története

Az ókortól kezdve rengeteg feltört titkosírás létezik.

Monoalfabetikus helyettesítés

Helyettesítő tábla, minden betűhöz egy jelet rendel.
Elvileg 26! féle lehetőség, de gyakorlatilag sokkal könnyebben feltörhető.
Hibája: átörökíti a nyelv gyakoriságait.

Polialfabetikus helyettesítés

Minden betűnél más számmal toljuk el az abc-t.
Ehhez kell egy kulcsszó, ami tartalmazza azt, hogy mikor mennyivel.
Ezt mindkettőnek ismernie kell.
Hibája: rövid a periódusa (a jelszó hossza), ha arra rájöttünk, akkor ismét lehet nézni a gyakoriságokat

Az előadó ezután bemutatott egy kis gépet, amelyet a II. VH-ban használt a magyar hadsereg
Hibája: egyenetlen a kulcs

One-time-pad kulcs

Véletlenszerű
Egyenletes
Egy kulcsot csak egyszer használnak

Közös hibája ezeknek a kulcsoknak: az adó és a vevő oldalnak előre meg kell egyeznie a titkos kulcsban
Ez az internet korában nem kielégítő

Ez a probléma 1976-ban merült fel mint a nyilvános kulcsú titkosítás problémája
(W. Diffie – M. E. Hellman)

Nyilvános kulcsú titkosítás

1978 – több megoldás is van.
Egyik: RSA (Rivest – Shamir – Adleman)

Felhasználja:
a kongruencia fogalmát (bevezette: Christian Goldbach 1730, elméletét kidolgozta: C.F. Gauss 1801)

Fermat-tétel:
Ha $(p, a) = 1$ és p prím, akkor $a^p - 1 \equiv 1 \mod p$.

Euler-tétel (általánosítás):
Ha $(a, n) = 1$, akkor $a^{\varphi(n)} \equiv 1 \mod n$.

Megjegyzés a továbbiakhoz:
Ha $n = pq$, akkor $\phi(n) = (p - 1)(q - 1)$.

RSA módszer (ha **A** azt akarja, hogy akárki tudjon titkosan üzenni neki)

1. **A** választ két nagy prímet, ezeket jelölje p és q.

2. **A** kiszámolja $n = pq$ értékét.

3. **A** választ egy e számot, amely relatív prím $\phi(n)$-hez.

4. **A** kiszámolja, hogy melyik d szám(ok)ra igaz, hogy $ed \equiv 1 \mod \phi(n)$.

Ekkor:
e és n a nyilvános kulcsa,
p, q és d rejtve marad (d a titkos magán kulcsa).

Most következik az m üzenet kódolása (amit elküldünk **A**-nak):

1. m-et bontsuk fel $m_1, \ldots, m_k$ részekre úgy, hogy minden m_i kisebb (rövidebb) legyen n-nél.

2. Ezekből elkészítjük a rejtjeles blokkokat: $c_i \equiv (m_i)^e \mod n$.

3. Elküldjük az ezekből képzett üzeneteket.

A fogadó (**A**) dekódolása:

$$(c_i)d \equiv (m_i)ed = (m_i)^{1+k\phi(n)} = m_i (m_i^{\phi(n)})^k \equiv m_i \mod n,$$

mivel $m_i^{\phi(n)} \equiv 1 \mod n$ az Euler-tétel szerint.

Gondoljuk meg: d-t csak $\phi(n)$ ismeretében lehet meghatározni. Ez viszont ekvivalens n faktorizálásával, azaz p és q megtalálásával n ismeretében. Tehát:

Kérdés: *lehet-e faktorizálni nagy számokat*?

Az RSA nyilvánosságra hozott ilyen nagy számokat (két nagy prím szorzata), pl.:
RSA-155 (155 jegyű 10-es számrendszerben) – ezt a számot 1999-ben faktorizálták.

Megszületett az igény a hitelesítésre az interneten: *digitális aláírás*.

Legyen a hitelesítendő üzenet: $m = m_1, \ldots, m_k$.

