Angewandte Kryptographie

Einführung, Historische Chiffren

Prof. Dr.-Ing. Kerstin Lemke-Rust

Hochschule Bonn-Rhein-Sieg

31. März 2016

Hochschule
Bonn-Rhein-Sieg

Inhalt: Angewandte Kryptographie

1. Einführung in die Kryptographie und Kryptoanalyse, historische Chiffren.
2. Theorie der Kryptosysteme.
3. Stromchiffren
4. Blockchiffren
5. Hashfunktionen
6. Public-Key Kryptosysteme.
7. Public-Key Signatursysteme.

Literatur

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography: `http://www.cacr.math.uwaterloo.ca/hac/` (frei verfügbar!).
- Christof Paar, Jan Pelzl: Understanding Cryptography, Springer. (Volltext über Bibliothek!)
- Bruce Schneier: Angewandte Kryptographie, Wiley.
- Nigel Smart: Cryptography: An Introduction, Mcgraw-Hill, Buch ist online verfügbar: `http://www.cs.bris.ac.uk/~nigel/Crypto_Book/`
- Buchmann: Einführung in die Kryptographie, Springer.
- Douglas R. Stinson: Cryptography, Chapman & Hall.

Einführung

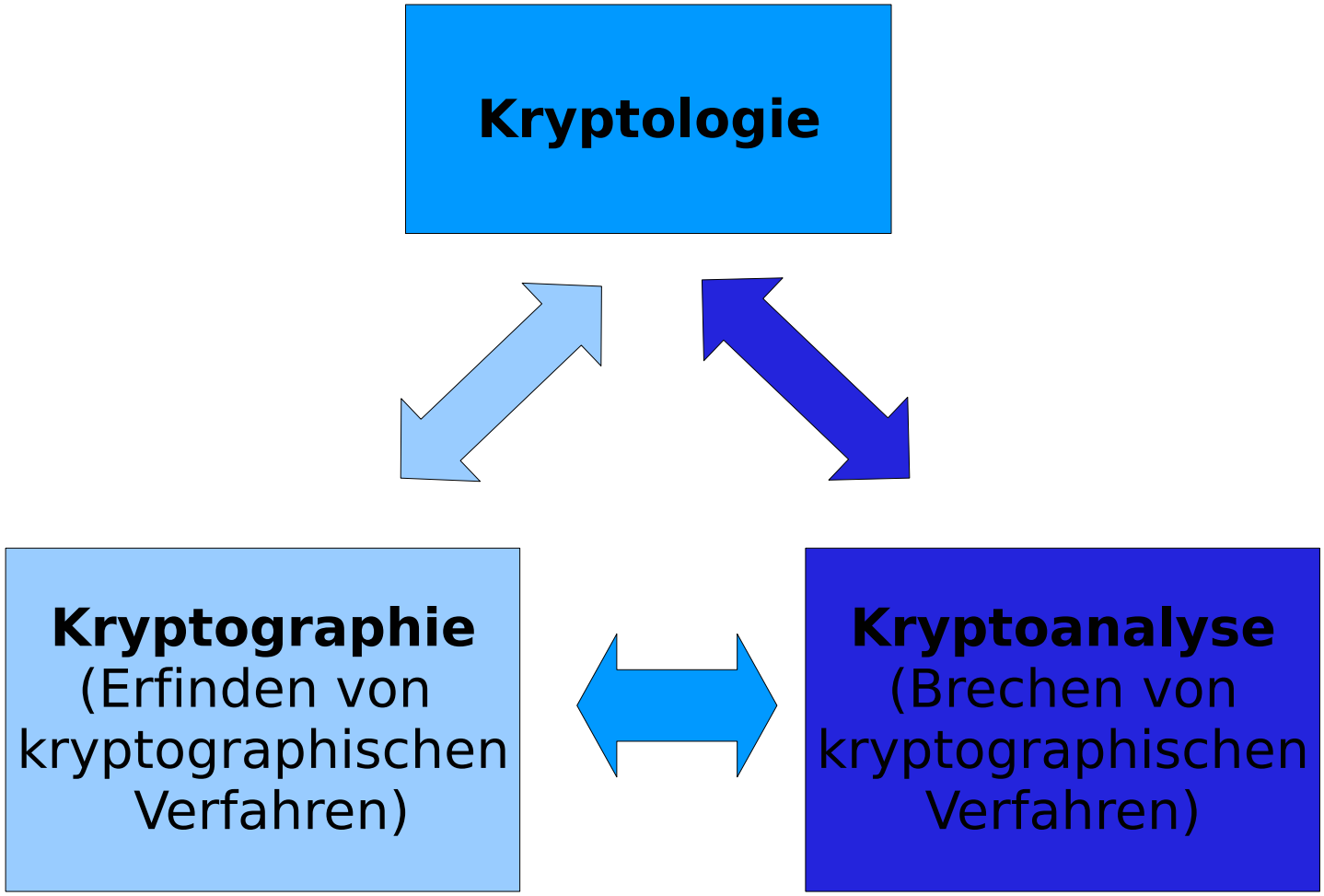
Was ist Kryptographie?

- Kryptographie ist die Wissenschaft der Geheimschriften.
- Kryptographie bietet (mathematische) Verfahren und Algorithmen für die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit.

