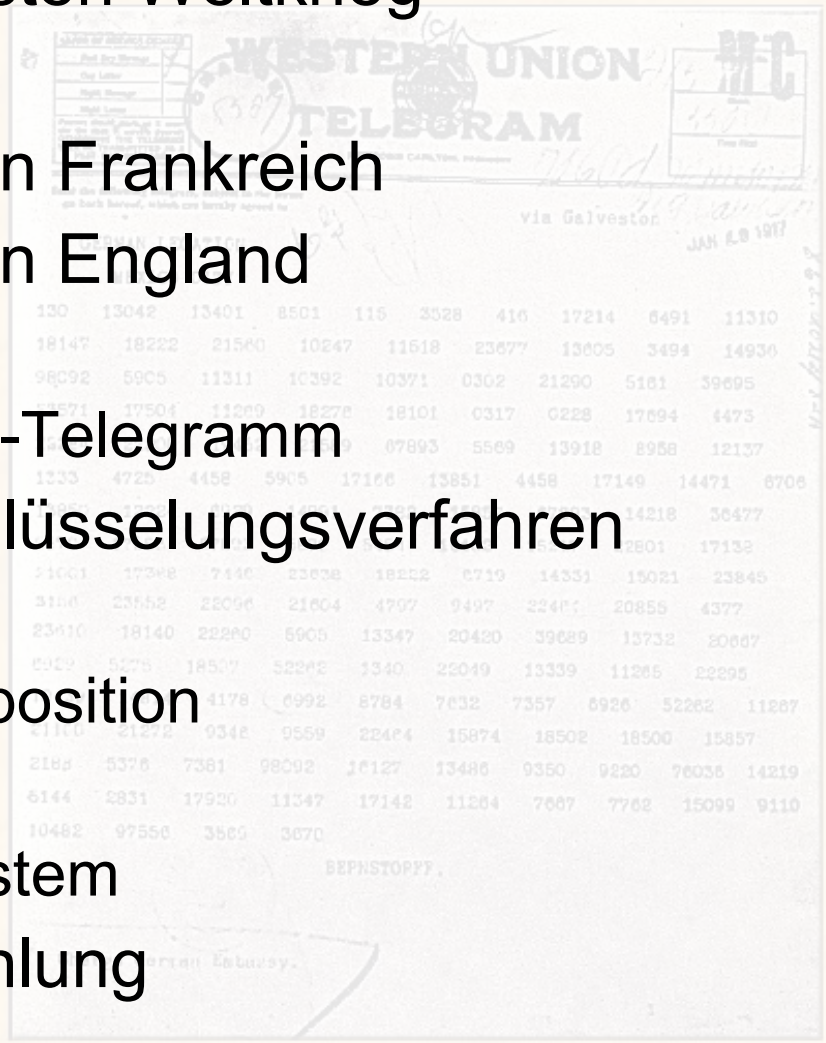
Jan Bundrock

Kryptographie im Ersten Weltkrieg

Seminar
Geschichte der Verschlüsselung

Übersicht

- Fakten zum Ersten Weltkrieg
- Funktechnik
- Kryptographie in Frankreich
- Kryptographie in England
  - ROOM 40
  - Zimmermann-Telegramm
- Diverse Verschlüsselungsverfahren
  - Codebücher
  - Spaltentransposition
  - Playfair
  - ADFGVX-System
- Literaturempfehlung

