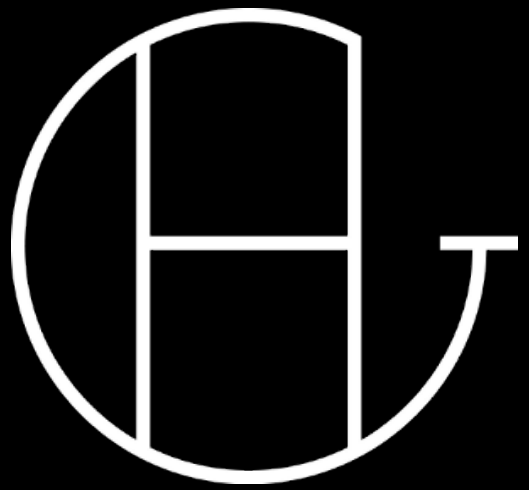


HoGent

BEDRIJF
EN
ORGANISATIE

Coding For Dummies

Jens Buysse

Inhoud

Cryptografie

Het woord cryptografie betekent letterlijk geheim schrijven of verborgen schrijven, het is voortgekomen uit de 2 griekse woorden

- kruptos en
- graphein

wat samen geheim schrijven betekent.

De eerste codes

Zowel de Romeinen als de Grieken verdiepten zich in de grondbeginselen van cryptografie.

- Optische signalen m.b.h.v. toortsen
- vlaggen
- spiegels
- ...

De eerste codes

Polybius

Code ontwikkeld door Griekse militair.

$$\begin{bmatrix} & 1 & 2 & 3 & 4 & 5 \\ 1 & A & B & C & D & E \\ 2 & F & G & H & I & J \\ 3 & K & L & M & N & O \\ 4 & P & Q & R & S & T \\ 5 & V & W & X & Y & Z \end{bmatrix}$$

Wat betekent volgend geheimschrift?

$$\begin{bmatrix} 12 & 53 & 34 & 54 & 15 & 43 & 51 & 12 & 11 & 15 \\ 53 & 34 & 44 & 54 & 32 & 51 & 21 & 53 & 23 & 41 \end{bmatrix}$$

Polybius

Er werden twee reeksen van fakkels opgesteld:

1. Eerste 5 fakkels duiden de rij aan
2. Tweede 5 fakkels duiden de kolom aan

Aenas' Telegraaf

Aenas' Telegraaf

1. Partij A heft een brandende fakkel
2. Partij B heft ten antwoord ook een brandende fakkel
3. Partij A laat fakkel zaken en kranen worden open gezet
4. Partij A heft opnieuw brandende fakkel op zodat kranen gesloten kunnen worden.

Caesarscode

Elke letter wordt vervangen door de letter die een afgesproken aantal plaatsen (bv. 3) verder in het alfabet staat.

Code

EDG LV D SODQ ZKLFK FDQQRW EHDU D FKDQJH

Caesarscode - zwaktes

Wat zijn de zwaktes van deze codering en hoe zou je deze aanpakken?

Caesarscode - zwaktes

Wat zijn de zwaktes van deze codering en hoe zou je deze aanpakken?

- Biedt slechts 25 mogelijkheden tot versleuteling. (Computer kan dit makkelijk kraken)
- De letter E komt heel erg vaak voor in de taal. Door te tellen welke letter het meest voorkomt kan je al goed raden wat de E zal zijn.
- Je weet ook al wat de woorden zijn.

Code

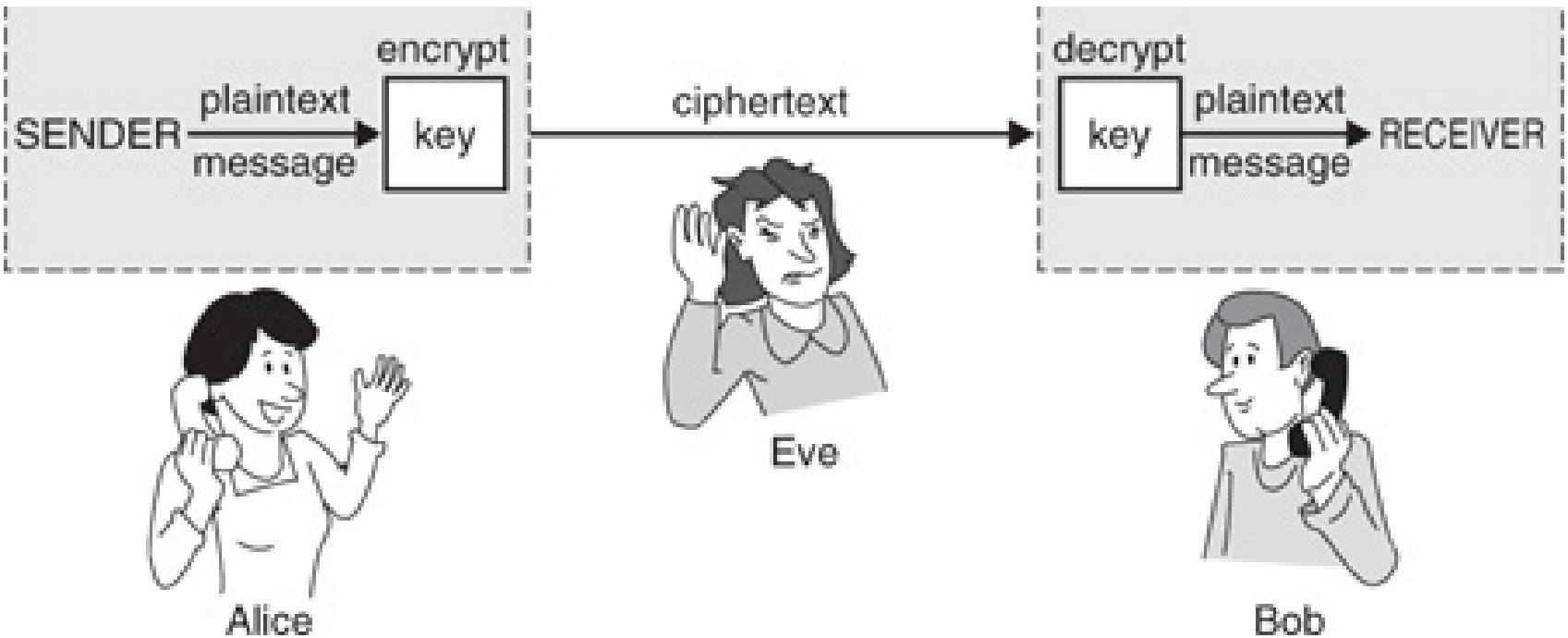
ROHXD VDBCK ANJTC QNUJF MXRCC XBNRI NYXFN ARWJU UXCQN ALJBN BXKBN AENRC

Scytale

Code

ANACD DEIOR SUTWB AOTIR FNSUE ELNTF EHRMA IYNE

Adam, Alice & Eve



Cryptografieindeling

Symmetrisch Wanneer de sleutel om te versleutelen en ontsleutelen dezelfde is. Versleuteling kan enkel veilig gebeuren wanneer er een veilige sleuteluitwisseling tussen Alice en Bob gebeurd is.

Assymetrisch Of ook publieke sleutel cryptografie waarbij het versleutelen en ontsleutelen met een verschillende sleutel moet.

We merken op dat hedendaagse versleutelingsmechanismen vaak geen gelaagde combinatie van bovengenoemde types zijn.