Cyber security les 1

Introductie, Toetsing en Ciphers

Nova College

Programma

- Introductie
- Toetsing
- Lessenopbouw
- Ciphers

Introductie: cyber security

- Waar denken jullie aan bij Cyber security?

Introductie: cyber security

- De onderwerpen:
  - Encryptie
  - Algorithmes
  - Wetgeving
  - Awareness
  - Data
  - Netwerken
  - Hacking
  - Social enigneering
  - En meer…

Toetsing – 2 delig

- Set encryptie en beveiliging opdrachten – Voorwaardelijk
  - Ciphers opdracht
  - Hashing opdracht
  - JWT opdracht
  - Database injection Opdracht
  - Wachtwoorden opdracht

- Cyber security examen - Schriftelijk

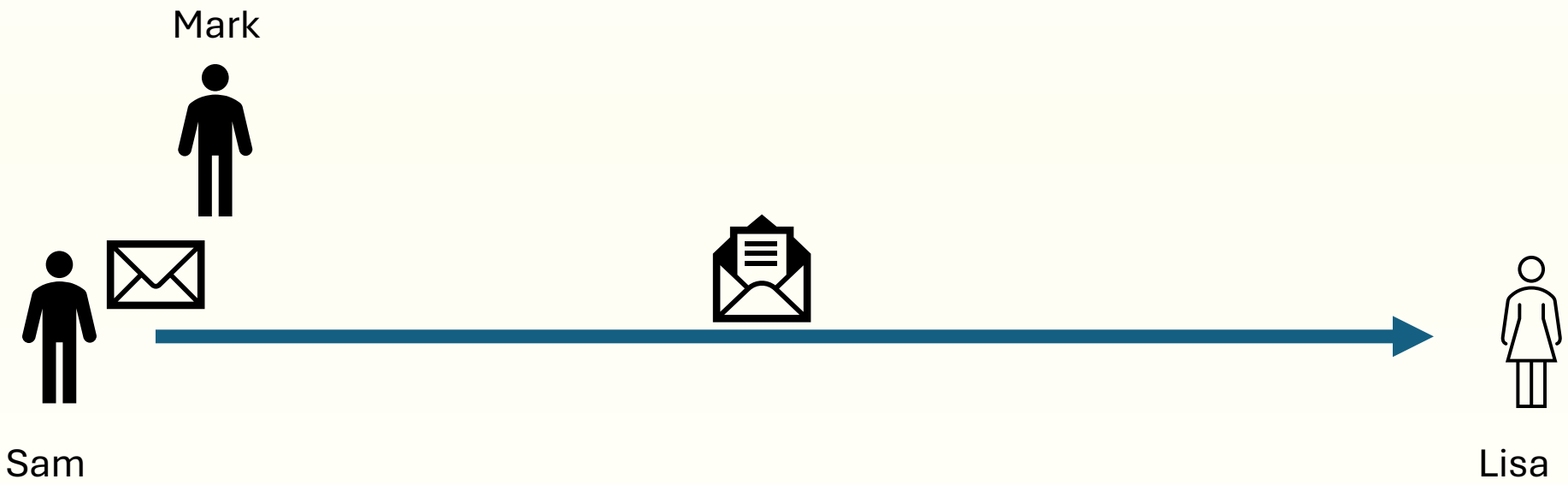
Lesopbouw

1. Terugblik
2. Theorie
3. Tussenopdracht/demo
4. Vervolg Theorie
5. Programeeropdracht / zelfstudie
6. Afsluiten

Leerdoelen

- Aan het einde van de les
  - Weten we wat Cyber security in gaat houden
  - Weten we hoe Cyber security getoets gaat worden
  - Hebben we kennis van Atbash ciphers
  - Hebben we kennis van caesar ciphers
  - Hebben we kennis van Vignere ciphers
  - Kunnen we Ciphers toepassen in code

Berichten versturen !



