Topic: the secret is the key

Spreker: Han Vinck

Senior Professor in Digital Communications, Univ. Duisburg-Essen

UNIVERSITÄT DUISBURG ESSEN

Open-Minded

mijn vakgebied – de digitale kommunikatie –

= binair (met symbool 0 of 1) overdragen van DATA

Kwaliteit: fouten-correctie

Betrouwbaar: authentiek, geheim, veilig, …

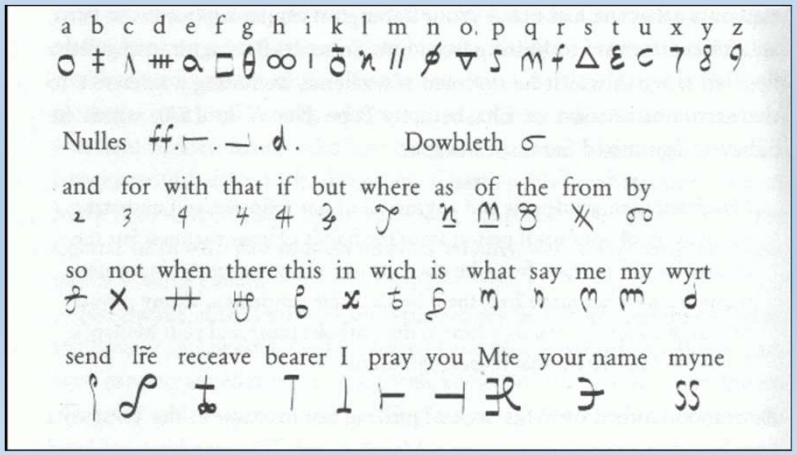
Efficient: alleen noodzakelijke informatie

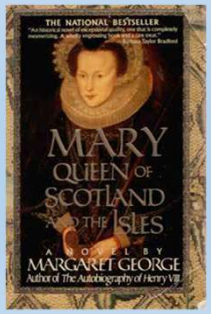
Data reduction/compression

Twee „geheim“ schrijf-principes: stegano- & cryptography

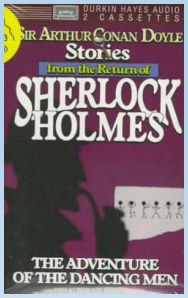
An ancient example is that of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden.

Stegano-graphy = **verborgen** schrijven





Crypto-graphy = **geheim** schrijven

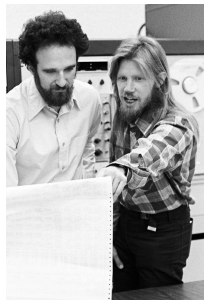


Inhoud voordracht

- 2 Klassieke versleutel (vercijfer – crypto) principes met **één** geheime sleutel
  - substitutie (vervangen) en transpositie (verplaatsen)

- DE doorbraak (1976) voor veilige communicatie in grote netwerken: Public-Key
  - „Publiek  Privé“

sleutel paar



Diffie-Hellman

2 Klassieke vercijferings principes met één sleutel

- van leesbaar naar onleesbaar - met **een** geheime sleutel (algorithme) - door

- **Substitutie**(vervangen) w o r s t => x p d r t => w o r s t

- **Transpositie**(verplaatsen) w o r s t => o t w s r => w o r s t

versleuteld kommuniceren met één gemeenschappelijke geheime sleutel

Zender en ontvanger hebben **dezelfde** geheime sleutel (hoe?)

Leesbaar

vercijfer

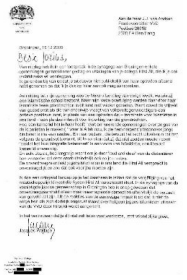
zender

Versleuteld onleesbaar

afluisteraars

ontcijfer

ontvanger



Leesbaar

Diplomatieke veilige (*perfecte zekerheid*) kommunicatie

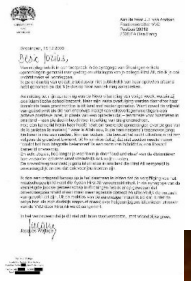
Eerst de sleutel

versleuteld

tekst

Bij eenmalig sleutel gebruik: **perfecte zekerheid** haalbaar!(one-time pad, **Vernam cypher**)
Iedere dag: sleutel transport van Washington naar Moscow, en v.v.
Perfekte zekerheid: Versleutelde data geeft geen informatie over het oorspronkelijke bericht.

Diplomatieke veilige (*perfecte zekerheid*) kommunicatie

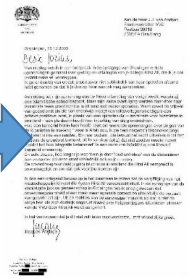


versleuteld

tekst

na aankomst koerier de versleutelde tekst (cryptogram)

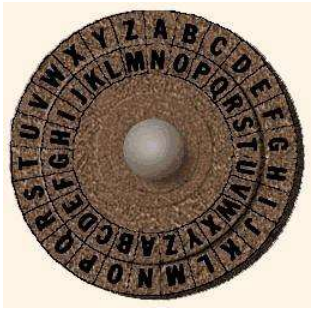
versleuteld



tekst

Bij eenmalig sleutel gebruik: **perfecte zekerheid** haalbaar!(one-time pad, **Vernam cypher**)
Iedere dag: sleutel transport van Washington naar Moscow, en v.v.

crypto-graphie => geheim schrijven is al duizenden jaren oud*



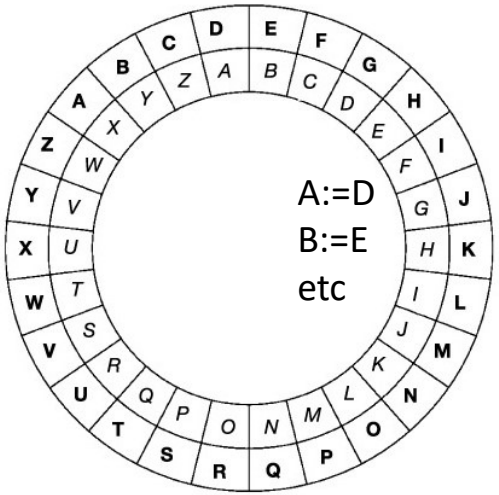
Egypte Griekenland ROME Amerika Duitsland

en Belgie, nu (1997) wereld standaard

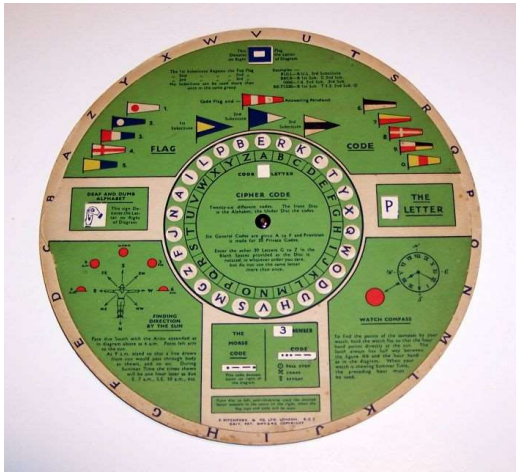
AES encryption

Met gebruikt vervanging (substitutie) en verplaatsing (diffusion)

Doel: verwarring



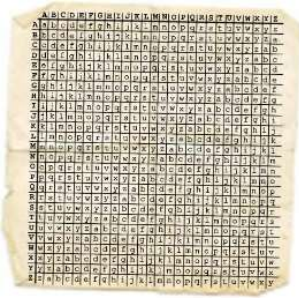
Caesar disk (simpel)

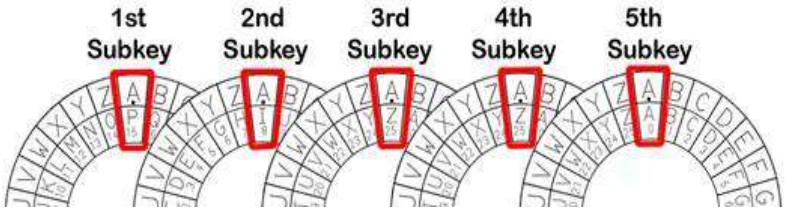


Boys scout wheel

Vigenere, 1573

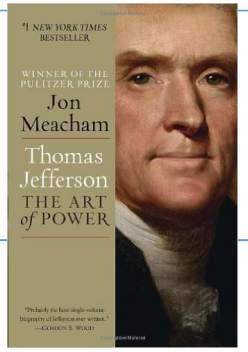
Simpele
Implementatie
Gemakkelijk
voor de soldaten





Multi-disk system (PIZZA)

Moeilijker: Jefferson machine

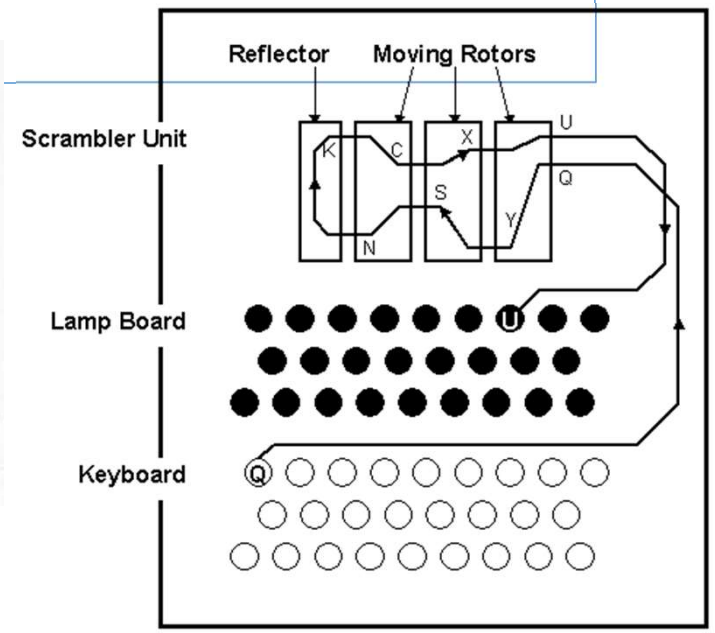


- Uitvinder: Thomas Jefferson, 3e President van de USA (1801–1809) - in 1795,
- Gebruikt door het USA leger van 1923 tot 1942

- versleutelen: draai **tekst** voor en stuur **willekeurige andere regel** (**code**)
- ontsleutelen: draai **code** voor en **zoek leesbare tekst** (D H I Y A I W M J K)
- **Waar zit het geheim**? (*= positie van de disks*)

Een bekend apparaat uit WII: nog moeilijker

One of the rarest surviving *Enigma* cipher machines has sold at *auction* for a record price of US$ 463 500.-



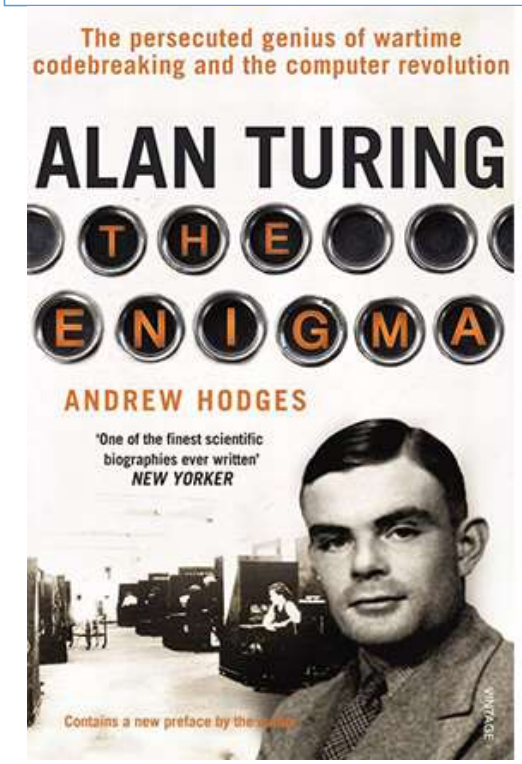
Q.=Y:=S:=N:=K:=C:=X:=U

Werkt als km teller

<u>Geheim:</u> positie disks en startpositie

General Heinz Wilhelm Guderian, *Schneller Heinz*, in zijn commandopost met een **<u>Enigma</u>**-apparaat tijdens de invasive van Frankrijk in 1940.

