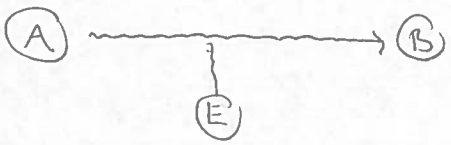
RSA-kryptografi

Kryptografi: Studien av "sikker kommunikasjon". Typisk utgangspunkt: Alice vil sende en melding til Bob, men Eve kan fange opp kommunikasjonen



Hvordan skal A og B kommunisere sikkert uten først å møtes for å avtale et sikkert krypteringssystem? Her kommer såkalt offentlig nøkkel-kryptografi inn i bildet. Bob lager en krypteringsnøkkel og gjør den kjent for alle i hele verden. Da kan alle kryptere meldinger og sende til Bob, men bare Bob kan dekryptere. RSA-systemet (Rivest, Shamir, Adleman, 1978) er et slikt system.

Lage RSA-systemet:

(1) Bob velger to ulike primtall p, q og setter $n = pq$.

(2) Bob velger et tall $1 < e < \phi(n)$ med $\gcd(e, \phi(n)) = 1$ (merk at $\phi(n) = (p-1)(q-1)$).

(3) Bob finner en $1 < d < \phi(n)$ med $ed \equiv 1 \pmod{\phi(n)}$. Dette er mulig siden den lineære kongr $ex \equiv 1 \pmod{\phi(n)}$ er løsbar ved Teorem 4.7.

(4) Bob offentliggjør tallparet $\{n, e\}$, dette er den offentlige nøkkelen. Tallparet $\{n, d\}$ er den hemmelige nøkkelen som Bob holder for seg selv, sammen med p, q og $\phi(n)$.

Kryptere: (1) Alice ønsker å sende meldingen M til Bob, hvor M er et tall med $1 \leq M \leq n$. Hun kjenner bare den offentlige nøkkelen $\{n, e\}$.

(2) Alice finner $1 \leq c \leq n$ med $M^e \equiv c \pmod{n}$.

(3) Alice sender den krypterte meldingen c til Bob. Eve kan plukke den opp

Dekryptere: (1) Bob mottar den krypterte meldingen c.

(2) Bob finner en $1 \leq \bar{M} \leq n$ med $c^d \equiv \bar{M} \pmod{n}$

(3) Da er $M = \bar{M}$!

Eksempel: Bob velger primtallene 5 og 11, får da $n = 5 \cdot 11 = 55$ og $\phi(n) = 4 \cdot 10 = 40$. Velger $e = 27$: har da $1 < e < \phi(n)$ og $\gcd(e, \phi(n)) = 1$. Løser så $ex \equiv 1 \pmod{\phi(n)}$, dvs

$$27x \equiv 1 \pmod{40}$$

Løsning: $x \equiv 3 \pmod{40}$, så det gir $d = 3$ (da er $1 < d < \phi(n)$ og $ed \equiv 1 \pmod{\phi(n)}$). Det gir:

$\{n, e\} = \{55, 27\}$ offentlig nøkkel

$\{n, d\} = \{55, 3\}$ hemmelig nøkkel.

Alice ønsker å sende $M = 2$. Må da finne c med $1 \le c \le n$ og $M^e \equiv c \pmod{n}$, dvs

$$1 \le c \le 55 \text{ og } 2^{27} \equiv c \pmod{55}$$

Har $2^6 \equiv 64 \equiv 9 \pmod{55}$ så $2^{24} \equiv (2^6)^4 \equiv 9^4 \equiv 6561 \equiv 16 \pmod{55}$ og videre $2^{27} \equiv 2^{24} \cdot 2^3 \equiv 16 \cdot 8 \equiv 128 \equiv 18 \pmod{55}$. Altså får Alice

$$c = 18$$

som hun sender til Bob (merk at Alice bare brukte $n = 55$ og $e = 27$).

Bob mottar $c = 18$, og må finne $\bar{M}$ med $1 \le \bar{M} \le n$ og $c^d \equiv \bar{M} \pmod{n}$, dvs

$$1 \le \bar{M} \le 55 \text{ og } 18^3 \equiv \bar{M} \pmod{55}.$$

Har $18^3 \equiv 5832 \equiv 2 \pmod{55}$, så Bob får

$$\bar{M} = 2$$

som var meldingen M som Alice krypterte. Bob brukte bare $n = 55$ og $d = 3$.

To spørsmål: (1) Hvorfor virker dette? Altså hvorfor er $\bar{M} = M$?

(2) Hvorfor er det sikkert?

Lemma La n være et kvadratfritt tall (et produkt av ulike primtall). Da er

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

for alle $a \in \mathbb{Z}$.

Bevis: Her $n = p_1 p_2 \cdots p_t$ og da $\phi(n) = (p_1 - 1) \cdots (p_t - 1)$. Se på p_1. Hvis $p_1 \mid a$ vil kongr $a^{\phi(n)+1} \equiv a \pmod{p_1}$ gjelde automatisk. Hvis $p_1 \nmid a$ er $a^{p_1 - 1} \equiv 1 \pmod{p_1}$ fra FT, som gir $a^{\phi(n)} \equiv (a^{p_1-1})^{(p_2-1)\cdots(p_t-1)} \equiv 1 \pmod{p_1}$, og da $a^{\phi(n)+1} \equiv a \pmod{p_1}$. Så $a^{\phi(n)+1} \equiv a \pmod{p_1}$ gjelder alltid. Siden $p_1, \ldots, p_t$ er ulike vil da $a^{\phi(n)+1} \equiv a \pmod{p_1 p_2 \cdots p_t}$. □

Lemma n kvadratfritt $\Rightarrow a^{k\phi(n)+1} \equiv a \pmod{n}$ $\forall a \in \mathbb{Z}$ og $k \geq 1$.

Bevis: Induksjon på k, hvor $k=1$ er ok fra forrige lemma. Anta

$$a^{k\phi(n)+1} \equiv a \pmod{n}$$

Får da

$$a^{(k+1)\phi(n)+1} \equiv a^{k\phi(n)+\phi(n)+1} \equiv a^{k\phi(n)} \cdot a^{\phi(n)+1} \overset{(*)}{\equiv} a^{k\phi(n)} \cdot a$$

$$\equiv a^{k\phi(n)+1} \overset{(**)}{\equiv} a \pmod{n}$$

Her brukte vi forrige lemma i $(*)$, og induksjonshypotesen i $(**)$ $\square$.

Bevis for $\bar{M} = M$:

Har $ed \equiv 1 \pmod{\phi(n)}$, dvs $ed - 1 = k\phi(n)$ for en $k \in \mathbb{Z}$. Merk at $k \geq 1$ (hvorfor?). Siden $M^e \equiv C \pmod{n}$ og $C^d \equiv \bar{M} \pmod{n}$ får vi da

$$\bar{M} \equiv C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k\phi(n)+1} \equiv M \pmod{n}$$

fra siste lemma. Siden $1 \leq \bar{M}, M \leq n$ er da $M = \bar{M}$.