RST28 – Moers

Rechenschieber für die Kryptographie

Kryptologie

- war früher die Wissenschaft, die sich mit dem Ver- und Entschlüsseln von Informationen beschäftigte,
- ist heute die Wissenschaft, die sich mit Informationssicherheit beschäftigt.

Rechenschieber für die Kryptographie

Teilgebiete der Kryptologie sind u. a.

- **Kryptographie,** die Lehre von der Verschlüsselung von Informationen
- **Kryptoanalyse,** die Lehre von der Entschlüsselung von Informationen

Gliederung

- **Monoalphabetische Verschlüsselung**
  - **Rechenschieber**
- **Polyalphabetische Verschlüsselung**
  - **Rechenschieber**
- **Rechenschieber von Faber-Castell (?) und Aristo**

Monoalphabetische Verschlüsselung

Eine Verschlüsselung heißt **monoalphabetisch**, falls jeder Buchstabe des Alphabets stets zu demselben Buchstaben chiffriert wird. Eine monoalphabetische Verschlüsselung kann man also immer so darstellen, dass man unter das „Klartextalphabet“ ein „Geheimtextalphabet“ schreibt.

Klartext:	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
Geheimtext:	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

Eine monoalphabetische Verschlüsselung kann man also immer so darstellen, dass man unter das „Klartextalphabet“ ein „Geheimtextalphabet“ schreibt.

„Moers“ wird hier zu: FHXKL

Monoalphabetische Verschlüsselung

Der „**Caesar**“ - Die von Julius Caesar benutzte Verschlüsselung

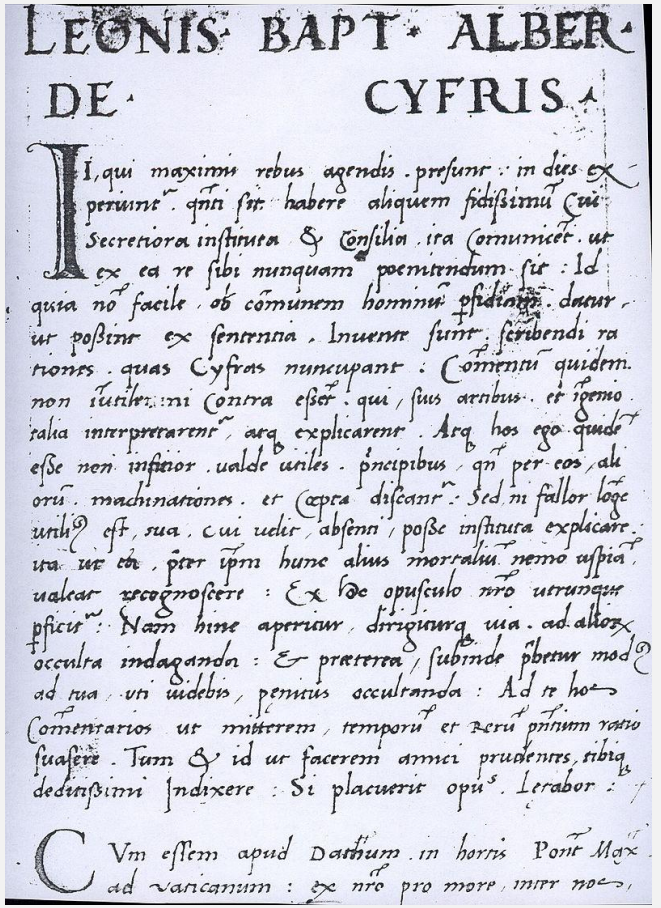
Klartext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Exakt diese Verschlüsselung soll Caesar in seiner militärischen Korrespondenz benutzt haben.

„Moers“ wird hier zu: PRHUV

Monoalphabetische Verschlüsselung

1466 wird erstmals von Leon Battista Alberti (1404 - 1472) eine Chiffrierscheibe beschrieben.



LEONIS BAPT. ALBER.
DE CYFRIS.