Az aláírás: $s_i = (m_i)^d$.

Elküldi az (m_i, s_i, e, n) üzenetet.

Ellenőrzés: igaz-e, hogy

$(s_i)^e \equiv (m_i)^{ed} \equiv m_i \mod n$?

Ha igen, akkor hiteles az aláírás.

Megjegyzés: Valójában, mivel így az ellenőrzés túl sok műveletből állna, és egy számítógépnek is túl sok időbe telne az $(m_i)^{ed} \equiv m_i$ kongruenciát vizsgálni, ezért m_i–t összekeverik és lerövidítik (ez lesz: hash(m_i)) és s_i=(hash(m_i))^d a fenti $(m_i)^d$ helyett

Mindkét módszer biztonsága a faktorizáláson múlik.

Faktorizálási módszerek:

n leosztása √*n*–ig minden számmal (elég csak a páratlanokkal) – ez az „Erathosztenészi szita”.

az első 1 000 000 (eltárolt) prímmel leosztunk.

1874-ben úgy gondolták, hogy senki nem tudja majd faktorizálni a 8 616 460 799-et (10 jegy).

Az 1970-es években 20 jegyű számokig tudtak mindent faktorizálni.

1978: publikáció a Scientific Americában, mely szerint az RSA-129 -et évmilliókba telne faktorizálni.

1980: 50 decimális jegyig tudtak faktorizálni.

1994: RSA-129 faktorizációja.

1999: RSA-155 faktorizációja.

Prímekről

Tétel: Végtelen sok prím létezik (Euklidesz)

Bizonyítás: Tegyük fel, hogy csak véges sok prím van, ezek p_1, p_2, …, p_n.

Ekkor $p_1 \ldots p_n + 1$ minden prímnél nagyobb és egyikkel sem osztható, ami ellentmondás.

Tétel: Minden *n* számra létezik *n* darab egymást követő szám, amelyek egyike sem prím.

Bizonyítás: A következő *n* szám teljesíti a feltételeket:

$(n + 1)! + 2,\ (n + 1)! + 3, \ldots,\ (n + 1)! + n + 1.$

Becslések a prímek eloszlására:

Jelölje p_n az *n*-edik prímet, π(x) pedig az *x*-nél nem nagyobb pozitív prímek számát.

Keressük a $C_{1,p}$, $C_{2,p}$, $C_{1,\pi}$, $C_{2,\pi}$ függvényeket, melyekre: $C_{1,p} \le p_n \le C_{2,p}$ és $C_{1,\pi} \le \pi(x) \le C_{2,\pi}$.

Tétel: $pn \le 2^{2^{n-1}}$ minden n≥1 –re.

Bizonyítás: *n* szerinti teljes indukció, *n* = 1 –re triviálisan igaz.

$p_{n+1} \le p_1 p_2 \ldots p_n + 1$ (Euklidesz bizonyítása szerint).

Tegyük fel, hogy az állítás az *s* = 1, 2, …, *n* értékek mindegyikére teljesül.

Ekkor: $p_{n+1} \le p_1 p_2 \ldots p_n + 1 \le 2^M$,

ahol az *M* kitevő az $1 + 2 + 4 + \ldots + 2^{n-1}$ kettőhatványok összege, s ez kisebb, mint 2^n.

Tétel: log log $x \le \pi(x) \le (x+1)/2$ minden $x \ge 2$ –re, ahol a log most kettes alapú logaritmust jelent.

Bizonyítás: Legyen $\pi(x) = n$, azaz $p_n \le x < p_{n+1}$.

Ekkor

$$\log\log x < \log\log pn + 1 \le \log\log 2^{2^n} = n = \pi(x).$$

Ennél azonban pontosabb becslések kellenek.