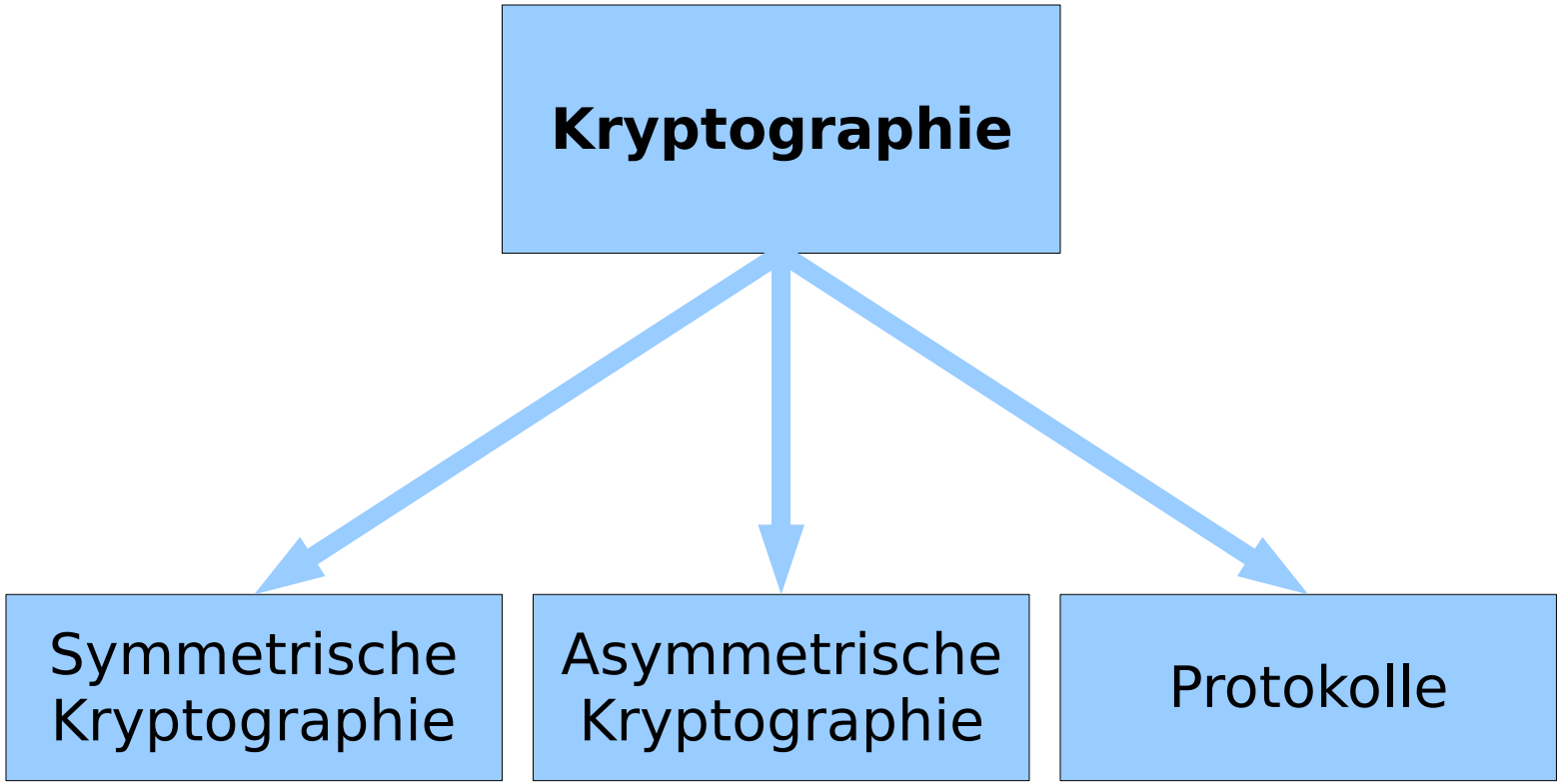
Historie

- Bis Mitte der 70-er Jahre: Forschung praktisch exklusiv nur bei militärischen Institutionen (NSA etc.)
- Jetzt sehr aktive und relevante Forschung auch in der freien Wissenschaft.

