Das Zimmermann-Telegramm

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

15.12.2015



über mich



Über Mich

- Bildungswissenschaft/Psychologie
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Geek, Nerd, Hacker seit knapp 20 Jahren
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen



Schulungs- und Beratungsangebote

- Sicher unterwegs im Internet
- Anonymität und Überwachung im Internet
- Security Awareness Kampagnen konzipieren
- Netzwerke absichern/Penetration Testing
- Die psychologischen Grundlagen des Social Engineerings
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten



Informationstechnologie und Sicherheitspolitik

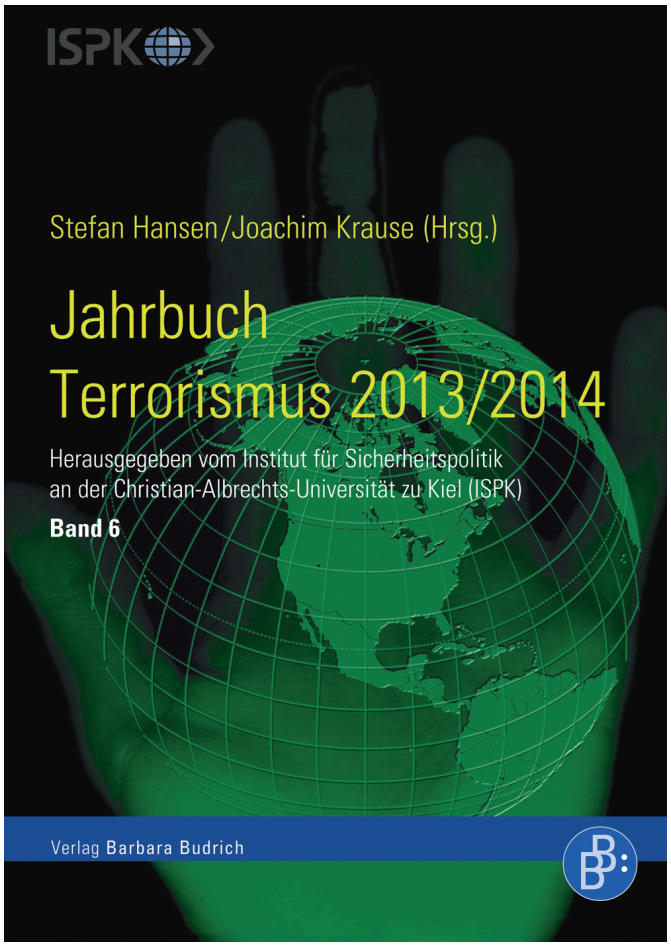
Sambleben, J. und Schumacher, S. (Herausgeber)



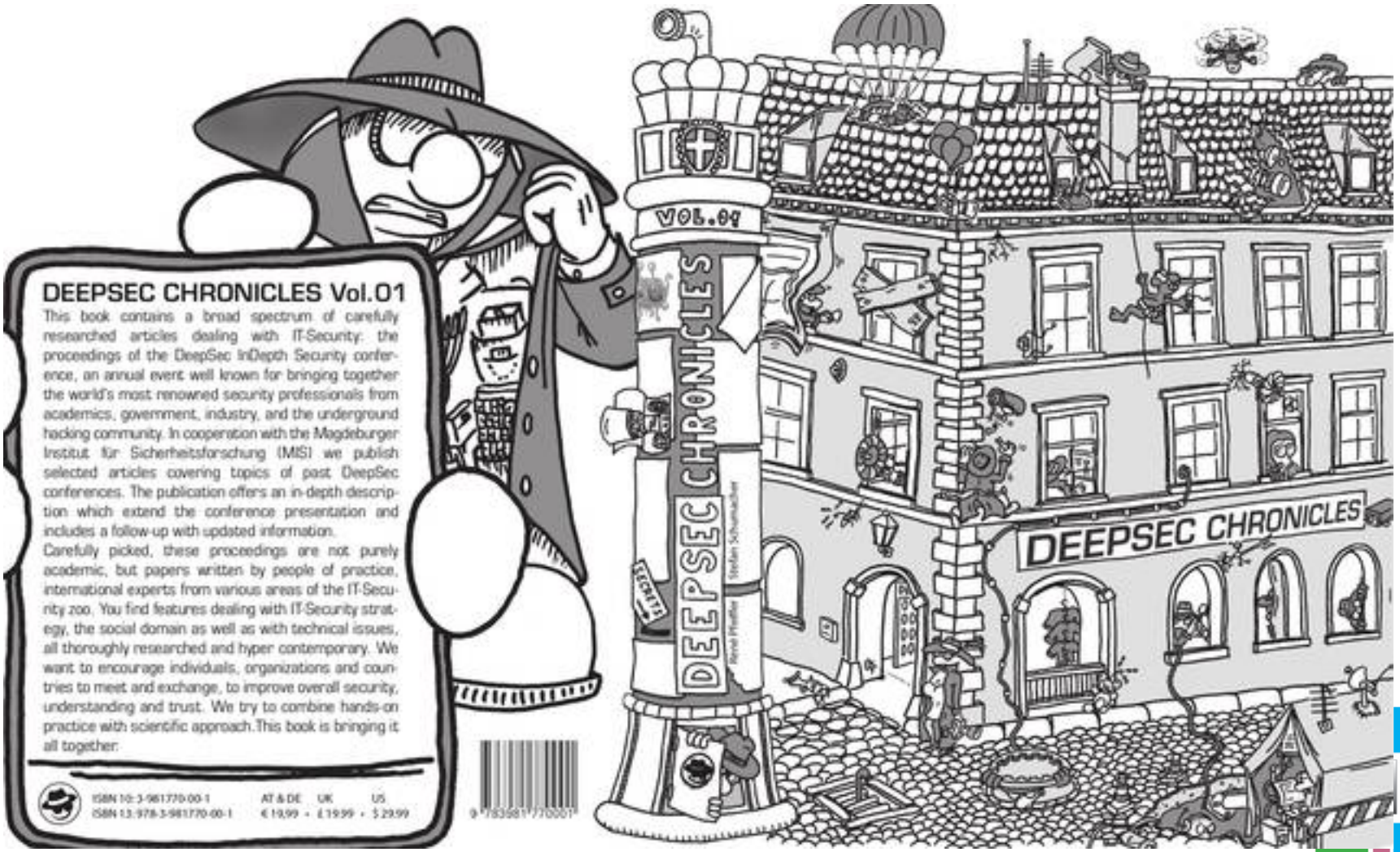
sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber, Institut für Sicherheitspolitik Kiel)



Stefan Schumacher:
Cyber-Terrorismus:
Reale Bedrohung oder Mythos?
S. 159 – 180


DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach.This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE UK US
€ 19,99 £ 19.99 $ 29.99
vol.01
DEEPSEC CHRONICLES
Stefan Schumacher
Ronni Pfeiffer
SECRETS
DEEPSEC CHRONICLES

- Stefan Schumacher and René Pfeiffer (editors)
- In Depth Security – Proceedings of the DeepSec Conference
- 360 Pages
- Magdeburger Institut für Sicherheitsforschung
- 978-3981770001
- `http://www.amazon.de/Depth-Security-Stefan-Schumacher/dp/3981770005/ref=sr_1_1?ie=UTF8&qid=1448888706`



Inhaltsverzeichnis

1 Politischer Hintergrund

2 Telekommunikation vor dem 1.WK

3 Kryptographie

4 Passwörter

5 Enigma



Zimmermann-Telegramm

- Arthur Zimmermann: 1916/17 Staatssekretär im Außenministerium
- USA Neutral
- Zimmermann sandte am 19.01.1917 die Zimmermann-Telegramm nach Mexiko
- über die deutsche Gesandtschaft in Washington D.C.