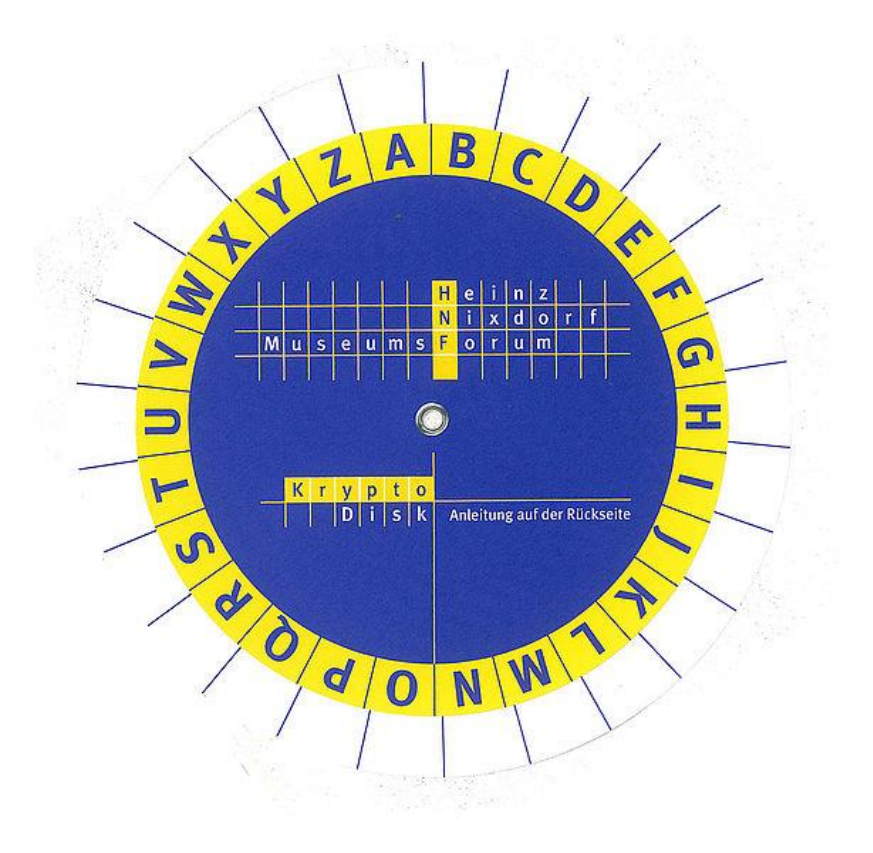
Monoalphabetische Verschlüsselung

Diese Chiffrierscheibe sah so aus.

Und so etwas kann man heute noch kaufen…

Monoalphabetische Verschlüsselung

Monoalphabetische Verschlüsselung



Monoalphabetische Verschlüsselung

Monoalphabetische Verschlüsselung

J. Hicks, London, 1893

Monoalphabetische Verschlüsselung

Die dänische Krypto

von

A/S The Danish Cipher Machine Co. Ltd.

Kopenhagen, ca. 1933

Monoalphabetische Verschlüsselung

Eine Variante der dänischen Krypto

Polyalphabetische Verschlüsselung

Im Gegensatz zur monoalphabetischen Verschlüsselung werden bei der **polyalphabetischen** Verschlüsselung für die Zeichen des Klartextes mehrere Geheimtextalphabete verwendet.

Zur Auswahl der verschiedenen Geheimalphabete benutzt man ein **Schlüsselwort**.

	Text																								
Schlüssel	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	Y
B	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
C	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
D	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
E	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
F	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
G	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
H	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