Ciphers – Atbash (Hebreeuws)

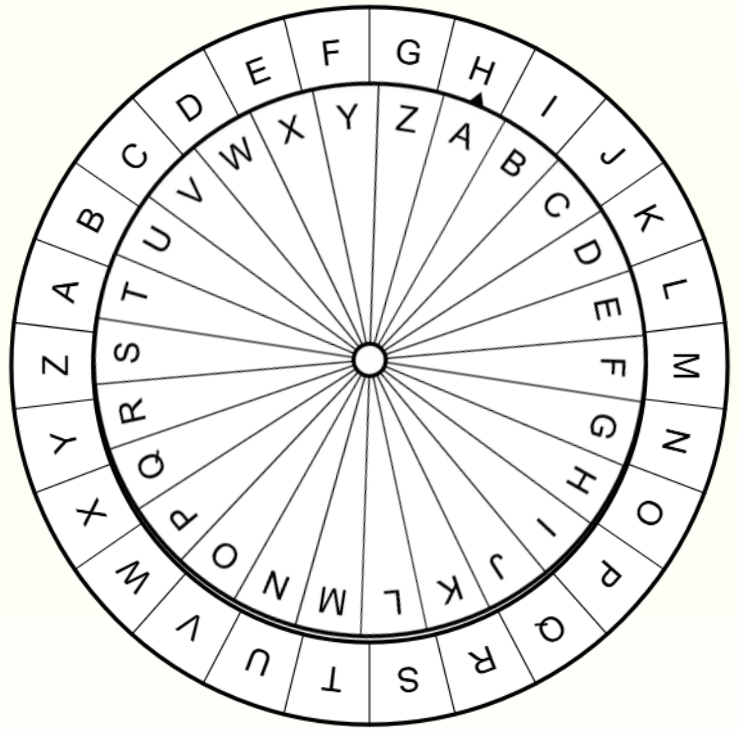
- Het alfabet omdraaien en dan herschrijven in de nieuwe vorm.
- Dit zorgde ervoor dat niemand de tekst snel kon lezen.

- Hallo = SzooL
- Mario = NziRl

Te makkelijk

Ciphers – Caesar (Romeins)

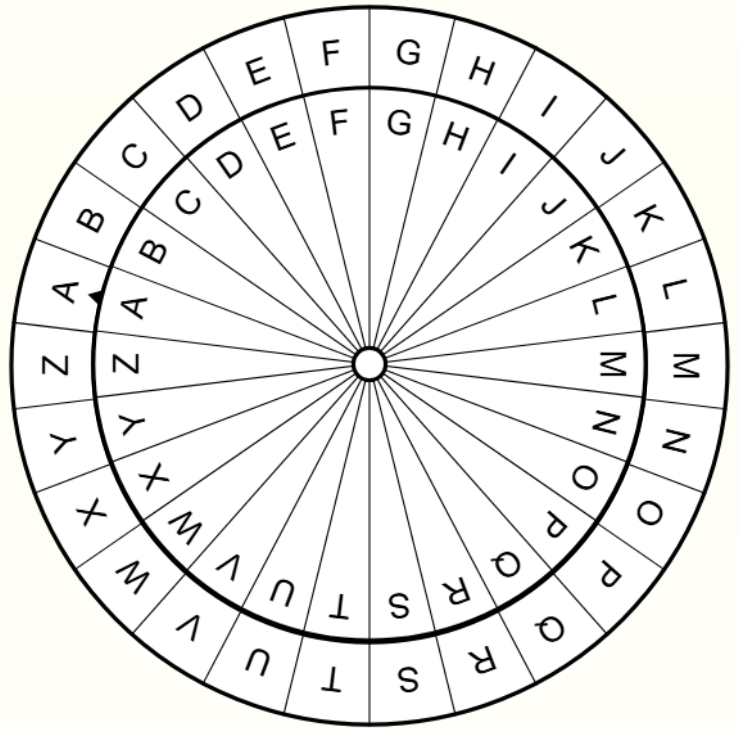
- Niet uitgevonden door caesar maar wel populair gemaakt.
- Een bericht kond nu in plaats van 2 versies, nu 26 versies hebben.
- De shift werd van te voren afgesproken of gedeeld met het bericht.
- Een shift van 7 leverde op:
- Hallo = Ohssv
- Mario = Thypv