Zimmermann-Telegramm

- Angebot an Mexiko auf deutscher Seite in den Krieg einzutreten
- Deutschland würde Mexiko unterstützen
- die 1848 verlorenen Gebiete zurückzubekommen
- u.a. Kalifornien, Nevada, Arizona, New Mexico, Utah, Teile Colorados und Wyomings



Zimmermann-Telegramm

- Telegramm wurde vom britischen Marinegeheimdienst abgefangen
- und konnte dechiffriert werden
- und die USA zum Kriegseintritt bewegen



Inhaltsverzeichnis

1 Politischer Hintergrund

2 Telekommunikation vor dem 1.WK

3 Kryptographie

4 Passwörter

5 Enigma

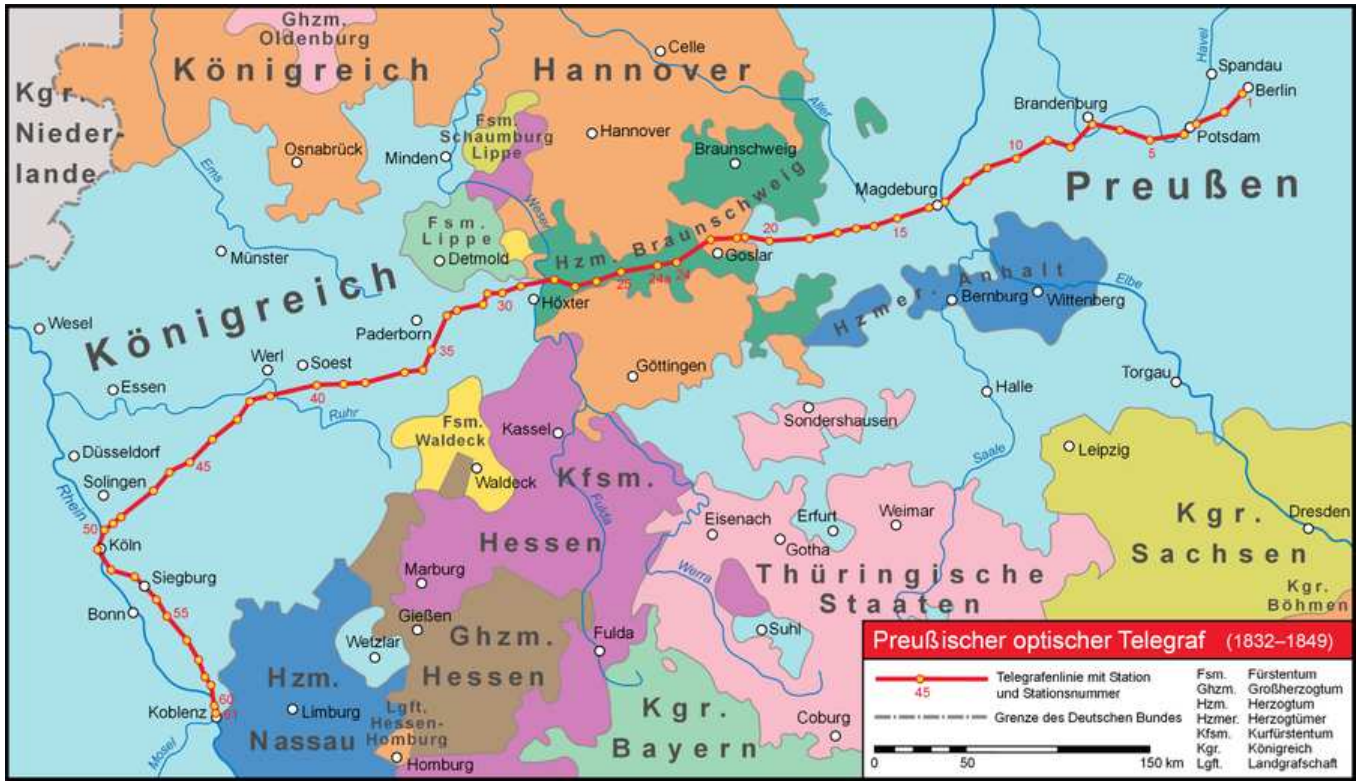


Preußische Optische Telegraf

- Zwischen 1832 und 1849 betrieben
- verband Berlin mit Koblenz
- 62 Telegrafenstationen mit Signalmasten
- 6 Winkerarme mit Seilzügen am Signalmast
- 7,5 – 15km Distanz



