Om RSA-kryptering

Populærvitenskapelig kilde: "The Code Book/The secret history of codes and code-breaking" av Simon Singh, Fourth Estate, ISBN 1-85702-889-9.

Utviklet i 1969-1975 av James Ellis, Clifford Cocks og Malcolm Williamson ved British Government Communications Headquarters (GCHQ).

Eksempel på "public key cryptography", offentliggjort av Whitfield Diffie, Martin Hellman og Ralph Merkle i 1976.

Realisert av Ron Rivest, Adi Shamir og Leonard Adleman ved MIT i 1977.

Fermats lille sats:
La a være et helt tall, og p et primtall. Da er $a^p \equiv a \bmod p$.

Bevis:
Ved induksjon på a. Anta $a^p \equiv a \bmod p$. Da er

$$(a+1)^p \equiv a^p + 1 \equiv a+1 \bmod p,$$

ved binomialformelen og induksjonshypotesen, siden hver binomialkoeffisient "p over i" er delelig med p for $0 < i < p$.

Q.E.D.

Det følger at $a^z \equiv a \bmod p$ for alle naturlige tall $z \equiv 1 \bmod p-1$.

La q være et annet primtall enn p.
På samme måte følger at $a^z \equiv a \bmod q$ for alle $z \equiv 1 \bmod q-1$.

La $n = pq$ og $m = (p-1)(q-1)$. Dersom

$$z \equiv 1 \bmod (p-1)(q-1) = m$$

så er $z \equiv 1 \bmod p-1$ og $z \equiv 1 \bmod q-1$, så $a^z \equiv a \bmod p$ og $a^z \equiv a \bmod q$, som medfører at

$$a^z \equiv a \bmod pq = n.$$

Korollar:
La a være et helt tall og p og q to forskjellige primtall. La n =pq og m = (p-1)(q-1). Da er $a^z \equiv a \bmod n$ for alle $z \equiv 1 \bmod m$.

La nå x og y være naturlige tall slik at $xy \equiv 1 \bmod m$. La z = xy. Se på funksjonene

$$f(a) = a^x \bmod n$$

og

$$g(b) = b^y \bmod n .$$

Da er

$$g(f(a)) \equiv (a^x)^y \equiv a^z \equiv a \bmod n .$$

Så oppfattet som funksjoner fra Z/nZ til Z/nZ (de hele tall modulo n) er f og g inverse funksjoner.

RSA-kryptering:
La a være en melding i klartekst. Den krypteres ved funksjonen f, så b = f(a) er den kodede meldingen. Den kan dekrypteres ved funksjonen g, siden $g(b) = g(f(a)) \equiv a \bmod n$.

Offentlig:
Modulus n, krypteringsnøkkel x.

Hemmelig:
Primtallene p og q, dekrypteringsnøkkelen y.

Gitt p og q kan vi beregne n = pq og m = (p-1)(q-1), men for store p og q er det vanskelig gitt n å finne faktoriseringen i p og q.

For å finne egnede x og y, dvs. med $xy = 1 \bmod m$, må x være relativt primisk til m. For hvis xy = 1 + km må største felles faktor i x og m dele xy og km, og dermed også 1 = xy - km.

Dersom x er relativt primisk til m, så den største felles faktoren er 1, kan vi bruke Euklids algoritme baklengs til å uttrykke 1 som en heltallig lineær-kombinasjon av x og m: 1 = xy - km. Da er $xy = 1 \bmod m$, som ønsket.