Ekvationer

Ex: Lös ekvationen $x+5=2$ i $\mathbb{Z}_7$.

Lösn: $x+5=2 \Rightarrow x=2-5=-3$.

$-3 \equiv 4 \pmod 7$

Vi har $3+4\equiv 0$. SVAR: $x=4$.

Ex: Lös ekvationen $2x=3$ i $\mathbb{Z}_7$. (2^{-1} är det element i $\mathbb{Z}_7$ så att $2\cdot 2^{-1}=1$

Lösn: $x=2^{-1}3=4\cdot 3=12=5$ $\quad 2\cdot 4=8\equiv 1 \pmod 7$

SVAR: $x=5$ $\quad \Rightarrow 4=2^{-1}$

Ex: Lös ekvationen $x^2 - 1 = 0$ i $\mathbb{Z}_8$. $x^2 \equiv 1 \pmod 8$

Lösn: Som vanligt har vi lösningarna $x = 1$ och $x = -1 = 7$.

$0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 = 1$, $4^2 = 16 = 0$

$5^2 = 25 = 1$, $6^2 = 36 = 4$, $7^2 = 1$

Vi har alltså fyra (!!) lösningar 1, 3, 5 och 7.

$x^2 - 1 = 0 \iff (x+1)(x-1) = 0$ $\quad 2 \cdot 4 = 0$

$x - 1 = 2$ och $x + 1 = 4 \Rightarrow x = 3$

Ex: Lös ekvationen $x^2+14x+6=0$ i $\mathbb{Z}_{17}$.

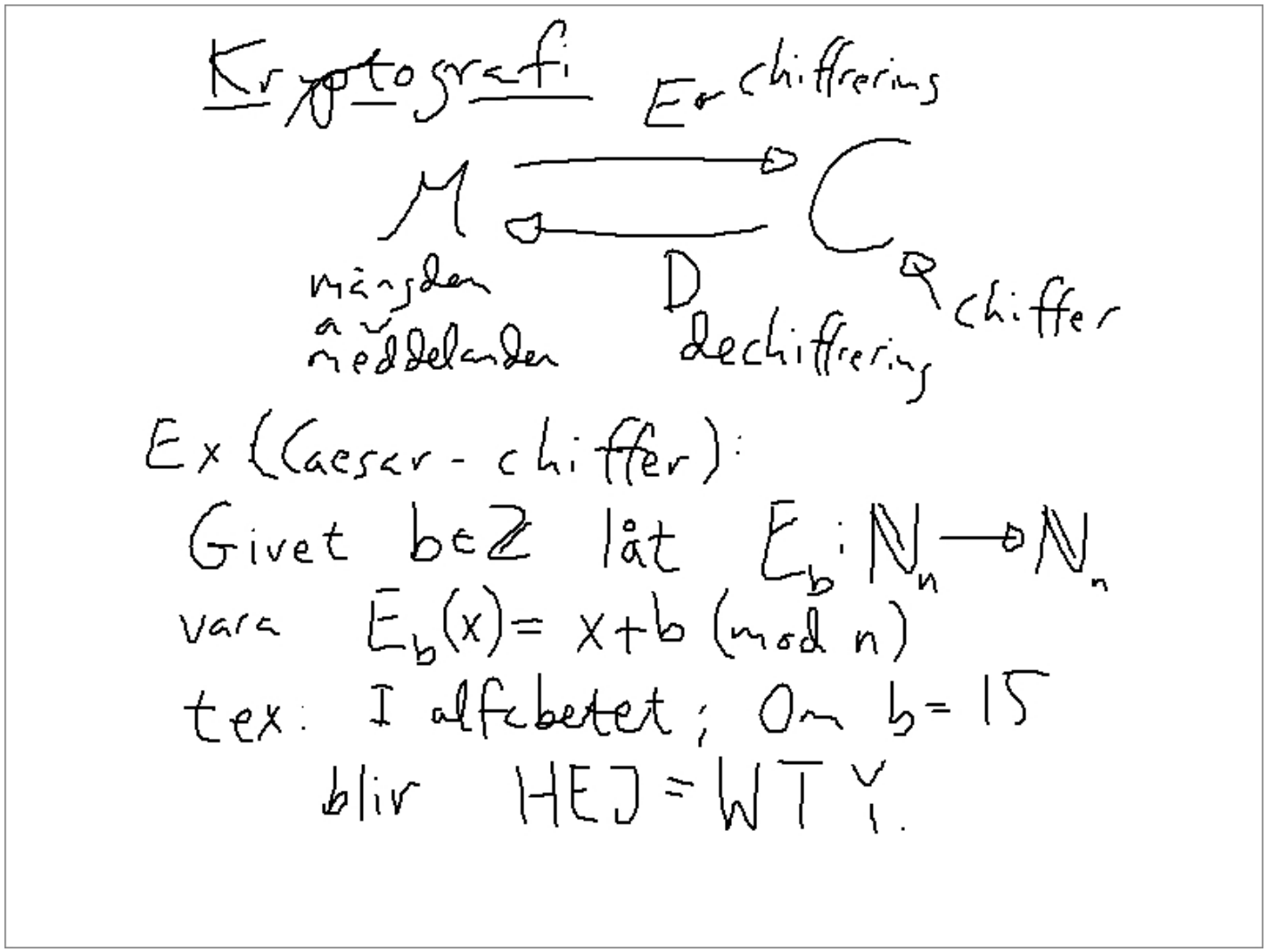
Lösn: $(x+7)^2+6-49 \equiv (x+7)^2-9 \pmod{17}$

$(x+7)^2 \equiv 9 \pmod{17}$

har lösningarna $x+7=\pm 3$

$\Rightarrow x = \begin{cases} 3-7=-4=13 \\ -3-7=-10=7. \end{cases}$

SVAR: $x=7$ eller $x=13$.