Telegrafenlinie



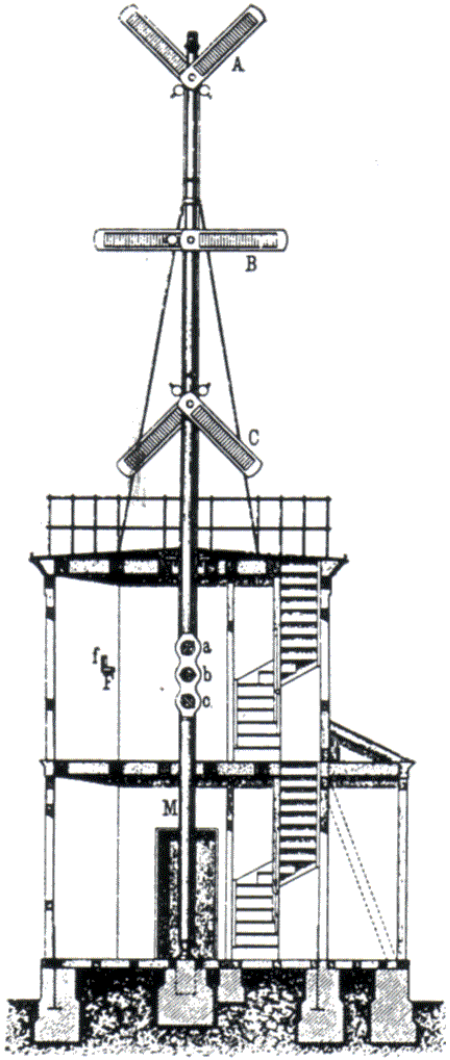
Telegraf in Flittard



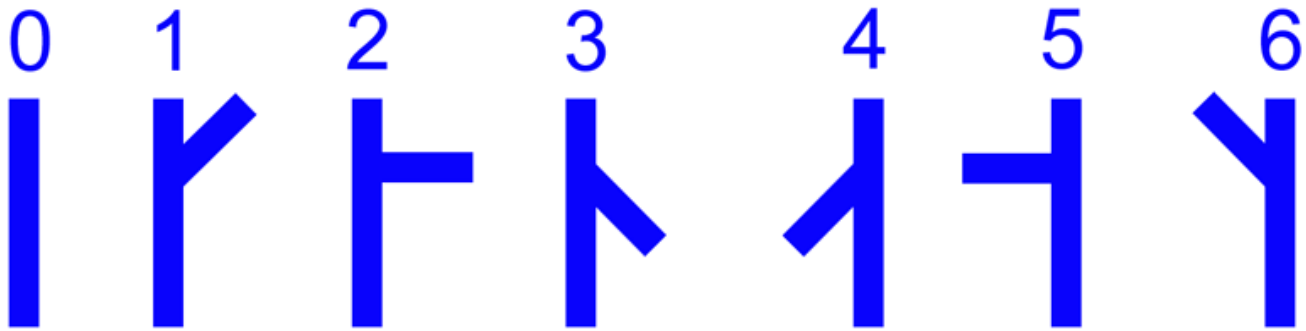
Telegraf in Flittard - Handhebel



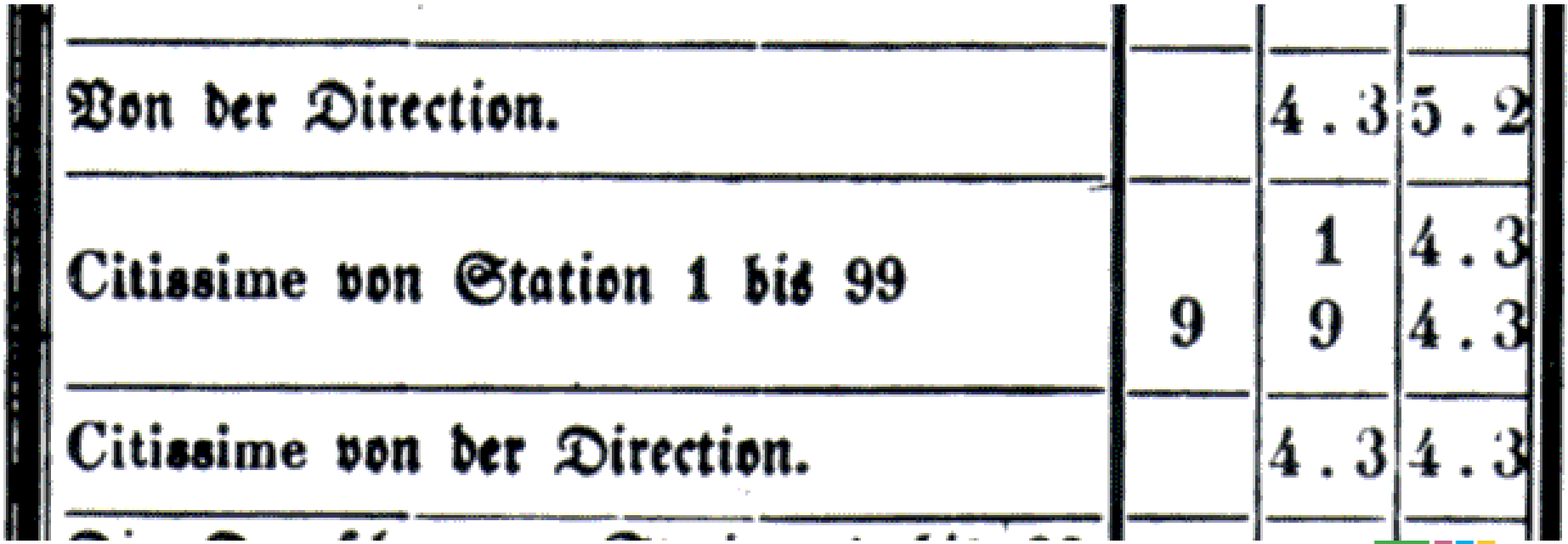
Telegraf - Schnittzeichnung



Hebelstellung 0-6



Code-Buch



Von der Direction.		4.3	5.2
Citissime von Station 1 bis 99	9	1 9	4.3 4.3
Citissime von der Direction.		4.3	4.3

Geschwindigkeit

- im Schnitt 1,5 Zeichen pro Minute ablesen und stellen
- 7,5 - 14 Minuten für ein Zeichen beim Durchlauf der Strecke
- 2 - 6 Nachrichten pro Tag transportiert
- 2.2.1840: Telegramm mit 210 Wörtern von Berlin nach Köln: 13 Stunden
- 17.3.1848 – Telegramm mit 30 Wörtern von Berlin nach Köln: 1,5 Stunden



Verlässlichkeit

- Abhängig von Wind und Wetter
- Tageslicht und freie Sicht
- 1848: Anschlag auf Station 43
- keine Verschlüsselung o.ä.



Elektrische Telegrafie

- Erste Versuche ab 1833 durch Weber, Gauß, Steinheil
- 1837: private Versuche durch den preußischen Telegrafendirektor O'Etzel
- 1846: erste Versuchsstrecke an der Bahnstrecke Berlin - Potsdam
- 1849: Inbetriebnahme der elektromechanischen Telegrafenlinien Berlin - Frankfurt; Berlin - Köln
- massive Unterstützung durch Eisenbahnlinien

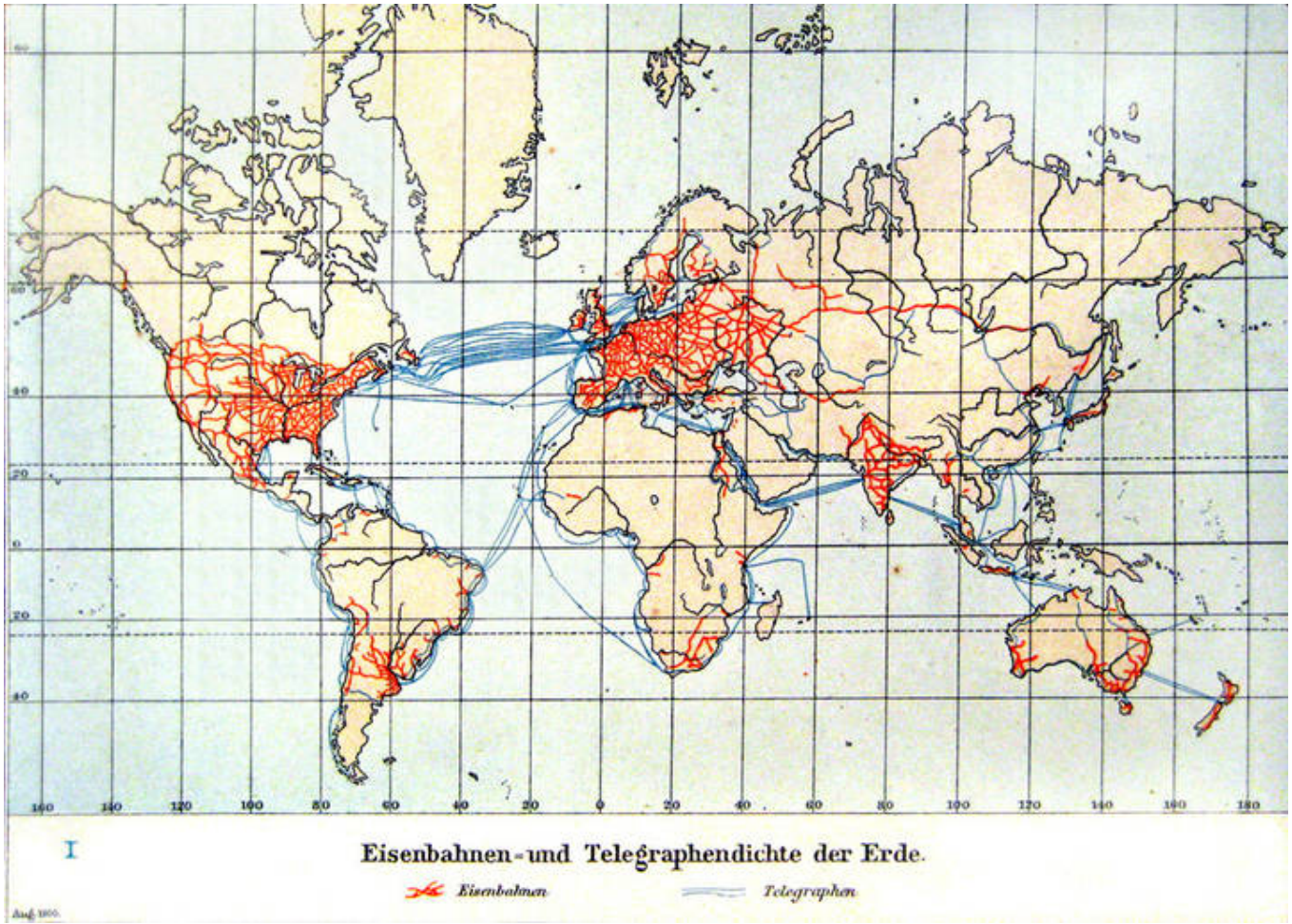


Elektrische Telegrafie

- Übertragung von codierten Signalen per Kabel
- z.B. Morsecode, Zeigertelegraph von Siemens und Halske
- unabhängig vom Wetter und Licht
- zuverlässiger und schneller
- kann größere Strecken überwinden
- z.B. per Seekabel, die aber korrodierten und rissen