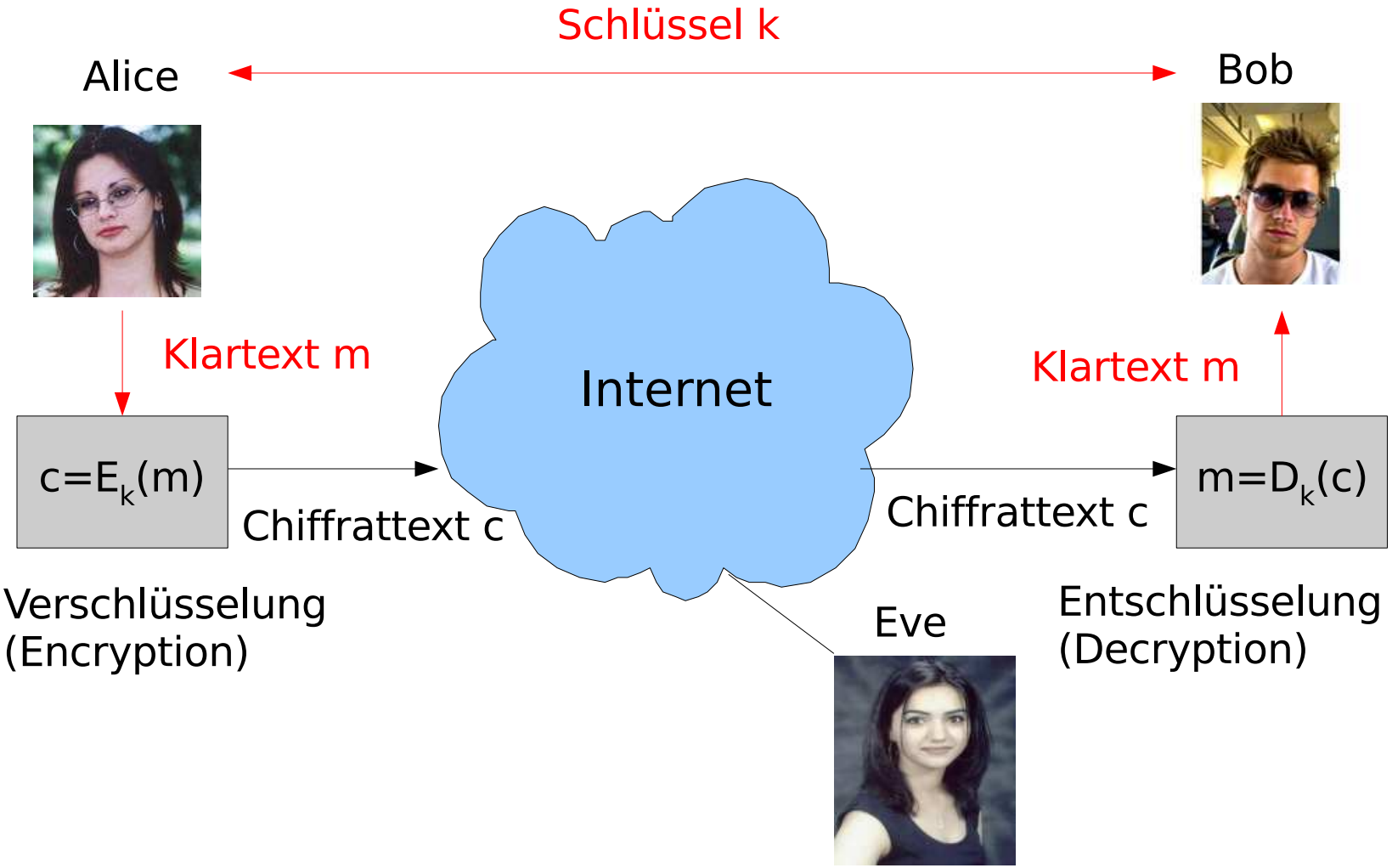
Kryptologie



Kryptographie



Symmetrische Verschlüsselung



Symmetrische Verschlüsselung

Erreichbare Sicherheitsziele durch Verschlüsselung

Sicherheitsziel:

- Vertraulichkeit

Voraussetzungen für die Sicherheit bei symmetrischer Verschlüsselung

- Etablierter symmetrischer Kryptoalgorithmus mit einer hinreichend großen Anzahl möglicher Schlüssel.
- Schlüssel k muss zufällig erzeugt werden.
- Kommunikationspartner müssen Schlüssel k vorher über einen abhörsicheren und integren Kanal (z.B. bei persönlichem Treffen) vereinbart haben.
- Schlüssel k muss beim Speichern und Verarbeiten durch Kryptoalgorithmus gegen Auslesen und Modifikation geschützt sein.

Kryptosystem

Definition

Ein *Kryptosystem* ist ein 5-Tupel $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ mit den folgenden Eigenschaften

1. $\mathcal{P}$ ist eine endliche Menge von Klartexten (Plaintexts),
2. $\mathcal{C}$ ist eine endliche Menge von Chiffrattexten (Ciphertexts),
3. $\mathcal{K}$ ist eine endliche Menge von möglichen Schlüsseln (Keys),
4. Für jedes $k \in \mathcal{K}$ gibt es eine Verschlüsselungsfunktion $E_k \in \mathcal{E}$ mit $E_k : \mathcal{P} \to \mathcal{C}$ und eine dazugehörige Entschlüsselungsfunktion $D_k \in \mathcal{D}$ mit $D_k : \mathcal{C} \to \mathcal{P}$, so dass $D_k(E_k(x)) = x$ für jedes Element $x \in \mathcal{P}$.

Kerckhoffs Prinzip

Kerckhoffs Prinzip

Die Sicherheit eines Kryptosystems beruht auf der Geheimhaltung des kryptographischen Schlüssels. Sie beruht nicht auf der Geheimhaltung der Kryptoalgorithmus.

> *The best algorithms we have are the ones that have been made public, have been attacked by the world's best cryptographers for years, and are still unbreakable.*
>
> Bruce Schneier

Kryptoanalyse: Angreifermodell

Annahmen

1. Der Angreifer kennt den verwendeten Kryptoalgorithmus (“*der schwächere Angriff*”) oder
2. Der Angreifer kennt den verwendeten Kryptoalgorithmus nicht (“*der stärkere Angriff*”).

