Tjugonde föreläsningen

# PRIMTAL OCH KRYPTERING

- $\mathcal{M} \underset{D}{\overset{E}{\rightleftarrows}} \mathcal{C}$

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

  **Offentlig nyckel, envägsfunktioner**

- **Fermats lilla sats**

  $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$, $p$ **primtal**

  **Så:** $s \equiv 1 \pmod{m} \Rightarrow x^s \equiv x \pmod{n}$,

  **om** $n = pq$, $m = (p-1)(q-1)$; $p, q$ **olika primtal**

- **RSA**

  $p, q$ **olika (stora) primtal,**

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

  $$ed = 1 \text{ i } \mathbb{Z}_m \quad \text{(obs! } m\text{)}$$

  $E(x) = x^e$, $D(x) = x^d$ **i** $\mathbb{Z}_n$ **(obs!** $n$**)**

  **Elektronisk signatur**

- **Primalitetstest**

  **Fermattestet**

  **Pseudoprimtal, carmichaeltal**

  **Miller-Rabins test**

- **Öks4**