(Diskret matte D, ht17: F20, on 11 okt 2017)

Om **kryptering**

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

$$\mathcal{M} \underset{D}{\overset{E}{\rightleftarrows}} \mathcal{C}\ , \qquad D = E^{-1}$$

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.

Sats: Låt p, q vara olika primtal, $n = pq$, $m = (p-1)(q-1)$ $(= \phi(n))$.
Då gäller $s \equiv_m 1 \ \Rightarrow\ x^s \equiv_n x$, 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 $ed \equiv_m 1$ (Euklides)
Offentliggör n, e och **hemlighåll** d.
$E : \mathbb{Z}_n \to \mathbb{Z}_n$, $E(x) = x^e$ och $D : \mathbb{Z}_n \to \mathbb{Z}_n$, $D(x) = x^d$ ger då $D = E^{-1}$.

$E(x)$ **beräknas** med $f_0, f_1 : \mathbb{Z}_n \to \mathbb{Z}_n$, givna av $f_0(t) = t^2$, $f_1(t) = t^2 \cdot x$:
Om e är $(e_k e_{k-1} \dots e_1 e_0)_2$ binärt är

$$E(x) = f_{e_0}(f_{e_1}(\dots(f_{e_{k-1}}(f_{e_k}(1)))\dots)).$$

Elektronisk signatur :
1. Sänd $D(x)$. 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 kan läsa, bara någon med D_B kunde ha skrivit.

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

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

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 (sammansatt,) kvadratfritt och $p \mid N \ \Rightarrow\ (p-1) \mid (N-1)$ (för p primtal)
ex. $561 = 3{\cdot}11{\cdot}17$, $1105 = 5{\cdot}13{\cdot}17$, $1729 = 7{\cdot}13{\cdot}19, \dots, 314821 = 13{\cdot}61{\cdot}397$

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

$$\boxed{\text{Är } \ b^u \equiv_N 1 \ \text{ eller } \ b^{u \cdot 2^i} \equiv_N -1 \ \text{ för något } \ i,\ 0 \le i < r \ ?}$$

Nej : N sammansatt Ja : Vet ej (säkert)

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

Starka pseudoprimtal, bas b : sammansatta, klarar M-R:s test, bas b.
ex. $2047 = 23 \cdot 89$, bas 2