(SF1662 Diskret matte, vt15: F20, on 22 april 2015)

Om **kryptering**

$\mathcal{M}$ och $\mathcal{C}$: Meddelanden (klartext) och chiffer (krypterad text),
E och $D(= E^{-1})$: Kryptering och dekryptering,

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

Traditionellt : E och D är bara kända av behöriga.

Nytt (1976): **Offentlig nyckel**, E en **envägsfunktion**, känd av "alla".
Svårt att bestämma E^{-1} ur E.

Fermats lilla sats: Om **p primtal** och $p \nmid a$ gäller $a^{p-1} \equiv 1 \pmod{p}$,
så för alla $a \in \mathbb{Z}$ gäller $a^p \equiv a \pmod{p}$.

Sats: Låt p, q vara olika primtal, $n = pq$, $m = (p-1)(q-1)$.
Då gäller $s \equiv 1 \pmod{m} \Rightarrow x^s \equiv x \pmod{n}$, alla $x \in \mathbb{Z}$

Så **RSA-algoritmen** :

- **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 och **hemlighåll** d (och m, som kastas).

Då gäller för $\boldsymbol{E, D : \mathbb{Z}_n \to \mathbb{Z}_n}$ med $\boldsymbol{E(x) = x^e, D(x) = x^d}$ att $\boldsymbol{D = E^{-1}}$.
$E(x), D(x)$ kan **beräknas** med upprepad **kvadrering** $\pmod{n}$ av x och **multiplikation** $\pmod{n}$ av rätt $x^{2^i} \pmod{n}$.

Elektronisk signatur :

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

2. B sänder $E_A(D_B(x))$ (eller $D_B(E_A(x))$) till A. Bara någon med D_A (och E_B) kan läsa, bara någon med D_B (och E_A) kunde ha skrivit.

Fermattestet (bas b, $1 < b < N$), test om N är ett primtal:

Är $b^{N-1} \equiv 1 \pmod{N}$?	Nej: N sammansatt Ja: Vet ej (säkert)

Pseudoprimtal, bas b : sammansatt tal som klarar fermattestet, bas b.
ex. $341 = 11 \cdot 31$, bas 2.

N är ett **carmichaeltal** omm ett pseudoprimtal för **alla** b med $\text{sgd}(b, N) = 1$
$\Leftrightarrow$ N är kvadratfritt och för primtal p gäller $p \mid N \Rightarrow (p-1) \mid (N-1)$
ex. $561 = 3 \cdot 11 \cdot 17, \ldots, 1729 = 7 \cdot 13 \cdot 19, \ldots, 41041 = 7 \cdot 11 \cdot 13 \cdot 41, \ldots, 488881 = 37 \cdot 73 \cdot 181$

Miller-Rabins test (starkare) (bas b, $1 < b < N$, $N - 1 = u \cdot 2^r$, u udda):

Är $b^u \equiv 1 \pmod{N}$ eller $b^{u \cdot 2^i} \equiv -1 \pmod{N}$, något i, $0 \le i < r$?	Nej: N sammansatt Ja: Vet ej (helt säkert)

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