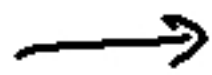


KRYPTON, avsn. 3.2 (sid 51 och vidare)

Säker överföring av data

Avsändaren
förvanskar
data



Data
skickas



Mottagaren
har en
liten device
som
återskapar
meddelandet

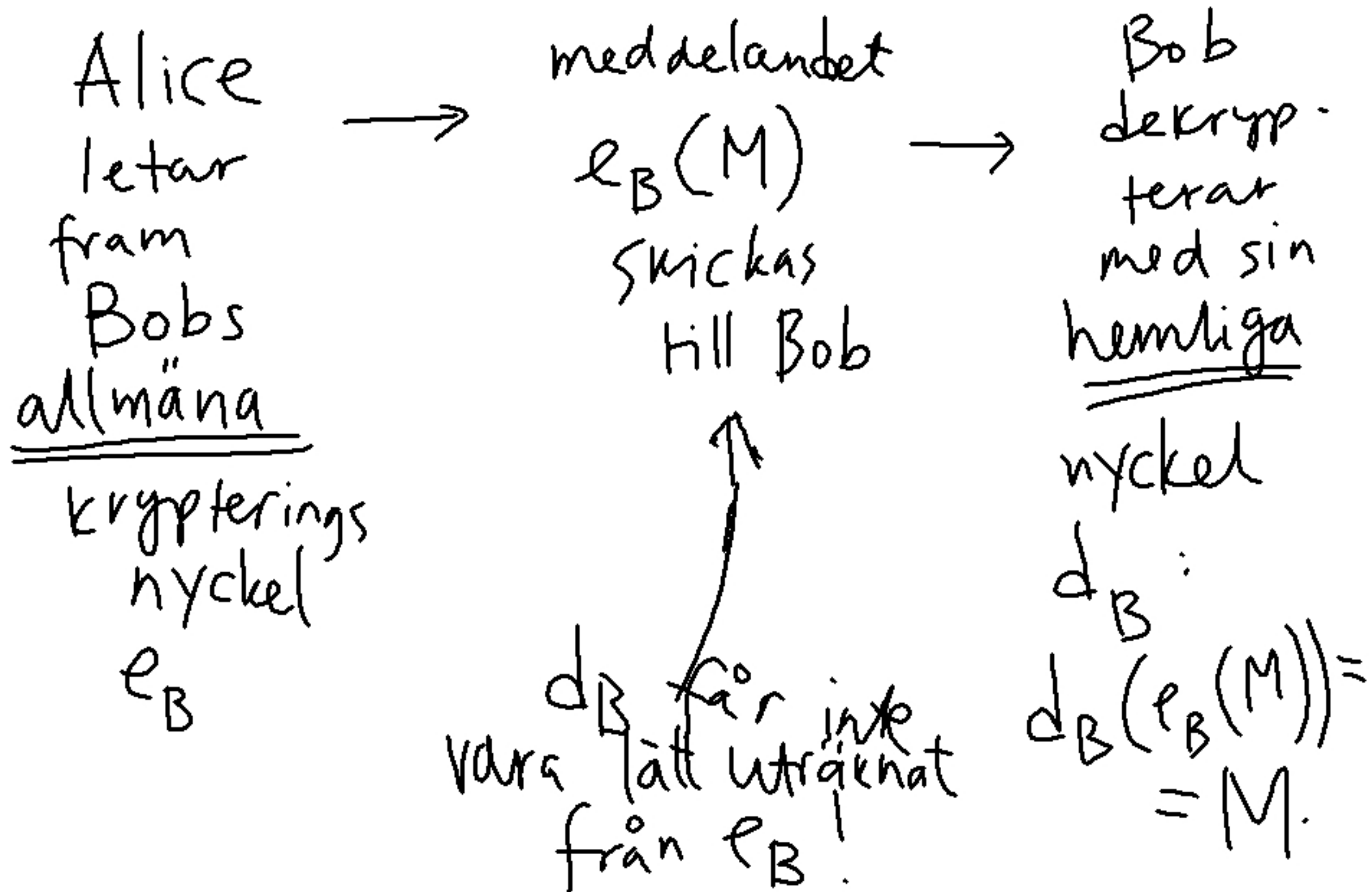
- 1) ÖVERQNSKOMMELSE
Krypteringsfunktionen
och dekrypteringsfunktionen
skall vara varandras
inverser.