Polyalphabetische Verschlüsselung

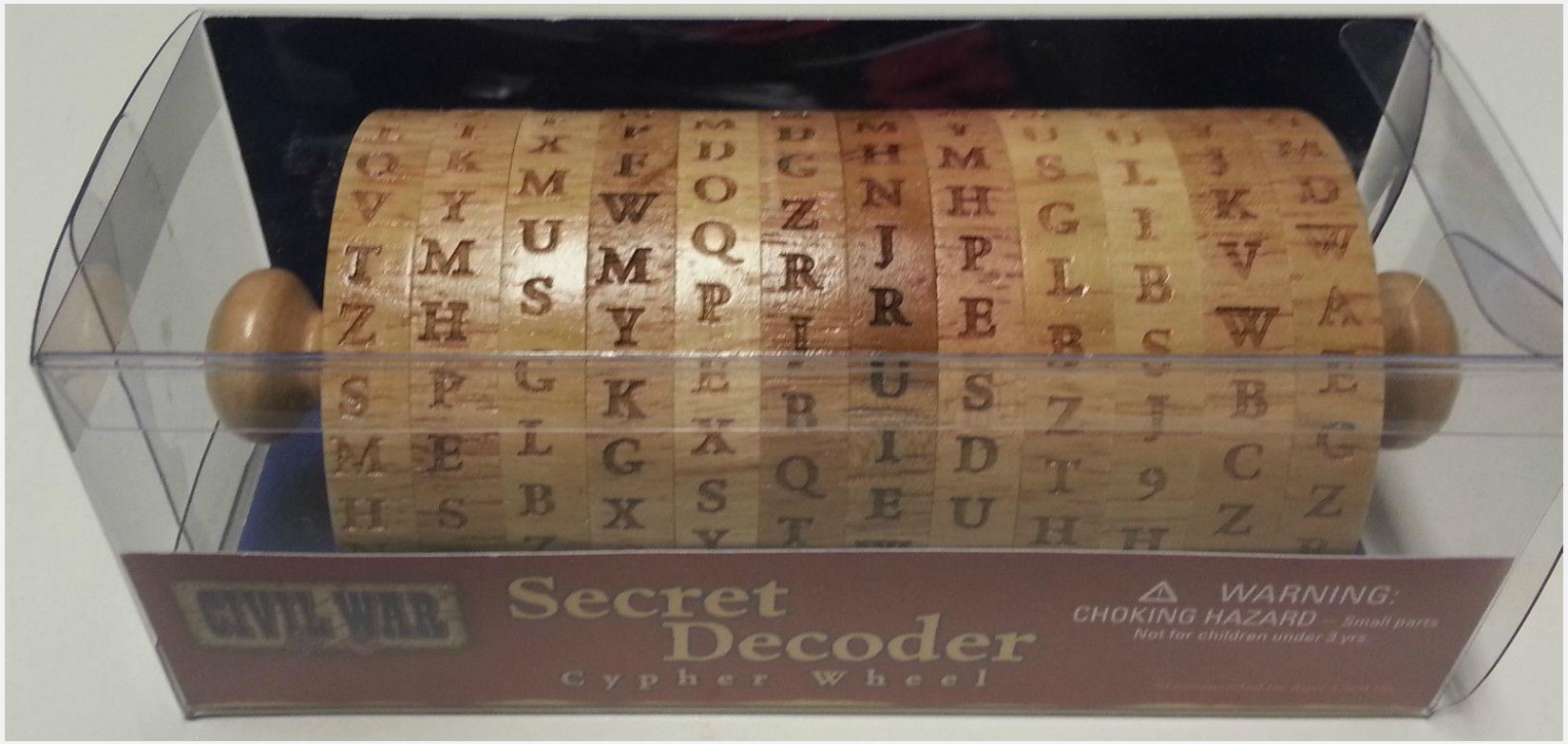
Klartext:	M	O	E	R	S
Schlüssel:	G	A	B	E	
Geheimtext:	G	O	D	N	M

Schlüssel \ Text	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	Y
B	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
C	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
D	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
E	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
F	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
G	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
H	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

