

# Cryptografie & geheimschrift: hoe computers en chips met elkaar praten

Ingrid Verbauwhede  
Computer Security & Industrial Cryptography  
Departement Elektrotechniek  
K.U.Leuven



## Outline

- Geheimschrift voor computers en chips: waarom?
- Voorbeelden voor mensen
- Voorbeelden voor computers
- Een paar moeilijke woorden
  - Cryptografie
  - Substitutie
  - Transpositie

## Geheimschrift

- Cryptography = κρυπτός + γράφω  
cryptos + grafo = 'verborgen' + 'schrijven'
- Waarvoor gebruik je dit?

**Verbergen van informatie:  
tekst, muziek, data**

**Op slot zetten zodat je het kan openen  
*alleen* als je de juiste sleutel hebt!**

## Sloten



**Mechanische wieltjes  
Geheime code: 4 cijfers**

**Hoeveel mogelijkheden?**

**10.000**



**Elektronische berekeningen  
Geheime code: 64 bits**

**Hoeveel mogelijkheden?**

**10.000.000.000.000.000.000**

## Elektronische sloten



## Wat moet zo'n slot kunnen?

Tekst geheimhouden

Betaal Bob €10

Getekend: *Anna*

Tekst niet wijzigen: €10 of €10000

Tekst niet kopiëren

Tekst ondertekenen  
- Digitale handtekening

Betaal Bob €10000

Getekend: *Annabel*

En nog meer. . .

## Geheimhouden en tóch informatie??

- 10 vrijwilligers
- De 1ste kiest een willekeurig getal tussen 20 en 100
  - Heb je een leuke juf/meester voor wiskunde? = plus 1
  - Is de wiskunde juf/meester nogal saai? = plus 0
- We fluisteren dit in het oor van de volgende
- De laatste fluistert het resultaat terug in het oor van de 1ste.
- De 1ste trekt het willekeurig getal af van het resultaat en zegt het resultaat luidop.
- Resultaat: XXX op 10 vinden de juf of meester leuk !!

***Niemand heeft zijn persoonlijk antwoord aan de juf gezegd !!***



### PROTOCOL

## Hoe maak je zo'n code?





## Opgave:

IJ PNSIJWZSNAJWXNYJNY NX XZUJW!

□□ □□□□□□□□□□□□□□□□ □□ □□□□

Welke sleutel ???  
Hoe gevonden???

*Moeilijk woord: frequentie analyse*

## Vigenère cijfer

Frequentie analyse is te gemakkelijk

Kies een codewoord: *timo (19-8-12-14)*

Herhaal het code woord

AfspraakOmMiddernacht  
timotimotimotimotimot  
.....



Blaise de Vigenère (1523 - 1596)

## Alle Caesar cijfers onder elkaar

- 0 ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 1 BCDEFGHIJKLMNOPQRSTUVWXYZA
- 2 CDEFGHIJKLMNOPQRSTUVWXYZAB
- 3 DEFGHIJKLMNOPQRSTUVWXYZABC
- ...
- 25 ZABCDEFGHIJKLMNPOQRSTUVWXYZ

## Tabula recta

Afspraak  
+ timotimo  
= tnedkimy

*Hoe breken?*

*Frequentie  
Analyse  
Maar moeilijker*

	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

## Onbreekbaar! Vernam cijfer

**Truk: maak de code evenlang als de tekst  
Code moet bestaan uit willekeurige letters**

**Bv.: de tekst uit een boek (niet echt willekeurig...)**

AfspraakOmMiddernachtAanSchoolpoort...  
LangGeledenToenDeDierenNogSprakenWo  
.....

## Transpositie

- Tot nu toe alleen 'substitutie'
- = Letter vervangen door andere letters
- Transpositie = letters door elkaar mengen
- Voorbeeld:

KOE  
KEO  
OKE  
OEK  
EOK  
EKO

CODE  
COED  
CDOE  
CDEO  
CEOD  
CEDO  
OCDE  
OCED

...