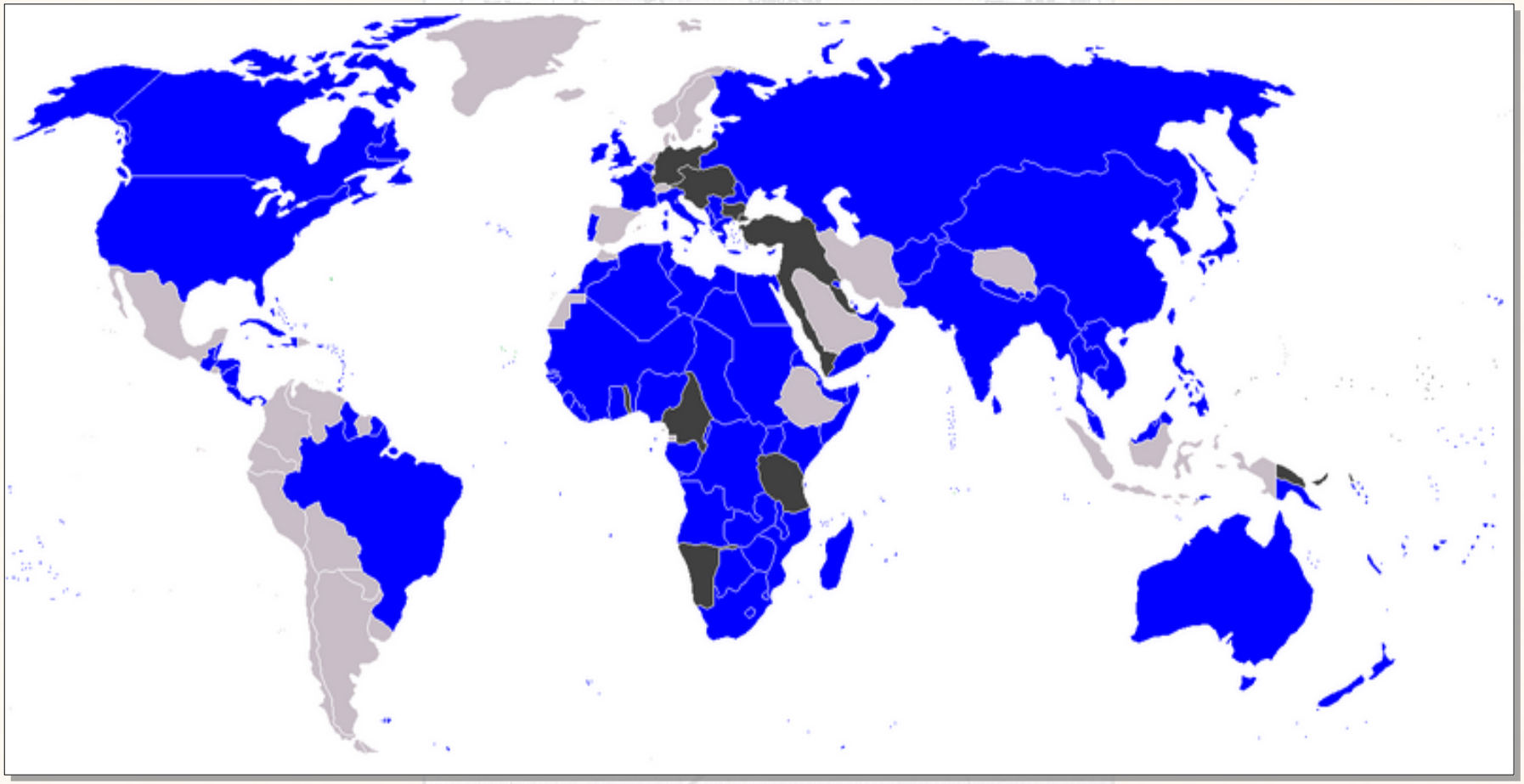


Fakten zum Ersten Weltkrieg

- 28. Juli 1914 – 11. November 1918

Fakten zum Ersten Weltkrieg

- Weltkarte 1918

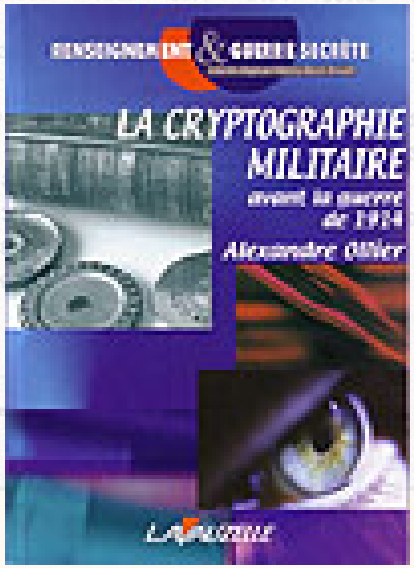


Funktechnik

- 1894 entdeckt von Guglielmo Marconi
- 1901 erste transatlantische Funkbotschaft
- hohes Interesse für das Militär

