Cursus Cryptografie

POLYALFABEET

17-02-2016

Klassieke systemen

Transpositie
- Route
- Kolom
- Rooster

Monoalfabetisch
- Caesar
- Homofoon
- Monome-dinome
- Playfair
- Bifid
- ADFGVX
- Nomenclatuur
- Code
- Encicode

Polyalfabetisch
- Porta
- Vigenère
- Beaufort
- Nihilist
- Progressie
- Autoclaaf
- Wheatstone
- Multiplex
- One-time-pad

Machine
- Hagelin
- Kryha
- Enigma
- Purple

Substitutie

Monoalfabetisch
- letter-voor-letter: Caesar, Monoalfabeet
- digram: Playfair
- meervoudig: Nomenclatuur, Code, Encicode
- gemengd: Monome-dinome, Fractionering

Polyalfabetisch periodiek
- eenvoudig: Porta, Vigenère, Beaufort
- langperiodiek: Hagelin, Enigma
- meer alfabetten: Multiplex

Polyalfabetisch aperiodiek
- Autoclaaf, One-Time-Pad

Periodieke systemen

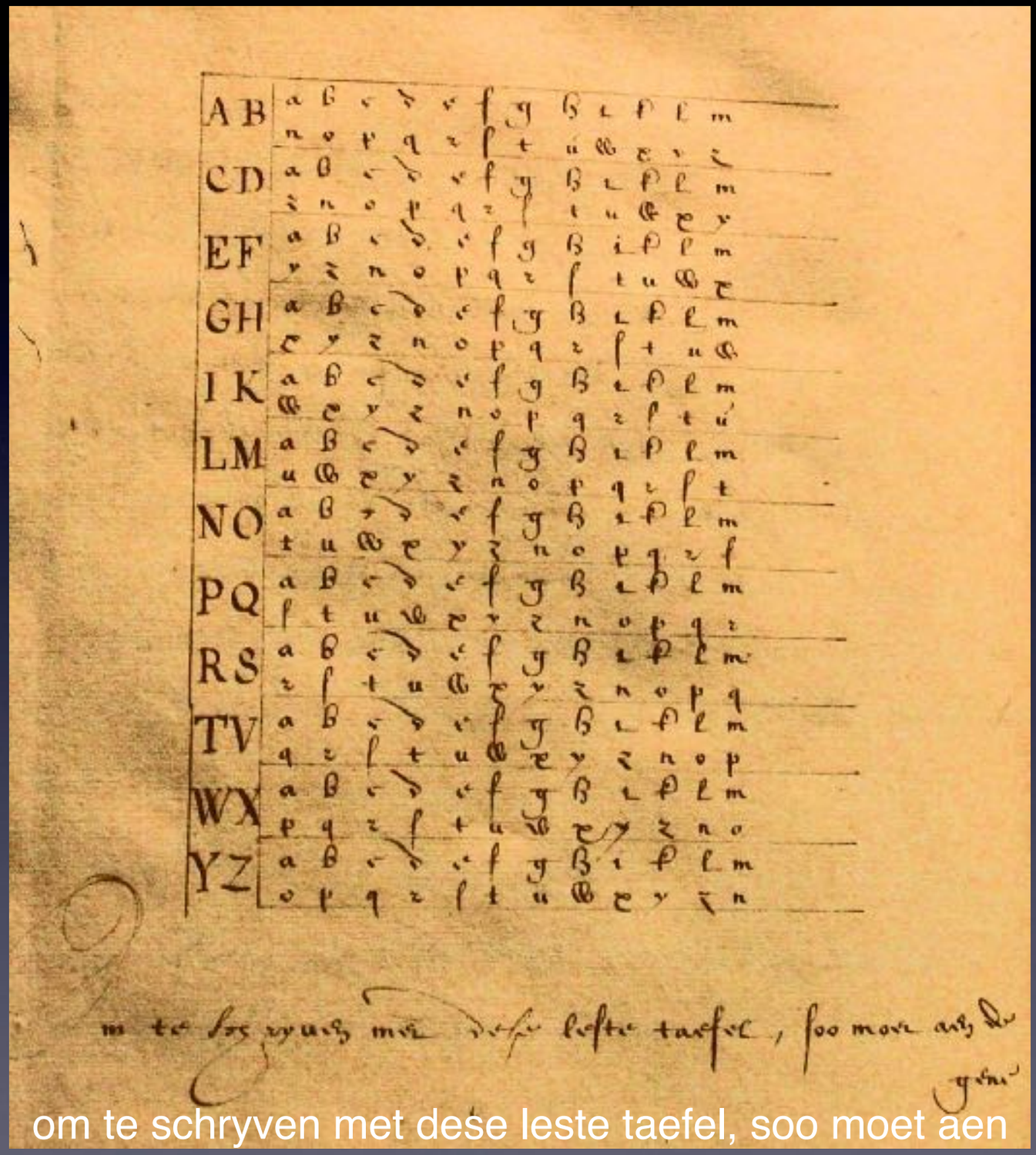
Eindige sleutel herhaald gebruikt

$K = k_1 k_2 \ldots k_p$ p = periode

- normaal alfabet *Porta, Vigenère*