Enigma *(raadsel)* oplossing door Alan Turing (1912-1954) grondlegger informatica – kunstmatige intelligentie

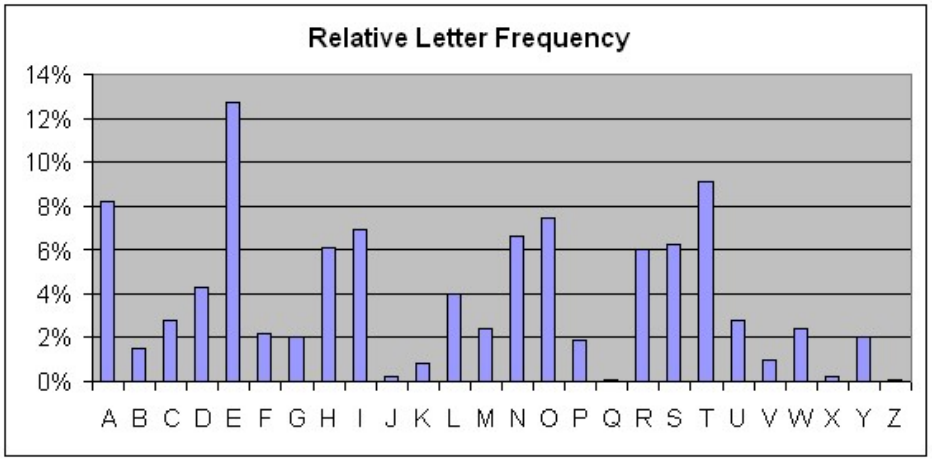


Marian Rejewski

het oorspronkelijke **„kraak“** idee komt van <u>poolse</u> wiskundigen

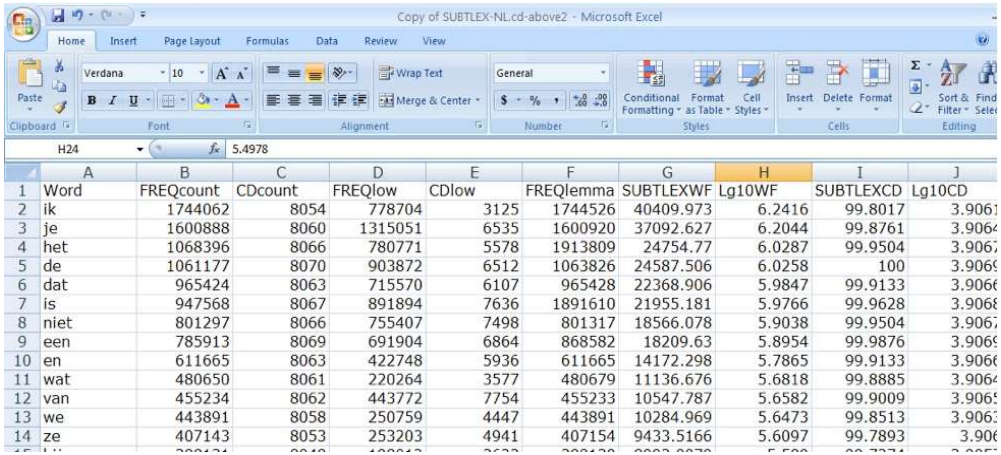
<u>Geheim</u>: positie disks en startpositie

Door o.a. gebruik te maken van statistiek en bekende woorden in tekst vindt de vijand de sleutel (met vriendelijke groet, heil H.....)!



Tellen:

Het weer is niet best: e: 5, t: 3, i: 2, s: 2



	A	B	C	D	E	F	G	H	I	J
1	Word	FREQcount	CDcount	FREQlow	CDlow	FREQlemma	SUBTLEXWF	Lg10WF	SUBTLEXCD	Lg10CD
2	ik	1744062	8054	778704	3125	1744526	40409.973	6.2416	99.8017	3.9061
3	je	1600888	8060	1315051	6535	1600920	37092.627	6.2044	99.8761	3.9064
4	het	1068396	8066	780771	5578	1913809	24754.77	6.0287	99.9504	3.9067
5	de	1061177	8070	903872	6512	1063826	24587.506	6.0258	100	3.9069
6	dat	965424	8063	715570	6107	965428	22368.906	5.9847	99.9133	3.9066
7	is	947568	8067	891894	7636	1891610	21955.181	5.9766	99.9628	3.9068
8	niet	801297	8066	755407	7498	801317	18566.078	5.9038	99.9504	3.9067
9	een	785913	8069	691904	6864	868582	18209.63	5.8954	99.9876	3.9069
10	en	611665	8063	422748	5936	611665	14172.298	5.7865	99.9133	3.9066
11	wat	480650	8061	220264	3577	480679	11136.676	5.6818	99.8885	3.9064
12	van	455234	8062	443772	7754	455233	10547.787	5.6582	99.9009	3.9065
13	we	443891	8058	250759	4447	443891	10284.969	5.6473	99.8513	3.9063
14	ze	407143	8053	253203	4941	407154	9433.5166	5.6097	99.7893	3.906

Hoe vaak worden Nederlandse woorden gebruikt?

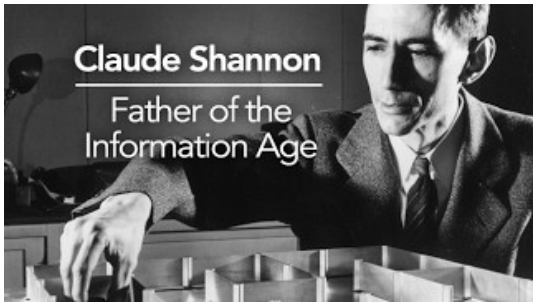
Marc Brysbaert Emmanuel Keuleers
Vakgroep Experimentele Psychologie, Universiteit Gent

Note: korte woorden komen vaak voor (efficiente codering!)

Hoeveel samenhang (redundantie, overbodige letters) zit er in tekst

Klassieke ontcijferingsmethoden
zijn op aanwezige samenhang gebaseerd

- D.z. T.kst k.nt . W..rsch..nl..k w.l l.z.n



Claude Shannon

(≈ 4/5 van de tekst kun je weglaten)

Echter: moderne data (0 of 1) is vaak geen tekst!

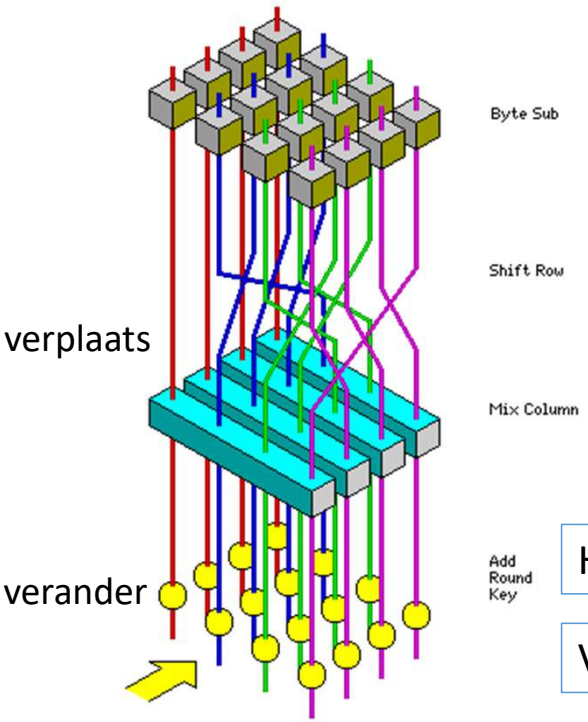
Een ander „klassiek“ principe: transpositie (diffusion)

- Letters van plaats verwisselen: transpositie

- Doel: (diffus …nen) eruit te halen

Voorbeeld:

Moderne systemen gebruiken ook substitutie en transpositie: Rijndael cipher uit Leuven, een **wereldstandaard** sinds 1997!



Universitaire innovatie van Vincent Rijmen en Joan Daemen .

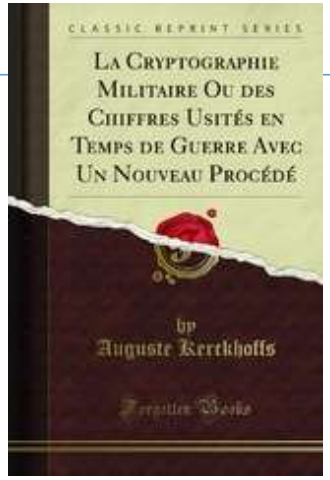
Hun algoritme is gekozen vanwege de combinatie van veiligheid, prestatie, efficiëntie, eenvoud en flexibiliteit. (verslaat IBM, Intel, ...)

Het algorithme is openbaar! **De sleutel is geheim!**

Het is de opvolger van de DES standaard (*complexiteit 10**16.8*)

Voorbeeld: 128 bits bericht versleuteld met 128 bits geheim (*complexiteit 10**38.4*)

BELANGRIJK: de machine (methode) is openbaar, de sleutel is geheim
- *Kerckhoffs principle* -



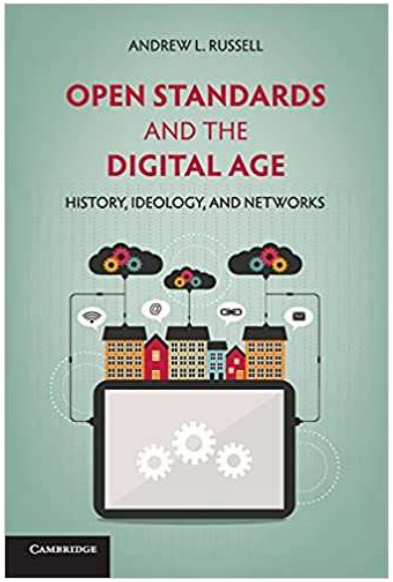
Waar blijft de sleutel?