Jelölés: (e $=\lim_{n\to\infty}(1+1/n)^n$, az e alapú logaritmust ln x-szel jelölve:)

$$Li(x) = \int_0^x \frac{dt}{\ln t}$$

Gauss 14 éves korából származik az a sejtése, hogy π(x) közelítőleg egyenlő ezzel. 3 000 000-ig le is ellenőrizte. Ez ekvivalens azzal, hogy $\pi(x) \ln x / x \to 1$, ha $x \to \infty$ ($x/\ln x$ értékét könnyebb számolni). A sejtést 1896-ban bizonyította egymástól függetlenül Hadamard és de la Vallée Poussin. Belátták, hogy

$\pi(x) = x / \ln x + O(x/\ln^2 x)$ (abszolút hiba),

itt $f(x) = O(g(x))$ azt jelenti, hogy létezik olyan c konstans, amelyre $|f(x)/g(x)| < c$.

Ebből becsülhető, hogy mi az esélye annak, hogy egy véletlen, de adott méretű szám prím.

Még egy fontos tudnivaló a prímek eloszlásával kapcsolatban:

Euler sejtette, hogy az első *n* prímszám reciprokösszege végtelenbe tart:

$$\lim_{n\to\infty}(1/p_1+1/p_2+\ldots+1/p_n)=\infty.$$

Mertens megadta bizonyította ezt, egyben pontosan megadta az *x*-nél kisebb prímek reciprokösszegének a nagyságrendjét is:

Tétel: Létezik *c* konstans, amelyre igaz, hogy

$$\Sigma_{p\le x}(1/p) = \ln\ln x + c + O(1/\ln x)$$

(c az ún. Mertens-állandó).

Megjegyzés: A prímek (jóval) sűrűbben vannak, mint a 2-hatványok vagy a négyzetszámok, de az első 10^{16} prím reciprokösszege még mindig kisebb, mint 4.

Faktorizáció

Fermat ötlete:

Legyen *n* összetett. Keressünk olyan *x*,*y* számokat, amelyekre $x^2 - y^2 = (x - y)(x + y) = n$.

Ekkor $x - y$ és $x + y$ jó eséllyel tényleges osztója *n*-nek. (x - y nem 1)

Az ötlet továbbfejlesztése:

Nagy számokra: keresünk *x*,*y* -t, hogy $x^2 \equiv y^2 \mod n$.

Ha *n* osztója $x^2 - y^2$-nek, akkor *pq* osztója $(x - y)(x + y)$-nak.

Rossz az az eset, ha *n* osztója $x - y$-nak, vagy x + y-nak.

Mindenképp igaz, hogy *p* osztója az egyik tényezőnek, és ha *q* nem osztója ugyanannak a tényezőnek, akkor sikerült szétválasztanunk a két prímet, és lényegében kész a faktorizáció, ugyanis:

Ha $p \mid x - y$, akkor $p = (x - y, n)$, ha $p \mid x + y$, akkor $p = (x + y, n)$. tehát két ismert szám legnagyobb közös osztóját kell megkeresni, amire az euklideszi algoritmus gyors (hatékony) algoritmus! És sikerült *n*-et felbontanunk!

Hogyan találunk két ilyen négyzetszámot

Definíció: Legyen *B* pozitív egész. y pozitív egész szám B-sima (B-smooth), ha egyik prím osztója sem nagyobb B-nél.

Segédtétel (Pomerance, ez a faktorizáció fő tétele): Ha $y_1, y_2, \ldots, y_k$ B-sima számok és $k > \pi(B)$, akkor létezik olyan *K* részhalmaza az $\{1,2,\ldots,k\}$ indexhalmaznak, melyre $Z = \Pi_{j \in K \text{ és } j \leq \pi(B)}(y_j)$ négyzetszám.

1. Keressünk $k > \pi(B)$ db x_i számot, amelyek négyzetének *n*-es maradéka (y_i)B-sima.
2. Ekkor a fenti tétel szerint ki tudunk választani néhány y_i-t, hogy azok szorzata négyzetszám (y^2).
3. És az ezen y_i-khez tartozó x_i-k szorzata legyen *x.*
4. Így pedig teljesül az $x^2 \equiv y^2$ kongruencia.

Ezután, az előadó felvázolta, hogy hogyan keresünk ilyen x_i számokat kvadratikus szitával. Majd pedig ennek műveletigényéről mondott pár szót.