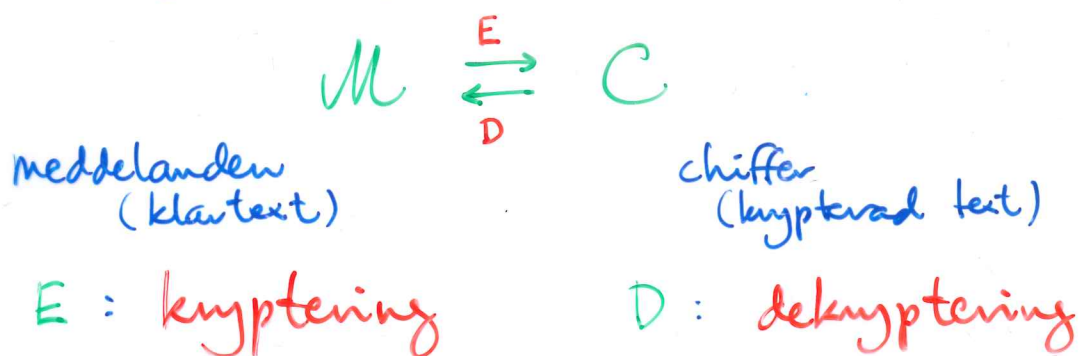


Sist

F20

Kryptering



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

Traditionellt: E, D bara kända av behöriga

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

Svårt bestämma E^{-1} av E

Öffentlig nyckel

Sats: Låt p, q vara olika primtal,

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

$$\text{Då } s \equiv_m 1 \Rightarrow x^s \equiv_n x, \text{ alla } x \in \mathbb{Z}$$

Så RSA:

Tag p, q stora, olika, primtal ($\approx 10^{100}$)

beräkna $n = pq$, $m = (p-1)(q-1)$

Välj e med $\text{sgd}(e, m) = 1$ och

finn d med $ed \equiv_m 1$ (Euklides)

Offentliggör n, e , hemlighåll d

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

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

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

$$E(x) = f_{e_0}(f_{e_1}(\dots(f_{e_n}(1))\dots))$$

$$f_0, f_1: \mathbb{N}_n \rightarrow \mathbb{N}_n, \quad f_0(t) \equiv_n t^2, \quad f_1(t) \equiv_n t^2 x$$

$$e = (e_n \dots e_1 e_0)_2$$

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.

Är (det stora) talet N ett primtal?

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

$$\text{Är } b^{N-1} \equiv_N 1 \text{ ?}$$

Nej: N sammansatt

Ja: Vel ej

Pseudoprimtal, bas b :

sammansatt, klarar Fermattestet, bas b

$$\text{ex } 341 = 11 \cdot 31, \text{ bas } 2$$

N Carmichaeltal om

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

$$\Leftrightarrow \text{kvadratfritt, } p \mid N \Rightarrow (p-1) \mid (N-1)$$

$\nwarrow$ primtal

$$\text{ex } 561 = 3 \cdot 11 \cdot 17, 1729 = 7 \cdot 13 \cdot 19, \dots, 314821 = 13 \cdot 61 \cdot 397$$

Låt $N-1 = u \cdot 2^r$, ^{udda} Då

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

Är $b^u \equiv_N 1$ eller $b^{u \cdot 2^i} \equiv_N -1$, $\forall i, 0 \leq i < r$?

Nej: N 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