om p känd:

vi vet att $p \cdot q = n$ så $q = \frac{n}{p}$

$\Phi(n) = (p-1)(q-1) = (p-1)(\frac{n}{p} - 1)$

$ak \equiv 1 \mod (p-1)(\frac{n}{p} - 1)$ enkelt

p.s.s med q.

[8.6]

$3x \equiv 4 \mod 5$

$x = 3 + 5n$ eftersom

$3 \times 2 = 6 \equiv 1 \mod 5$

$3 \times 3 = 9 \equiv 4 \mod 5 \leftarrow$

x

[8.25]

$x^2 \equiv 3 \mod 5 \iff x \cdot x \equiv 3 \mod 5$

$[x] = \{[0], [1], [2], [3], [4]\}$ så

$[x^2] = \{[0], [1], [4], [9], [16]\} = \{[0], [1], [4]\}$

rest vid div. med 5 — [3] finns ej med!

∴ NEJ

[8.26]

$x^2 + x + 2 \equiv 0 \mod 4$

$[x] \in \{[0], [1], [2], [3]\}$ eller $[a^{p-1}] = [1] \mod p$ prime

$[x^2] \in \{[0], [1], \underset{=0}{[4]}, \underset{=1}{[9]}\}$

∴ $x \equiv 1$ eller $x \equiv 2 \mod 4$ ger lösningar.

[8.22]

om m, p eller q är känt så kan a enkelt beräknas.
(k, n) kända.

$\left.\begin{array}{l} \text{om } m \text{ känd:} \\ m = \Phi(n) \\ ak \equiv 1 \mod 1 \end{array}\right\}$ enkelt.

[8.23]

$(k, N) = (5, 91)$

a) $91 = 7 \cdot 13 = pq$

$\phi(N) = \phi(91) = (7-1)(13-1) = 6 \cdot 12 = 72$

$ak \equiv 1 \mod \phi(N) \Rightarrow$

$5a \equiv 1 \mod 72$

$5a + 72b = 1$

$72 = (14) \cdot 5 + 2$

$5 = (2) \cdot 2 + 1 \Rightarrow 1 = 5 - (2)(72 - (14) \cdot 5) =$

$= 5 - (2) \cdot 72 + (28) \cdot 5 =$

$= (29) \cdot 5 - (2) \cdot 72$

$\boxed{a = 29}$

b) $x = 6$

$k(6) = 6^5 \mod 91 \equiv \{216 = 2 \cdot 91 + 34\} \equiv 34 \cdot 6^2 =$

$34 \cdot 36 = \{34 \cdot 25 =, 1224\} = 1224 = 13 \cdot 91 + 41 \equiv 41 \mod 91$

<u>SVAR</u>: 41

c) $A(41) = 41^{29} \mod 91 = 6$

Hur räkna utan räknare??

[8.18] $k = 7$ $n = 35$, $(7, 35)$

$\uparrow$

krypterings nyckel

a) Bestäm avkrypteringsnyckel

$N = 35 = 7 \cdot 5 = pq$

$\phi(N) = (5-1)(7-1) = 4 \cdot 6 = 24$

$ak \equiv 1 \mod 24$

$7a \equiv 1 \mod 24$

$a = 7$

b) Avkryptera $x = 17$

$17^7 \mod 35 = 3 \mod 35$

c) Avkryptera $y = 8$

$8^7 \mod 35 = 22$

[8.10]

$$\begin{cases} x \equiv 7 \mod 17 & sgd(17,13) = 1 \\ x \equiv 9 \mod 13 & sgd(17,12) = 1 \\ x \equiv 3 \mod 12 & sgd(13,12) = 1 \end{cases}$$ ok!

$N = 17 \cdot 13 \cdot 12 = 2652$

$x = b_1 N_1 x_1 + b_2 N_2 x_2 + b_3 N_3 x_3$

$x \equiv 7 \mod 17$, $b_1 = 7$ $\quad N_1 = \frac{2652}{17} = 156$

$x \equiv 9 \mod 13$, $b_2 = 9$ $\quad N_2 = \frac{2652}{12} = 204$

$x \equiv 12 \mod 12$, $b_3 = 12$ $\quad N_3 = \frac{2652}{12} = 221$

$156 x_1 \equiv 1 \mod 17$

$3 x_1 \equiv 1 \mod 17$

$x_1 = 6$

$204 x_2 \equiv 1 \mod 13$

$9 x_2 \equiv 1 \mod 13$

$x_2 = 3$

$221 x_3 \equiv 1 \mod 12$

$5 x_3 \equiv 1 \mod 12$

$x_3 = 5$

vi får att

$x = 7 \cdot 156 \cdot 6 + 9 \cdot 204 \cdot 3 + 3 \cdot 221 \cdot 5 = 6552 + 5508 + 3315 =$

$x = 15\,375 \mod 2652$

13 260

$x = 2115 \mod 2652$

SVAR: $2115 + 2652n$

[8.9]

$$\begin{cases} x \equiv 0 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 3 \mod 7 \end{cases}$$

sgd $(3,5) = 1$
sgd $(3,7) = 1$
sgd $(5,7) = 1$ ok!

$$\begin{array}{lcccccc} & \text{mod } 3 & & \text{mod } 5 & & \text{mod } 7 & \\ x = & 5 \cdot 7 \cdot 3 & + & 3 \cdot 7 \cdot 2 & + & 3 \cdot 5 \cdot 3 & = 192 \\ x = & 35 \cdot 3 & + & 21 \cdot 2 & + & 15 \cdot 3 & = 192 \end{array}$$

mod 3:

$x \equiv 2 \mod 3$ ej ok

$2 \cdot 3 \equiv 0 \mod 3$ ok! Mult. med 3

mod 4:

$x \equiv 21 \equiv 1 \mod 5$

$1 \cdot 2 \equiv 2 \mod 5$ ok.

mod 7

$x \equiv 15 \equiv 1 \mod 7$

$1 \cdot 3 \equiv 3 \mod 7$

$x = 192 \mod 105$

$x = 87 \mod 105$