Diskret matematik 2018-05-02 #15

Kryptering

Någon som avlyssnar krypteringsmetod och meddelande ska inte kunna avkoda det

Sats **Fermats lilla sats (variant)**
Låt p vara ett primtal, och a ett godtyckligt heltal.
Om $k \equiv 1 \pmod{p-1}$, då är
$a^k \equiv a \pmod{p}$

Sats **Fermats lilla sats ++**
Låt p, q vara olika primtal, och a ett godtyckligt heltal.
Om $k \equiv 1 \pmod{(p-1)(q-1)}$, då är
$a^k \equiv a \pmod{pq}$

Kan bevisas med lagranges sats ($(\mathbb{Z}_p^*, \cdot)$, $\langle a \rangle$, $a^{p-1} = 1$ i $\mathbb{Z}_p$)

Bevis Eftersom $k \equiv 1 \pmod{(p-1)(q-1)}$ så är
$k \equiv 1 \pmod{p-1}$ & $k \equiv \pmod{q-1}$

Enligt FLS så är
$a^k \equiv a \pmod{p}$ & $a^k \equiv a \pmod{q}$

Alltså: $p \mid a^k - a$ & $q \mid a^k - a$
Enligt aritmetikens fundamentalsats
så gäller $pq \mid a^k - a$

Alltså $a^k \equiv a \pmod{pq}$ ▨

Ex. Modulo $143 = 11 \cdot 13$ gäller det att $a^{121} \equiv a \pmod{143}$
för alla heltal a, eftersom $121 \equiv 1 \pmod{10 \cdot 12}$

RSA-krypto Parametrar (n, m, e, d)

Vi vill ta emot ett meddelande bestående av $a \in \mathbb{N}$

1) Välj 2 olika primtal p & q
2) Räkna ut $n = pq$ & $m = (p-1)(q-1)$

Vi vill att n ska vara stort nog att $a < n$
(eller så kan a styckas upp och skickas i mindre delar)

3) Välj en offentlig krypteringsnyckel e: ett tal som är relativt prim till m (dvs $\gcd(e, m) = 1$.
t.ex ett primtal $< m$ som inte delar m)

4) Räkna ut dekrypteringsnyckeln d som är den multiplikativa inversen till e modulo m: dvs d så att $e \cdot d \equiv 1 \pmod{m}$.
Denna finns eftersom $\gcd(e, m) = 1$
Hur räknar vi ut d?
T.ex. genom att omvandla till en diofantisk ekvation
$ex + my = 1$
och lösa denna genom Euklides algoritm "läst baklänges".
ta $d = x$.

5) Offentliggör talen n & e
→ m & d måste hållas hemliga.

6) Be personen som vill skicka $a \in \mathbb{N}$ till oss att skicka talet $b \equiv a^e \pmod{n}$ istället.

7) Vi tar emot b och får tillbaka a genom att beräkna $b^d \equiv (a^e)^d = a^{ed} \equiv a \pmod{n}$ enl. FLS++.

För att räkna ut a från b så måste en veta d, och för att räkna ut d måste en veta m, och för att räkna ut m måste en faktorisera n.

Snabb potensräkning

Via upprepad kvadrering

Ex 4 $7^{81} \bmod 18$

$81 = 64 + 16 + 1 \Rightarrow 7^{81} = 7^{64+16+1} = 7^{64} \cdot 7^{16} \cdot 7 \equiv 7 \cdot 7 \cdot 7 \equiv 13 \cdot 7 = 91 \equiv 1 \pmod{18}$

RSA - exempel i anteckningar på Canvas.

Felkorrigerande koder

Exempel med "Robot på Mars" på Canvas

Def^n $\{0,1\}^n = \{\text{bit-strängar av längd } n\}$

t.ex. $\{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
elementen kallas ord

En (binär) kod av längd n är en delmängd $\mathcal{C} \subseteq \{0,1\}^n$ "lista över tillåtna ord"
Orden i $\mathcal{C}$ kallas kodord.

Def^n För två ord $x, y \in \{0,1\}^n$ definierar vi avståndet $\delta(x,y)$ genom (positionen)
$\delta(x,y) =$ antalet bitar där x & y skiljer sig
Hamming-avstånd.

Ex $\delta(1101, 1000) = 2 \qquad \delta(1010101, 1100100) = 3$

Def^n För en kod $\mathcal{C} \subseteq \{0,1\}^n$ skriver vi $\delta = \delta(\mathcal{C})$ för minimidistansen mellan två ord i koden, dvs.

$$\delta(\mathcal{C}) = \min\{\delta(x,y) : x \neq y \in \mathcal{C}\}$$

Potentiellt $\binom{|\mathcal{C}|}{2}$ distanser att beräkna.