Forelesning 15
KRYPTOGRAFI

- Hva er kryptologi?
- Symmetrisk kryptografi
- Nøkkelutveksling
- Enveisfunksjoner
- Litt mer tallteori
  - ↳ Fermats lille teorem
  - ↳ Eulers φ-funksjon

Hva er kryptologi?

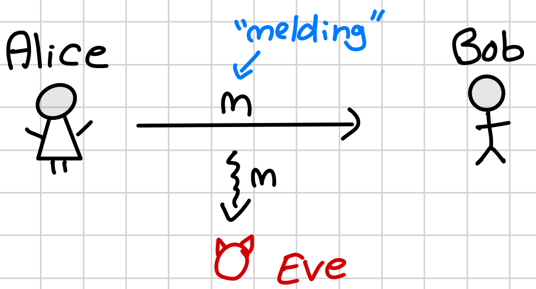
(Kryptografi + kryptanalyse)

- Kryptografi:
  <u>Designe</u> koder som lar oss
  - Komminusere hemmelig
  - Signere ting digitalt
  - Bruke nettbank og avgi stemmer digitalt

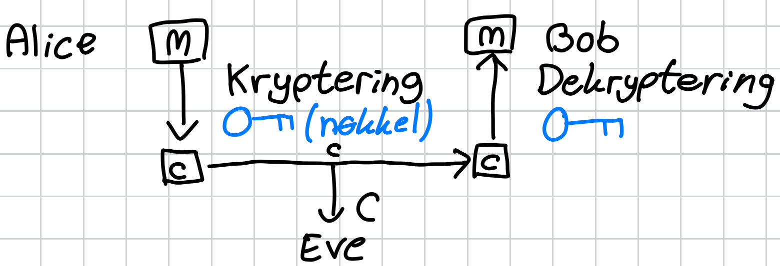
- Kryptanalyse
  Kunsten å knekke kryptografenes koder

Vi deler grovt sett inn i
- symmetrisk kryptografi
- asymmetrisk kryptografi ("offentlig nøkkel-krypto")

Symmetrisk kryptografi



Alice vil sende Bob en melding uten at Eve kan lese den



Chifferteksten c skal være uforståelig hvis du ikke har nøkkelen

(Selv om du kjenner til krypteringsfunksjonen)

Eksempel (Cæsarchiffer)

Kryptering: Erstatt hver bokstav i meldingen med den som kommer k plasser senere i alfabetet

Dekryptering: Erstatt hver bokstav i chifferteksten med den som er k plasser tidligere i alfabetet

Nøkkel: tallet k

La m = CHÆRRITY
$k = 4$
c = GLBVVMXȦ

Merk: Cæsarchiffer er på ingen måte sikkert

Ikke pensum

Standardmetode: Advanced Encryption Standard (AES)

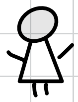
Utfordring: Alice og Bob må bli enige om en nøkkel

Løsning: tallteori!

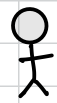
Diffie-Hellman nøkkelutveksling (DH)

Setup: alle kjenner til et primtall p og et grunntall g (base)

Alice



Bob



Velg $a \in \{2, \dots, p-2\}$ $\xrightarrow{A}$ Velg $b \in \{2, \dots, p-2\}$

Regn ut $A = g^a \bmod p$ $\xleftarrow{B}$ Regn ut $B = g^b \bmod p$

$$B^a \bmod p = (g^b)^a \bmod p = g^{b \cdot a} \bmod p = k$$

$$A^b \bmod p = (g^a)^b \bmod p = g^{a \cdot b} \bmod p$$

Eve ser p, g, A og B (men ikke a og b)
Hvis hun kan beregne $a = \log_g A \bmod p$ eller $b = \log_g B \bmod p$ kan hun beregne $k = g^{a \cdot b} \bmod p$

Enveisfunksjoner

DH-nøkkelutveksling er sikkert fordi modulær eksponensiering er en <u>enveisfunksjon</u>:

$$x \longrightarrow f(x) \text{ er lett}$$

$$f(x) \longrightarrow x \text{ er vanskelig}$$

$A = g^a \bmod p$ går raskt å regne ut for store tall

$a = \log_g A \bmod p$ er vanskelig å regne ut for store tall

En annen enveisfunksjon er multiplikasjon av store primtall p og q

$$p, q \rightsquigarrow n = p \cdot q \text{ går raskt}$$

$$n \rightsquigarrow p \text{ og } q \text{ er vanskelig}$$

Eksempel (Diffie-Hellman)