## Hoe doen chips en computers dat nu?

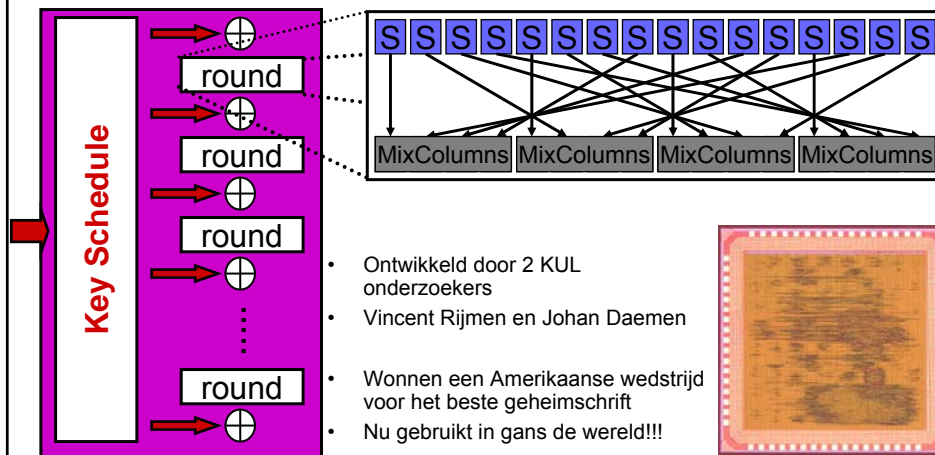
- Computers tellen met 0 en 1

$$\begin{array}{r} 7 \\ + 5 \\ \hline = 12 \end{array}$$

$$\begin{array}{r} 0111 \\ + 0101 \\ \hline = 1100 \end{array}$$

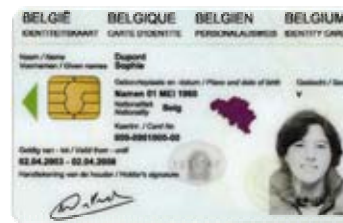
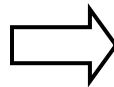
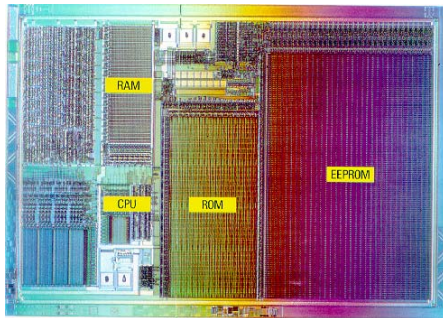
- Verder doen ze hetzelfde: substitutie en transpositie
- Substitutie = cijfers vervangen door andere
- Transpositie = cijfers door elkaar halen

## Voorbeeld: Rijndael



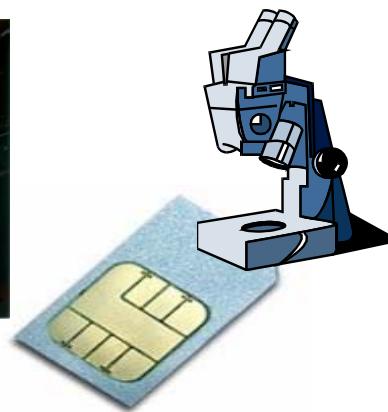
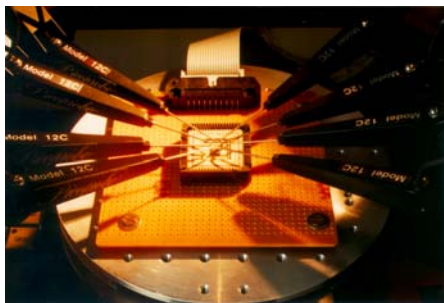
- Ontwikkeld door 2 KUL onderzoekers
- Vincent Rijmen en Johan Daemen
- Wonnen een Amerikaanse wedstrijd voor het beste geheimschrift
- Nu gebruikt in gans de wereld!!!

## Chip voor een slimme kaart



## Worden chips ook gebroken?

**JA, spijtig genoeg,  
maar we proberen het moeilijk te maken...**



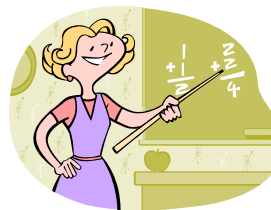
## Wat waren de moeilijke woorden?

- Cryptografie
- Substitutie
- Transpositie
- Frequentie analyse
- Protocol



## Wat moet je studeren?

- Op school: rekenen en wiskunde
- Wetenschappen
- Taal
- Creatief zijn!
- Nieuwsgierig zijn!



- Ingenieur is iemand die:  
*Nieuwsgierig is om te weten hoe en waarom iets werkt*  
*Creatief om nieuwe oplossingen te vinden*