Polyalphabetische Verschlüsselung

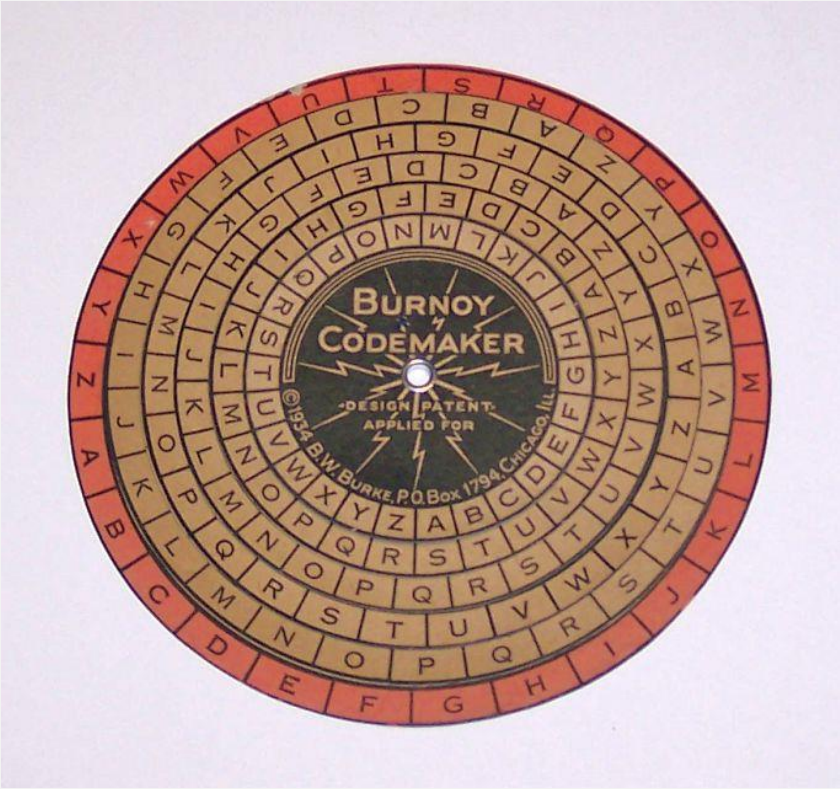
Etienne Bazérie, 1891

Polyalphabetische Verschlüsselung



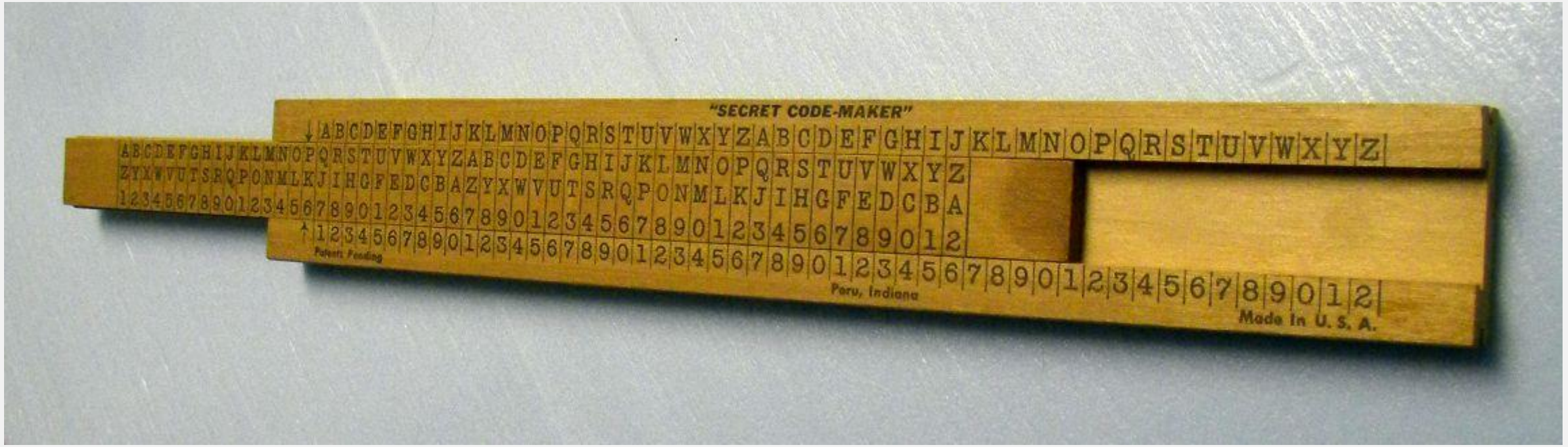
Jefferson-Walze

Polyalphabetische Verschlüsselung



Charles Wheatstone, 1837

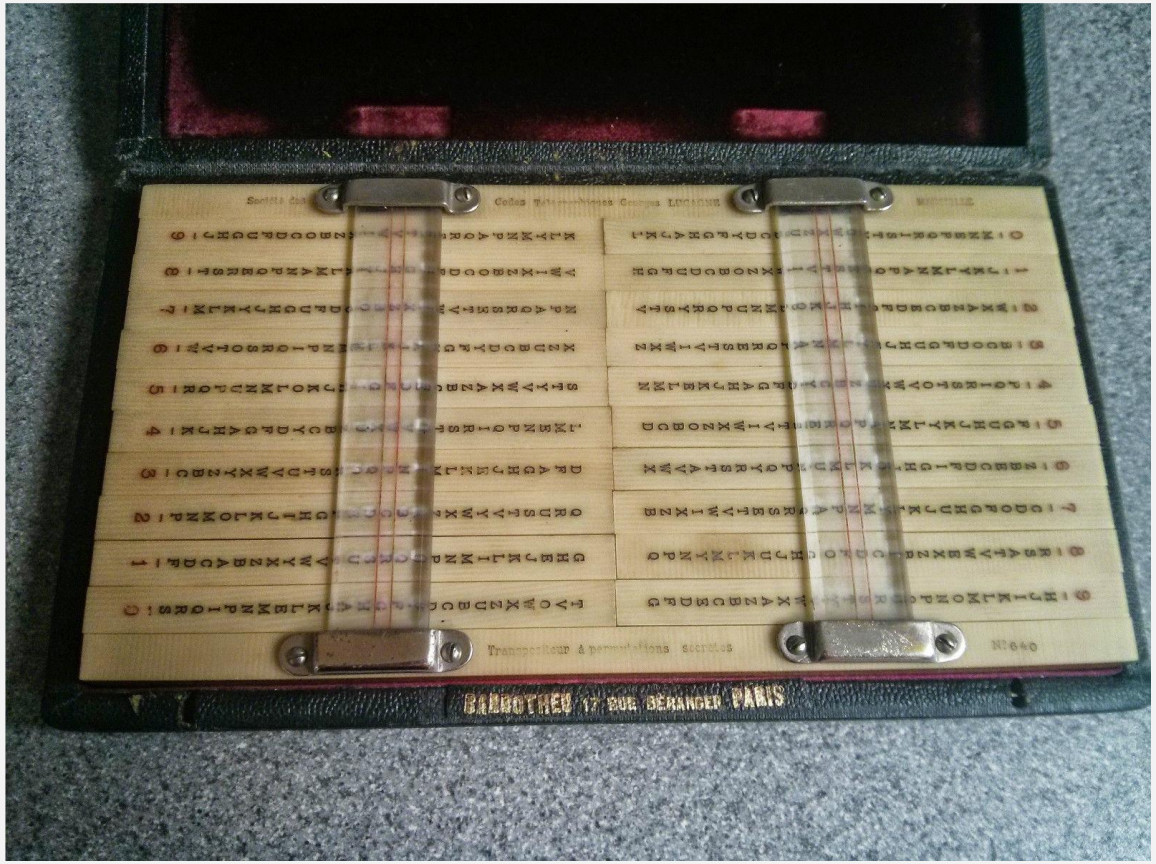
Polyalphabetische Verschlüsselung