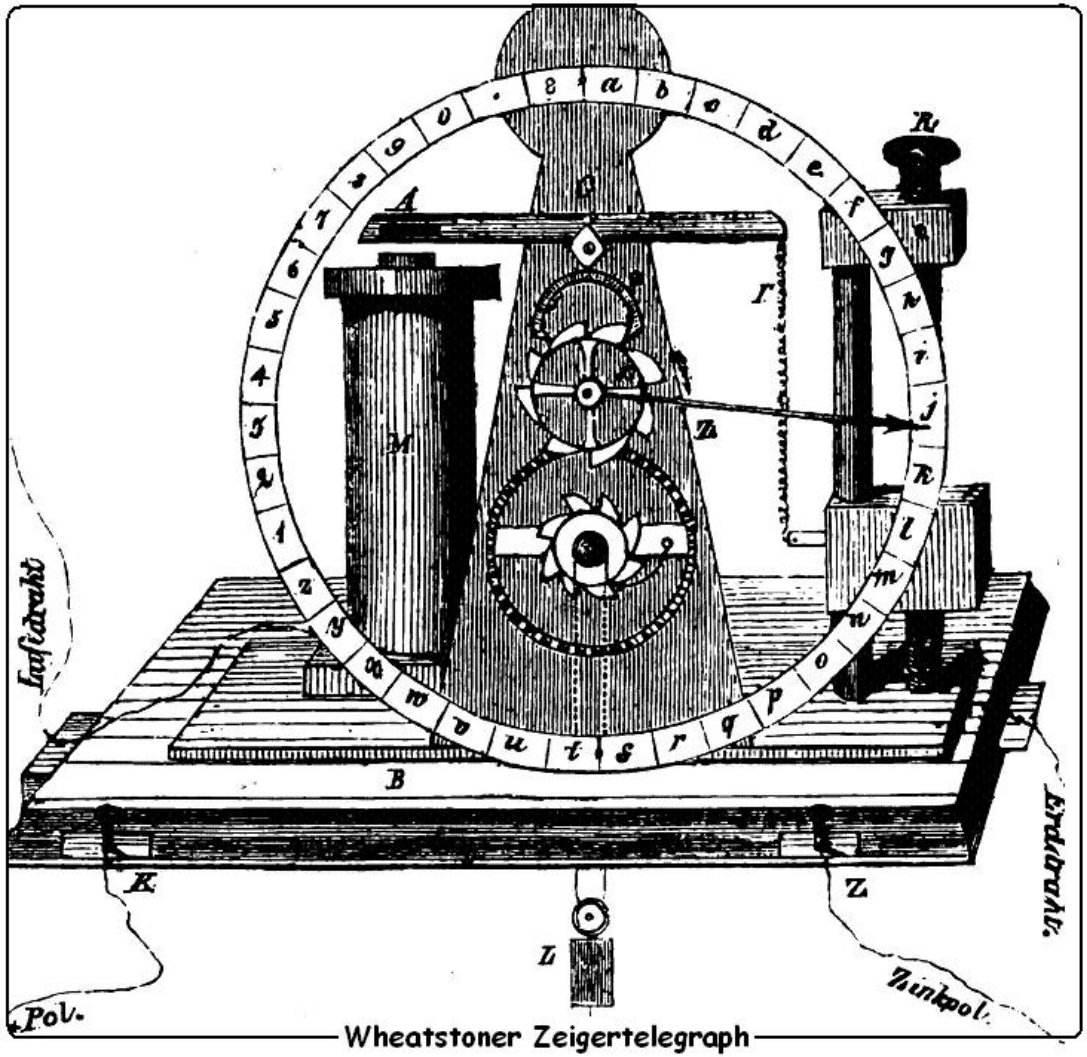
Code-Buch


Eisenbahnen-und Telegraphendichte der Erde.
Eisenbahnen
Telegraphen

Zeigertelegraf Siemens und Halske



Schema Zeigertelegraf



Funktelegrafie

- 1909 Nobelpreis für Marconi und Braun
- 20.09.1898: Funkverbindung am Physikalischen Institut in Strassburg durch Ferdinand Braun
- 24.09.1900: Funkstrecke Cuxhaven - Helgoland (62km)
- Marconi errichtete 1899 die erste Funkstrecke über den Ärmelkanal
- 12.12.1901: erste Transatlantikverbindung von Cornwall nach Neufundland
- Übertragen wurden Morsezeichen
- heftige Konkurrenz zwischen Marconi und Telefunken
- Funker durften Notrufe von Konkurrenzsendern nicht annehmen
- Deutsches Seenotzeichen ...—... 1906 international übernommen



Morsezeichen

- Drei Zeichen: Punkt (.), Strich (-), Pause ( )
- dit, dah, *Schweigen*
- Punkt ist kleinste Zeiteinheit, Strich ist 3x Strich, Zwischen Buchstaben Pause von 1 Strich, Zwischen Wörtern Pause von 7 Punkten
- häufige Buchstaben weniger Zeichen



Funktelegrafie

- Funktelegrafie immer bedeutender
- Einsatz bei vielen zivilen und militärischen Marinen
- Keine Abstimmung in den ersten Jahren
- verbindliche Regeln durch ITU durchgesetzt
- z.B. nach dem Titanic-Untergang
- Einsatz im Militär durch Telegrafentruppen, Fernmelder



Funktelegrafie

- sollte 1920 in den deutschen Armeen eingeführt werden
- Fernschreiber schon vor dem 1.WK ausgesondert
- kein Material, Nachwuchs, logistisches Chaos
- Information konnte nicht geteilt werden
- führte u.a. zum Stellungskrieg durch falsche Lagebeurteilung
- Kommunkationslösungen durch einzelne Truppenteile
- Feldtelefone der Artillerie für VB erhöhten die Kampfkraft massiv
- Kommunikation der Truppenteile untereinander bzw. mit Führern



Inhaltsverzeichnis

1 Politischer Hintergrund

2 Telekommunikation vor dem 1.WK

3 Kryptographie

4 Passwörter

5 Enigma



Kerckhoffs' Prinzip

Auguste Kerckhoffs 1883

1. Eine verschlüsselte Nachricht darf ohne Schlüssel nicht effizient zu entschlüsseln sein;
2. die Kommunikationspartner dürfen keinen Schaden erleiden, wenn das Verschlüsselungssystem bekannt wird;
3. der Schlüssel muss leicht zu merken und auswechselbar sein;
4. die Kryptogramme müssen übertragbar sein;
5. der Chiffrierapparat und die Dokumente müssen transportierbar sein;
6. das System muss einfach zu benutzen sein;
7. das Chiffriersystem sollte von Experten gut untersucht sein.

Caesar

Xrffva, 31. Qrmrzore. Zrvar yvror Znzn! Qnf jveq aha jbuy rva ynatre Fpuervoroevrs jreqra, qraa vpu unor – qvr Xnegr erpuarg avpug – ynatr avpugf iba zve uöera ynffra. Nyf vpu qnf yrgmgrzny fpuevro, fgrpxgr vpu abpu va qra Jrvuanpugfibeorervghatra, wrgmg yvrtra qvr Jrvuanpugfgntr fpuba mheüpx.



Caesar

Xrffva, 31. Qrmrzore. Zrvar yvror Znzn! Qnf jveq aha jbuy rva ynatre Fpuervoroevrs jreqra, qraa vpu unor – qvr Xnegr erpuarg avpug – ynatr avpugf iba zve uöera ynffra. Nyf vpu qnf yrgmgrzny fpuevro, fgrpxgr vpu abpu va qra Jrvuanpugfibeorervghatra, wrgmg yvrtra qvr Jrvuanpugfgntr fpuba mheüpx.



Caesar

Xrffva, 31. Qrmrzore. Zrvar yvror Znzn! Qnf jveq aha jbuy rva ynatre Fpuervoroevrs jreqra, qraa vpu unor – qvr Xnegr erpuarg avpug – ynatr avpugf iba zve uöera ynffra. Nyf vpu qnf yrgmgrzny fpuevro, fgrpxgr vpu abpu va qra Jrvuanpugfibeorervghatra, wrgmg yvrtra qvr Jrvuanpugfgntr fpuba mheüpx.



Caesar

Xrffva, 31. Qrmrzore. Zrvar yvror Znzn! Qnf jveq aha jbuy rva ynatre Fpuervoroevrs jreqra, qraa vpu unor – qvr Xnegr erpuarg avpug – ynatr avpugf iba zve uöera ynffra. Nyf vpu qnf yrgmgrzny fpuevro, fgrpxgr vpu abpu va qra Jrvuanpugfibeorervghatra, wrgmg yvrtra qvr Jrvuanpugfgntr fpuba mheüpx.

Kessin, 31. Dezember. Meine liebe Mama! Das wird nun wohl ein langer Schreibebrief werden, denn ich habe – die Karte rechnet nicht – lange nichts von mir hören lassen. Als ich das letztemal schrieb, steckte ich noch in den Weihnachtsvorbereitungen, jetzt liegen die Weihnachtstage schon zurück.



Caesar

Xrffva, 31. Qrmrzore. Zrvar yvror Znzn! Qnf jveq aha jbuy rva ynatre Fpuervoroevrs jreqra, qraa vpu unor – qvr Xnegr erpuarg avpug – ynatr avpugf iba zve uöera ynffra. Nyf vpu qnf yrgmgrzny fpuevro, fgrpxgr vpu abpu va qra Jrvuanpugfibeorervghatra, wrgmg yvrtra qvr Jrvuanpugfgntr fpuba mheüpx.