Im Regelfall kennt der Angreifer den Kryptoalgorithmus.

Angriffsziel

1. Das Angriffsziel ist die Dechiffrierung eines Chiffrats (“*der schwächere Angriff*”).
2. Das Angriffsziel ist der geheime kryptographische Schlüssel (“*der stärkere Angriff*”).

Im Regelfall ist das Angriffsziel der geheime kryptographische Schlüssel.

Kryptoanalyse: Angreifermodell

Abstufungen im Angreifermodell

1. "ciphertext only attack": Der Angreifer kennt nur den Chiffrattext y ("*der stärkste Angriff*").
2. "known plaintext attack": Der Angreifer kennt ein (oder mehrere) Klartext-Chiffrattext-Paare (x, y).
3. "chosen plaintext attack": Der Angreifer kann den Klartext x wählen und erhält den dazugehörigen Chiffrattext y.
4. "chosen ciphertext attack": Der Angreifer kann den Chiffrattext y wählen und erhält den dazugehörigen Klartext x ("*der schwächste Angriff*")

Im Regelfall betrachten wir "ciphertext only attack".

Inhalt: Historische Chiffren

Übersicht

1. Additive Chiffre
2. Substitutionschiffre
3. Permutationschiffre
4. Vigenère-Chiffre
5. Enigma

Additive Chiffre (Shift Cipher)

Definition

Es sei $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_N$. Für $0 \leq k < N$, definiere als

- Verschlüsselungsfunktion $E_k(x) = (x + k) \bmod N$ und als
- Entschlüsselungsfunktion $D_k(y) = (y - k) \bmod N$.

N ist die Anzahl von Buchstaben im Alphabet, z.B. 26.

Bemerkung

Für $k = 3$ ist der Spezialfall einer additiven Chiffre als *Caesar Chiffre* bekannt.

Beispiel: Additive Chiffre

Zuordnung von Buchstabe zu Zahl

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example

Aus dem Klartext ‘‘BahnhofBonn’’ bzw. ‘‘1 0 7 13 7 14 5 1 14 13 13’’ wird mit dem Schlüssel $K = 15$ der Chiffrattext ‘‘16 15 22 2 22 3 20 16 3 2 2’’ bzw. ‘‘QPWCWDUQDCC’’.

Addition modulo 26:

1	0	7	13	7	14	5	1	14	13	13
15	15	15	15	15	15	15	15	15	15	15
16	15	22	2	22	3	20	16	3	2	2

Kryptoanalyse: Additive Chiffre, "ciphertext only attack"

Schwachstelle

Kleiner Schlüsselraum: Es gibt nur N mögliche Schlüssel bzw. $N - 1$ wirksame Schlüssel.

Angriff: Ausprobieren aller Schlüssel

Bei $N = 26$ können alle möglichen Schlüssel von einem Angreifer direkt ausprobiert werden ("Exhaustive Key Search" oder "Brute Force"). Der richtige Schlüssel ist gefunden, wenn der Klartext "sinnvoll", d.h. lesbar ist.

Substitutionschiffre (Substitution Cipher)

Definition

Es sei $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_N$. Für jede Permutation $\pi \in \mathcal{K}$ definiere als

- Verschlüsselungsfunktion $E_k(x) = \pi(x)$ und als
- Entschlüsselungsfunktion $D_k(y) = \pi^{-1}(y)$, wobei π^{-1} die inverse Permutation zu π ist.

N ist die Anzahl von Buchstaben im Alphabet, z.B. 26.

Schlüsselraum

Die Anzahl möglicher Permutationen ist $N!$. Bei $N = 26$ folgt ein Schlüsselraum von $26! \approx 2^{88}$. Brute Force ist damit praktisch (fast) ausgeschlossen!

Beispiel: Substitutionschiffre

Permutation π

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

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

Example

Aus dem Klartext ‘‘BahnhofBonn’’ wird der Chiffrattext ‘‘NXGSGFPNFSS’’.

Inverse Permutation π^{-1}

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

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

Kryptoanalyse: Substitutionschiffre, “ciphertext only attack”