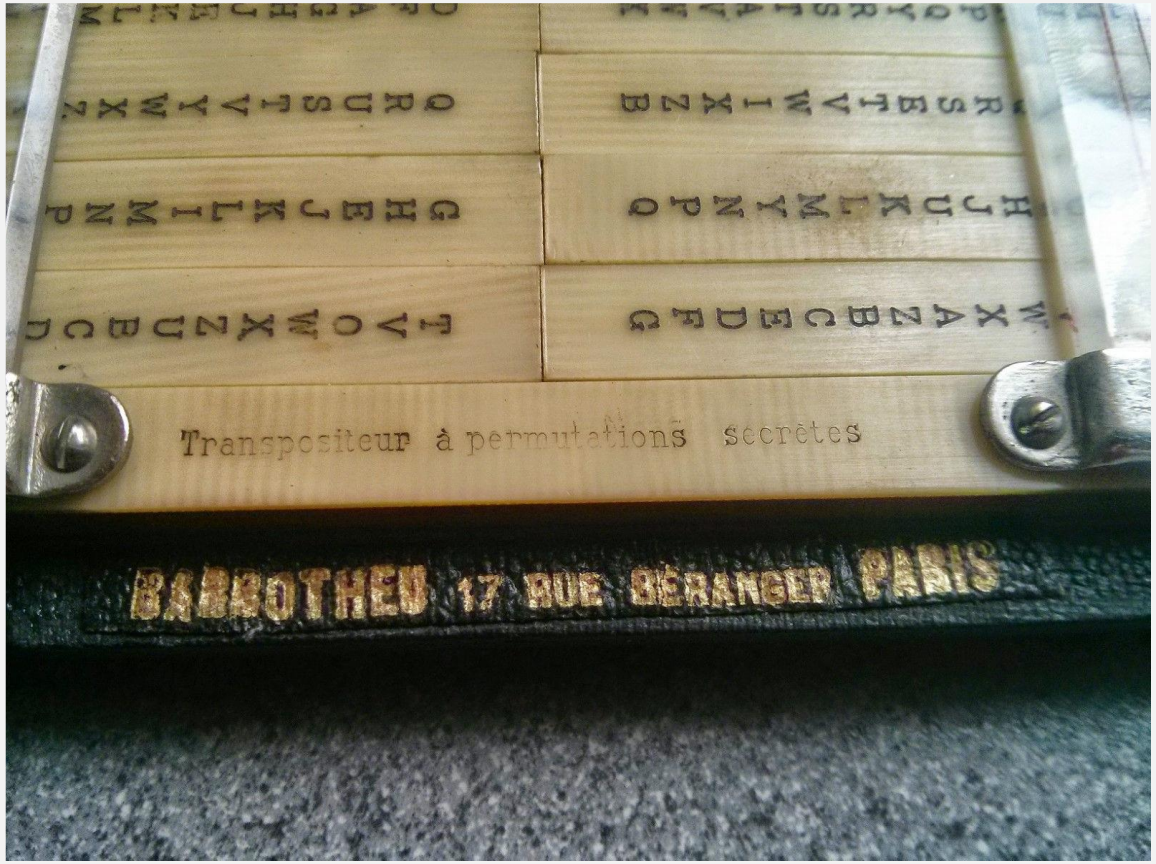


Polyalphabetische Verschlüsselung

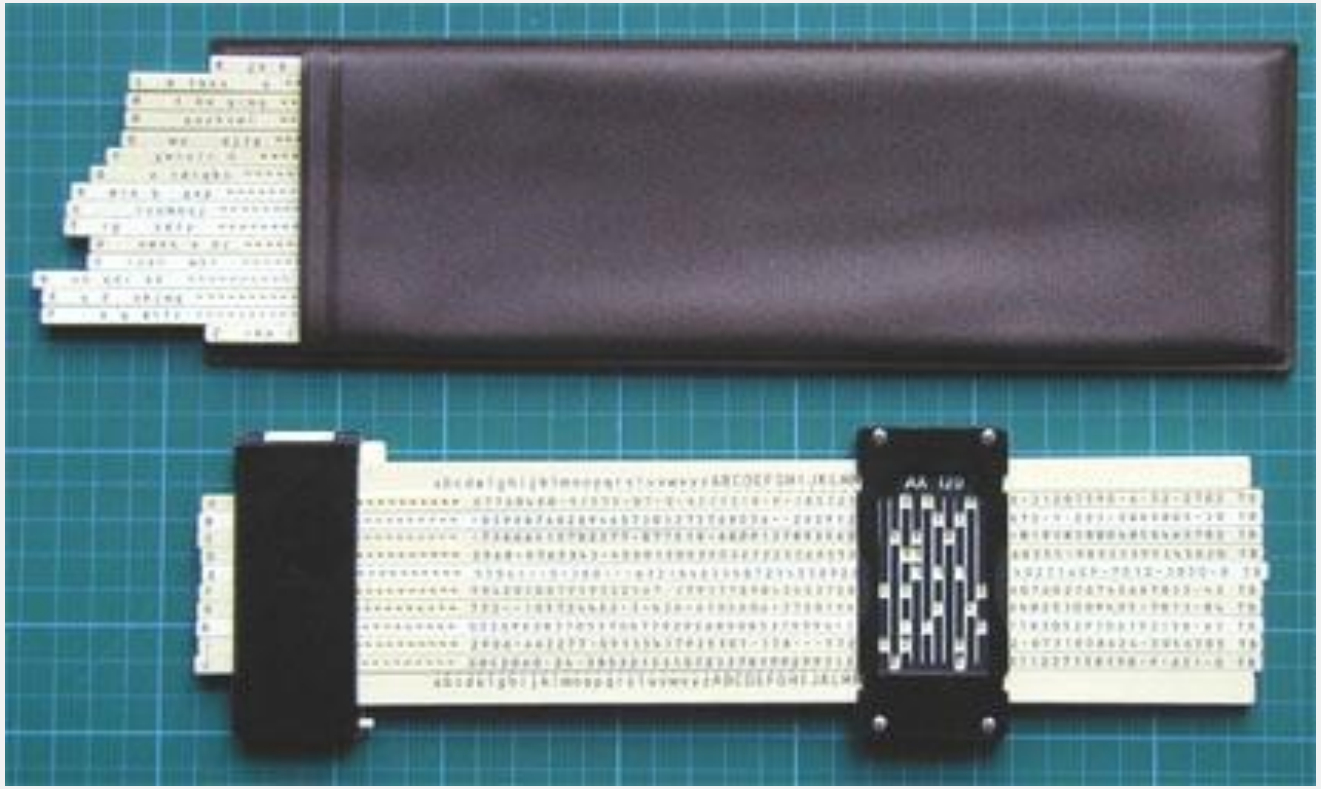
Polyalphabetische Verschlüsselung

Polyalphabetische Verschlüsselung





Polyalphabetische Verschlüsselung



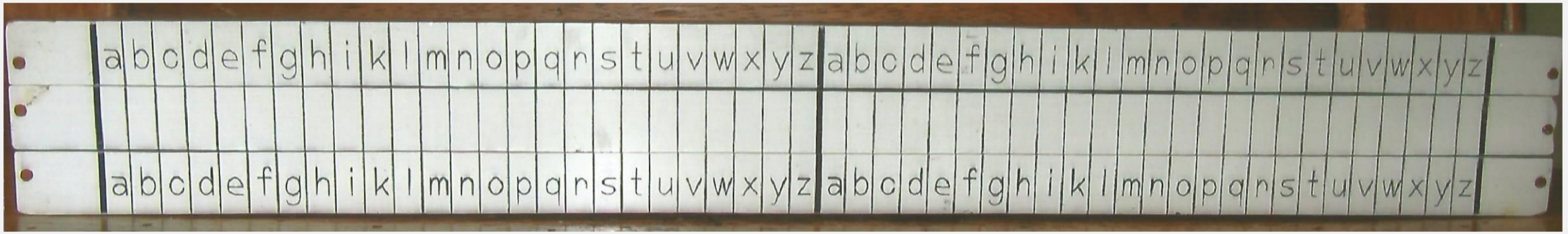
Reihenschieber,
Zentralstelle für das Chiffrierwesen,
Bonn, 1957,
1992 freigegeben

Aus der Zentralstelle für das Chiffrierwesen, einer Dienststelle des BND in Bonn, ging 1991 das ***Bundesamt für Sicherheit in der Informationstechnik*** (BSI) hervor.

Polyalphabetische Verschlüsselung

Reihenschieber, ***Zentralstelle für das Chiffrierwesen***, Bonn, 1957, 1992 freigegeben

Faber-Castell (?)