Veilig, zelfs met openbaarheid van de machine (methode)

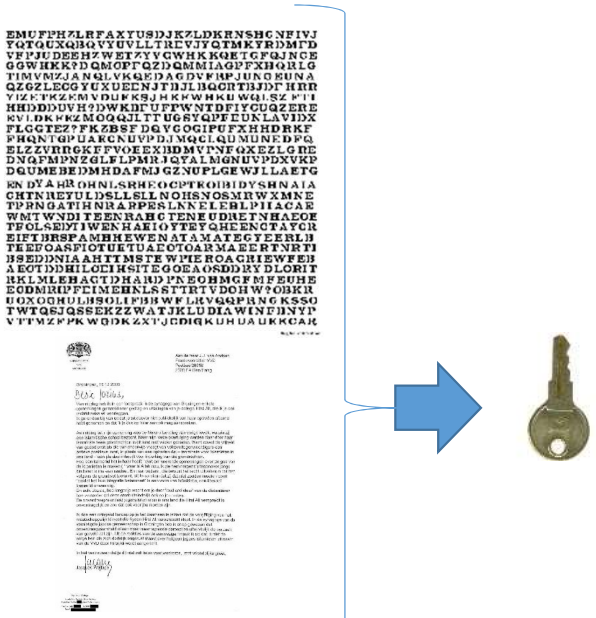
Auguste Kerckhoffs (1835–1903) was a Dutch linguist and cryptographer who was **professor of languages** at the École des Hautes Études Commerciales in Paris in the late 19th century.
Kerckhoffs was born in Nuth, the Netherlands, as **Jean Guillaume Auguste Victor François Hubert Kerckhoffs**, son of Jean Guillaume Kerckhoffs, mayor of the village of Nuth, and Jeanette Elisabeth Lintjens.

Why a public “open” standard is safer?

- **open to reviews and auditing from security experts all over the world**
- **greater interoperability & flexibility**
- **Free for all to implement, with no royalty or fee**
- **Interesting: Commercially, Technically and Judicial**
- **Can have a certificate**
- **security without the limits of a proprietary algorithm.**



Het afluister probleem



vercijfer machine

Known plaintext – ciphertext attack

Versleuteld onleesbaar

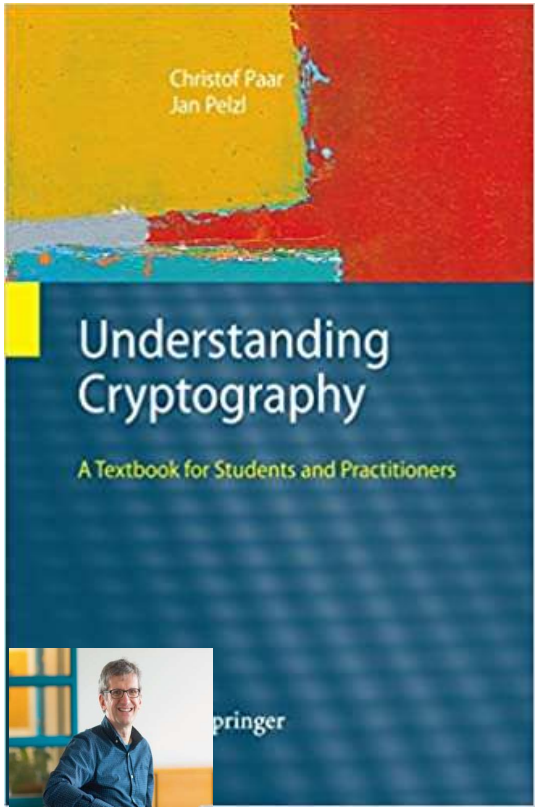
ontcijfer

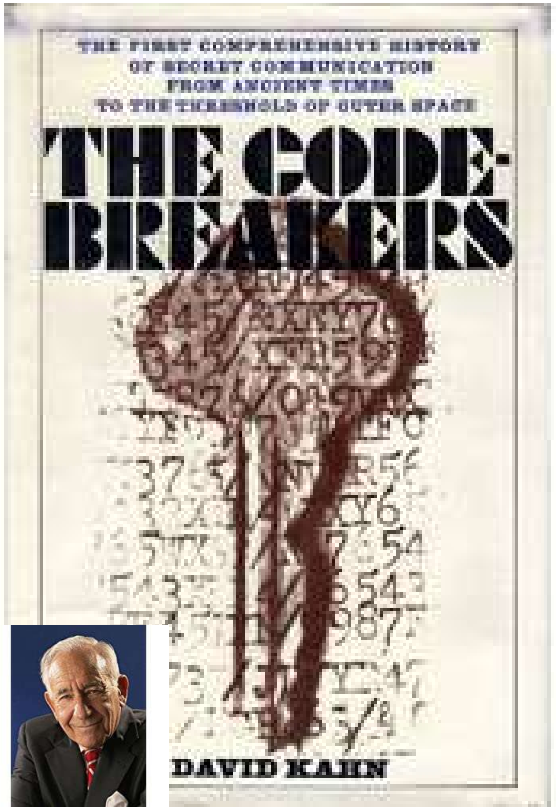
Leesbaar

ciphertext only attack

Het vinden van de sleutel moet zeer moeilijk zijn! (denk aan quantum computers)

interessante boeken met veel geschiedenis



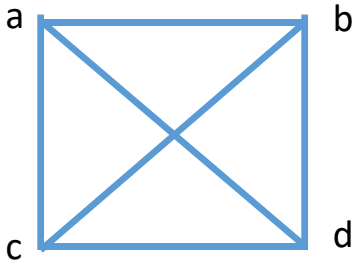


VROEGER EN NU

	Vroeger	Nu
Bericht:	Tekst	‚willekeurige' data
Analyse:	Linguistics	Data science
Machine:	engineering, intuitie	Algorithms, pure wiskunde
Type:	verbinding A => B	netwerk (internet)
Gebruik:	militair	algemeen (bank, winkel, …)

deel 2: Hoe communiceren we op een veilige manier in netwerken?

- Hoeveel verschillende sleutels heb je nodig wanneer **4** personen met elkaar willen communiceren?



Het antwoord is 6 (voor iedere verbinding **één**)

- Hoeveel sleutels heb je nodig wanneer **8** personen met elkaar willen communiceren?

Het antwoord is 28 (N(N-1)/2 = ongeveer (NxN)/2)

Sleutel-transport? Sleutel-beheer?

Digital Trust Center

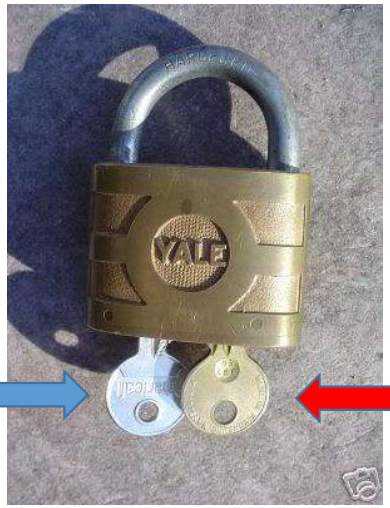

EUREKA!

Doorbraak 1: Diffie en Hellman, 1976
Een gezamenlijk geheim construeren zonder uitwisseling van geheimen

(R-G-B)

 De geheimen blijven geheim: oplossing voor het sleutelprobleem!

Doorbraak 2: 1976 slot met 2 verschillende sleutels



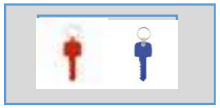
Alleen om slot te openen → ← **Alleen om slot te sluiten**

! een betrouwbare instantie geeft de sloten uit!

Digital Trust Center

This padlock sold for $81.01 (Plus $6 Shipping)

Wat doen we met het 2-sleutel principe?

- Iedereen heeft een uniek sleutel  PAAR

privé  sleutel en een publieke sleutel 

Hoe werkt het?

Belangrijke eigenschap:

Met een bekende publieke sleutel, kun je de privé sleutel niet vinden

NODIG: een betrouwbaar certificerings instituut!

Gebruik de publieke sleutel voor het versleutelen

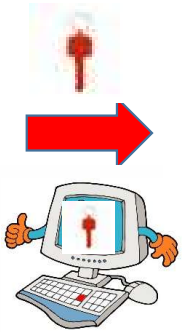
We gaan Schreurs een bericht sturen en zoeken de publieke sleutel van Schreurs op in een –betrouwbaar- boek

Lijst met publieke sleutels

Publieke sleutel van Schreurs
(een rij getallen)

publiek

Schreurs gebruikt zijn privé sleutel



We kunnen nu iedereen in het netwerk
Een versleuteld bericht sturen

Alleen met het correcte sleutel paar kun je ontsleutelen

En de privé sleutel om veilig een contract te ondertekenen

We zoeken de publieke sleutel van de afzender op in een –betrouwbaar- boek

Lijst met publieke sleutels

Schreurs

publiek

We weten:
ciphertext,
publieke sleutel
en het contract:
=> private key ???

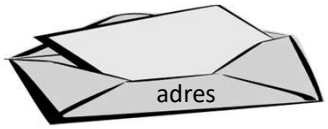
privé Schreurs

Iedereen kan de handtekening controleren

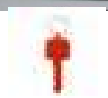
Alleen met de passende publieke sleutel (bij de privé sleutel)kun je het bericht ontsleutelen

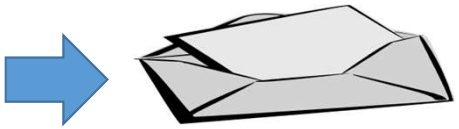
Een andere (oude) methode met een betrouwbare postbode?

Alleen Marian heeft de prive sleutel



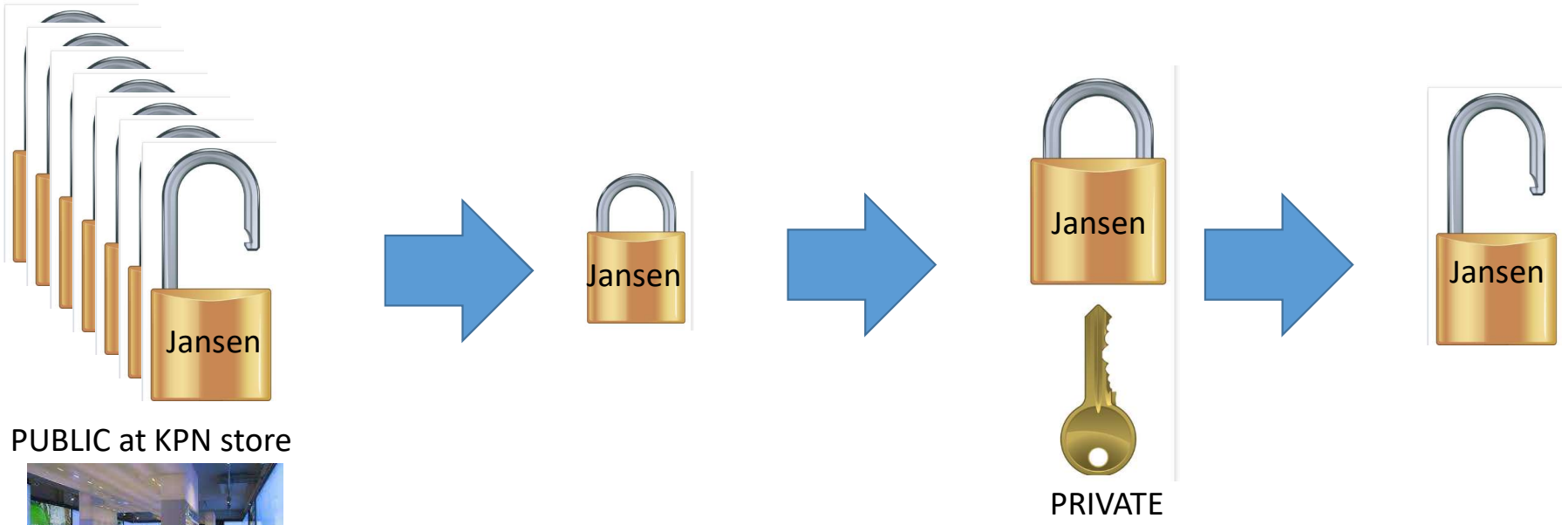
voor Marian





Onthoud: iedereen (public) kan een brief in de bus gooien!