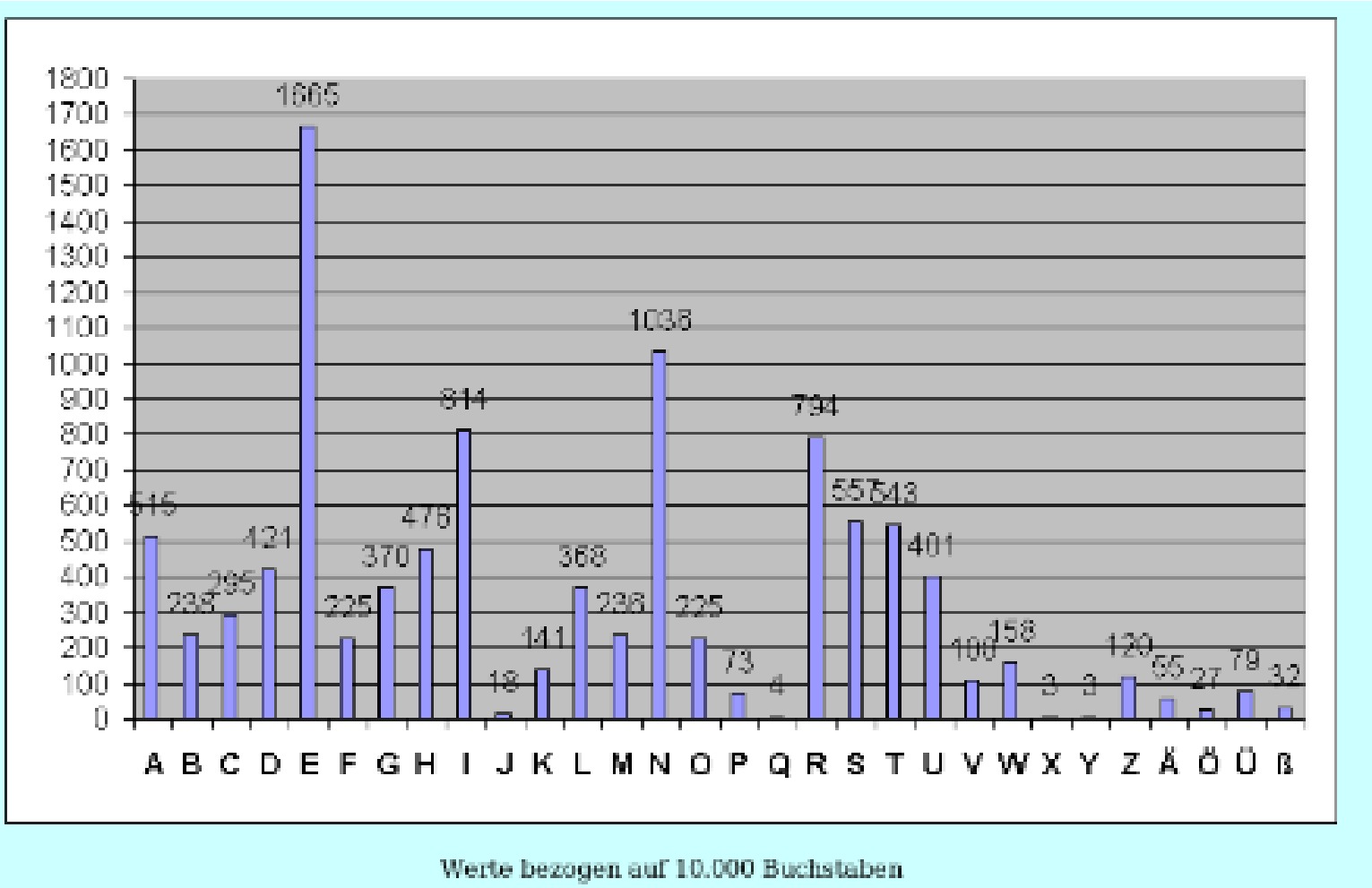
Schwachstelle

Die Häufigkeit der Buchstaben und Buchstabenkombinationen in einer Sprache findet sich im Chiffrattext wieder!

Angriff: Häufigkeitsanalyse

Durch eine Analyse der Häufigkeit von Buchstaben und Buchstabenkombinationen in dem Chiffrattext kann die verwendete Permutation re-konstruiert werden.

Buchstabenhäufigkeit in der deutschen Sprache



Permutationschiffre (Permutation Cipher)

Definition

Es sei $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_N)^m$. Es sei $\mathcal{K}$ gegeben durch die Permutationen von $\{1, ..., m\}$. Für eine Permutation $\pi \in \mathcal{K}$ definiere als

- Verschlüsselungsfunktion $E_\pi(x_1, x_2, ..., x_m) = (x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(m)})$ und als
- Entschlüsselungsfunktion $D_\pi(y_1, y_2, ..., y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, ..., y_{\pi^{-1}(m)})$. wobei π^{-1} die inverse Permutation zu π ist.

N ist die Anzahl von Buchstaben im Alphabet, z.B. 26, m ist die Blocklänge.

Schlüsselraum

Die Anzahl möglicher Permutationen ist $m!$. Bei $m = 10$ folgt ein Schlüsselraum von $10! \approx 2^{22}$. Brute Force ist kann bei großen Werten von m damit praktisch (fast) ausgeschlossen werden!

