God Morgon!

schemat

	Mån	Ons	Tor	Fre
LV4			idag	X
LV5	X	ingen inlämning gamla övningar inlämning A4 nya övningar	by popular demand	X
LV6	strukturell induktion		grafer 1	grafer 2

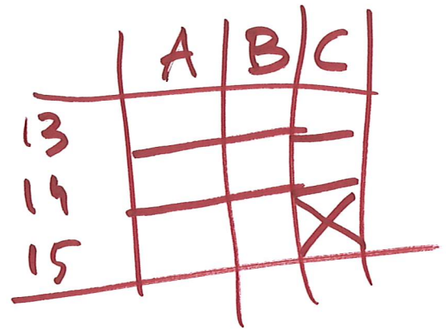
koen@chalmers.se
Subject: "POPULAR"

övningar

onsdagar ~13 - ~16

3 tillfällen

grupper 1-8



kom!

kom gärna i tid

inlämningsuppgifter

första deadline: feedback

"reject"

10-15 min

sista deadline

Fermat's
lilla sats

~1640

$$a^{p-1} \equiv 1 \pmod{p}$$

$\Rightarrow\!\Leftarrow$ (p primtal , $p \nmid a$) — $\gcd(a,p)=1$

$\nmid$ glömde

$$a^p \equiv a \pmod{p}$$

(p prim)

delning inte tillåtet:

$2 \cdot 3 \equiv 2 \cdot 5 \pmod 4$

$3 \not\equiv 5 \pmod 4$

Fermat's sista sats

$x^n + y^n = z^n$

inga lösningar för

$n \geq 3$, $x, y, z \geq 1$

multiplikativ invers ("delning")

$a \cdot b \equiv a \cdot c \pmod m$

alltid ⇑

⇓ ?

$b \equiv c \pmod m$

$u \cdot a \cdot b \equiv u \cdot a \cdot c \pmod m$

$b \equiv c \pmod m$

om $\gcd(a,m) = 1$

pulverizer

då har vi u, v

$a \cdot u + m \cdot v = 1$

$a \cdot u \equiv 1 \pmod m$

$m \mid (a \cdot u - 1)$

p primtal, $p \nmid a$

$1 \cdot a, \ 2 \cdot a, \ 3 \cdot a, \ 4 \cdot a, \ \ldots, \ (p-1) \cdot a$

vad blir resten efter delning med p?

$0 \leq r \leq p-1$

$1 \leq i, j \leq p-1$:

$i \cdot a \overset{?}{\equiv} j \cdot a \pmod{p}$

$i \equiv j \pmod{p}$

$i = j$

faktiskt $1 \leq r \leq p-1$

eftersom $p \nmid i \cdot a$

alla tal i sekvensen har olika rest efter delning med p!

1, 2, 3, 4, ..., p-1
(möjligtvis inte i den ordningen)

$$1\cdot a \cdot 2\cdot a \cdot 3\cdot a \cdot \ldots \cdot (p-1)\cdot a$$

$$\equiv$$

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$$

(eftersom $1 \leq i \leq p-1$, $\gcd(i,p)=1$ eftersom p är prim)

$$a^{p-1} \equiv 1 \pmod{p}$$

1 möjligt bevis

- kongruensräkning
- induktion

encrypt

decrypt

kryptografi

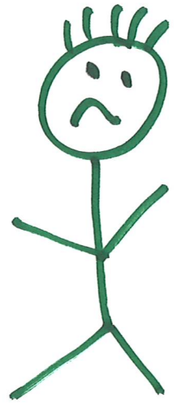
m

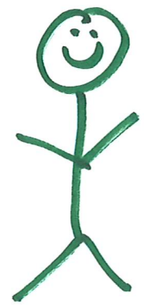
encrypt (m,k)

m'

decrypt(m';k) = m

A





B

kod k

kod k

shared key

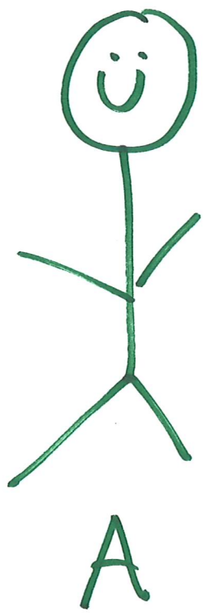
decrypt (encrypt (m,k),k)=m

RSA kryptografi

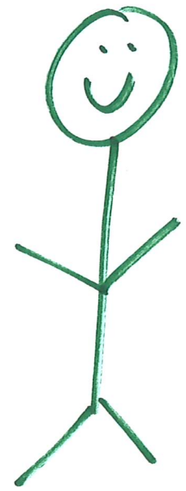
public key

min kod är k_B !!!

encrypt (m, k_B) - - - -> m'



A



B

decrypt $(m', k'_B) =$ m

decrypt (encrypt $(m, k_B), k'_B) =$ m

70-talet RSA krypto, steg

För beredelser:

① välja två olika primtal p, q

② räkna ut $N = p \cdot q$

③ räkna ut $M = (p-1) \cdot (q-1)$

④ välj e, d sådant att $e \cdot d \equiv 1 \pmod{M}$

$d \equiv e^{-1}$

(d är e's multiplikativa invers)

$e = 2^{16} - 1$

(e är publikt, räkna ut d med pulverizer)

hemligt: p, q, M, d

publikt: N, e

⑤ om någon skickar ett meddelande m till mig

$$m^e \equiv m' \pmod{N}$$

m' ← encryptade meddelandet

⑥ när jag får m' räknar jag ut

$$m'^d \equiv m \pmod{N}$$

m ← decryptade meddelandet

korrekthet:

$e \cdot d \equiv 1 \bmod M$
$M = (p-1) \cdot (q-1)$
$N = p \cdot q$

$$(m^e)^d \equiv m \pmod{N}$$

$$(m^e)^d = m^{e \cdot d}$$

$$= m^{k \cdot M + 1} \quad \text{(för något } k\text{, eftersom } e \cdot d \equiv 1 \pmod{M}\text{)}$$

$$= m^{k \cdot (p-1) \cdot (q-1)} \cdot m$$

$$\left(m^{k \cdot (p-1)}\right)^{q-1} \cdot m \qquad \left(m^{k \cdot (q-1)}\right)^{p-1} \cdot m$$

$$\equiv 1 \cdot m \pmod{q} \qquad \equiv 1 \cdot m \pmod{p}$$

$$\equiv m \pmod{q} \qquad \equiv m \pmod{p}$$

$$\equiv m \pmod{p \cdot q}$$

$$\equiv m \pmod{N}$$

vet $N = p \cdot q$

hur hitta p, q?

primtalsfaktorisering

RSA challenge (wikipedia)