2) Dekrypteringsfunktionen
skall vara svår att
komma fram till.

3) n personer utbyter data,
 $\binom{n}{2}$ olika krypto-dekrypt
par av funktioner.

Allt för stort för stora n .

Meddelandet M ska skickas



RSA (Rivest, Shamir, Adelman 1977)

Välj 2 olika primtal, p och q .

Låt $n = pq$, $m = (p-1)(q-1)$

Hitta nu 2 tal e och d sådana
att

$$ed = km + 1 \text{ för något } k.$$

a krypteras till

resten vid divisionen av a^e med n
 a^e dekrypteras till resten vid div av $(a^e)^d$ med n .

Hur hittar man e och d ?

T.ex välj e relativt primt med m

(dvs $\text{SGD}(e, m) = 1$), vanligtvis
är e ett
primtal $< m$
då

$$1 = X \cdot m + Y \cdot e \quad \text{enligt Euklides
baklänges}$$

Välj Y som d .
men se till att $Y > 0$

Notation

resten vid division med n brukar
betecknas med $(\text{mod } n)$

$(a < n)$ krypteras alltså till
 $a^e (\text{mod } n)$

frågan är nu varför

$$\left[a^e (\text{mod } n) \right]^d (\text{mod } n) = a?$$

Till hjälp har man

Fermat's lilla sats (3.4) p primtal, $p \nmid a$. Då gäller

$a^{p-1} - 1$ är delbart med p .

generalisering: (3.5) p, q primtal
 $p \nmid a, q \nmid a$

$a^{(p-1)(q-1)} - 1$ är delbart med pq

$$a^{ed} = a^{km+1} =$$

$$= a \cdot a^{km} =$$

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

$$= a \pmod{n}$$

↑
ger
rest
1 vid
div. med
n

Exempel

$$p = 47, q = 11$$

$$n = p \cdot q = 517$$

$$m = (p-1)(q-1) = 460$$

Välj $e = 97$, ett primtal < 460 .

$$460 = 4 \cdot 97 + 72$$

$$97 = 1 \cdot 72 + 25$$

$$72 = 2 \cdot 25 + 22$$

$$25 = 1 \cdot 22 + 3$$

$$22 = 7 \cdot 3 + 1$$

Euklides baklänges ger

$$1 = (-147) \cdot 97 + 31 \cdot 460$$

$$-147 = 313 - 460$$

$$1 = 313 \cdot 97 - 66 \cdot 460$$

e blir 97 och d blir 313

meddelandet "50"

krypteras

$$50^{97} \bmod (517)$$

$$97 = 64 + 32 + 1$$

$$50^1 = 50 \bmod 517$$

$$50^2 = 2500 = -85 \pmod{517}$$

$$50^4 = (-85)^2 = -13 \pmod{517}$$

$$50^8 = (-13)^2 = 169 \pmod{517}$$

$$(50)^{16} = (169)^2 = 126 \pmod{517}$$

$$(50)^{32} = -151 \pmod{517}$$

$$(50)^{64} = 53$$

$$50^{97} = \underbrace{50^{64}}_{\substack{\text{ger rest} \\ 53}} \cdot \underbrace{50^{32}}_{\substack{\text{ger} \\ \text{rest} \\ -151}} \cdot \underbrace{50}_{\substack{\text{ger} \\ \text{rest} \\ 50}} =$$

$$= 53 \cdot (-151) \cdot 50 \pmod{517} =$$

$$= \boxed{8} \pmod{517}$$

~~8~~ krypterad meddelandet.

Dekryptering av "8"

$$8^{313} =$$

$$8^{313} \pmod{517} = 8^{256+32+16+8+1}$$

potens av 8

$$8$$

$$8^2$$

$$8^4$$

$$8^{16}$$

$$8^{32}$$

$$8^{64}$$

$$8^{128}$$

$$8^{256}$$

rest vid div mod 517

$$8$$

$$64$$

$$-40$$

$$184$$

$$251$$

$$-73$$

$$-159$$

$$52$$

$$8^{313} =$$

$$= 8^{256} \cdot 8^{32} \cdot 8^{16} \cdot 8^8 \cdot 8^1 =$$

$$= 52 \cdot 251 \cdot 184 \cdot 49 \cdot 8 \pmod{517} =$$

$$= 50 \pmod{517}$$