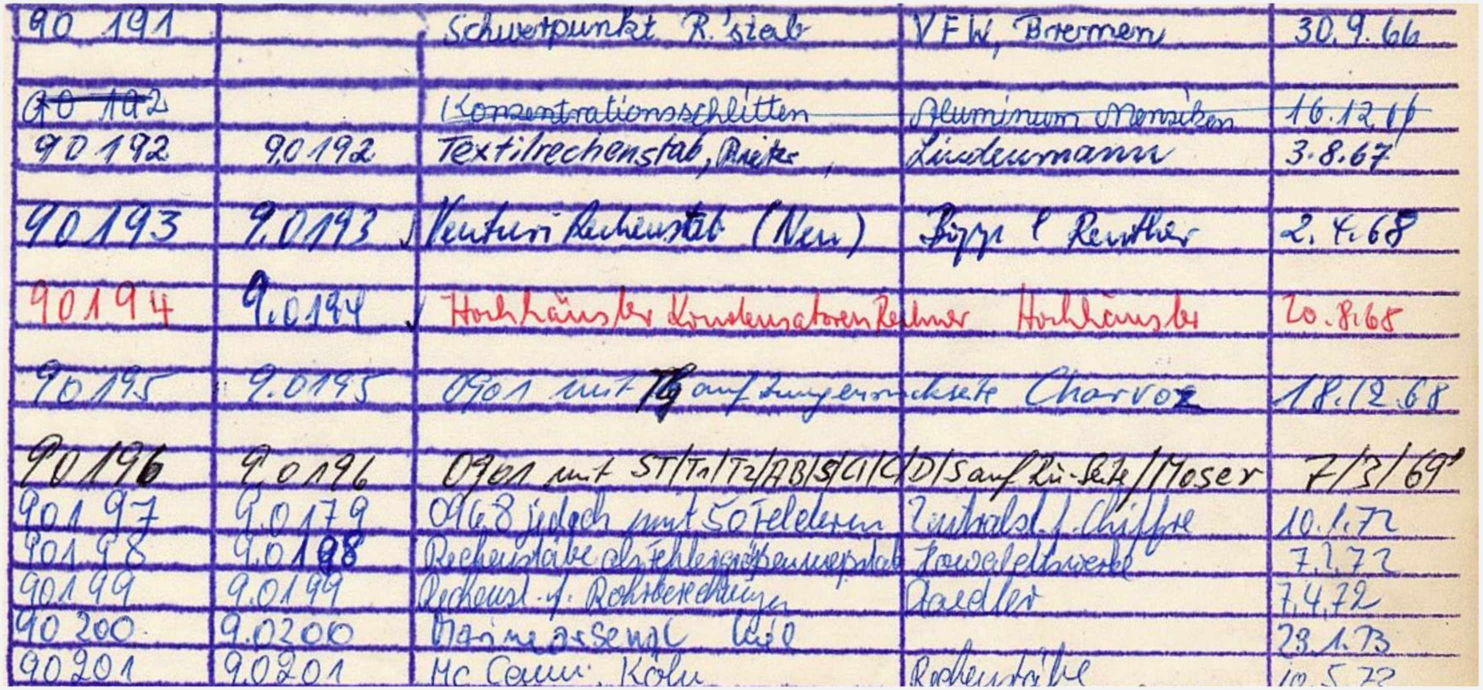
Aristo

Aristo 90197, 1972, 60 x 6 x 1 cm

Aristo

Aristo 90197, 1972, 60 x 6 x 1 cm

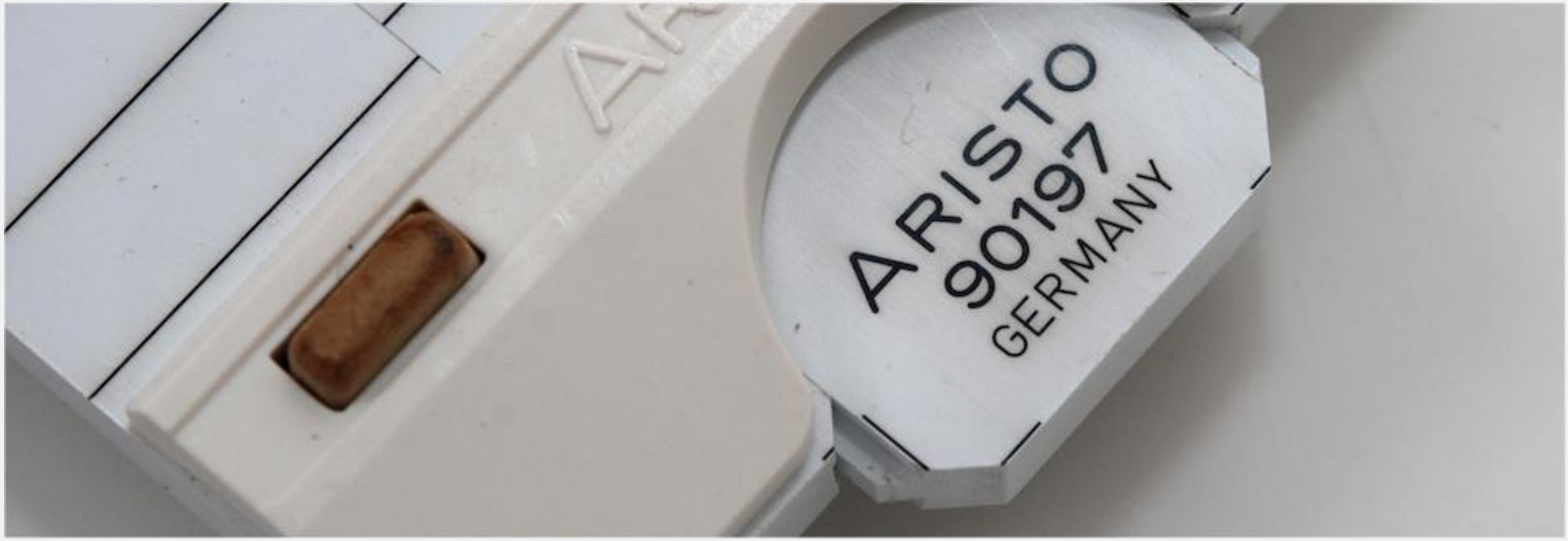
Aristo



90 191		Schwerpunkt R.'stab	VFW, Bremen	30.9.66
~~90 192~~		~~Konzentrationsschlitten~~	~~Aluminium [illegible]~~	~~16.12.66~~
90 192	9.0 192	Textilrechenstab, [illegible]	Lindemann	3.8.67
90193	9.0193	Venturi Rechenstab (Neu)	[illegible] & Reuther	2.4.68
90194	9.0194	Hochhäuser Kondensatoren Rechner	Hochhäuser	20.8.68
90195	9.0195	0901 mit Tg auf Zungenrückseite	Charvoz	18.12.68
90196	9.0196	0901 mit ST/T1/T2/AB/S/C1/C/D/S auf Rü-Seite	Moser	7/3/69
90197	9.0179	0968 jedoch mit 50 Teilen	Zentralst. f. Chiffre	10.1.72
90198	9.0198	Rechenstäbe als Fehlergrößenmeßstab	[illegible]werke	7.2.72
90199	9.0199	Rechenst. f. Rohrberechnungen	[illegible]	7.4.72
90200	9.0200	Marinearsenal Kiel		23.1.73
90201	9.0201	Mc Cann, Köln	Rechenstäbe	10.5.73

Aristo

90197	90179	0968 jedoch mit 50 Feldern	Zentralst. f. Chiffre	10.1.72



Aristo

Aristo 90197, 1972, 60 x 6 x 1 cm

RST28 – Moers