Beispiel: Permutationschiffre

Permutation π und π^{-1} mit $m = 5$

x	1	2	3	4	5
$\pi(x)$	3	5	1	2	4

x	1	2	3	4	5
$\pi^{-1}(x)$	3	4	1	5	2

Example

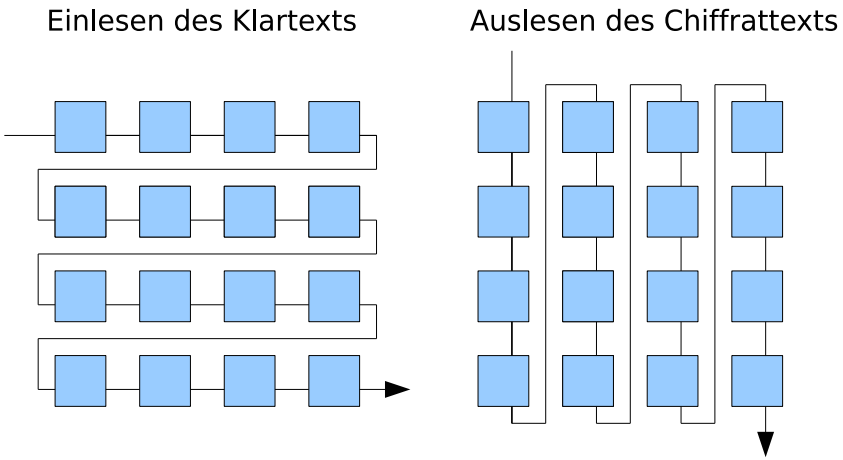
Aus dem Klartext ‘‘`BahnhofBonn`’’ bzw. ‘‘`Bahnh|ofBon|...`’’ wird mit der obigen Permutation ‘‘`HHBANBNOFO...`’’. $\pi(i)$ gibt die Stelle des Buchstabens aus dem Klartext an, der an Position i des Chiffrats erscheint. Umordnung der Buchstaben gemäß $\pi(1) = 3, \pi(2) = 5$, etc.:

1	2	3	4	5	1	2	3	4	5
B	A	H	N	H	O	F	B	O	N

3	5	1	2	4	3	5	1	2	4
H	H	B	A	N	B	N	O	F	O

Es ist festzulegen, wie mit einem Rest, der kleiner als die Blocklänge ist,

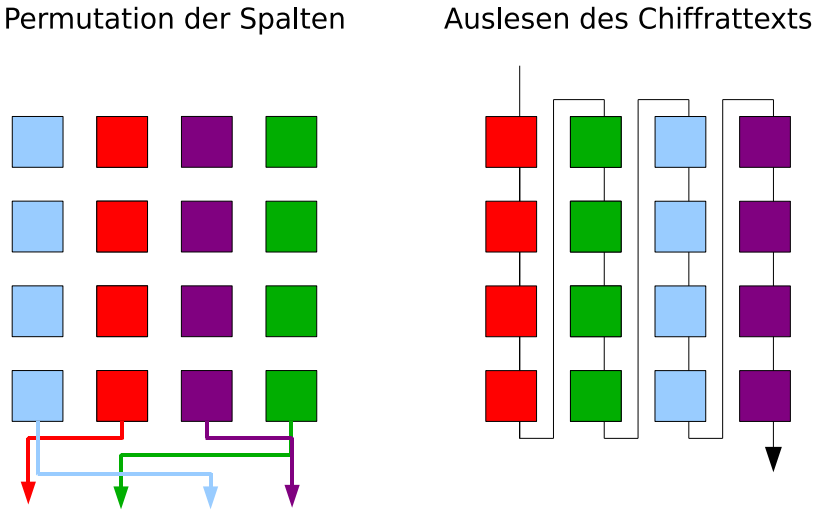
Beispiel: Einfache Spalten-Transposition



Beispiele

- Die Skytale in Sparta ist ein historisches Beispiel: Vertikales Beschreiben eines Pergamentbandes, das um einen Zylinder gewickelt wird.
- B A H N
  H O F B
  O N N
  führt auf den Chiffrattext “BHOAONHFNNB”

Allgemeine Spalten-Transposition



Beispiel

B	A	H	N
H	O	F	B
O	N	N	

wird zu

A	N	B	H
O	B	H	F
N		O	N

und führt auf den Chiffrattext “AONNBBHOHFN”

Kryptoanalyse: Permutationschiffre, "ciphertext only attack"

Schwachstelle

Die Häufigkeit der Buchstaben in einer Sprache findet sich im Chiffrattext wieder, nicht aber die Häufigkeit von Zeichenkombinationen.

Angriff: Ausprobieren mit Häufigkeitsanalyse von Zeichenkombinationen und Kontextanalyse (bei kleiner Zeilen- bzw. Blocklänge)

- Für jede mögliche Permutation: Bestimmung der Häufigkeitsverteilung von Buchstabenkombinationen und Kontextanalyse in dem Chiffrattext.

Kryptoanalyse: Permutationschiffre, “ciphertext only attack”

Angriff: Häufigkeitsanalyse von Zeichenkombinationen und Kontextanalyse (bei großer Zeilen- bzw. Blocklänge)

- Suche nach häufigen Wörtern oder charakteristischen Zeichenkombinationen (“sch”, “ck”, “ch” in der deutschen Sprache) als ein Ansatzpunkt für das Rekonstruieren der Permutation.

Vigenère-Chiffre

Definition

Es sei $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_N)^m$. Für einen Schlüssel $K = (k_1, k_2, ..., k_m)$ definiere als

- Verschlüsselungsfunktion
  $E_k(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ..., x_m + k_m) \bmod N$ und als
- Entschlüsselungsfunktion
  $D_k(y_1, y_2, ..., y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m) \bmod N$.

N ist die Anzahl von Buchstaben im Alphabet, z.B. 26, m ist ein positiver Integer.

Schlüsselraum

Die Anzahl möglicher Schlüssel ist N^m. Bei $N = 26$, $m = 8$ folgt ein Schlüsselraum von $26^8 \approx 2^{38}$. Bei größeren Werten von m kann Brute Force ausgeschlossen werden.