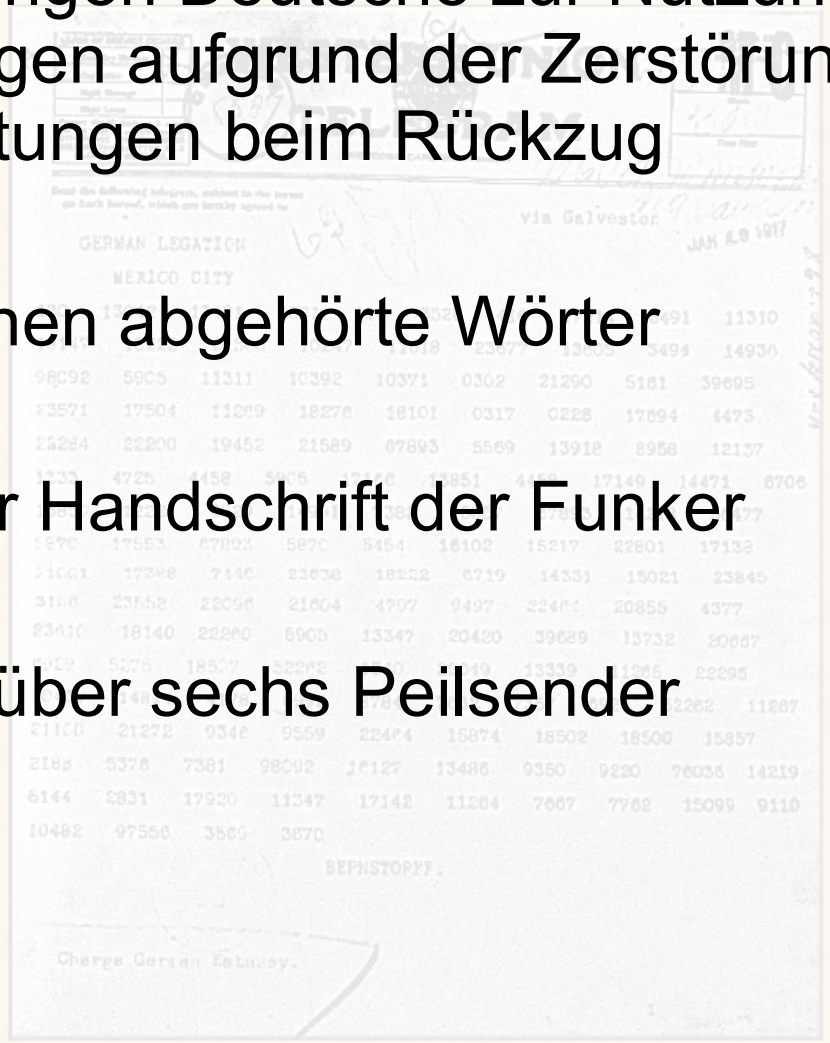
Kryptographie in Frankreich

- 1870 Frankreich verliert den Krieg gegen Preußen
- seit diesem Zeitpunkt Beginn einer “Kryptoindustrie”
- wichtigstes Werk *“La Cryptographie militaire”* von Auguste Kerckhoff von Nieuwenhof (1883)



Kryptographie in Frankreich

- Franzosen zwangen Deutsche zur Nutzung von Funkverbindungen aufgrund der Zerstörung von Telegraphenleitungen beim Rückzug
- über 100 Millionen abgehörte Wörter
- Auswertung der Handschrift der Funker
- Ortung zudem über sechs Peilsender