Public and private key



Een andere (oude) methode

- Het contract lezen kan iedereen
- veranderingen alleen mogelijk door het verbreken van het zegel

Basis van de realisatie: complexe wiskundige problemen

nu de bezigheid van vele pure wiskundigen (bijv. Discrete logarithme, elyptic curve, …)

VOORBEELD

- Moeilijk: Product van twee priemgetallen P en Q, vind P en Q 143

- Simpel: Product twee grote priemgetallen P x Q = 11 x 13 = 143

Priemgetallen: > 500 digits lang

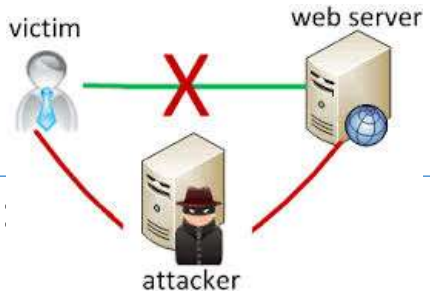
Wat hebben we gezien?

- **Een** sleutel: substitutie en transpositie (confusion en diffusion)
  - **sleutel is geheim**: de manier waarop openbaar (Kerckhoffs principe)
  - **Systeem openbaar**: noodzakelijk voor handel, export/import

- **Twee** sleutel systeem: privé en publieke sleutel PAAR
  - Maakt veilige netwerk kommunicatie mogelijk
  - Voor versleutelen en ondertekenen (belangrijk voor internet - ekonomie)
  - Is gebaseerd op pure wiskunde (bijv. Priemgetallen)

Waar bewaart U de sleutel?

Discussie



- Fouten in het protocol kunnen fataal zijn
  - bv. Man in the middle attack
  - vulnerabilities in Smart Light Bulbs operated over the Zigbee IoT radio protocol

- Pure WISKUNDE is zeer belangrijk:

  het ontcijferen van gecodeerde, onderschepte boodschappen. (data is geen taal meer!)

  het bedenken van "wiskundig" veilige systemen (pure wiskunde)

- Fouten in het gebruik (bv. gelekte server-sleutel)

Privacyexperts liepen er tot nu toe mee weg: PGP, oftewel Pretty Good Privacy. Deze technologie om veilig mail uit te wisselen zonder pottenkijkers blijkt nu lek.

Een ander systeem zonder gemeenschappelijke sleutel

Een schijnbaar perfecte oplossing, maar wie ziet het probleem?

Interessante dagelijkse digitale objecten?

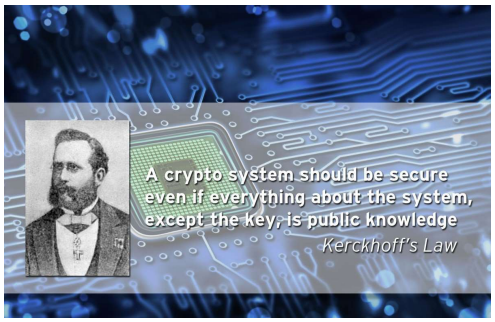
Onze maatschappij is wel erg ingewikkeld geworden!

Two important applications

- Network connection: home - work
- client-bank communication

Enkele sleutelfiguren in de ontwikkelingen

Th. Jefferson

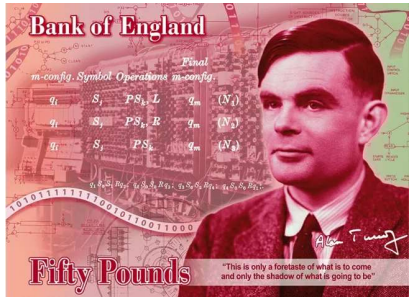


Kerckhoffs

Shannon

Diffie-Hellman

Rijmen/Daemen

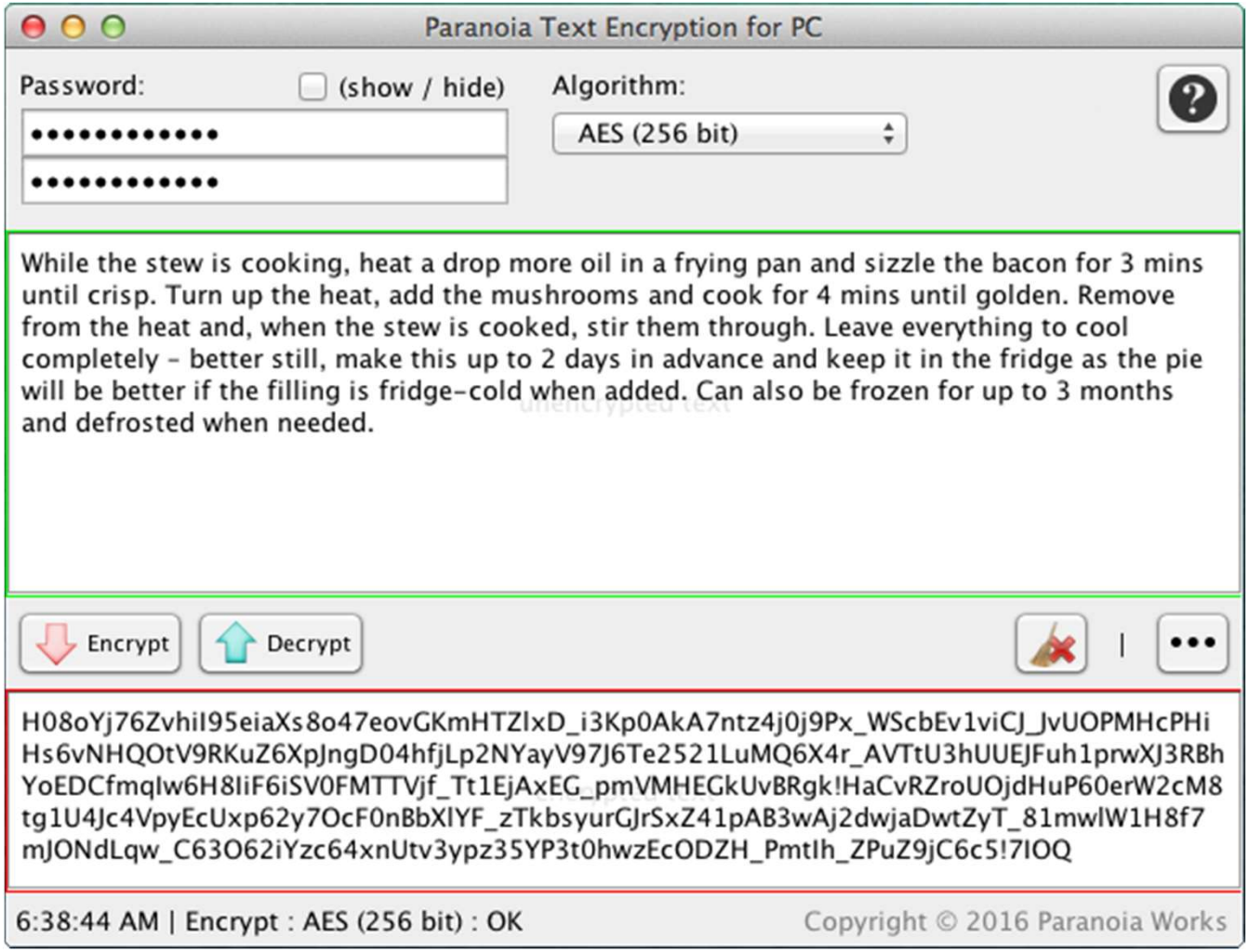


Turing

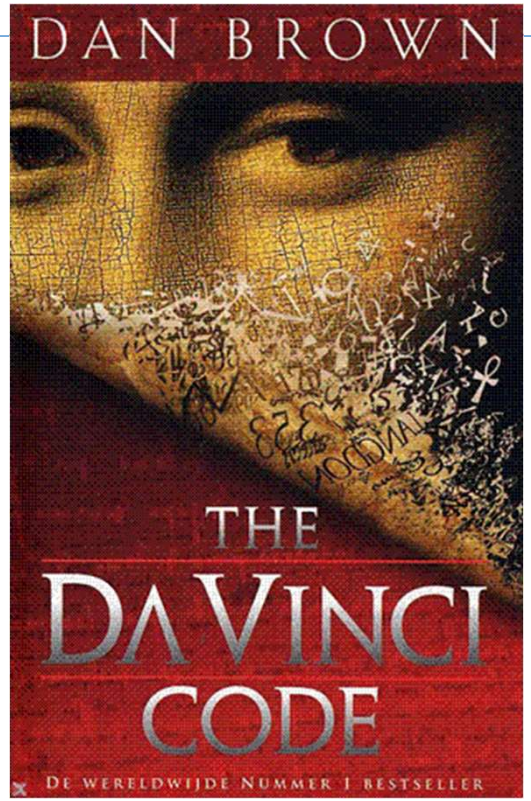
Discussie (2)

- Geheim houden van een systeem is een slecht principe (Kirchhoffs):
  - Crypto-AG afluister schandaal (T-450 zwak systeem)

- Open Standaards in de cryptographie (DES, AES):
  - Voor de export
  - certificering
  - meer onderzoek aan systeem


Paranoia Text Encryption for PC
Password:
(show / hide)
Algorithm:
AES (256 bit)
While the stew is cooking, heat a drop more oil in a frying pan and sizzle the bacon for 3 mins until crisp. Turn up the heat, add the mushrooms and cook for 4 mins until golden. Remove from the heat and, when the stew is cooked, stir them through. Leave everything to cool completely – better still, make this up to 2 days in advance and keep it in the fridge as the pie will be better if the filling is fridge-cold when added. Can also be frozen for up to 3 months and defrosted when needed.
Encrypt
Decrypt
H08oYj76ZvhiI95eiaXs8o47eovGKmHTZlxD_i3Kp0AkA7ntz4j0j9Px_WScbEv1viCJ_JvUOPMHcPHi
Hs6vNHQOtV9RKuZ6XpJngD04hfjLp2NYayV97J6Te2521LuMQ6X4r_AVTtU3hUUEJFuh1prwXJ3RBh
YoEDCfmqIw6H8IiF6iSV0FMTTVjf_Tt1EjAxEG_pmVMHEGkUvBRgk!HaCvRZroUOjdHuP60erW2cM8
tg1U4Jc4VpyEcUxp62y7OcF0nBbXlYF_zTkbsyurGJrSxZ41pAB3wAj2dwjaDwtZyT_81mwlW1H8f7
mJONdLqw_C63O62iYzc64xnUtv3ypz35YP3t0hwzEcODZH_PmtIh_ZPuZ9jC6c5!7IOQ
6:38:44 AM | Encrypt : AES (256 bit) : OK
Copyright © 2016 Paranoia Works

Uit de Da Vinci code: cryptex, wie heeft het?