- teruglopend alfabet *Beaufort*
- gemengd alfabet in verschillende varianten
- sleutelwoord of sleutelzin
- lange sleutel door progressie *Kryha, Hagelin*
- lange sleutel door rotor *Enigma, Sigaba, Fialka*

Porta

Giovanni Battista Porta
1535–1615
1563 *De Furtivis Literarum Notis*



om te schryven met dese leste taefel, soo moet aen

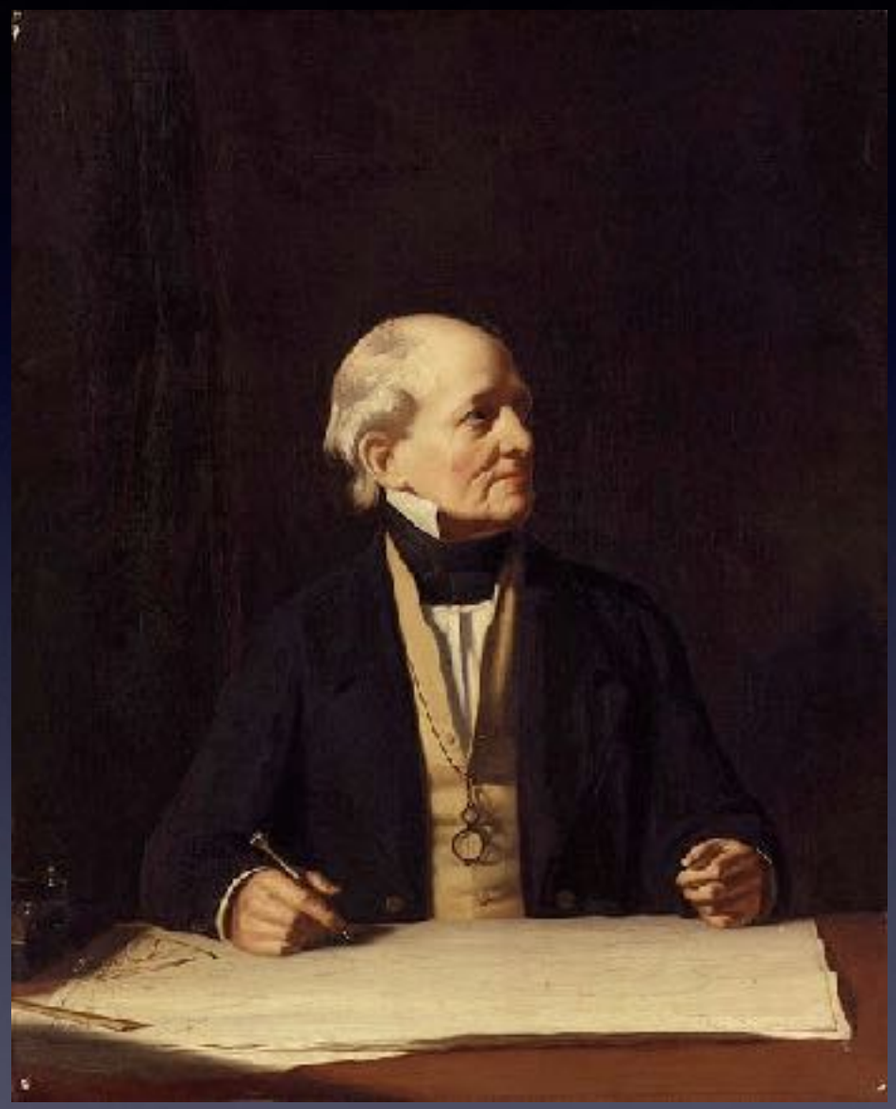
Vigenère

Blaise de Vigenère
1523–1596
1563 *Traicté des Chiffres*

	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

vercijfer: sleutel M → S ↓ = E
ontcijfer: sleutel M → E ↑ = S

Beaufort



Sir Francis Beaufort
1774–1857

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

vercijfer: sleutel M → X ↑ P
ontcijfer: sleutel M → P ↑ X

Autoclaaf

Aperiodiciteit door terugkoppeling

cijfertekst autoclaaf

```
sleutel:PENTA GONKCN GDTOQOTGCD
     pt: VYAND NADERT WATERLINIE
     ct: KCNGD TOQOTG CDMSHZBTKH
```