Kryptographie in England

- zu Beginn der 1. Weltkrieges existierten keine kryptoanalytischen Einrichtungen

- Alfred Ewing gründete der erste Büro (später bekannt als ROOM 40)

ROOM 40

- zur Hochbetriebszeit mit 800 Funkern und 80 Kryptoanalytikern besetzt
  - Sprachwissenschaftler
  - Altphilologen
  - Kreuzworträtselsüchtige
- während des Krieges 15.000 Funksprüche entschlüsselt
- später ging der ROOM 40 in den Bletchley Park über
- größter Erfolg war die Entschlüsselung des Zimmermann-Telegramms

Zimmermann-Telegramm

- USA waren zu Beginn des Ersten Weltkrieges neutral, selbst nach der Versenkung der “RMS Lusitania”

- im November 1916 wird Arthur Zimmermann neuer deutscher Außenminister
  - will die militärischen Aggressionen Deutschlands ausbauen

Zimmermann-Telegramm

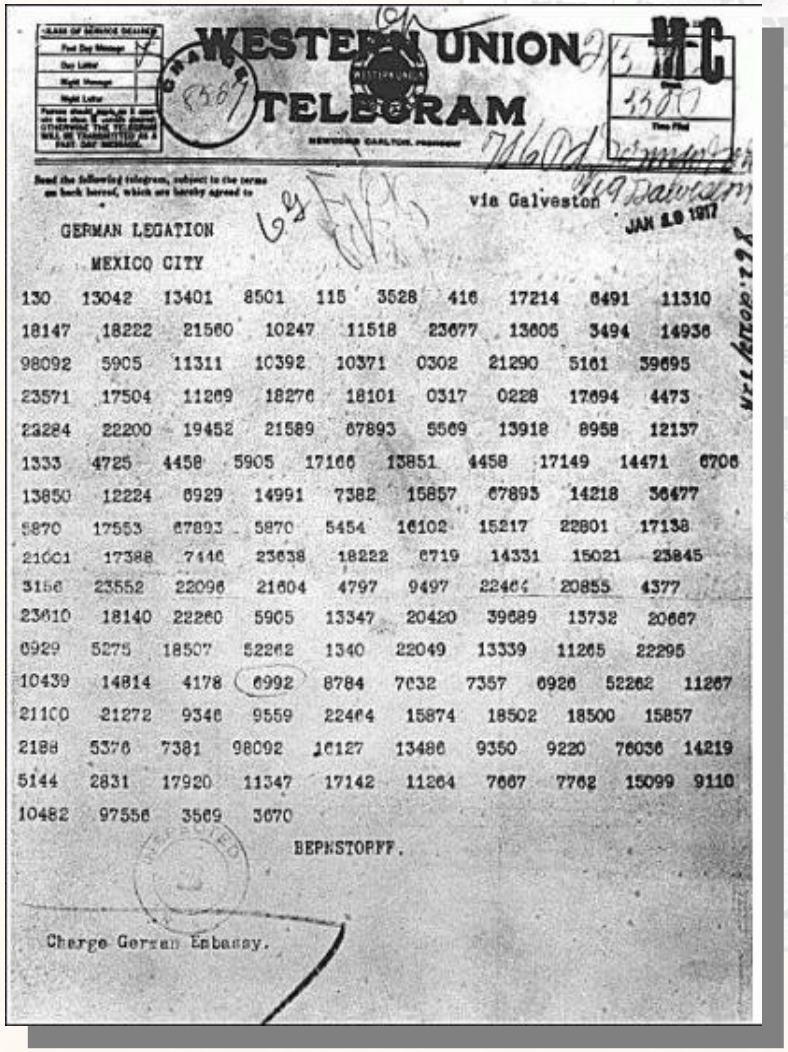
- am 1. Februar 1917 war der Beginn des uneingeschränkten U-Boot-Krieges
- zur Verzögerung / Vermeidung eines amerikanischen Kriegseintritts verfasst Zimmermann ein Telegramm an den Präsidenten von Mexico
- da die Engländer die deutschen Direktleitungen in die USA am Kriegsbeginn kappten, musste Zimmermann das Telegramm über Telegraphenleitungen schicken, die direkt an Großbritannien vorbeiführten