Ciphers – Caesar - zelf proberen

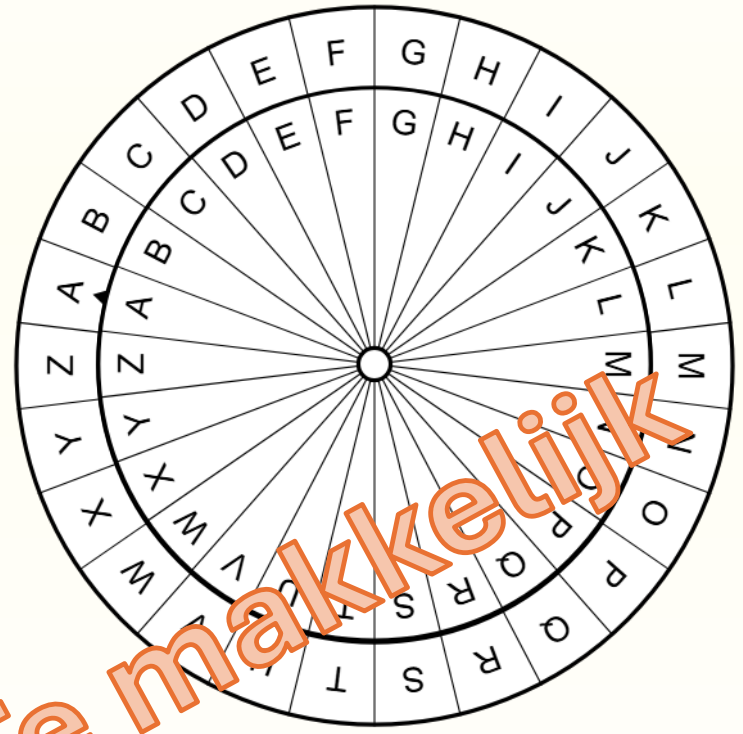
- Codeer:
- Ik kwam, ik zag, ik won (shift 8)
- Cleopatra (Shift 4)

- Decodeer:
- Oxmbizdso sc cswzov (Shift 10)
- Ijhwduynj xtrx snjy (Shift 5)



Ciphers – Caesar (Romeins)

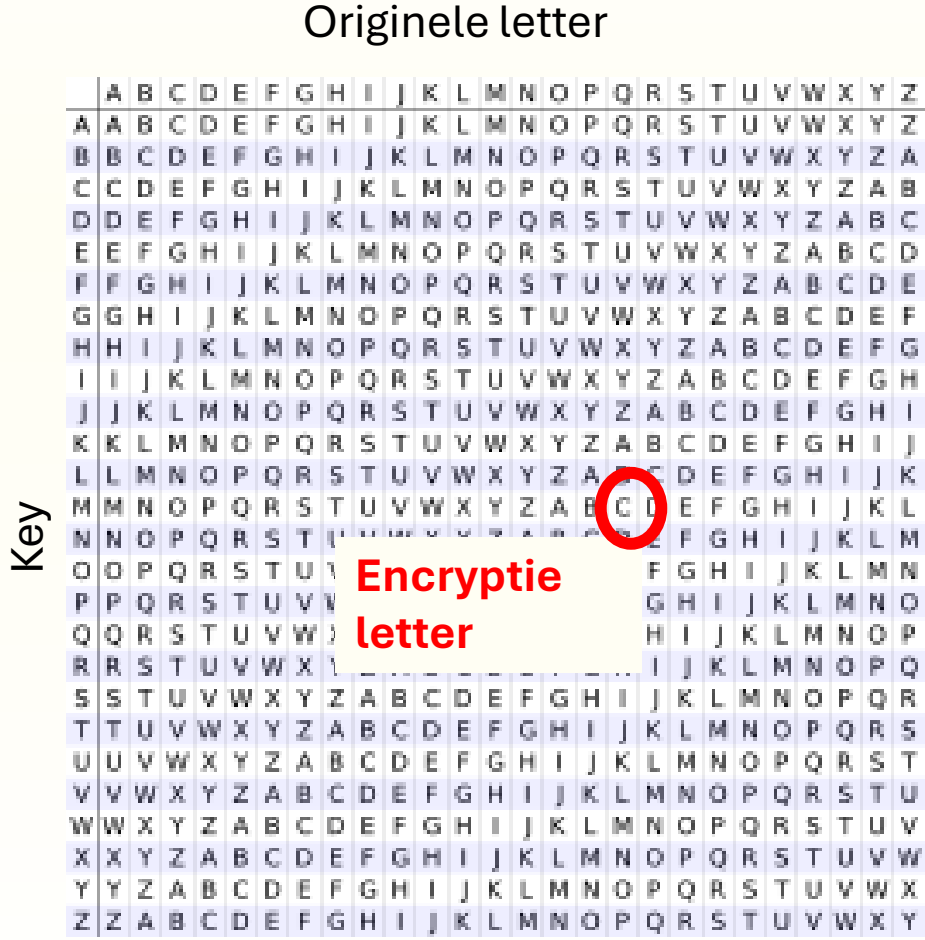
- Niet uitgevonden door caesar maar wel populair gemaakt.
- Een bericht kond nu in plaats van 2 versies, nu 26 versies hebben.
- De shift werd van te voren afgesproken of gedeeld met het bericht.
- Een shift van 6 leverde op:
- Hallo = Ohssv
- Mario = Thypv