klaartekst autoclaaf

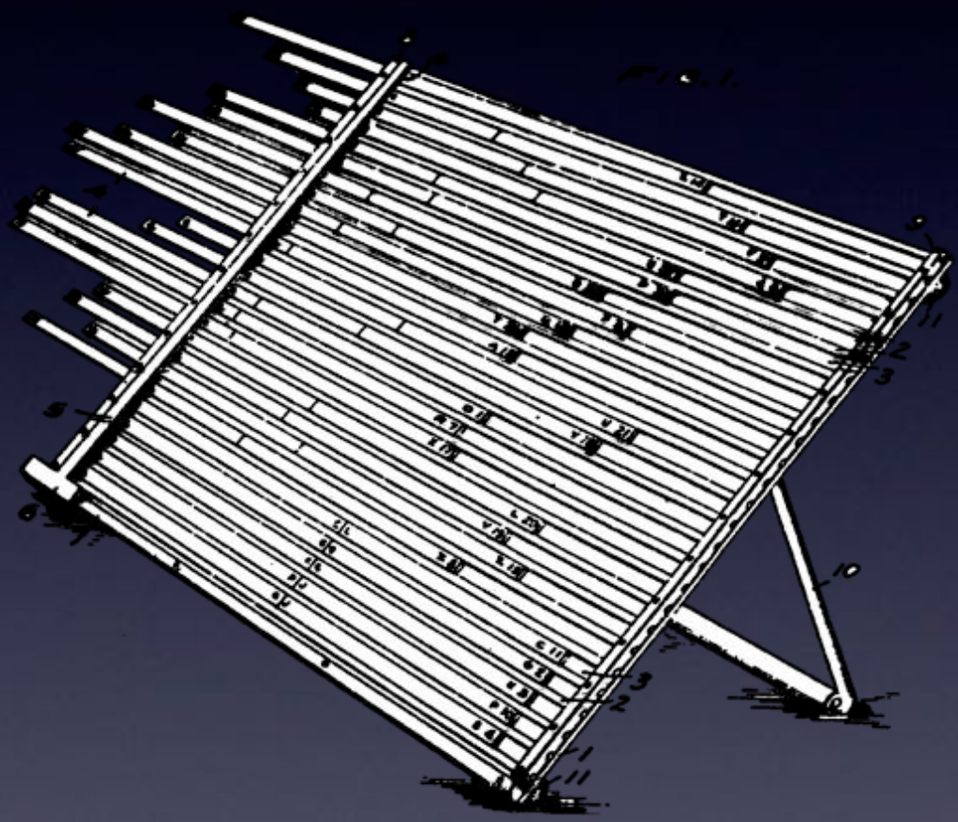
```
sleutel:PENTA GONVYA NDNADERTWA
     pt: VYAND NADERT WATERLINIE
     ct: KCNGD TOQZPT JDGEUPZGEE
```

Wheatstone

Charles Wheatstone
1802–1875

eveneens een autoclaaf

Multiplex



Jefferson cylinder (1790)
Etienne Bazeries (1891)
US Army M94-versie (1923)