Beispiel: Vigenère-Chiffre

Example

Aus dem Klartext ‘‘`BahnhofBonn`’’ bzw. ‘‘`1 0 7 13 7 14 5 1 14 13 13`’’ wird mit dem Schlüssel K=(2 10 25 3) der Chiffrattext ‘‘`3 10 6 16 9 24 4 4 16 23 12`’’ bzw. ‘‘`DKGQJYEEQXM`’’:

Addition modulo 26:

1	0	7	13	7	14	5	1	14	13	13
2	10	25	3	2	10	25	3	2	10	25
3	10	6	16	9	24	4	4	16	23	12

Kryptoanalyse: Vigenère-Chiffre, "ciphertext only attack"

Schwachstelle

Die Häufigkeitsverteilung der Buchstaben findet sich im Chiffrattext wieder!

Angriff: Häufigkeitsanalyse

- Erster Schritt: Bestimmung der Schlüssellänge m (mit Kasiski Test oder mit Koinzidenzindex)
- Zweiter Schritt: Bestimmung des Schlüssels (mit Koinzidenzindex oder Häufigkeitsverteilung)

Kryptoanalyse: Vigenère-Chiffre, Kasiski Test

Beobachtung

Die Abbildung von zwei identischen Abschnitte im Klartext ergibt im Chiffrattext dieselbe Sequenz, wenn der Abstand δ dieser identischen Abschnitte im Klartext ein Vielfaches der Schlüssellänge ist, d.h. wenn gilt: $\delta \equiv 0 \bmod m$.

Kasiski Test

- Lokalisiere identische Zeichenblöcke von mindestens drei Zeichen im Chiffrattext.
- Für jeden identischen Zeichenblock: Notiere die relativen Zeichenabstände zwischen identischen Blöcken im Chiffrattext
- Bestimme den größten gemeinsamen Teiler (der Mehrzahl) aller gefundenen Zeichenabstände. Dies ist mit guter Wahrscheinlichkeit die Schlüssellänge m.

Beispiel: Kryptoanalyse einer Vigenère-Chiffre mit dem Kasiski Test

Chiffrattext (aus Wikipedia)

AXTRX TRYLC TYSZO EMLAF QWEUZ HRKDP NRVWM WXRPI JTRHN IKMYF
WLQIE NNOXW OTVXB NEXRK AFYHW KXAXF QYAWD PKKWB WLZOF XRLSN
AAWUX WTURH RFWLL WWKYF WGAXG LPCTG ZXWOX RPIYB CSMYF WIKPA
DHYBC SMYFW KGMTE EUWAD LHSLP AVHFK HMWLK

Zeichenblockabstände

- "YBCSMYFW": $\delta = 14 = 2 \times 7$.
- "XRPI": $\delta = 98 = 2 \times 7 \times 7$

Mögliche Werte für m: 2,7 oder 14.

Kryptoanalyse: Vigenère-Chiffre, Koinzidenzindex

Idee für Rekonstruktion von m

Jeder m-te Klartextbuchstabe wird mit demselben Schlüsselbuchstaben verschlüsselt (m additive Chiffren).
Unterteile den Chiffrattext in m Subtexte wie folgt:

$\vec{y_1} = (y_1, y_{m+1}, y_{2m+1}, ...)$
$\vec{y_2} = (y_2, y_{m+2}, y_{2m+2}, ...)$
...
$\vec{y_m} = (y_m, y_{2m}, y_{3m}, ...)$

Wenn m korrekt ist, sollte sich die Häufigkeitsverteilung der natürlichen Sprache im Chiffrattext für alle $\vec{y_1}, \vec{y_2}, ..., \vec{y_m}$ wiederfinden lassen.

Kryptoanalyse: Vigenère-Chiffre, Koinzidenzindex

Koinzidenzindex

Der Koinzidenzindex $I_c(\vec{y})$ gibt die Wahrscheinlichkeit an, dass in einer Zeichenkette $\vec{y}$ der Länge n zwei zufällig gezogene Buchstaben identisch sind.

$$I_c(\vec{y}) = \frac{\sum_{i=0}^{N-1} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{N-1} f_i \cdot (f_i - 1)}{n(n-1)}$$

Hierbei ist f_i die Anzahl vom Buchstaben i des verwendeten Alphabets im Chiffrattext.

Unterscheidung: natürliche Sprache vs. Zufall

- Englische Sprache: $I_c \approx 0.065$,
- Deutsche Sprache: $I_c \approx 0.076$,
- Gleichverteilung aller 26 Buchstaben (Zufall): $I_c \approx 0.038$

Kryptoanalyse: Vigenère-Chiffre, Koinzidenzindex

Idee für Rekonstruktion des Schlüssels

Berechne

$$M_g(\vec{y_j}) = \frac{\sum_{i=0}^{N-1} p_i f_{i+g}}{n_j}$$

für alle $0 \leq g < N$. Hierbei ist f_i die Anzahl der Buchstaben i im Chiffrattext, p_i die Wahrscheinlichkeit des Buchstabens i in der natürlichen Sprache und n_j die Anzahl der Buchstaben in $\vec{y_j}$.