Verder zijn goede systemen (algorithmen-wiskunde) belangrijk: Het Venlo Incident

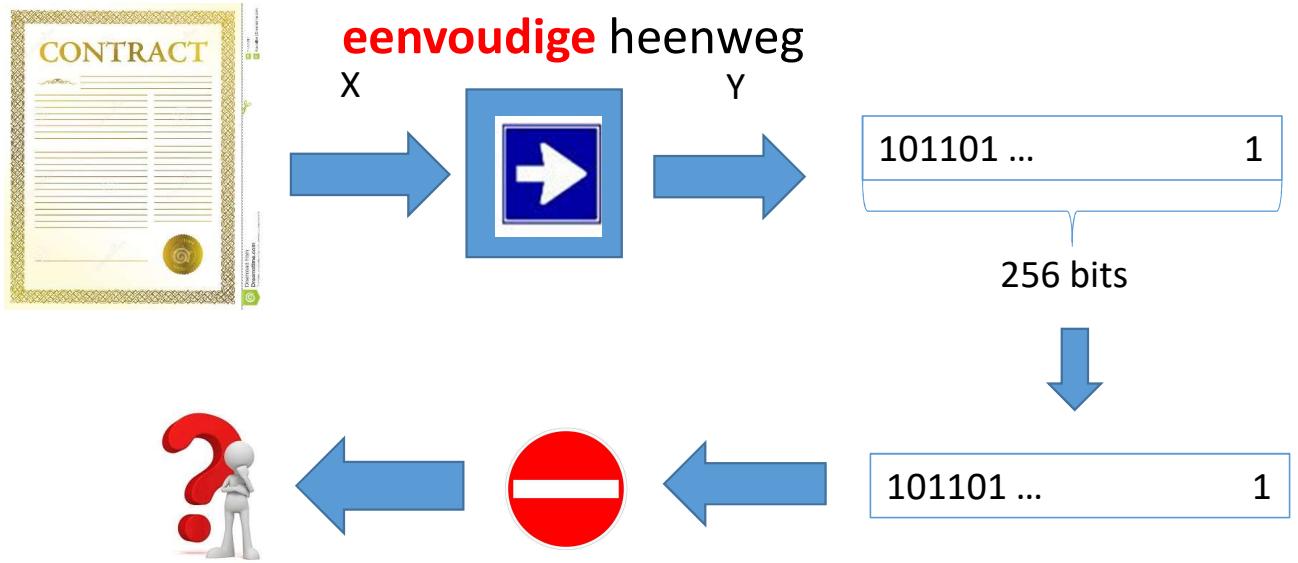
Henri Koot.

Ltn.Dirk Klop

- In de nacht van 8 op 9 november 1939 overschreed een Duitse SS commando-ee
  leiding van majoor Alfred Helmut Naujocks de grens met het soevereine en offic
  Nederland.
- Zij zouden Britse agenten ontmoeten in Café Backus aan de Herungerberg, op er
  meters afstand van de grens.
- De Britten was beloofd dat zij de generaal die de leider was van de samenzweer
  ontmoeten. Best en Stevens werden vergezeld door chauffeur J.F. Lemmens en d
  luitenant Dirk Klop, ondanks een waarschuwing door Henri Koot.
- **Deze specialist in cryptografie vond de door de vermeende Duitse samenzwee
  code (Playfair cipher) zo zwak, dat hij hen niet serieus nam en een Duitse valst**

Doorbraak 1: Diffie-Hellmann, 1976

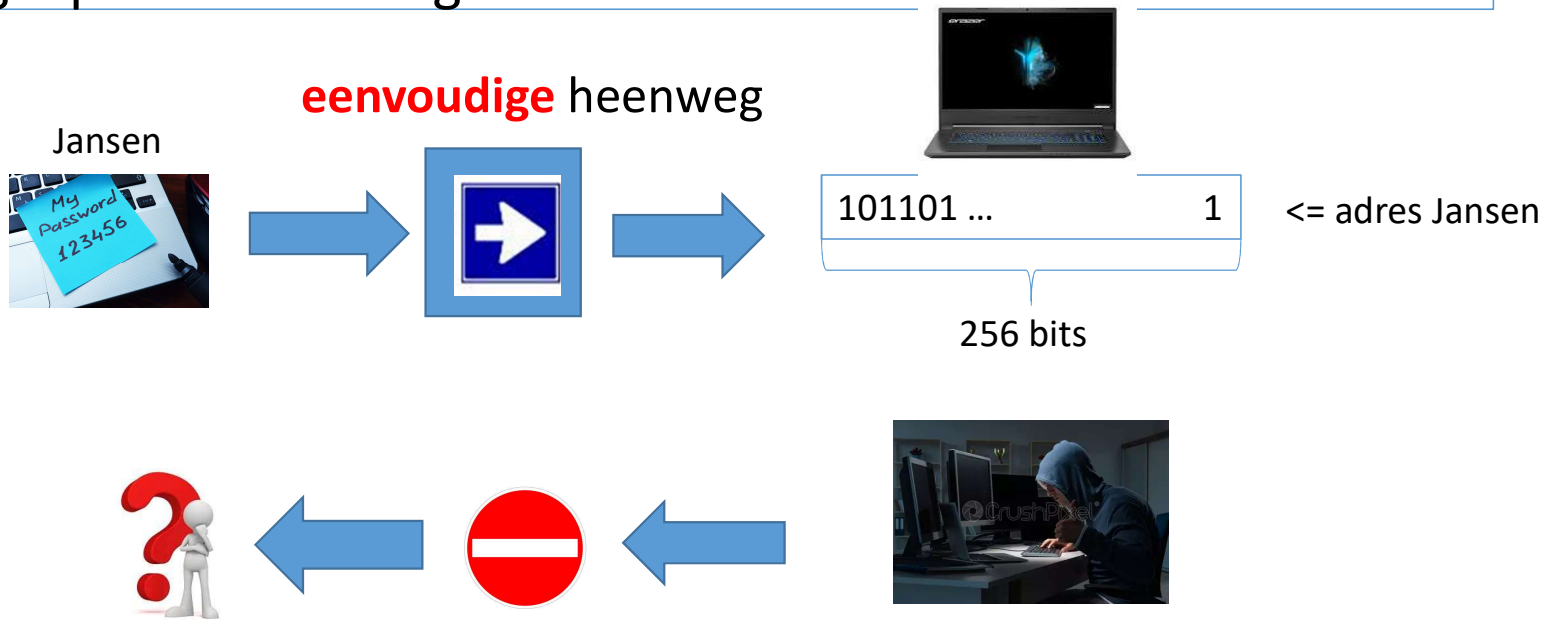
- ONE-WAY (Hash) function:



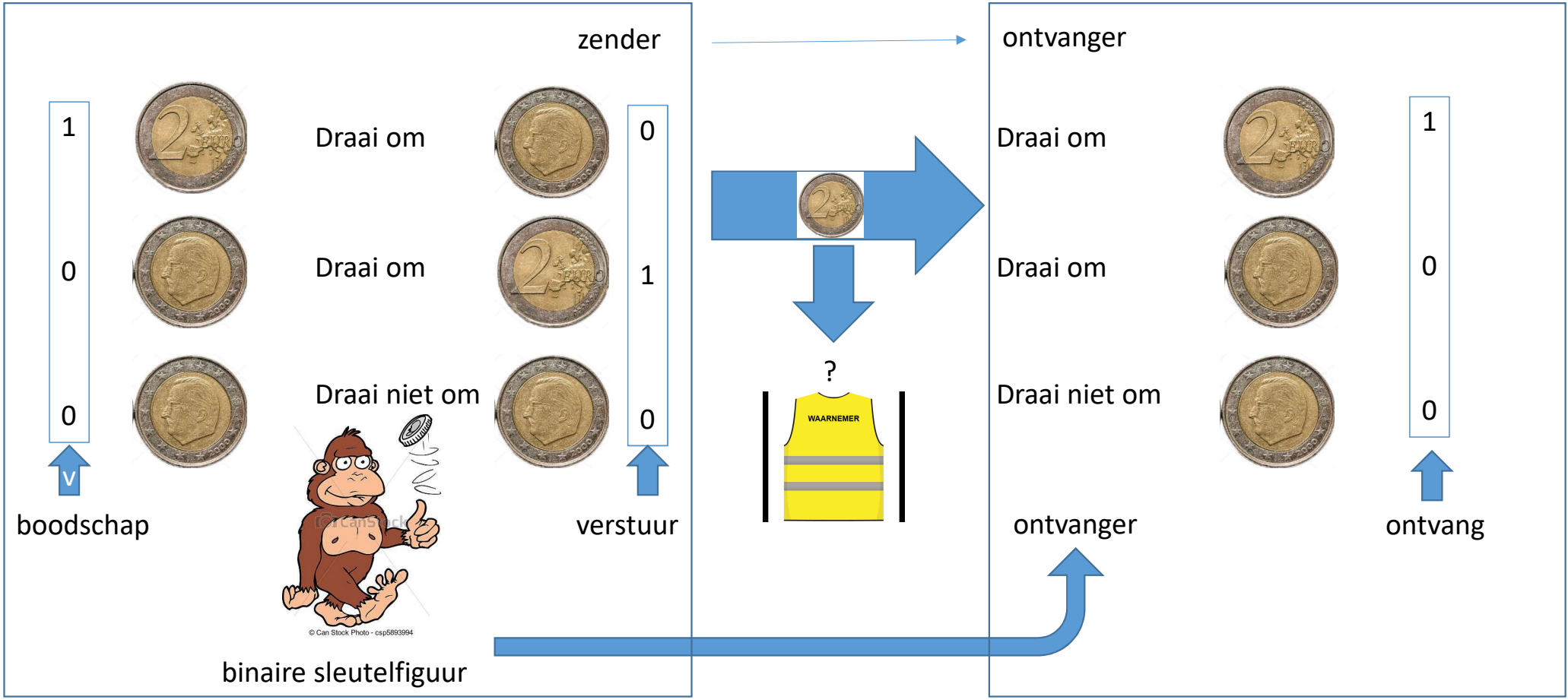
terugweg is **complex** ≈ onmogelijk

Doorbraak 1: Diffie-Hellmann, 1976

- Toepassing 2 password mangement



Het enige principe met perfekte veiligheid (maximale onzekerheid voor de afluisteraar)