Kessin, 31. Dezember. Meine liebe Mama! Das wird nun wohl ein langer Schreibebrief werden, denn ich habe – die Karte rechnet nicht – lange nichts von mir hören lassen. Als ich das letztemal schrieb, steckte ich noch in den Weihnachtsvorbereitungen, jetzt liegen die Weihnachtstage schon zurück.



grundlegende Verfahren

Definition (Transposition)

- Vertauschung der Stellen
- Anzahl der Transpositionen ist $n!$
- festes Muster in M grenzt Raum ein



Transposition: Skytale, ca 500 v. Chr.



grundlegende Verfahren

Definition (Substitution)

- Ersetzung der Zeichen durch andere Zeichen
- monoalphabetische: genau ein Geheimtextalphabet mit fester Zuordnung
- polyalphabetische: mehrere Geheimtextalphabete ohne feste Zuordnung

Caesar/Rot13: ist involutorisch

```
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
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
```



grundlegende Verfahren

Definition (Substitution)

- Ersetzung der Zeichen durch andere Zeichen
- monoalphabetische: genau ein Geheimtextalphabet mit fester Zuordnung
- polyalphabetische: mehrere Geheimtextalphabete ohne feste Zuordnung

Caesar/Rot13: ist involutorisch

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
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



grundlegende Verfahren

Definition (Substitution)

- Ersetzung der Zeichen durch andere Zeichen
- monoalphabetische: genau ein Geheimtextalphabet mit fester Zuordnung
- polyalphabetische: mehrere Geheimtextalphabete ohne feste Zuordnung

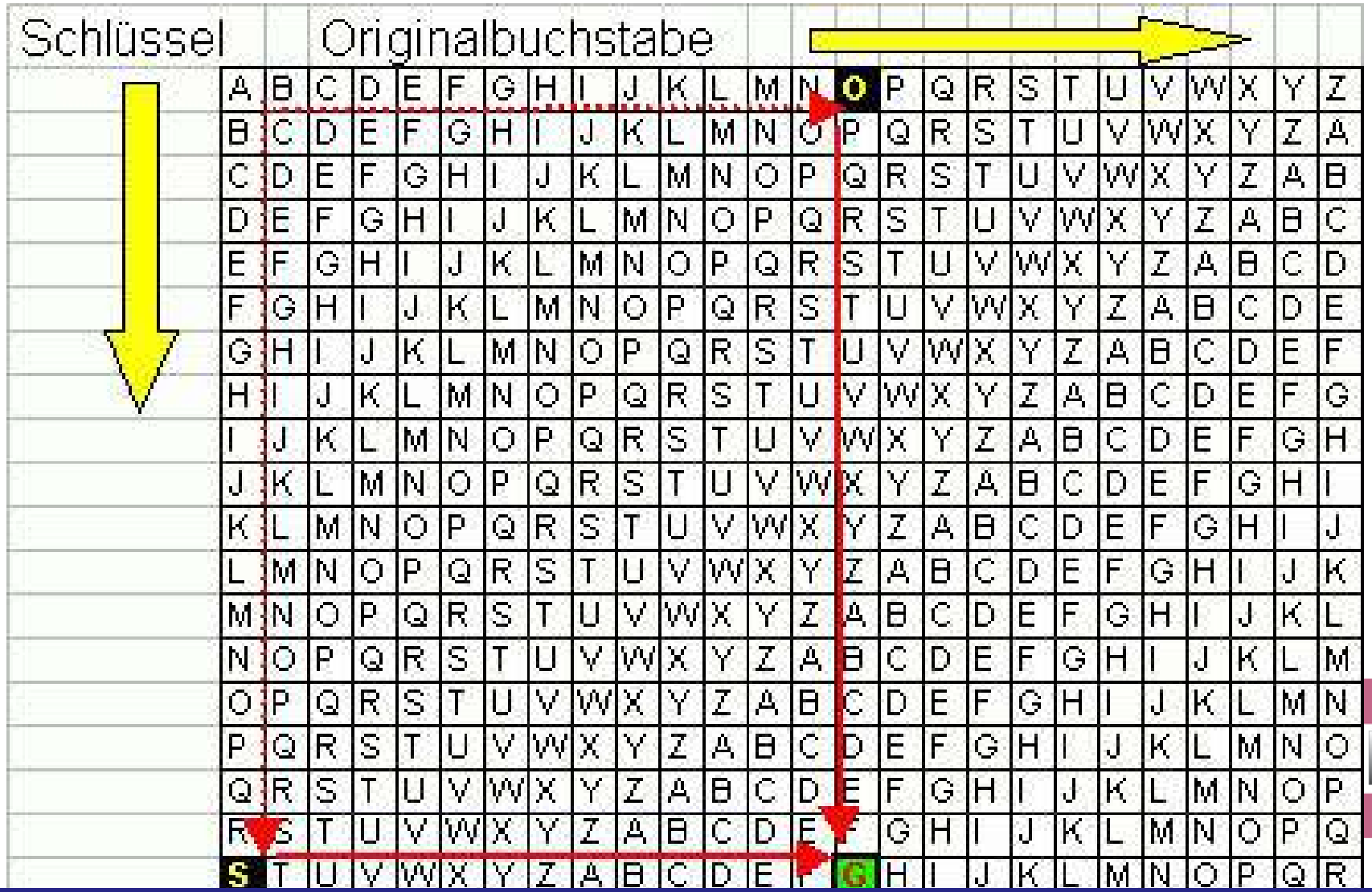
Caesar/Rot13: ist involutorisch

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

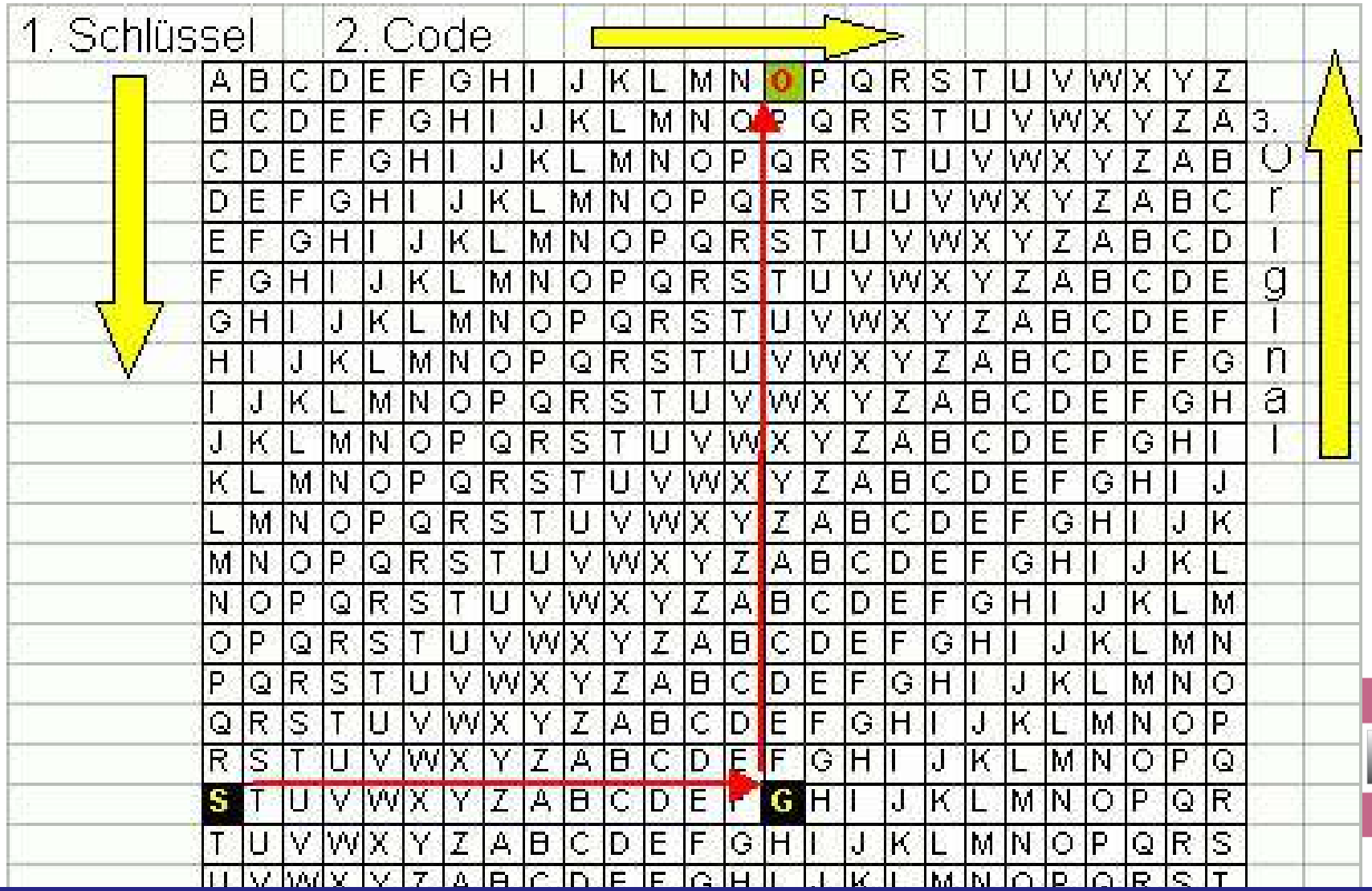
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M