Zimmermann-Telegramm

"Wir beabsichtigen, am ersten Februar uneingeschränkten U-Boot-Krieg zu beginnen. Es wird versucht werden, Vereinigte Staaten trotzdem neutral zu halten. Für den Fall, dass dies nicht gelingen sollte, schlagen wir Mexiko auf folgender Grundlage Bündnis vor. Gemeinsam Krieg führen. Gemeinsam Friedensschluss. Reichlich finanzielle Unterstützung und Einverständis unsererseits, dass Mexiko in Texas, New Mexico, Arizona früher verlorenes Gebiet zurückerobert. Regelung im einzelnen Euer Hoheit überlassen. Sie wollen Vorstehendes dem Präsidenten streng geheim eröffnen, sobald Kriegsausbruch mit Vereinigten Staaten feststeht, und Anregung hinzufügen, Japan von sich aus zu sofortigem Beitritt einzuladen und gleichzeitig zwischen uns und Japan zu vermitteln. Bitte den Präsidenten darauf hinweisen, dass rücksichtslose Anwendung unserer U-Boote jetzt Aussicht bietet, England in wenigen Monaten zum Frieden zu zwingen. Empfang bestätigen. Zimmermann"

Zimmermann-Telegramm

- Das verschlüsselte Zimmermann-Telegramm und die ersten Entschlüsselungen



WESTERN UNION TELEGRAM

via Galveston

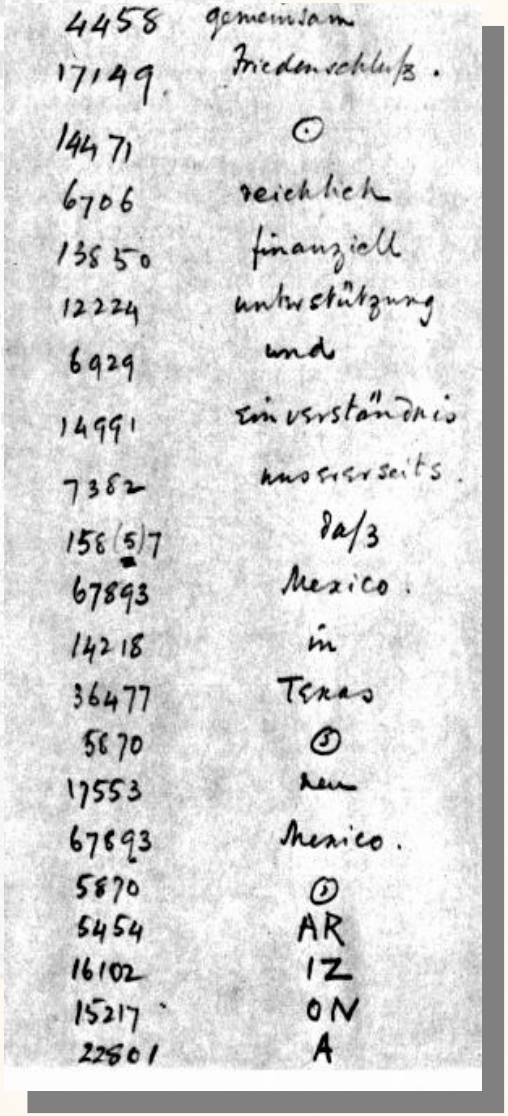
JAN 19 1917

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 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22098 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.