One-Time-Pad

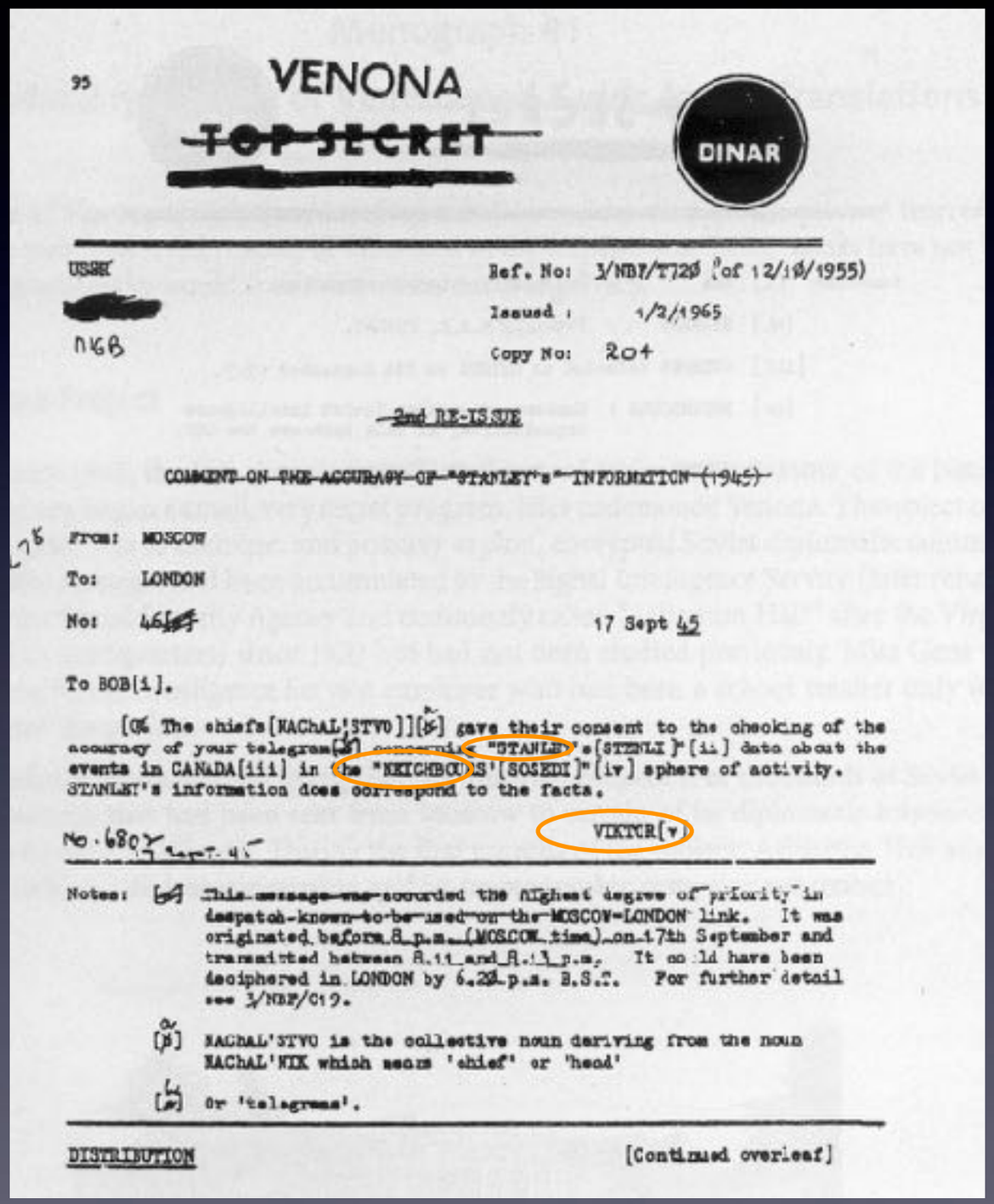
sleutel + klaartekst → cryptogram

- oneindig lange willekeurige eenmalige sleutel
- voordeel is absoluut onbreekbaar
- nadeel is veel sleutelmateriaal nodig

sleutelproductie met

- radioactief verval, electronische ruis
- loterij
- pseudorandom generator (niet onbreekbaar)

VENONA



95

VENONA

~~TOP SECRET~~ [redacted]

DINAR

USSR [redacted]

NKGB

Ref. No: 3/NBI/T720 (of 12/10/1955)

Issued : 1/2/1965

Copy No: 204

~~2nd RE-ISSUE~~

~~COMMENT ON THE ACCURACY OF "STANLEY's" INFORMATION (1945)~~

From: MOSCOW

To: LONDON

No: 46[illegible] 17 Sept 45

To BOB[i].

[α] The chiefs[NACHaL'STVO]][β] gave their consent to the checking of the accuracy of your telegram[γ] concerning "STANLEY's[STENLI]"[ii] data about the events in CANADA[iii] in the "NEIGHBOURS'[SOSEDI]"[iv] sphere of activity. STANLEY's information does correspond to the facts.

No.680 Sept. 45

VIKTOR[v]

Notes: [γ] ~~This message was accorded the~~ highest degree of priority in despatch known to be used on the MOSCOW-LONDON link. It was originated before 8 p.m. (MOSCOW time) on 17th September and transmitted between 8.11 and 8.14 p.m. It could have been deciphered in LONDON by 6.28 p.m. B.S.T. For further detail see 3/NBI/C19.

[β] NACHaL'STVO is the collective noun deriving from the noun NACHaL'NIK which means 'chief' or 'head'

[γ] Or 'telegrams'.

DISTRIBUTION [Continued overleaf]

KGB messages 1942-1945

blunder door deels hergebruik otp
VENONA van start in 1943
tot 1980 reconstructie additief en code

linken van codenamen aan personen
Stanley = Kim Philby Cambridge-5
Viktor = Gen. Fitin
Neighbours = GRU

Spionage tegen Manhattan project
Julius & Ethel Rosenberg † 19-6-1953
Burgess en Maclean 1951
1987 Peter Wright “Spycatcher”
1995 officieel openbaar