Substitution: Vigenere-Tabelle (†1596)



Substitution: Vigenere-Tabelle (†1596)



Schwächen

Substitution behält Muster im Text bei:

- Wortgrenzen
- Groß-/Kleinschreibung
- Buchstabenhäufigkeiten (ERNSTL)
- statistische Auswertung möglich
- Room 40; Bletchley Park; Bomba; Turing-Bombe; Perl-Skripte



Schwächen

Substitution behält Muster im Text bei:

- Wortgrenzen
- Groß-/Kleinschreibung
- Buchstabenhäufigkeiten (ERNSTL)
- statistische Auswertung möglich
- Room 40; Bletchley Park; Bomba; Turing-Bombe; Perl-Skripte



heutige Algorithmen

- basieren immer noch auf Substitution und Transposition
- mit mehreren Runden
- und komplexer
- und pseudozufälliger
- DES: 16 Runden von Substitution und Transposition
- Feistelnetzwerke



Codebücher

- seit den optischen Telegrafen verwendet
- vereinfachten und verkürzten Funkverkehr
- auch beim Morsen via Draht oder Funk weiter verwendet
- dienten der »Verschlüsselung« von militärischen Nachrichten
- Wörter wurden nummeriert, oft alphabetisch
- SMS-Code: HDGDL, BRB, CUL



Codebücher

- einteiliges Codebuch: Klartext und Chiffrat lexikographisch angeordnet
- Rückschlüsse leichter zu ziehen, das Muster bekannt
- zweiteiliges Codebuch: Klartext sortiert, Chiffrat nicht
- inverses Codebuch nötig, aber schwerer zu knacken
- Überschlüsselung durch Transposition oder Substitution

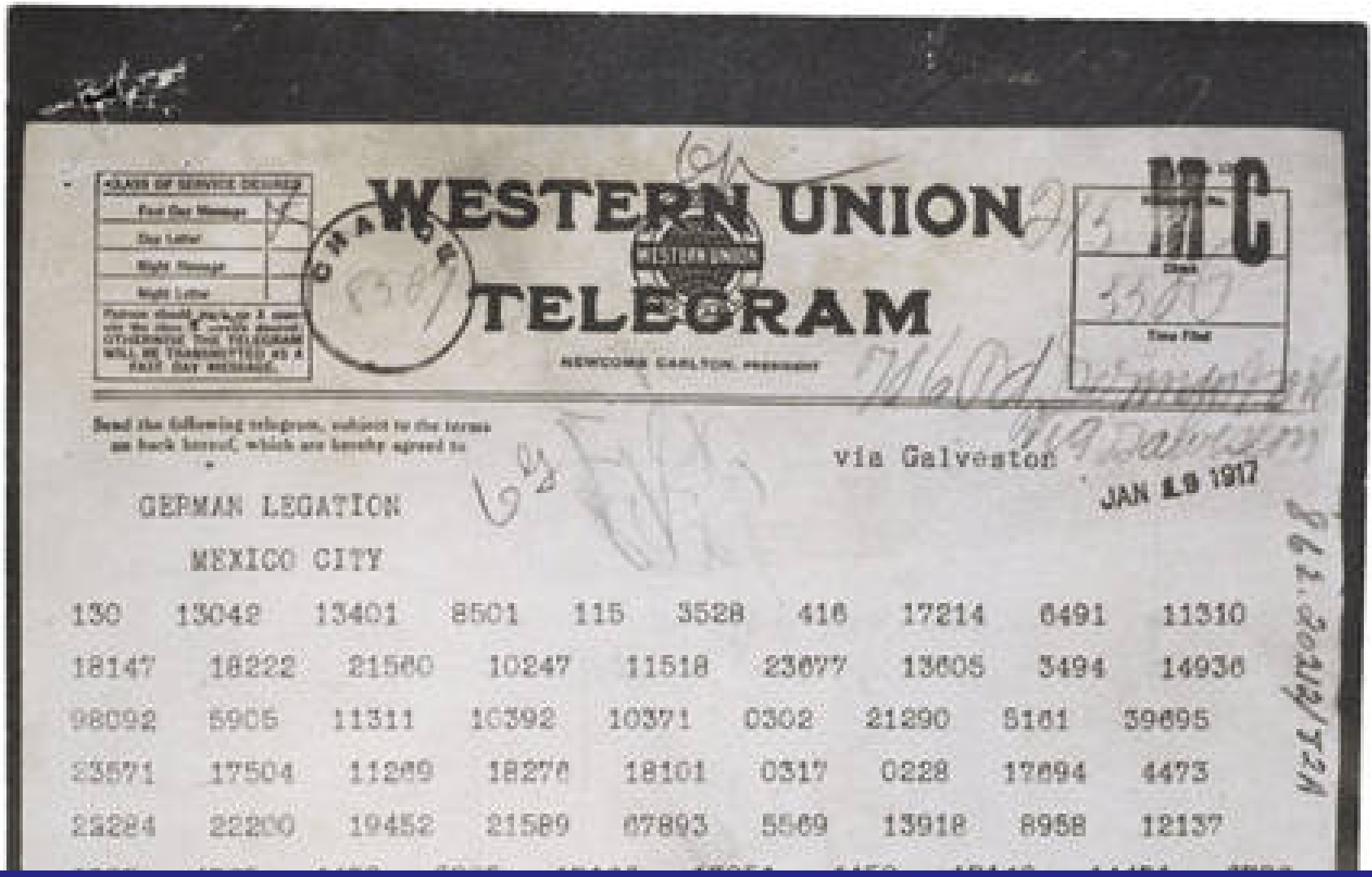


Codebücher

- Deutsche Marine nutzte Signalbücher
- 25.08.1914: SMS Magdeburg vor Estland aufgelaufen
- russische Taucher können 3 Signalbücher bergen
- 13.10.1914 wird dem britischen Marinegeheimdienst ein Codebuch geschenkt
- massiver strategischer und taktischer Vorteil



Zimmermann-Telegramm



WESTERN UNION

TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310

18147 18222 21560 10247 11518 23677 13605 3494 14936

98092 5905 11311 16392 10371 0302 21290 5161 39695

23571 17504 11269 18276 18101 0317 0228 17694 4473

25284 22290 19452 21589 67893 5569 13918 8958 12137

Zimmermann-Telegram

- britischer Marinegeheimdienst entziffert Teile des Telegramms
- überreicht Dechiffrat an die US-Regierung
- muss aber einen Monat mit der Veröffentlichung warten um den Codebruch zu verschleiern
- Legendierung: Telegramm in der deutschen Botschaft gestohlen
- Telegramm war nicht einmal doppelt chiffriert oder überschlüsselt



Inhaltsverzeichnis

1 Politischer Hintergrund

2 Telekommunikation vor dem 1.WK

3 Kryptographie

4 Passwörter

5 Enigma



Passwörter

- werden gehasht gespeichert
- Hash := mathematische Einwegfunktion
- Passwort $\rightsquigarrow$ Hash: einfach
- Hash $\rightsquigarrow$ Passwort: schwer
- `Magdeburg: 59aceadf846f772736c4b40eee7b155d`
- `magdeburg: 7712722364ae231b5f777bac5dd2eb80`
- `magdeburG: eadfc761160224295a58847eee4cbdfc`
- `MagdeBurg: 95be682b322a5dea1d1992fed8a3880d`



Wörterbuchangriffe

Kombinatorik

- fröhliches Passwortraten: alle Kombinationen probieren
- $Anzahl\ Kombinationen = verfuegbare\ Buchstaben^{Passwortlaenge}$
- 26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$
- 99 Buchstaben, 10 Stellen: $99^{10} = 90.438.207.500.880.449.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende (43xAlter des Universums!)