4458 gemeinsam
17149 Friedenschluß.
14471 ⊙
6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 einverständnis
7382 unserseits.
15857 da/3
67893 Mexico.
14218 in
36477 Texas
5870 ⊙
17553 nen
67893 Mexico.
5870 ⊙
5454 AR
16102 IZ
15217 ON
22801 A

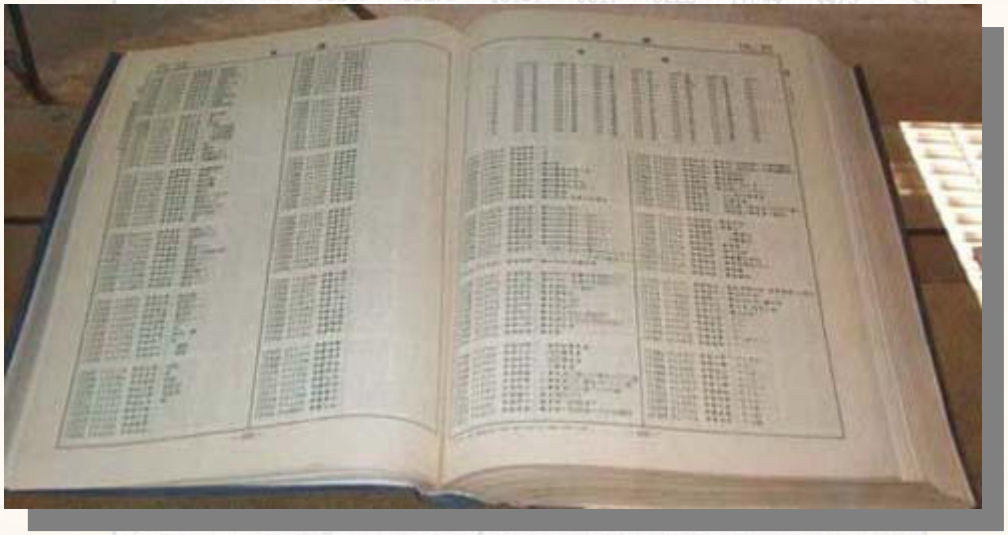
Zimmermann-Telegramm

- Entschlüsselung erfolgte durch William Montgomery und seinen Kollegen Nigel de Grey

- aufgrund dieses Telegramms traten die USA im April 1917 ins Kriegsgeschehen ein

Diverse Verschlüsselungsverfahren

- Codebücher
  - groß und unhandlich
  - wie ein Wörterbuch benutzbar
  - Problem, wenn es in die falschen Hände gelangte



Diverse Verschlüsselungsverfahren

- Spaltentransposition
  - Verfahren beruht auf der Umsortierung von Spalten und der folgenden spalten- und nicht zeilenweisen Auslesung
  - zu Beginn des Weltkrieges nutzen die Deutschen die doppelte Spaltentransposition
  - im November 1914 wechselten sie auf die Virgenére-Verschlüsselung mit dem Schlüsselwort “ABC” und anschliessender Spaltentransposition

