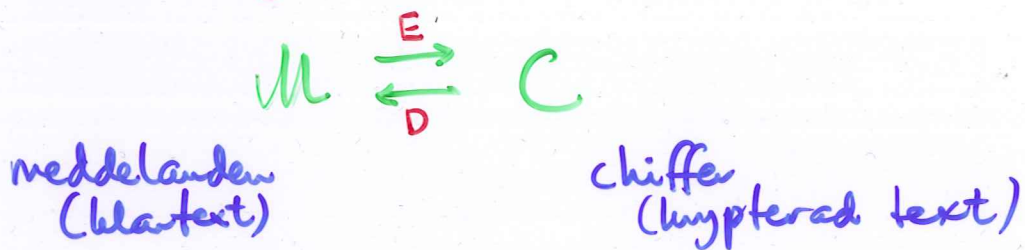


Sist
F20

Kryptering



E : kryptering

D : dekryptering

$$D = E^{-1}$$

Traditionellt : E, D bara kända av behöriga

Nytt (1976) : E envägsfunktion, känd av "alla"

Svårt bestämma E^{-1} ur E

Öffentlig nyckel

Sats : Låt p, q vara olika primtal,

$$n = pq, \quad m = (p-1)(q-1)$$

$$\text{Då } s \equiv 1 \pmod{m} \Rightarrow$$

$$x^s \equiv x \pmod{n} \text{ alla } x \in \mathbb{Z}$$

Fermats lilla sats : Låt p vara ett primtal

$$\text{Då } p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Så RSA:

Tag p, q stora, olika, primtal ($\approx 10^{150}$),

beräkna $n = pq$, $m = (p-1)(q-1)$

Välj e med $\text{sgd}(e, m) = 1$ och

finn d med $ed \equiv 1 \pmod{m}$ (Euklides)

Offentliggör n, e , hemlighåll d

$$E: \mathbb{Z}_n \rightarrow \mathbb{Z}_n, \quad E(x) = x^e$$

$$D: \mathbb{Z}_n \rightarrow \mathbb{Z}_n, \quad D(x) = x^d$$

$$D = E^{-1}$$

Elektronisk signatur

Sänd $D(x)$. Alla kan läsa (med E),
ingen utan D kunde ha skrivit.

B sänder $E_A(D_B(x))$ (eller $D_B(E_A(x))$)
till A. Bara A kan läsa, bara B
kunde ha skrivit.

Primalitetstest

Är (det stora) talet N ett primtal?

Fermatetestet (bas b , $1 < b < N$):

Är $b^{N-1} \equiv 1 \pmod{N}$?

Nej: N är sammansatt

Ja: Vet ej

Pseudoprimtal, bas b :

sammansatt, klarar Fermatetestet, bas b

ex $341 = 11 \cdot 31$, bas 2

N Carmichaeltal om

pseudoprimtal, alla b med $\text{sgd}(b, N) = 1$

$\Leftrightarrow$ sammansatt, kvadratfritt,

$$p \mid N \Rightarrow (p-1) \mid (N-1)$$

$\uparrow$ primtal

ex $561 = 3 \cdot 11 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, ...

$314821 = 13 \cdot 61 \cdot 397$, ...

Miller - Rabins test (bas b , $1 < b < N$):

Låt $N-1 = u \cdot 2^r$, u udda

Är $\begin{cases} b^u \equiv 1 \pmod{N} & \text{eller} \\ b^{u \cdot 2^i} \equiv -1 \pmod{N} & \text{, ngt } i, 0 \leq i < r \end{cases} ?$

Nej: N är sammansatt Ja: Vet ej

Sammansatta N klarar testet för färre
än $\frac{N}{4}$ av b med $1 < b < N$.

Starka pseudoprimtal, bas b :

sammansatta, klarar M-Rs test, bas b

ex $2047 = 23 \cdot 89$, bas 2