La $g = 2$ og $p = 13$
Anta at Alice trekker $a = 3$ og
Bob trekker $b = 7$

Da er $A = 2^3 \equiv 8 \pmod{13}$
$B = 2^7 = 128 \equiv 11 \pmod{13}$

Videre får vi at
Alice regner ut $B^a = 11^3 = 1331 \equiv 5 \pmod{13}$
Bob regner ut $A^b = 8^7 = 2097152 \equiv 5 \pmod{13}$

Hvordan finner vi dette raskt?

$$\frac{2097152}{13} = 161319 \text{ komma noe}$$

$161319 \cdot 13 = 2097147$, så $2097152 = 161319 \cdot 13 + 5$

Litt mer tallteori: Fermats lille teorem

Da vi regnet ut $3^{371} \bmod 5$ brukte vi at $3^4 \equiv 1 \pmod 5$ slik at $3^{4n} \equiv 1^n \equiv 1 \pmod 5$

Dette kan generaliseres!

Fermats lille teorem

La p være et primtall og la a være et heltall slik at $p \nmid a$

Da er $a^{p-1} \equiv 1 \pmod{p}$

Eksempel

$5^{16} \equiv 1 \pmod{17}$ og $3^{28} \equiv 1 \pmod{29}$

og $17^{28} \equiv 1 \pmod{29}$

Dette lar oss gjøre potensregning ganske raskt!

$12^{333} \bmod 31 = ?$

Først kan vi se at $12^{30} \equiv 1 \pmod{31}$

Vi har at $\frac{333}{30} = 11{,}1$

$30 \cdot 11 = 330 = 333 - 3$

$333 = 30 \cdot 11 + 3$

Det gir $12^{333} = 12^{30 \cdot 11 + 3} = (12^{30})^{11} \cdot 12^3$

$\equiv 1^{11} \cdot 12^3 \equiv 12^3 \equiv 1728 \equiv 23 \pmod{31}$

Men hva om modulusen ikke er et primtall?

Vi trenger et nytt verktøy: Eulers phi-funksjon (φ-funksjon) (eller Eulers totient-funksjon)

Den er definert slik:

$\varphi(n)$ = antall tall mellom 1 og n som er relativt primiske til n

Noen eksempler

For $n=1$ har vi at $\gcd(1,1)=1$ så $\varphi(1)=1$

For $n=4$ er 1 og 3 relativt primiske til 4, så $\varphi(4)=2$

For $n=5$ er 1, 2, 3, 4 relativt primiske til 5, så $\varphi(5)=4$

For n opp til 10 har vi

$$\varphi(1)=1 \quad \varphi(2)=1 \quad \varphi(3)=2 \quad \varphi(4)=2 \quad \varphi(5)=4$$

$$\varphi(6)=2 \quad \varphi(7)=6 \quad \varphi(8)=4 \quad \varphi(9)=6 \quad \varphi(10)=4$$

Kan se ut som at $\varphi(p)=p-1$ hvis p er et primtall (og det stemmer faktisk)

Vi kan beregne $\varphi(n)$ for alle n hvis vi kjenner primtallsfaktoriseringen til n

La $n = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_m^{k_m}$, eks $6860 = p_1^{k_1}\cdot p_2^{k_2}\cdot p_3^{k_3} = 2^2\cdot 5^1\cdot 7^3$

Da er

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

Symbolet $\prod$ er som summesymbolet $\sum$ bare med ganging

"stor pi"

Eksempel

$$\sum_{i=1}^{3} 2 = 2\cdot 1+2\cdot 2+2\cdot 3$$

$$\prod_{i=1}^{3}(i+1) = (1+1)\cdot(2+1)\cdot(3+1)$$

Hvis $n=6860=2^2\cdot 5^1\cdot 7^3$, får vi

$$\begin{aligned}
\varphi(n) &= \prod_{i=1}^{3}\left(p_i^{k_i}-p_i^{k_i-1}\right)\\
&= \left(p_1^{k_1}-p_1^{k_1-1}\right)\left(p_2^{k_2}-p_2^{k_2-1}\right)\left(p_3^{k_3}-p_3^{k_3-1}\right)\\
&= \left(2^2-2^1\right)\cdot\left(5^1-5^0\right)\left(7^3-7^2\right)\\
&= \underline{\underline{2352}}
\end{aligned}$$