Kryptografi
E chiffrering
M
C
D
mängden av meddelanden
dechiffrering
chiffer
Ex (Caesar-chiffer):
Givet b∈ℤ låt $E_b: \mathbb{N}_n \to \mathbb{N}_n$
vara $E_b(x) = x + b \pmod n$
tex: I alfabetet; Om b = 15
blir HEJ = WTY.

Klassiska krypton bygger på att nyckeln (som bestämmer E) måste hållas hemlig.

Kryptosystem med offentlig nyckel (1976 Diffie & Hellman)

Varje användare A väljer sin egen krypteringsfunktion E_A och en dekrypteringsfunktion D_A. E_A görs offentlig medan D_A hålls hemlig.

Om B vill skicka ett meddelande m till A så sänder han $E_A(m)$. A kan sedan dekryptera med hjälp av D_A, $D_A(E_A(m)) = m$.

Klassiskt: $\binom{n}{2}$ nycklar

Offentligt system: n st

RSA (Rivest, Shamir & Adleman)

Varje användare A i systemet väljer två hemliga primtal p, q (av lämplig storleksordning). Låt sedan $n = p \cdot q$ och $m = (p-1)\cdot(q-1)$. Användaren väljer också ett tal e, $1 < e < m$ med $SGD(e, m) = 1$ och beräknar $d = e^{-1}$ $(1 < d < m)$, $\mathbb{Z}_m$.

$$E_A(x) = x^e \pmod n, \quad D_A(y) = y^d \pmod n$$

Krypteringsnyckeln (n, e) görs offentlig medan d är hemlig, vilket betyder att p, q och m måste hållas hemliga.

Sats: $D_A(E_A(x)) = x$ för alla $x \in \mathbb{N}_n$.

Bevis: Vi ska alltså visa att

$$x^{ed} \equiv x \pmod{n}$$

Vi har att $ed \equiv 1 \pmod{m}$ så $ed = 1 + km$ för något heltal k.

$$X^{ed} = X^{1+km} = X \cdot X^{km}.$$

Vi vill visa att $X \cdot X^{km} \equiv X \pmod{n}$.

Om $SGD(x,n) = 1$ så säger Eulers sats att $x^{\phi(n)} \equiv 1 \pmod{n}$

men $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1) =$

$= m$. Det ger att $x^m \equiv 1$ så $x^{km} \equiv 1 \pmod{n}$

$\Rightarrow X \cdot X^{km} \equiv X \cdot 1 \equiv X \pmod{n}$.

Om $SGD(x,n) \neq 1$ så måste $p \mid x$ eller $q \mid x$.

Låt oss anta att $p \mid x$, det ger $p \mid x^{1+km} - x$

om $q \nmid x \Rightarrow SGD(q,x) = 1$ så $q \mid x^{q-1} - 1$ $\left(= x^{\phi(q)} - 1\right)$

$\Rightarrow q \mid x^{km}-1 \Rightarrow q \mid x \cdot x^{km}-x \Rightarrow$

$\Rightarrow n \mid x^{1+km}-x.$

Ex: Låt $n=77$ och $e=7$.
Dekryptera meddelandet
14.

Lösn: $n=77=7\cdot 11$ $m=(7-1)\cdot(11-1)=$
$=6\cdot 10=60$. Vi har att $SGD(7,60)=1$
$\Rightarrow$ det finns heltal k och l sådana
att $7k+60\cdot l=1$.

$60 = 7 \cdot 8 + 4 \quad 1 = 2 \cdot (60 - 7 \cdot 8) - 7 = 2 \cdot 60 - 17 \cdot 7$

$7 = 4 \cdot 1 + 3 \quad 1 = 4 - (7 - 4) = 2 \cdot 4 - 7$

$4 = 3 \cdot 1 + 1 \quad 1 = 4 - 3$

$e^{-1} = -17 \pmod{60}$

$d = 60 - 17 = 43.$

För att dekryptera ska vi beräkna

$$14^{43} \pmod{77}.$$

$14,\ 14^2 \equiv 196 \equiv 42,\ 14^3 \equiv 14 \cdot 42 \equiv 588 \equiv 49$

$14^4 \equiv 14 \cdot 49 \equiv 686 \equiv 70,\ 14^5 \equiv 14 \cdot 70 \equiv 980 \equiv 56$

$14^6 \equiv 14 \cdot 14^5 \equiv 14 \cdot 56 \equiv 784 \equiv 14$

$$14^{43} \equiv 14 \cdot (14^6)^7 \equiv 14 \cdot 14^7 \equiv 14^3 \equiv 49$$

SVAR: 49.

$$14^{43} \equiv 14\,(14^2)^{21} \equiv 14 \cdot 42^{21} \equiv 14 \cdot 42 \cdot (42)^{10}$$
$$\equiv 49 \cdot 70^{10} \equiv 49 \cdot (70^2)^5 \equiv 49 \cdot 4900^5 \equiv 49^6$$
$$\equiv (49^2)^3 \equiv 14^3 \equiv 49$$

Test: $49^e \equiv 49^7 \equiv 49 \cdot (49^2)^3 \equiv$
$\equiv 49 \cdot 14^3 \equiv 49^2 \equiv 14 \pmod{77}$

Elektronisk signatur:

Problem: Om A får ett meddelande från B, hur ska A då veta att det verkligen är från B?

(Vi antar $n_A = n_B$) Då kan man göra så här: B vill skicka meddelandet x men skickar istället $y = E_A(D_B(x))$.

A kan dekryptera för

$$E_B(D_A(y)) = E_B(D_A(E_A(D_B(x)))) = x.$$