Kryptografi

håndbog

Ordliste

Kryptografi (Kryptography)	Videnskab om kryp-tering og dechifrering af meddelelser.
Kryptering (Encryption)	Forvandler klartekst og meddelelsen til en chifferet tekst. Denne tekst skal være så, at den ikke er forståelig uden nøgle.
Dechiffrering/ Dekryptering (Decryption)	Ophæver krypteringen, altså fra en krypteret meddelelse og nøgle til klarteksten.
Meddelelse (Message)	Informationer, som skal nå frem fra senderen til mod-tageren.
Klartekst (Plaintext)	Den ikke-kodede meddelelse.
Chiffer (Cipher)	Den kodede meddelelse.
Nøgle (Key)	Hemmelig information, som kun afsende-ren/modtageren kender til. Den skal bruges for at kunne kryptere hhv.dechifrere
Bryde krypteringen (Breaking encryption)	Forsøg af en uvedkommende at få klarteksten uden dog at kende til nøglen.

Cæsar-skive

Kryptering

(Klartekst → Chiffer)

- Indstil **nøglen** på Cæsar-skiven.
- Udenfor: **Klartekst**-alfabet
- Indenfor: **Chiffer**-alafabet
- Aflæs på Cæsar-skiven for hvert klartekst-bogstav (**udenfor**) den chiffre-bogstav (**indenfor**) .

Dechifrering

(Chiffer → Klartekst)

- Indstil **nøglen** på Cæsar-skiven.
- Udenfor: **Klartekst**-alfabet
- Indenfor: **Chiffer**-alfabet
- Aflæs på Cæsar-skiven for hver chiffre-bogstav (**indenfor**) den dertil hørende klartekst-bogstav (**udenfor**).

Vigenère-tabel

Kryptering

(Klartekst → Chiffer)

- Skriv **meddelelsen** ind i meddelelseskolonnen.
- Skriv **nøglen** ind i nøglelinje

  (så mange gange efter hinanden, indtil der er tildelt et nøglebogstav til hvert bogstav fra meddelelsen).
- Oversæt hver enkel position ved hjælp af tabellen (Kolonne: **meddelelse**, linje: **nøgle**, skæringspunkt: **chiffer**,

  find skæringspunktet fra meddelelse og password)
- Skriv **resultatet** ind i chiffre-linjen.

Dechifrering

(Chiffer → Klartekst)

- Skriv **chiffre**-teksten ind i chiffre-linjen.
- Skriv **nøglen** ind i nøglelinjen

  (så mange gange efter hinanden, indtil der er tildelt et nøglebogstav til hvert bogstav fra meddelelsen)
- Oversæt hver enkel position ved hjælp af tabellen (kolonne: **meddelelsen**, linje: **nøgle**, skæringspunkt: **chiffer**,

  find så den kolonne, hvis skæringspunkt med nøglen er chiffre-bogstavet)
- Skriv **resultatet** ind i mededelelses-linjen.

Skytale

Kryptering

(Klartekst → Chiffer)

- Vælg en **cylinder**, denne er **nøglen**.
- Læg en papirstrimmel rundt om **cylinderen**.
- **Skriv på papirstrimlen langs længdeaksen**
- Tag strimlen af **cylinderen**, bogstaverne er så i en **blandet rækkefølge**.

Dechifrering

(Chiffer → Klartekst)

- Udvælg den rigtige **cylinder**.
- Læg den **beskrevne papirstrimmel** rundt om **cylinderen**.
- **Aflæs meddelelsen langs længdeaksen**.

Meddelelse:

Nøgle:

Chiffer:

Meddelelse:

Nøgle:

Chiffer:

Meddelelse:

Nøgle:

Chiffer:

Meddelelse:

Nøgle:

Chiffer: