Cryptografie

Inhoudsopgave

Wat is cryptografie?

- Cryptografie is de wetenschap van het geheimschrift met als doel het verbergen van de betekenis van berichten

Geschiedenis cryptografie

- Het oude Egypte (1900 v. Chr.): Hiërogliefen (onduidelijk)
- Grieken (1900 v. Chr.)
- De tijd van Caesar (100 v. Chr. – 44 v. Chr.): Caesar-encryptie

Hiërogliefen

Caesar-encodering

- Encryptie op basis van substitutie

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- Vervang letter in de bovenste regel met letter in onderste regel

N=-5

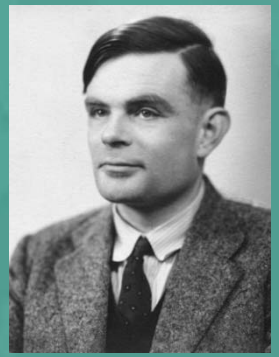
Origineel	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Gecodeerd	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

N=3

Origineel	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Gecodeerd	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Moderne cryptografie

- Tweede Wereldoorlog
  - Meest bekende codeermachine: ‘Enigma’ (in 1920 ontwikkeld)
  - Gebruikt door nazi’s
  - Eerst gekraakt door Polen
  - Toen door Britten
  - Sleutelfiguur: Alan Turing



Alan Turing

Enigma codeermachine

Moderne cryptografie

- Tegenwoordig veel manieren
- Belangrijk voor onder andere internetbankieren en spionage
- Complexe technieken maken veel gebruik van wiskunde en kansberekening

Oefening andere methodes

- Maak nu op Wikiwijs/hand-outs de opdrachten behorend bij “Caesarversleuteling”
- Lees hierna de stof behorend bij de andere drie methodes: “Patroon”, “Sleutelwoord” en “Kolomwissel”. Maak ook de bijbehorende opdrachten

Missie: Brief

- Jullie hebben een brief ontvangen van het hoofdkantoor. Deze brief moet je met je team ontcijferen. De brief en mogelijke manieren om deze te ontcijferen zijn te vinden op Wikiwijs/hand-out.