1	2	3	4
e	s	w	a
r	s	c	h
o	n	d	u
n	k	e	l

2	1	4	3
s	e	a	w
s	r	h	c
n	o	u	d
k	n	l	e

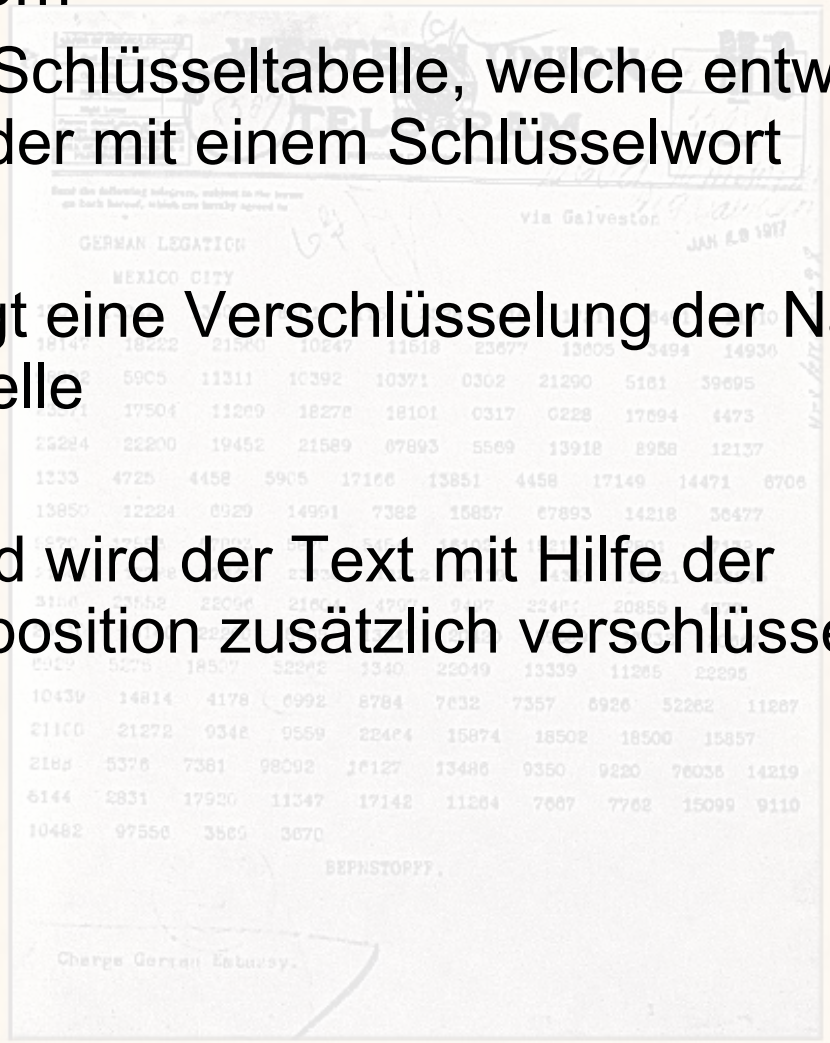
s	s	n	k	e	r	o	n	a	h	u	l	w	c	d	e

Diverse Verschlüsselungsverfahren

- ADFGVX-System
  - am 5. März 1918 von General Luffendorff eingeführt
  - Franzosen standen zunächst vor einem unlösbaren Problem
  - als quasi Einzelkämpfer entschlüsselte jedoch Georges Painvin am 2. Juni 1918 einen ADFGVX Funkspruch
  - deutschen Truppen verloren deshalb eine Schlacht nördlich von Paris

Diverse Verschlüsselungsverfahren

- ADFGVX-System
  - benötigt 6x6 Schlüsseltabelle, welche entweder zufällig gefüllt wird oder mit einem Schlüsselwort
  - danach erfolgt eine Verschlüsselung der Nachricht mit der Schlüsseltabelle
  - abschliessend wird der Text mit Hilfe der Spaltentransposition zusätzlich verschlüsselt



Diverse Verschlüsselungsverfahren

- ADFGVX-System – Beispiel

Key #1: geheim

	A	D	F	G	V	X
A	g	e	h	i	m	a
D	b	c	d	f	j	k
F	l	n	o	p	q	r
G	s	t	u	v	w	x
V	y	z	0	1	2	3
X	4	5	6	7	8	9