Wörterbuchangriffe

Kombinatorik

- fröhliches Passwortraten: alle Kombinationen probieren
- $Anzahl\ Kombinationen = verfuegbare\ Buchstaben^{Passwortlaenge}$
- 26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$
- 99 Buchstaben, 10 Stellen: $99^{10} = 90.438.207.500.880.449.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx$ 570 Millionen Jahrtausende (43xAlter des Universums!)
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40\ Minuten$



Wörterbuchangriffe

Kombinatorik

- fröhliches Passwortraten: alle Kombinationen probieren
- $Anzahl\ Kombinationen = verfuegbare\ Buchstaben^{Passwortlaenge}$
- 26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$
- 99 Buchstaben, 10 Stellen: $99^{10} = 90.438.207.500.880.449.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx$ 570 Millionen Jahrtausende (43xAlter des Universums!)
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40\ Minuten$

Inhaltsverzeichnis

1 Politischer Hintergrund

2 Telekommunikation vor dem 1.WK

3 Kryptographie

4 Passwörter

5 Enigma



Enigma

- 23.02.1918 meldet Dr.-Ing. Arthur Scherbius die Enigma zum Patent an
- international vermarktet
- Mitte der 1920er vom Markt genommen, da militärisches Interesse
- ca. 30 000 – 200 000 Enigmas im 2. WK produziert
- eingesetzt bei Reichswehr, Polizei, Geheimdienst, Wehrmacht, SS, SD, Reichspost, Reichsbahn



Enigma



Aufbau

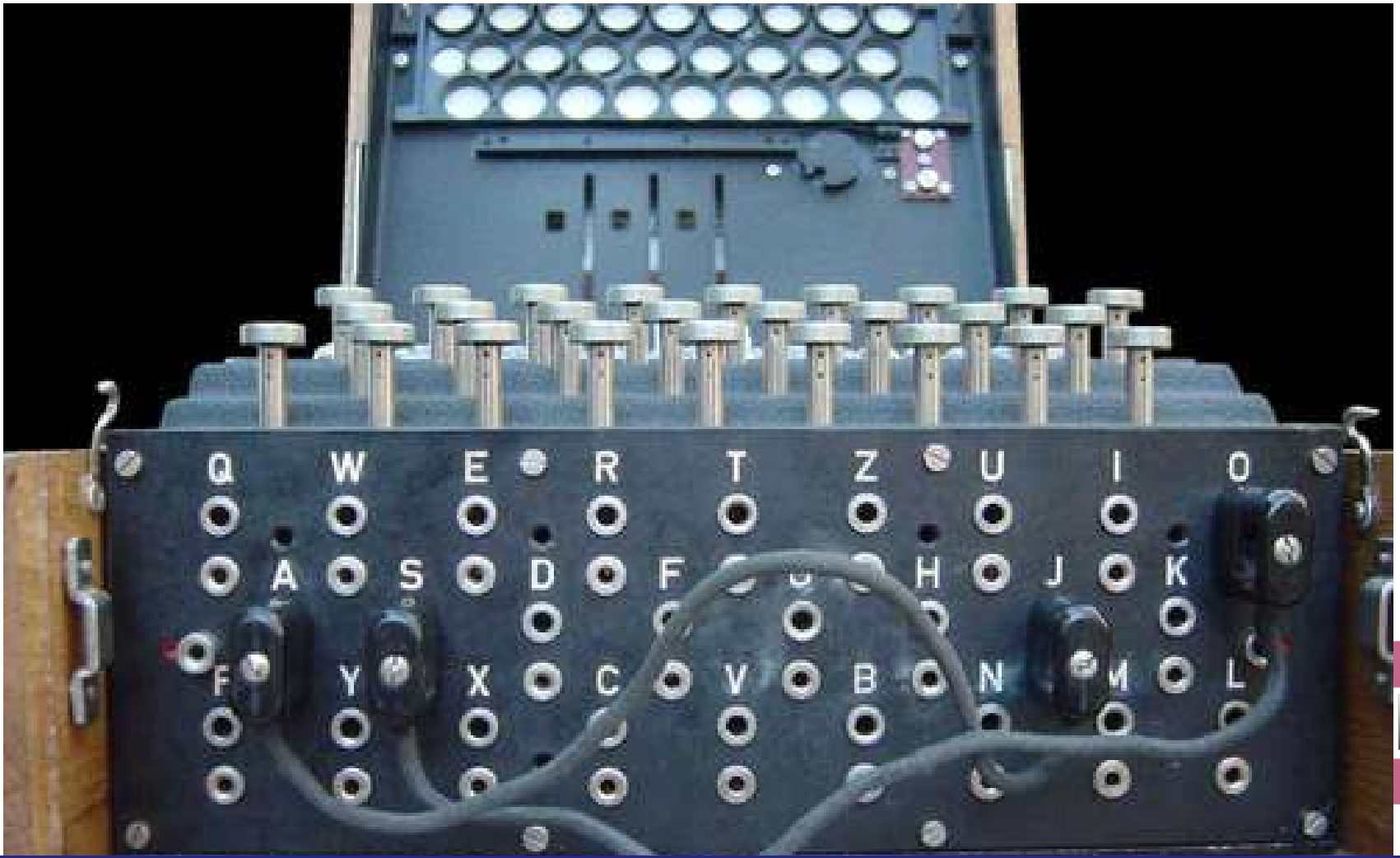
Tastatur	Eingabe
Steckerbrett	monoalphabetische Substition des Eingabebuchstabens
Walzen	elektrisch: polyalphabetische Substitution der Eingabe, mechanisch: Änderung der Walzenlage nach 26 Umdrehungen $\rightsquigarrow$ Änderung des Alphabets
Umkehrwalze	lenkt den Stromfluss der Eingabe wieder zur Ausgabe zurück $\rightsquigarrow$ Involutorisch
Walzen	Strom fließt wieder über die Walzen zurück
Steckerbrett	nochmals monoalphabetische Substition des Eingabebuchstabens
Leuchtanzeige	Anzeige des Chiffrats

