Forelesning 16
ASYMMETRISK KRYPTOGRAFI

- Litt mer om Eulers φ-funksjon + Eulers teorem
  $\gcd(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$
- Asymmetrisk kryptografi
  - ↳ Hva er forskjellen fra symmetrisk kryptografi?
- RSA-kryptering
  - ↳ Hvordan og hvorfor funker det?
  - ↳ Er det sikkert?

$c = m^e \bmod n$
$m = c^d \bmod n$
$ed \equiv 1 \pmod{\varphi(n)}$

Forrige gang

Vi så på Eulers φ-funksjon:

φ-funksjon = antall tall mellom 1 og n som er relativt primiske til n

Dersom $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ så er

$$\varphi(n) = \prod_{i=1}^{n} (p_i^{k_i} - p_i^{k_{i-1}})$$

↑ produkt

Eksempel

La $n = 3969 = 3^4 \cdot 7^2 = p_1^{k_1} \cdot p_2^{k_2}$

Da er $\varphi(n) = \prod_{i=1}^{2} (p_i^{k_i} - p_i^{k_{i-1}})$

$= (3^4 - 3^3) \cdot (7^2 - 7^1) = 2268$

Så mellom 1 og 3969 er det nøyaktig 2268 tall m slik at $\gcd(m, 3969) = 1$

Merk: Dersom p er et primtall får vi:
$\varphi(p) = (p^1 - p^0) = p - 1$

I tillegg er φ det vi kaller en multiplikativ funksjon, som betyr at hvis $\gcd(m,n) = 1$
så er $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

For primtall p og q og $n = p \cdot q$ får vi at

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

Vi er nå klare for følgende resultat:

Eulers teorem

Hvis $n \geq 1$ og $\gcd(a,n) = 1$, så er

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

Eksempel

Regn ut $5^{72} \bmod 12$. Vi har at $\gcd(5,12) = 1$, og vi har $\varphi(12) = 4$.

Så $5^{\varphi(12)} = 5^4 \equiv 1 \pmod{12}$ og

$5^{72} = 5^{4 \cdot 18 + 1} = (5^4)^{18} \cdot 5 \equiv 1^{18} \cdot 5 \equiv 5 \pmod{12}$

Asymmetrisk kryptografi ("offentlig nøkkel-krypto")

Husk: Symmetrisk kryptografi:

- Alice og Bob har en felles nøkkel k
- Denne brukes til både kryptering og dekryptering
- Alice og Bob må bli enige om k

Med asymmetrisk kryptografi:

- Bob har to nøkler:

  en offentlig nøkkel (brukes til kryptering. Alle vet hva denne er) og en hemmelig nøkkel (brukes til dekryptering, kun Bob vet hva den er)

- Alice krypterer en melding med den offentlige nøkkelen
- Bob dekrypterer chiffertekst med den hemmelige nøkkelen

Hvis meldingen er en symmetrisk nøkkel, er dette en nøkkelutveksling!

RSA-kryptering

- Verdens første offentlig nøkkel-krypteringprotokoll (1977)
- Oppfunnet av Ron Rivest, Adi Shamir og Leonard Adleman

Anta at Alice vil sende en melding til Bob.
Det gjøres slik:

- Bob genererer en hemmelig og en offentlig nøkkel
  - ↳ Velger to <u>hemmelige</u> primtall p og q
  - ↳ Beregne $n = p \cdot q$ (n er ikke hemmelig)
  - ↳ Velg en <u>offentlig</u> krypteringseksponent e, slik at $e \perp \varphi(n)$ ($\gcd(e, \varphi(n)) = 1$)
  - ↳ Finn en <u>hemmelig</u> dekrypteringseksponent d, slik at $e \cdot d \equiv 1 \pmod{\varphi(n)}$
    (Med andre ord $e \cdot d = t \cdot \varphi(n) + 1$)

Den offentlige nøkkelen er (n, e)
Den hemmelige nøkkelen er (p, q, d)

Bob sender (n, e) til Alice.
Alice krypterer en melding m ved å regne ut

$$c = m^e \bmod n$$

og sender c til Bob.

Bob dekrypterer ved å beregne $c^d \bmod n$.

$$c^d = m^{e \cdot d} = m^{t \cdot \varphi(n) + 1} = (m^{\varphi(n)})^t \cdot m$$
$$\equiv 1^t \cdot m \equiv m \pmod{n}$$

↑ Her antar vi litt i det stille at $m \perp n$, og bruker $m^{\varphi(n)} \equiv 1 \pmod{n}$, men dette funker uansett i RSA fordi n er "kvadratfritt" (mer om dette i notatene)

Eksempel

Bob velger $p=5$ og $q=17$.
Da er $n=p\cdot q=85$ og
$\varphi(n)=(p-1)\cdot(q-1)=4\cdot 16=64$.
Velg e slik at $\gcd(e,\varphi(n))=1$ f.eks $e=5$
Da har vi $\gcd(e,\varphi(n))=\gcd(5,64)=1$ ✓

Beregn d slik at
$$e\cdot d\equiv 1 \pmod{\varphi(n)}$$
$$5\cdot d\equiv 1 \pmod{64}$$
Det er det samme som å løse $5d+64y=1$

Bruker Eulids algoritme:
$$64=12\cdot 5+4$$
$$5=1\cdot 4+1$$

$$1=5-1\cdot 4=5-1\cdot(64-12\cdot 5)=64\cdot(-1)+5\cdot 13$$
Så $d=13$

Da har vi offentlig nøkkel $(n,e)=(85,5)$
og hemmelig nøkkel $(p,q,d)=(5,17,13)$

Alice har en melding, f.eks $m=7$
Hun krypterer og får
$$c=m^e=7^5=16807\equiv 62 \pmod{85}$$

Alice sender $c=62$ til Bob som dekrypterer:
$$c^d=62^{13}=62^{8+4+1}=62^8\cdot 62^4\cdot 62$$
$$\equiv 16\cdot 21\cdot 62\equiv 7 \pmod{85}$$
$7=m$

Oppsummert

Bob velger $p=5, q=17$ og finner $n=85$ og $\varphi(n)=64$

Bob velger $e=5$ og finner $d=13$ $(13\cdot 5\equiv 1 \pmod{64})$

Alice velger $m=7$ og regner ut $c=m^e\equiv 62 \pmod{85}$

Bob dekrypterer $c^d\equiv 7\equiv m \pmod{85}$

Er dette sikkert?

Altså, hva kan Eve gjøre?
Eve får vite n, e og c,
men ikke p, q, d eller $\varphi(n)$.

Hvis Eve kan beregne $\varphi(n)$ kan hun også
beregne d fra e (med $e \cdot d \equiv 1 \pmod{\varphi(n)}$)

Men! For å finne $\varphi(n) = (p-1)\cdot(q-1)$ må hun
kunne faktorisere n.

Dette er vanskelig dersom p og q er store!

OBS!

Det vi har sett på her kalles ofte "textbook RSA",
og regnes ikke egentlig som sikker i praksis
(selv med store tall).

Hvorfor? Flere grunner!
Ett eksempel er:
↳ Textbook RSA er deterministisk:
Hvis jeg krypterer samme melding to ganger
(med samme nøkkel) får jeg samme chiffertekst

⇒ En angriper kan kryptere alle mulige meldinger
og finne en match

⇒ Dumt hvis det som krypteres f.eks. er hvem
jeg stemmer på ved stortingsvalg

Løsning: Tilføy litt "tilfeldig støy" før du krypterer
(padding)