Key #2: ROSENDUFT

R	O	S	E	N	D	U	F	T
6	5	7	2	4	1	9	3	8
A	X	F	D	A	A	F	X	A
G	D	G	D	G	A	V	F	F
F	X	A	A	A	D	F	D	D
G	F	X	G	F	A	D	A	F

angriffmorgenfrueh

↓

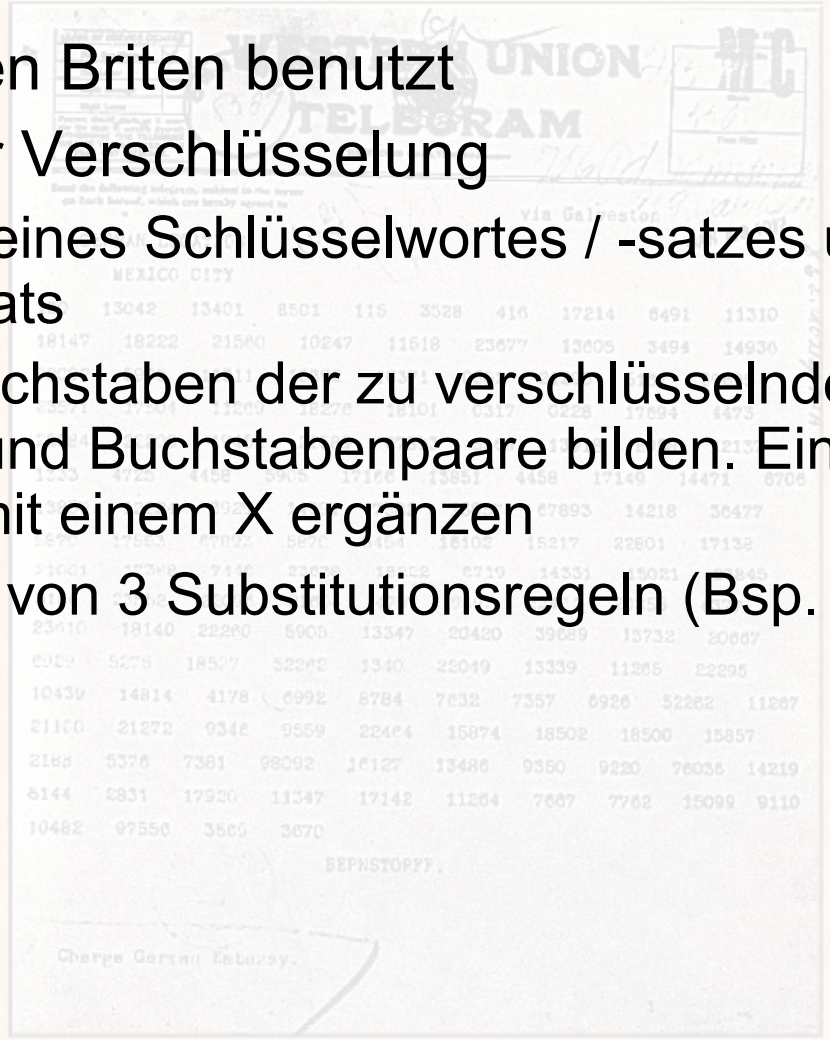
AXFDAAFXAGDGDGAVFFFXAAADFDDGFXGFADAF

↓

AADADDAGXFDAAGAFXDXFAGFGFGAXAFDFFVFD

Diverse Verschlüsselungsverfahren

- Playfair
  - wurde von den Briten benutzt
  - 3 Schritte der Verschlüsselung
    - Festlegen eines Schlüsselwortes / -satzes und Füllen eines 5x5 Quadrats
    - Gleiche Buchstaben der zu verschlüsselnden Nachricht mit X ergänzen und Buchstabenpaare bilden. Einzelne Buchstaben ebenfalls mit einem X ergänzen
    - Anwenden von 3 Substitutionsregeln (Bsp. an der Tafel)



Literaturempfehlung

- Singh, Simon: *Codes – Die Kunst der Verschlüsselung.* 2. Aufl. München: dtv 2005
  - eher für jüngere Leser gedacht, dafür sehr verständlich geschrieben
- Singh, Simon: *Geheime Botschaften – Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* 5. Aufl. München: dtv 2004
  - ausführlicher als das oben erwähnte Buch und etwas anspruchsvoller
- Kahn, David: *The Codebreakers.* Scribner Book Company 1996
  - sehr ausführlich und interessant geschrieben