11.16 Kryptografi

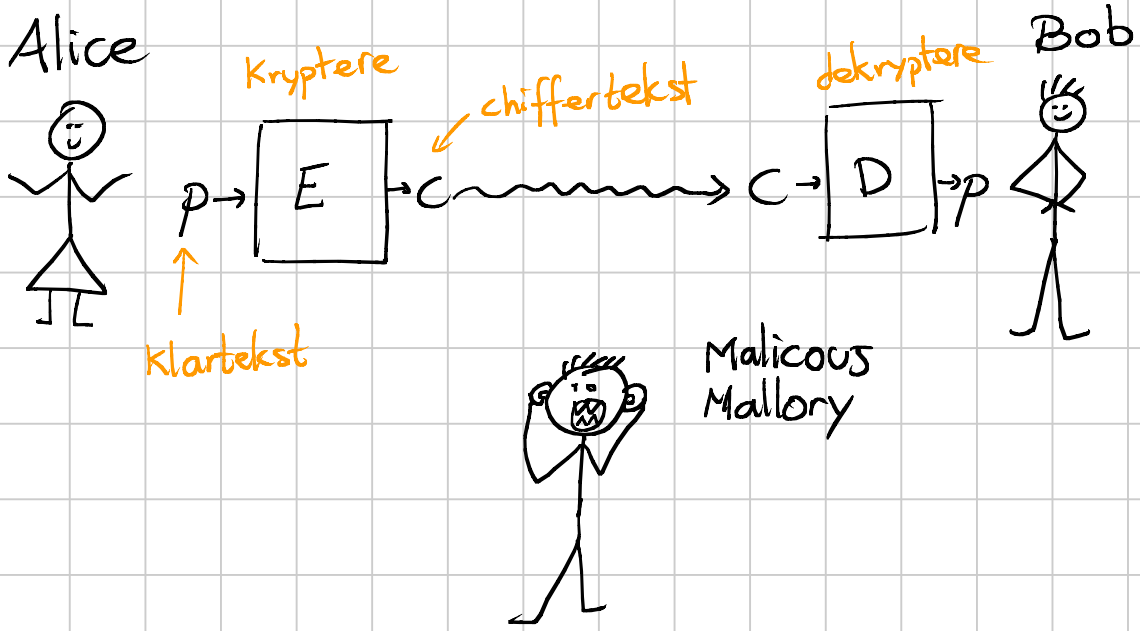
HØGSKOLEN I SØR-TRØNDELAG

I F N N F M J H N F M E J O H !

H E M M E L I G M E L D I N G

F S E V T N B S U ?

E R D U S M A R T ?



A	B	C	D	E	F	...	Y	Z
1	2	3	4				25	0

tabell 1

Hill-Chiffer

HØGSKOLEN I SØR-TRØNDELAG

① Velg en 2×2-matrise med heltallselementer

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

② Grupper klarteksten i par (+ evt. fyll, slik at antall tegn blir partall).
Bytt ut bokstav med numerisk verdi (tabell 1)

③ $E(p) = Ap = c$ for hvert par

④ Bytt ut tallene i hver c med bokstaver

Eksempel:

$$A = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix}$$

Klartekst: OL ER BRA

grupperer: OL ER BR AA (fyll)

15,12 5,18 2,18 1,1

krypterer: $p_1 = \begin{bmatrix} 15 \\ 12 \end{bmatrix}$ $p_2 = \begin{bmatrix} 5 \\ 18 \end{bmatrix}$ $p_3 = \begin{bmatrix} 2 \\ 18 \end{bmatrix}$, $p_4 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$$c_1 = Ap_1 = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix}\begin{bmatrix} 15 \\ 12 \end{bmatrix} = \begin{bmatrix} 252 \\ 123 \end{bmatrix} = \begin{bmatrix} 18 \\ 19 \end{bmatrix} \longrightarrow$$

$252 : 26 = 9$ (10, 18/26)
234
18

$123 : 26 = 4$
104
19

$$c_2 = Ap_2 = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix}\begin{bmatrix} 5 \\ 18 \end{bmatrix} = \begin{bmatrix} 238 \\ 167 \end{bmatrix} = \begin{bmatrix} 4 \\ 11 \end{bmatrix}$$

$\vdots$

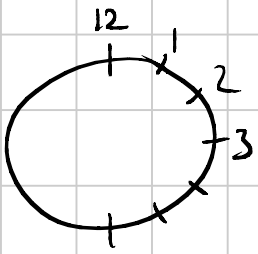
chiffertekst: 18 19 4 11

R S D K

Modulo-aritmetikk

$14 : 12 = 1$
12
2

$17 : 12 = 1$
12
5

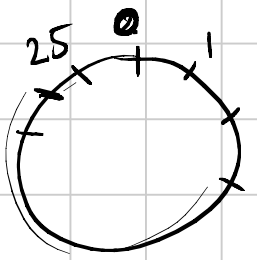


$27 = 1 \pmod{26}$

Def. $a = b \pmod{m}$ hvis $a - b = k \cdot m$, $k \in \mathbb{Z}$

△

$8 = 3 \pmod{5} \Leftrightarrow 8 - 3 = 1 \cdot 5$
$13 = 1 \pmod{2} \Leftrightarrow 13 - 1 = 6 \cdot 2$
$-4 = 9 \pmod{13} \Leftrightarrow -4 - 9 = (-1) \cdot 13$
$26 = 0 \pmod{13} \Leftrightarrow 26 - 0 = 2 \cdot 13$
$26 = 0 \pmod{26} \Leftrightarrow 26 - 0 = 1 \cdot 26$



$-4 = 22 \pmod{26}$

$-4 = 48 \pmod{26}$

$3 \cdot 3^{-1} = 1 \pmod{26}$

$3 \cdot 9 = 27 = 1 \pmod{26}$

a	1	3	5	7	...
a^{-1}	1	9			

Hvordan dekryptere $c = Ap$?

Gange med $A^{-1} \pmod{26}$: $A^{-1}c = A^{-1}Ap = p$

Når er A invertibel?

Korollar 11.16.4: En kvadratisk matrise A er inverterbar modulo 26 $\Leftrightarrow$ residuet til $\det(A)$ modulo 26 ikke er delelig med 2 eller 13.

$$A = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix}$$

$\det(A) = 8 \cdot 9 - 11 \cdot 1 = 61$

$61 = 9 \pmod{26}$

9 er ikke delelig med 2 el. 13, så A^{-1} eksisterer.

$9^{-1} = 3 \pmod{26}$

$$A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$$

$$= 3 \begin{bmatrix} 9 & -11 \\ -1 & 8 \end{bmatrix} = \begin{bmatrix} 27 & -33 \\ -3 & 24 \end{bmatrix} = \begin{bmatrix} 1 & 19 \\ 23 & 24 \end{bmatrix} \pmod{26}$$

sjekk: $AA^{-1} = I$:

$$AA^{-1} = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} 1 & 19 \\ 23 & 24 \end{bmatrix} = \begin{bmatrix} 261 & 416 \\ 208 & 235 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

ok.