Te makkelijk

Ciphers – Vignere (Italiaans/Frans)

- Bedacht door een Italiaan en populair gemaakt door een Franse diplomaat.
- Encryptie stappen:
  1. Kies een key (een woord van 5 of meer karakters lang)
  2. Eerste letter van je originele bericht bovenin aanstippen
  3. Eerste letter van de key aanstippen aan de zijkant
  4. Letter op het kruispunt is je cipher letter
  5. Herhaal dit tot je key op is en begin opnieuw met de key
- Decryptie stappen:
  1. Zoek de eerste letter op de key
  2. Kijk door de rij heen tot je de eerste letter van de encryptie kan vinden
  3. Kijk in welke column je zit, dit is de letter van het originele bericht
  4. Herhaal dit tot je het gehele bericht hebt



Nova College

Ciphers – Vignere – zelf proberen

- Encryptie:
  - Key: Nacht
  - Bericht: Sneeuw vanavond

- Decryptie:
  - Key: Vignere
  - Cipher: Ymiecgxdm qnr yizt rnrx hpzka

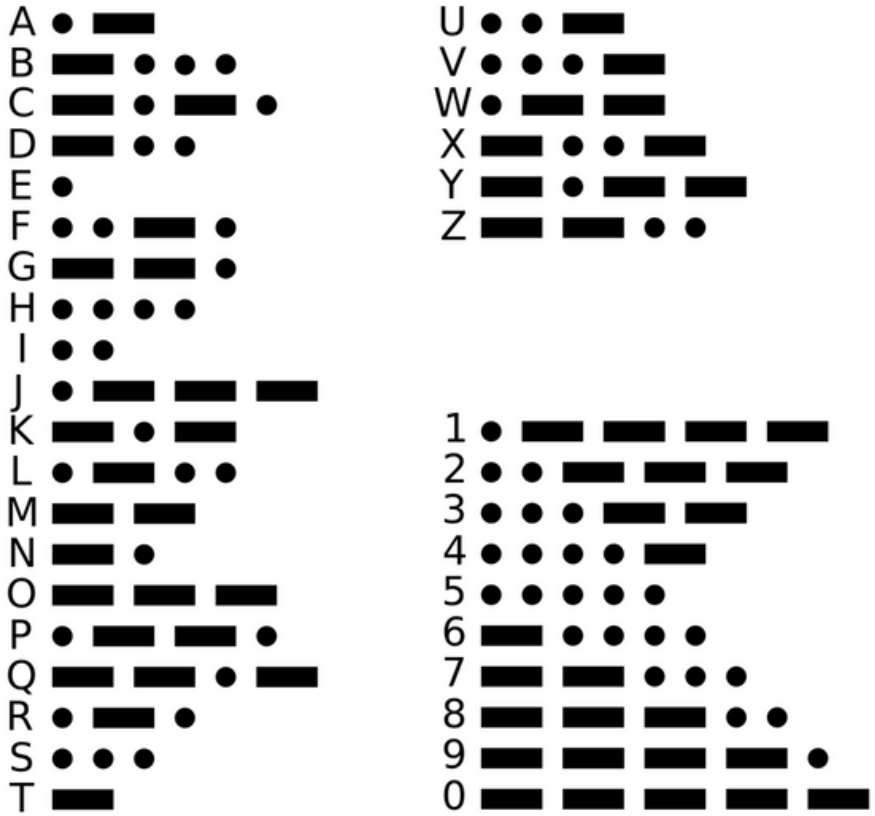
Originele letter

Key

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

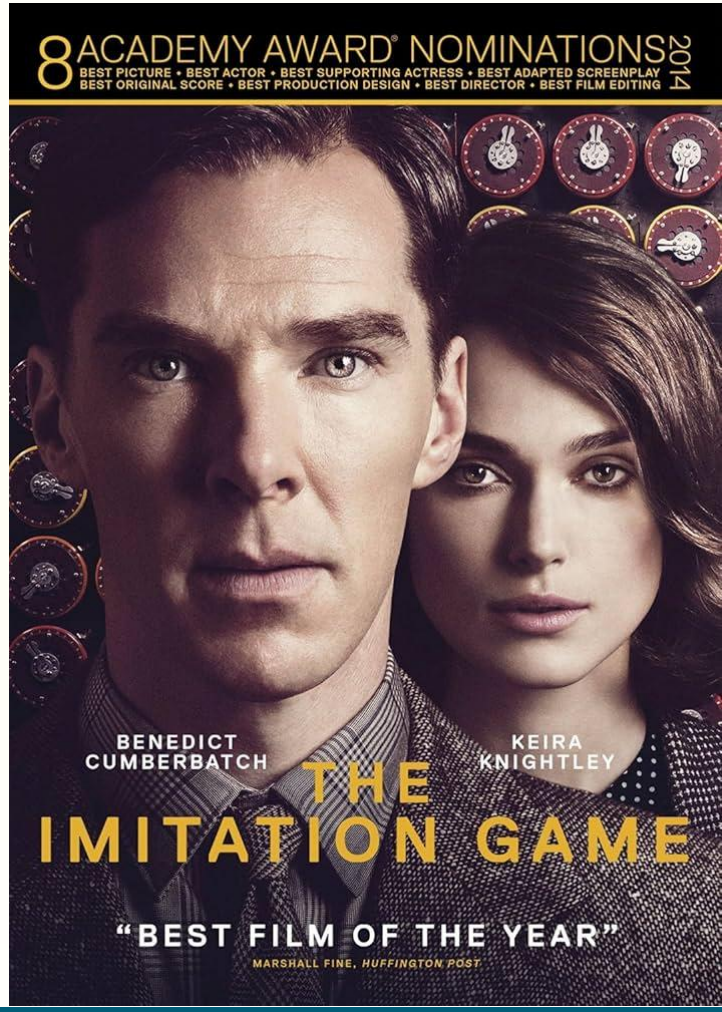
Andere ciphers en vroege methodes zijn:

- Morse code
- Bitwise / Bacon
- Numeral
- Enigma



Film aanrader: The imitation game

- WW2 film over het breken van de enigma code
- Gaat ook over Alan Turing, de grootvader van IT



Nova College

Programeer opdrachten

- Kijk op de Dummymeneer GitHub voor de opdrachten van Cyber security en de slides
- Hier komen ook extra materialen op te staan om te helpen met het examen.
- https://github.com/DummyMeneer/Cyber-Security

Volgende week:

- Beveiliging
- Algorithmes
- Encryptie
  - Hashing
  - RSA