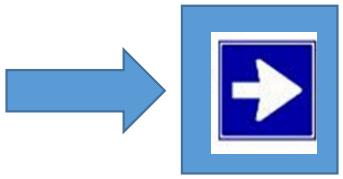


Gebruik

- Toepassing: password mangement

„eenvoudige“ heenweg

Jansen



101101 … 1 <= adres Jansen

101101 … 1 256 bits

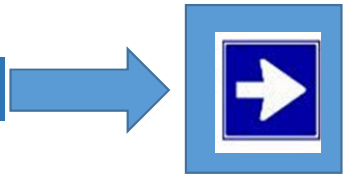
Controleer de Hash van Jansen

Belangrijke Eigenschap Hash

Iedere verandering zelfs “1 bitje” geeft groot verschil

„eenvoudige“ heenweg

Jansen

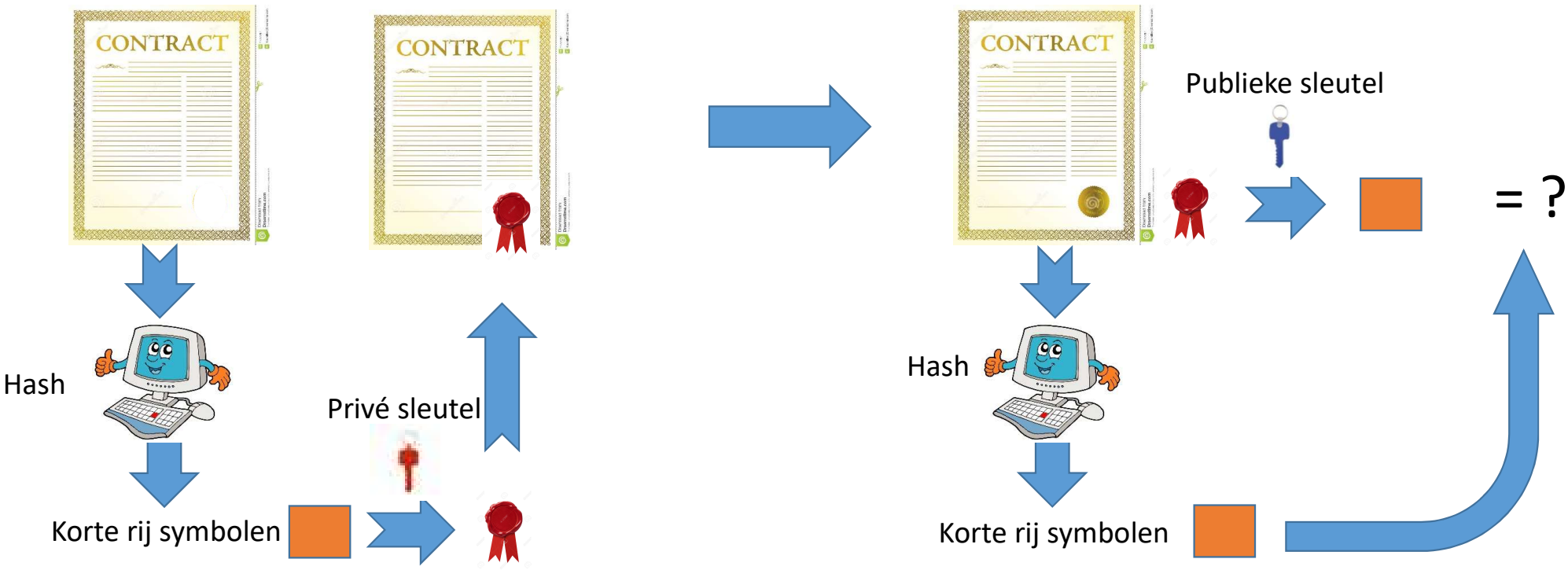


101101 … 1 <= adres Jansen

110011 … 1 256 bits

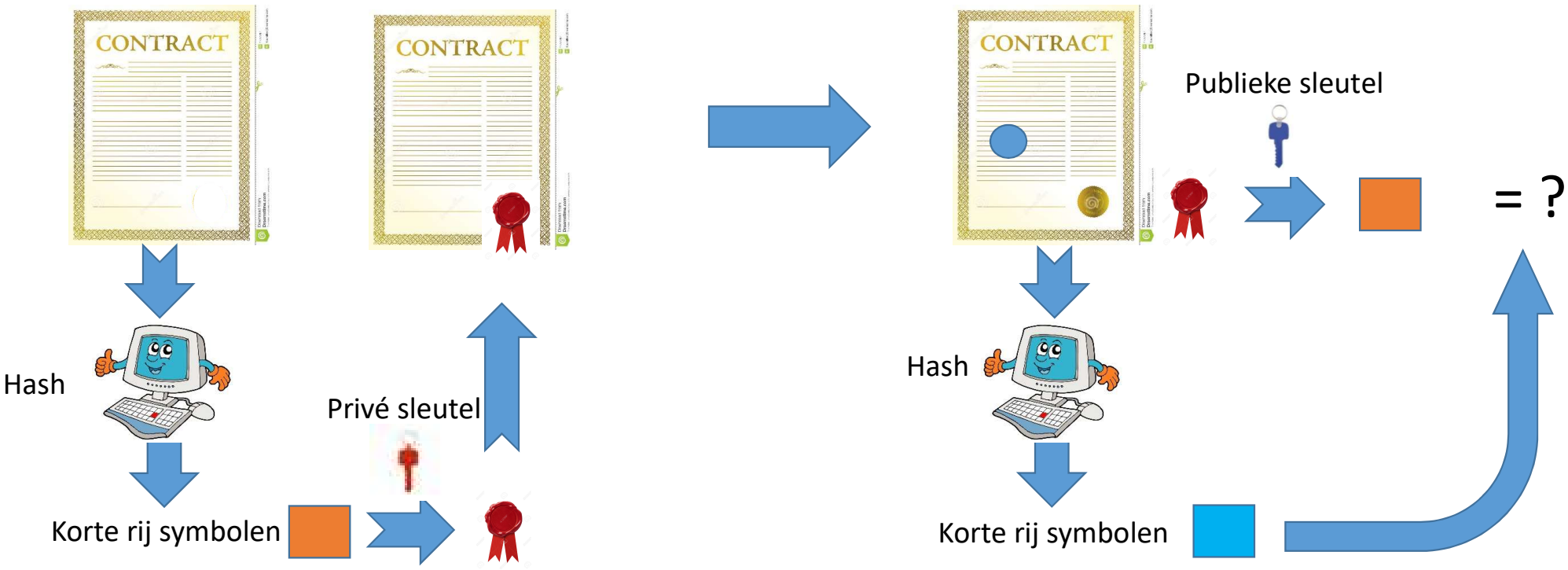
Controleer de Hash van Jansen

We kunnen simpel (met een Hash) een digitale handtekening zetten!

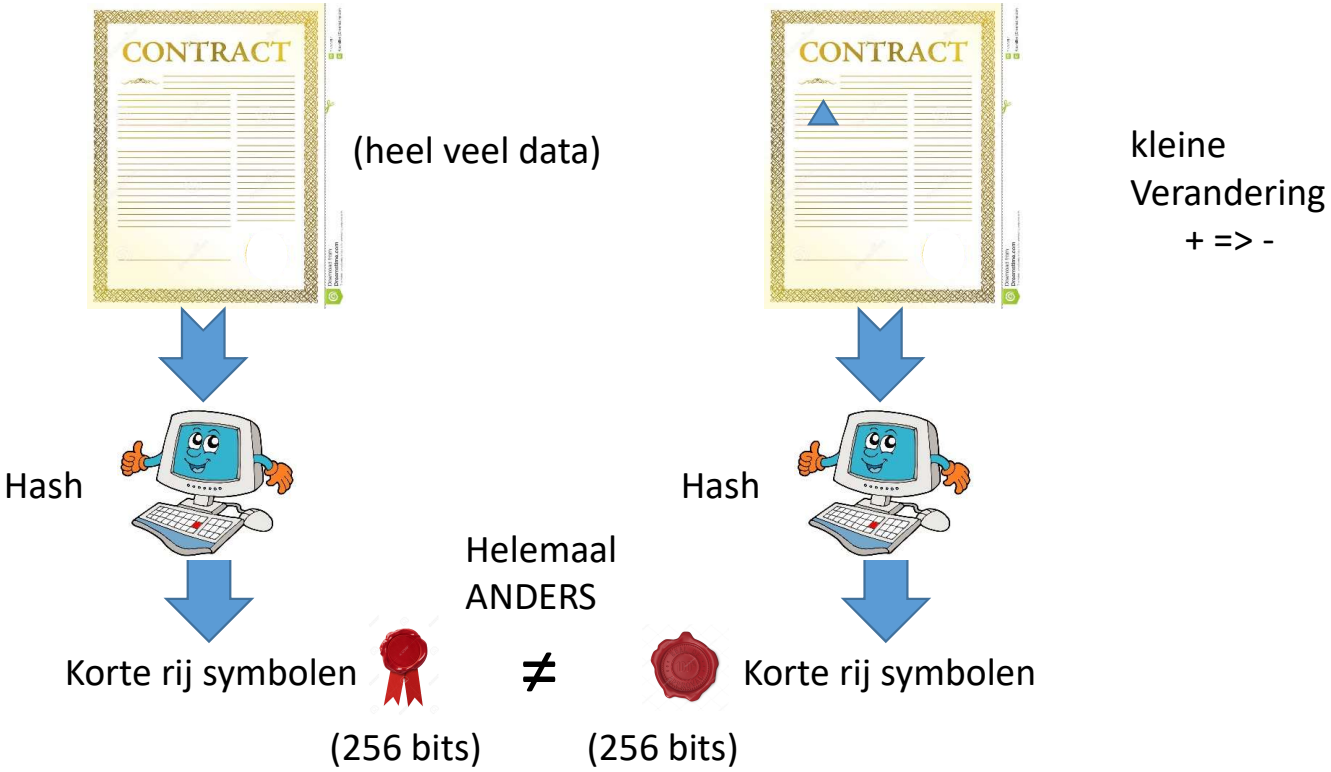


We kunnen simpel een digitale handtekening zetten!

Q: Wat gebeurt er bij een verandering in de text?



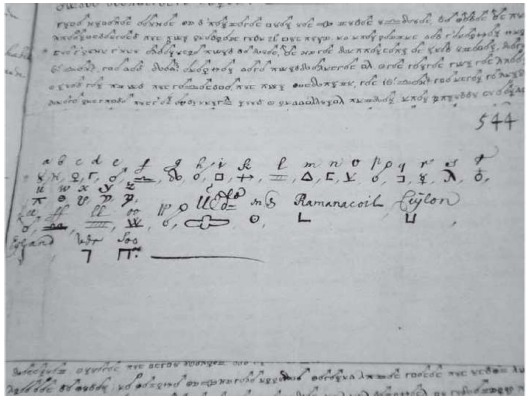
Belangrijke eigenschap voor de digitale handtekening



Block chain

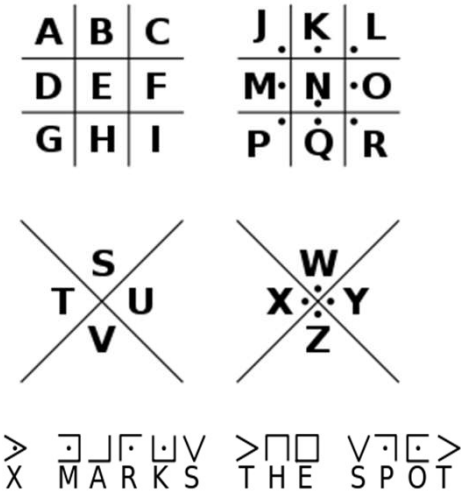
Enkele oude voorbeelden

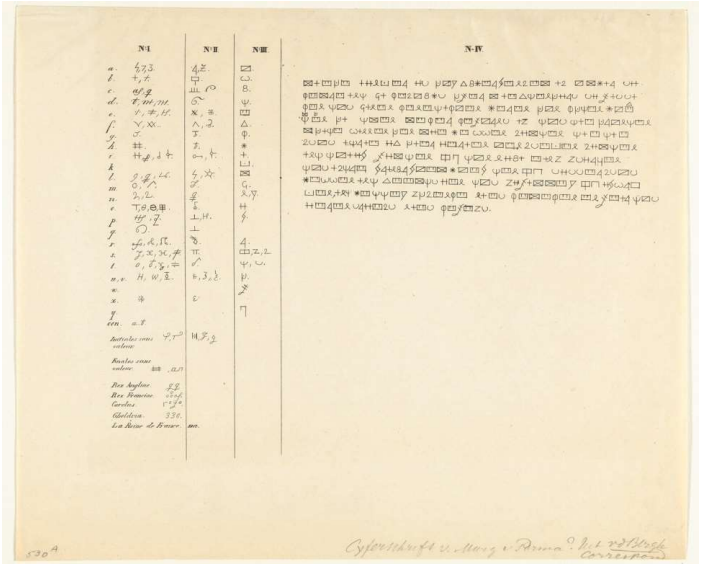
VOC en geheimschrift



Pagina van Joannes Leeuwensons geheimschrift met op de voorgrond de sleutel. Nationaal Archief (Den Haag):

