

Tjugonionde föreläsningen

KRYPTERING

- $\mathcal{M} \xrightleftharpoons[D]{E} \mathcal{C}$

E kryptering, $D(=E^{-1})$ dekryptering

Offentlig nyckel, envägsfunktioner

- Från Fermats lilla sats

$$s \equiv 1 \pmod{m} \Rightarrow x^s \equiv x \pmod{n},$$
$$n = pq, m = (p-1)(q-1); p, q \text{ olika primtal}$$

- RSA

$$E(x) \equiv x^e \pmod{n}, D(x) \equiv x^d \pmod{n}$$
$$n = pq, ed \equiv 1 \pmod{m}$$

Elektronisk signatur

- Primalitetstest

Fermattestet

Pseudoprimtal, carmichaeltal

Miller-Rabins test