Involution: Maschine ver- und entschlüsselt mit selbem



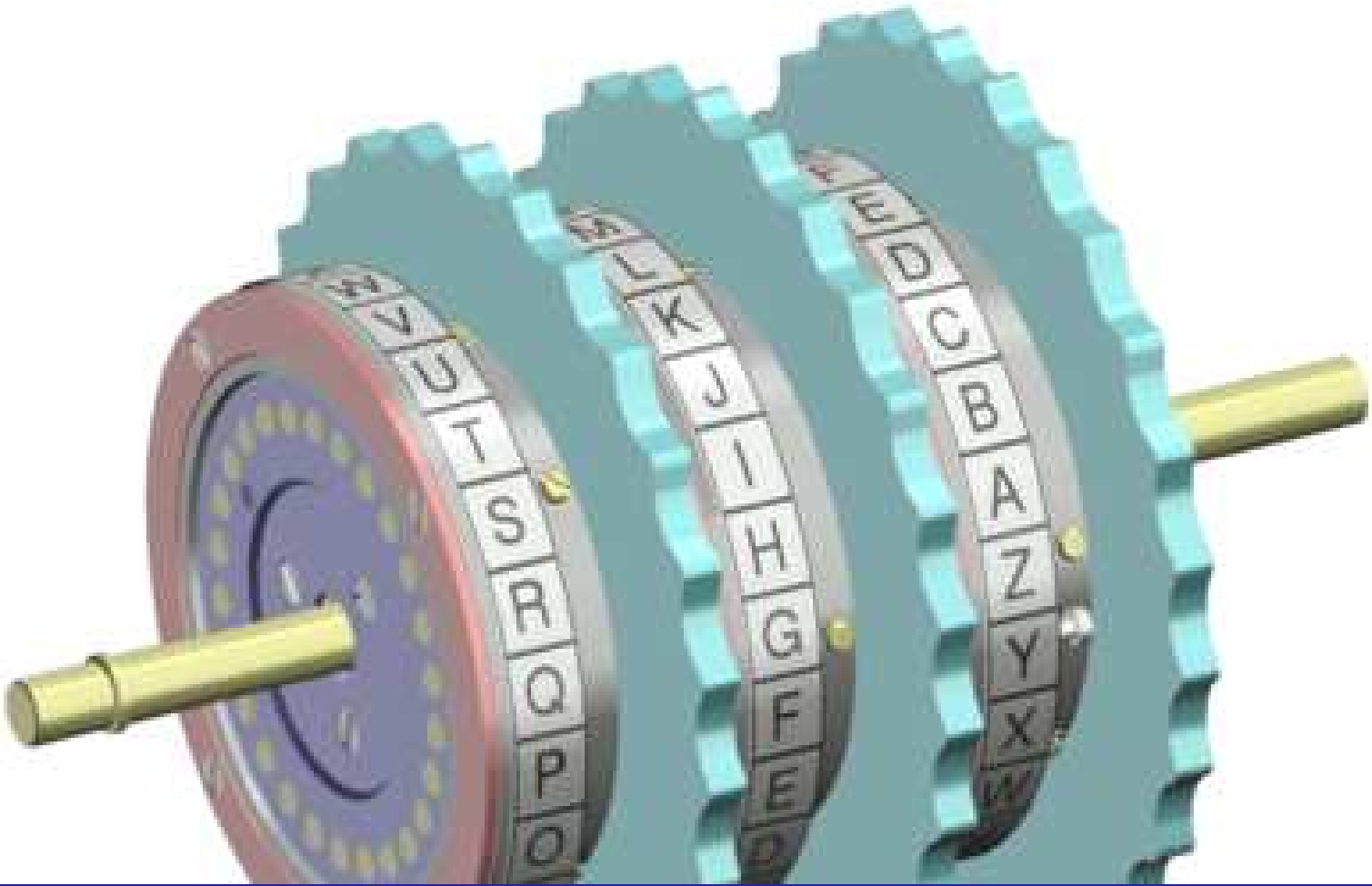
Enigma

Steckerbrett



Enigma

Walzensatz



Verdrahtungsschema

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

UKW	A	AE	BJ	CM	DZ	FL	GY	HX	IV	KW	NR	OQ
UKW	B	AY	BR	CU	DH	EQ	FS	GL	IP	JX	KN	MO
UKW	C	AF	BV	CP	DJ	EI	GO	HY	KR	LZ	MX	NW

Schlüsseltafel

Tag	UKW	Walzenlage	Ringstellung	---- Steckerverb
31	B	I IV III	16 26 08	AD CN ET FL GI J
30	B	II V I	18 24 11	BN DZ EP FX GT H
29	B	III I IV	01 17 22	AH BL CX DI ER F



Schwächen

- Involution vereinfachte den Aufbau, Ver- und Entschlüsselung möglich
- *¿Durch diesen Rückgang des Stromes durch den Chiffrierwalzensatz findet eine weitere Verwürfelung statt. Infolge dieser Anordnung ist es möglich, mit verhältnismäßig wenig Chiffrierwalzen auszukommen und trotzdem eine große Chiffriersicherheit aufrechtzuerhalten.¿* aus DRP Nr. 452 194
- fixpunktfreie Permutation $\rightsquigarrow$ Eingabe $\neq$ Ausgabe $\rightsquigarrow$ Verringerung der Alphabete



Fixpunkte

Alle Permutationen aus A B C D

ABCD ABDC ACBD ACDB ADBC ADCB
BACD BADC BCAD BCDA BDAC BDCA
CABD CADB CBAD CBDA CDAB CDBA
DABC DACB DBAC DBCA DCAB DCBA



Fixpunkte

Alle Permutationen aus A B C D
Alle Fixpunkt-Permutationen fallen weg

ABCD ABDC ACBD ACDB ADBC ADCB
BACD BADC BCAD BCDA BDAC BDCA
CABD CADB CBAD CBDA CDAB CDBA
DABC DACB DBAC DBCA DCAB DCBA



Fixpunkte

Alle Permutationen aus A B C D
Alle Fixpunkt-Permutationen fallen weg
Alle fixpunktfreien Permutationen werden benutzt

ABCD ABDC ACBD ACDB ADBC ADCB
BACD BADC BCAD BCDA BDAC BDCA
CABD CADB CBAD CBDA CDAB CDBA
DABC DACB DBAC DBCA DCAB DCBA



Fixpunktfreiheit: Nichts ist jemals es selbst

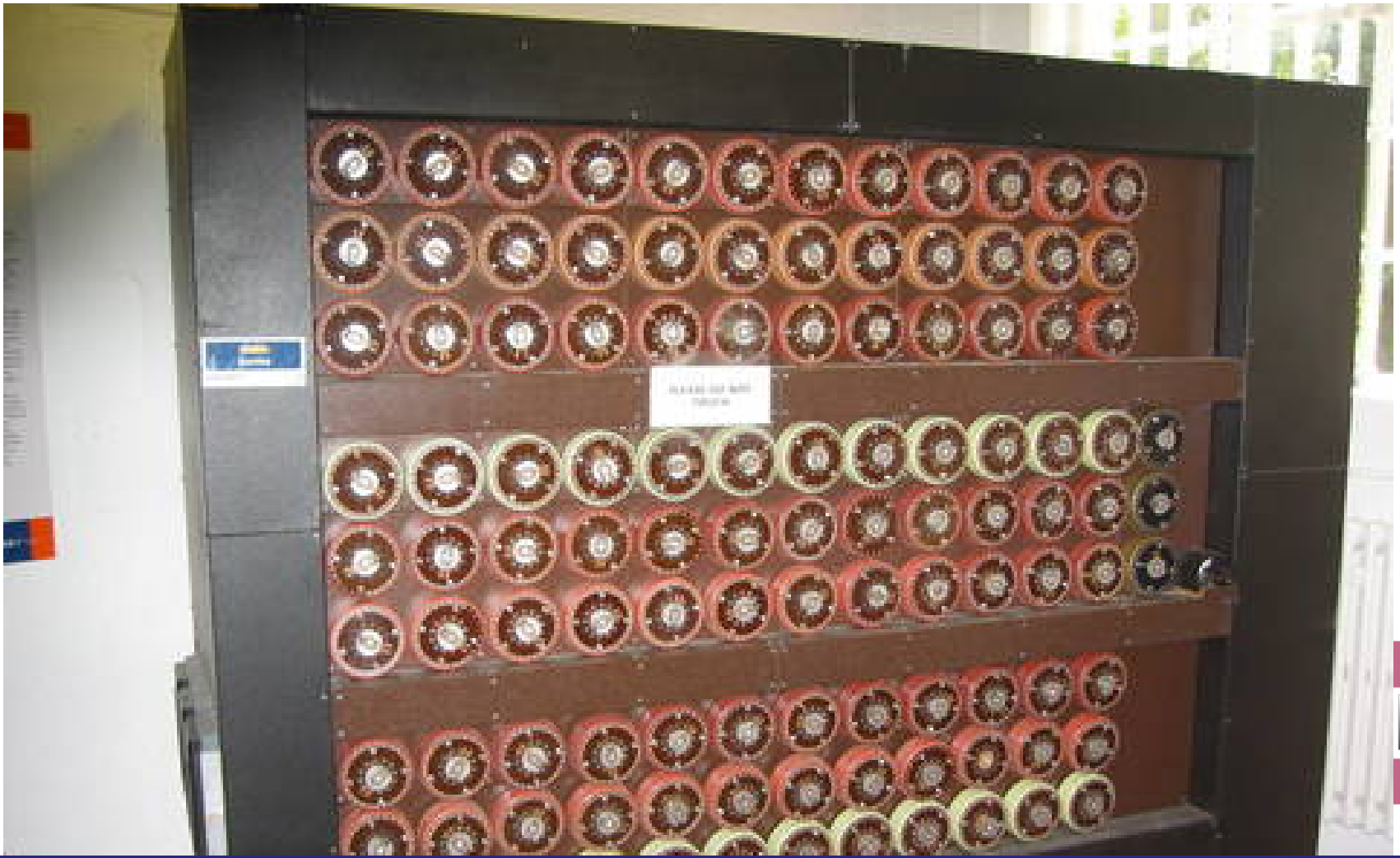
Ein A ist nie ein A, ein B nie ein B, ... $\rightsquigarrow$ Cribs

```
   BHNCXSEQKOBIIODWFBTZGCYEHQQJEWOYNBDXHQBALHTSSDPWG
1  OBERKOMMANDODERWEHRMACHT
 2  OBERKOMMANDODERWEHRMACHT
  3  OBERKOMMANDODERWEHRMACHT
   4  OBERKOMMANDODERWEHRMACHT
    5  OBERKOMMANDODERWEHRMACHT
     6  OBERKOMMANDODERWEHRMACHT
      7  OBERKOMMANDODERWEHRMACHT
```



Enigma

Turing-Bombe



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co