Rozenkruisersgeheimschrift

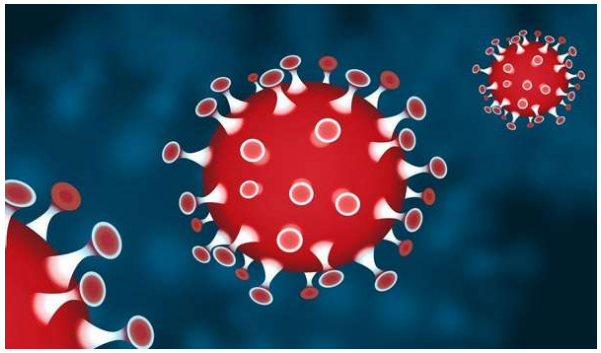




het geheimschrift gebruikt door Margaretha van Parma in haar correspondentie, 1567.

http://www.geheugenvannederland.nl/?/nl/items/RIJK04:RP-P-OB-79.031

Corona en private key



Indien je beschikt over PGP versleutelingsmogelijkheden, verstuur dan een PGP encrypted bericht. Gebruik hiervoor de PGP NCSC jaarkey.
https://www.ncsc.nl/contact/pgp-key
Vergeet niet je eigen PGP key mee te sturen in de bericht zodat wij PGP encrypted terug kunnen sturen.

Screenshot_2020-10-31 CVD-meldingen formulier

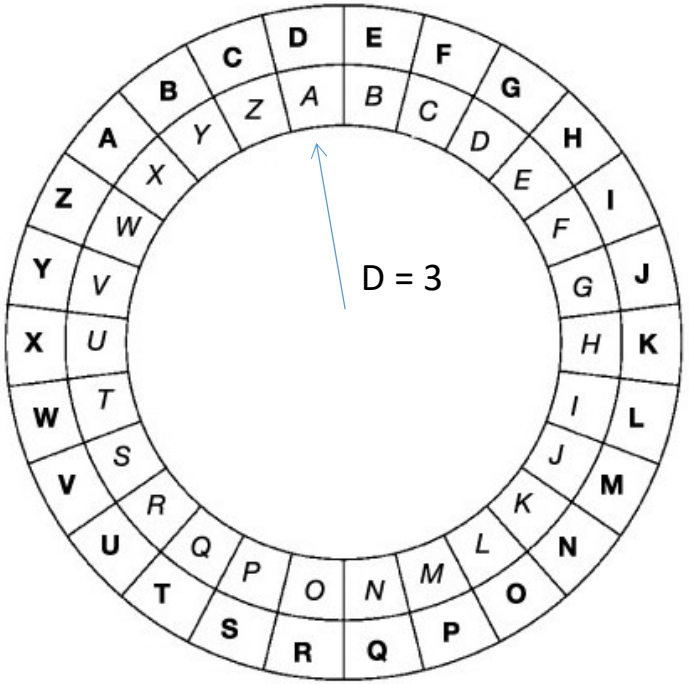
Screenshot_2020-10-31 PGP-key

voorbeeld

De wiskundige Hieronymus Cardanus (1501–1576) is de vermoedelijke uitvinder van het cardan-rooster, een sjabloon dat bestaat uit een vel papier of karton met een aantal gaten. Dit wordt op een leeg vel papier gelegd en door de gaten wordt de klare tekst geschreven. Na verwijdering van het sjabloon wordt de ruimte tussen deze woorden volgeschreven, zodat het geheel eruit ziet als een onschuldige boodschap. De ontvanger legt eenzelfde sjabloon op de tekst en kan de geheime boodschap door de gaten lezen. De sleutel wordt dus bepaald door het sjabloon.

beter: gebruik een variable verschuiving met een sleuteltekst

A:	verdraai over 0 posities
B	1
C	2
D	3
…	



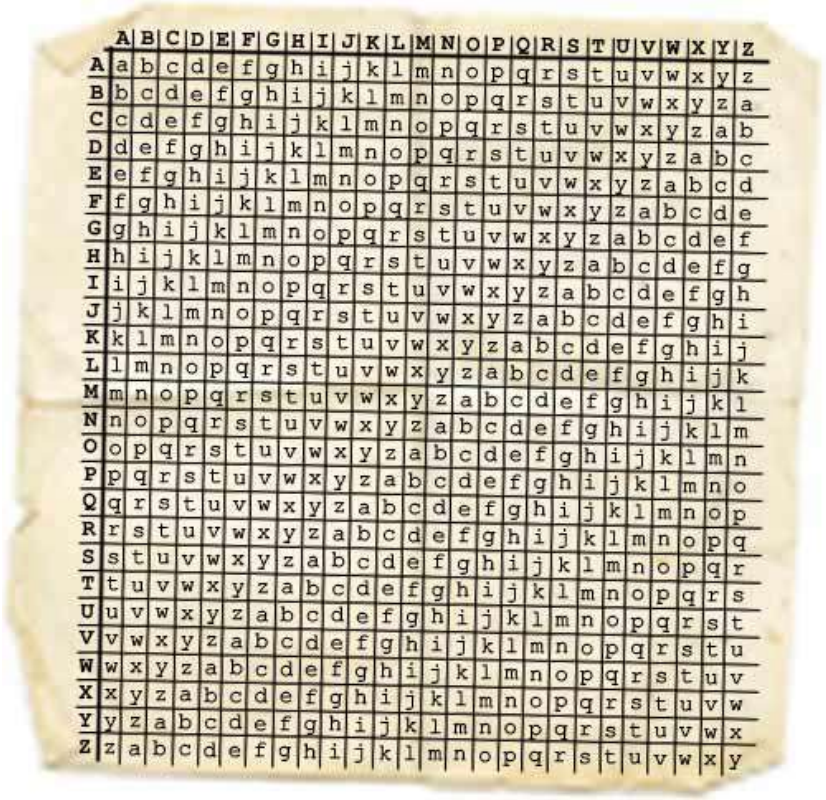
c r y p t o c r y p t o c r … sleutel

2 17 25 15 19 14 2 17 25 15 19 14 etc.... Sleutel

h e e l v e e l p l e z etc …

j v d a o s g c o a x n ciphertext

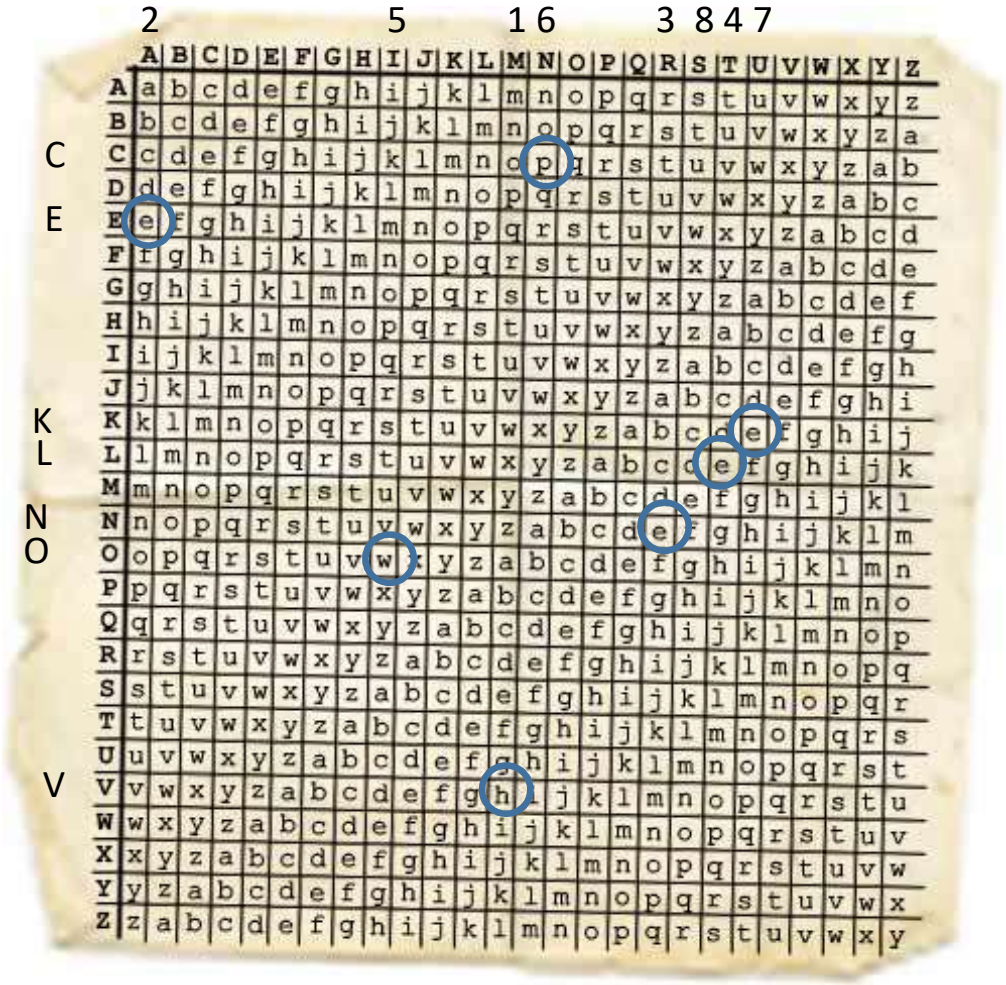
Je kunt ook een tabel gebruiken



	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

Blaise de Vigenére, a French diplomat and cryptographer born in 1523

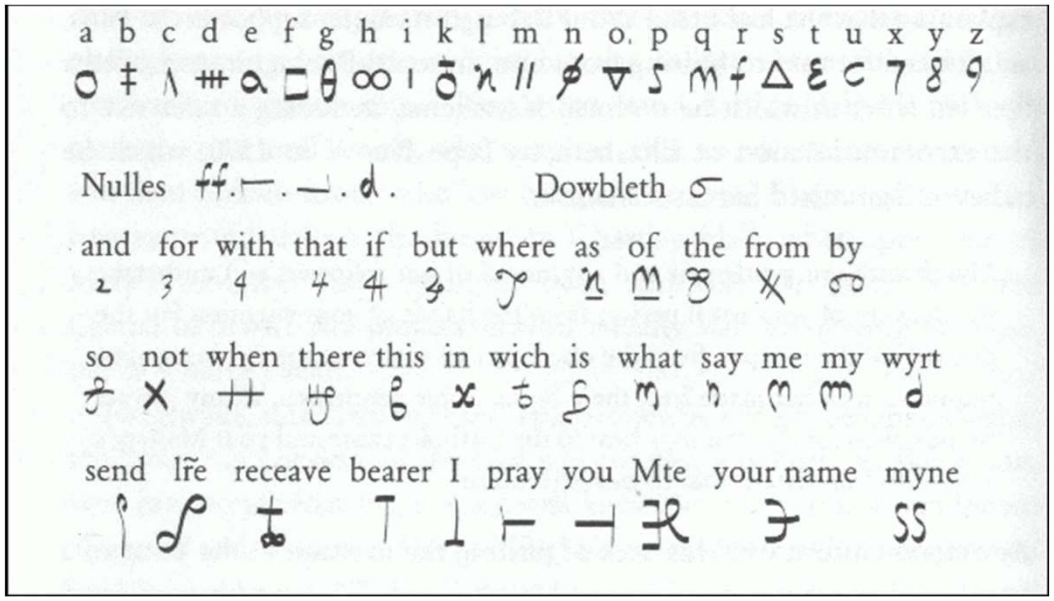
geheim:	martinus
Tekst:	venlock
Ciphertekst:	heeewpe
Hoe terug?	

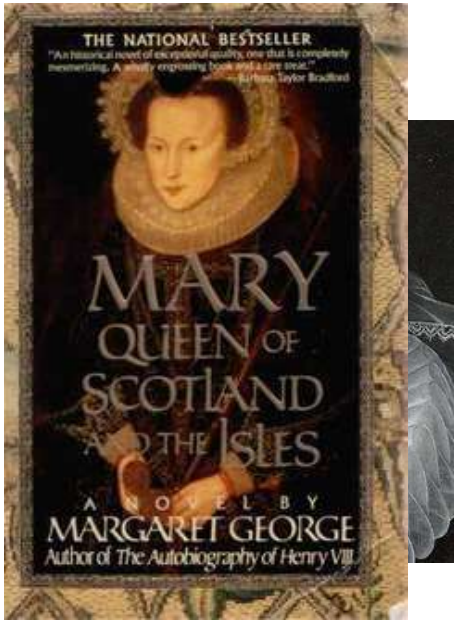


Het belang van goede sleutels: een voorbeeld
het tragische verhaal van koningin Mary van Schotland (16e eeuw)

- Mary wilde koningin Elizabeth I van Engeland vermoorden
- De geheime berichten van Mary werden ontcijferd door de spionnen van Elizabeth
- Mary werd gearresteerd en de ontcijferde berichten werden als bewijs gebruikt voor verraad
- Ze werd schuldig bevonden en geexecuteerd in 1587

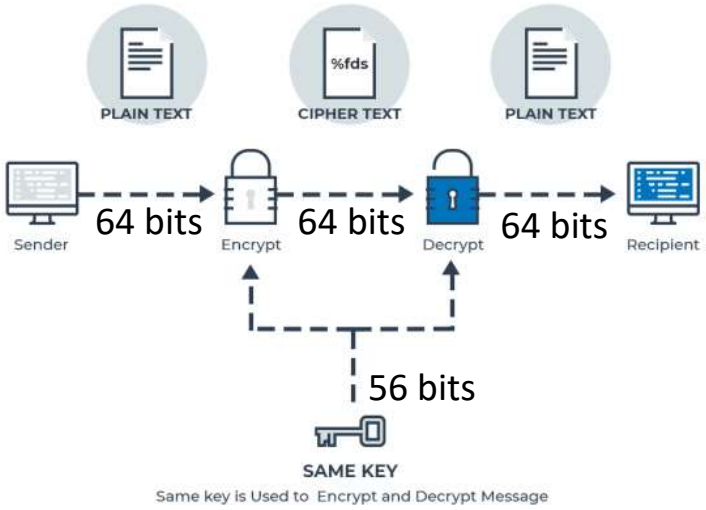
Haar sleutel





voorbeeld

- Data Encryption Standard (DES) van 1977 - 2000



Data Encryption Standard (DES)

- Most widely used block cipher in the world
- Adopted in 1977 by National Bureau Standards (NBS)
- Encrypts 64-bit data using 56-bit key
- Has widespread use
- Has been considerable controversy over its security

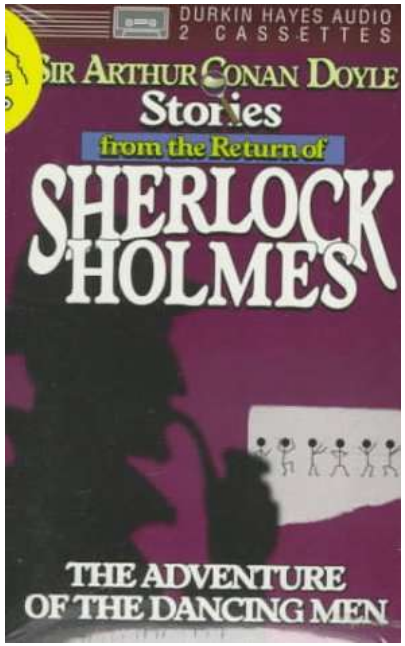
Ik ben:

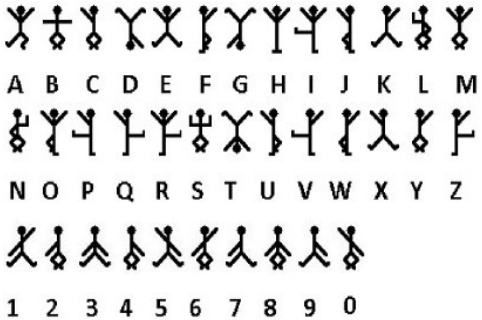
- Han Vinck
- Senior Professor in Digitale Kommunicatie (1990-)
  Univ. Duisburg-Essen
- Gehuwd met Martie Vinck-Huinen
- 2 zoons, 4+ kleinkinderen
- Geb. Breda
- Woon in Venlo sinds 1993 (nu Gr. Kerkstraat)
- Hobby: muziek

Geheim-schrijven = vertalen van *leesbaar* in *onleesbaar*
d.m.v. een *geheim (sleutel)*

ook crypto-grafie
from Greek κρυπτός *kryptós*, "hidden, secret";
and γράφειν *graphein*, "writing",

voorbeeld



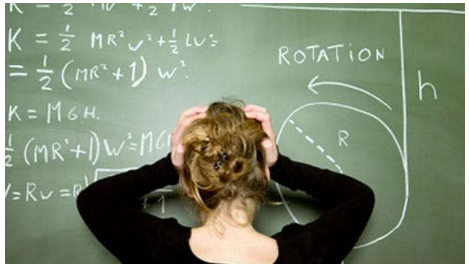


Vriend:
gebruik **gemeenschappelijke geheime** sleutel
voor het leesbaar maken

Vijand:
gebruik **taalkundige analyse**
voor het leesbaar maken

Waarschuwing: Er zit een heleboel wiskunde achter.
Q: hoe te realiseren met de computer?

- 1. het logarithme probleem y = r^x
  - het is moeilijk om x te vinden als we y en r kennen
  - Voorbeeld: 81= $3^?$

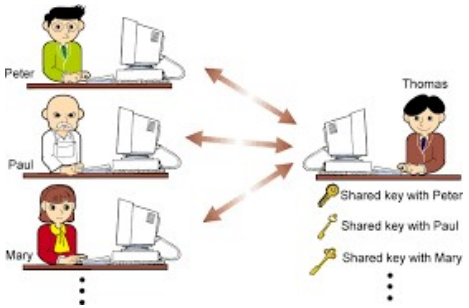


- 2. gegeven n = p x q is het product van twee grote priemgetallen
  - Voorbeeld: 143 = ? (= 13 x 11)
  - Het is moeilijk om p en q te vinden als we n kennen

sleutelprobleem

- A => B kommunicatie: hoe komen A en B veilig aan dezelfde **geheime** sleutel

- In netwerk kommunicatie met N deelnemers:

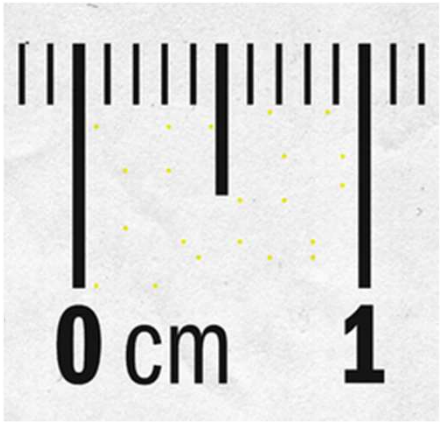


  - aantal sleutels = ongeveer $N^2/2$

  - sleutelbeheer: genereren van sleutels en opslag

Digital Trust Center

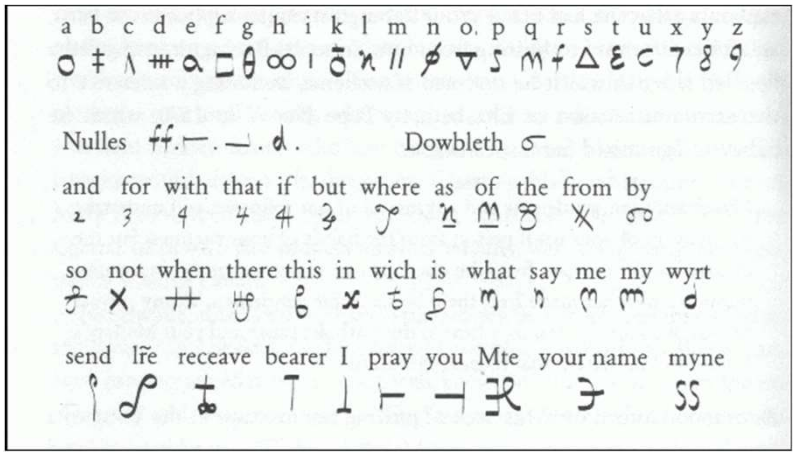
Twee „geheim“ schrijf-principes: stegano- & cryptography

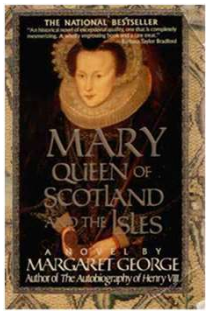


Look at the yellow dots.
They encode the date, time
and serial number of the printer.

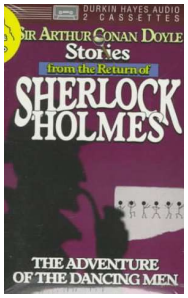
An ancient example is that of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden.

Stegano-graphy = **verborgen** schrijven





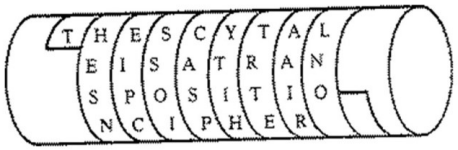
Crypto-graphy = **geheim** schrijven



Ouderwetse transpositie ciphers

Transposition Ciphers

Scytale Cipher (contd.)



T	F	N	W	O
H	O	P	M	R
E	X	J	U	B
Q	U	I	C	K

T	F	N	W	O
H	O	P	M	R
E	X	J	U	B
Q	U	I	C	K

Route Cipher

Rail Fence Cipher

plaintext	T	H	E	Q	U	I	C	K	B	R	O	W	N	F	O	X	
1	T				U				B				N				= TUBN
2		H		Q		I		K		R		W		F		X	= HQIKRWFX
3			E				C				O				O		= ECOO
ciphertext	T	U	B	N	H	K	I	K	R	W	F	X	E	C	O	O	