Entscheidungsstrategie:

$k := arg\max_g M_g$ ist der beste Kandidat für k_j. Für den korrekten Kandidaten wird der Koinzidenzindex einer natürlichen Sprache erwartet.

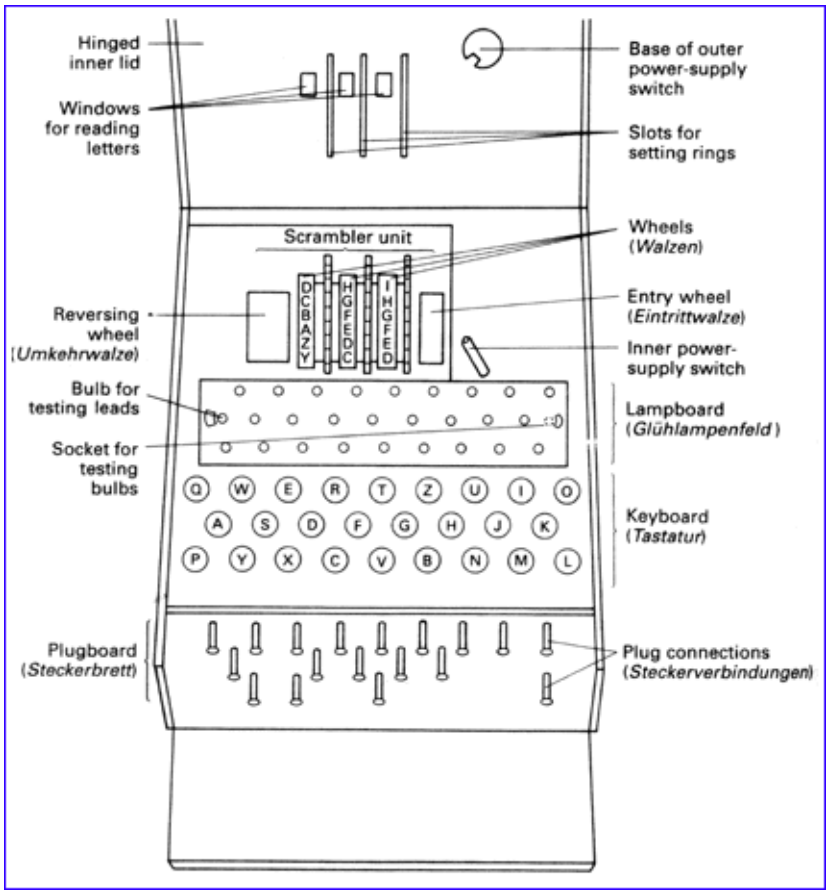
Alternativstrategie (Häufigkeitsverteilung)

Der Buchstabe mit der größten Häufigkeit in $\vec{y_j}$ entspricht vermutlich dem Buchstaben mit der größten Häufigkeit im verwendeten Alphabet (Reduktion auf additive Chiffre).

Zusammenfassung: Kryptoanalyse von historischen Chiffren

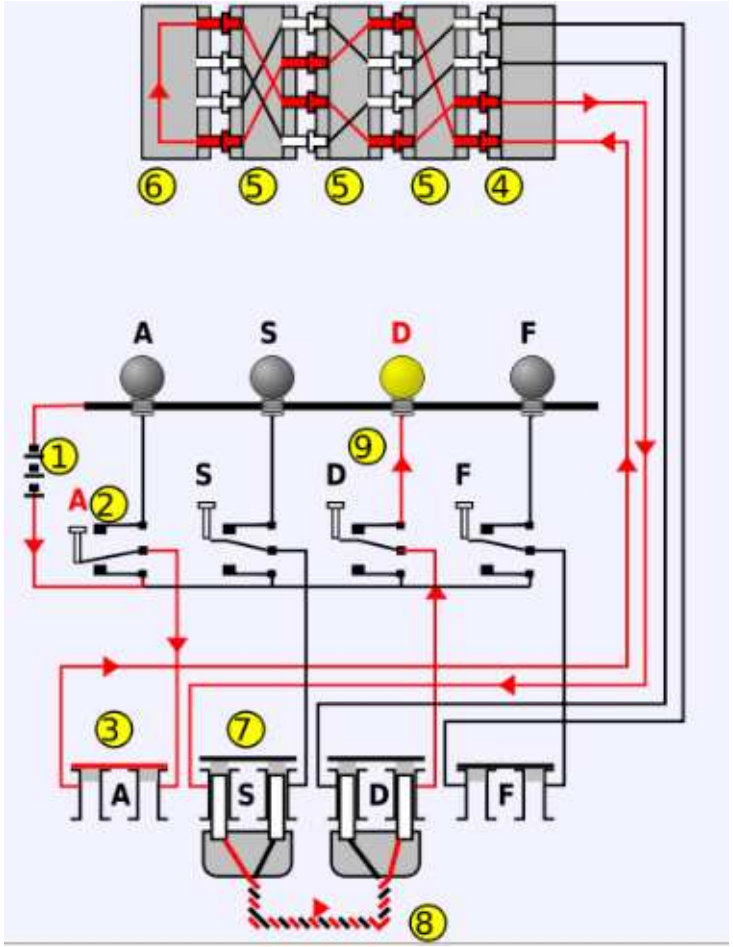
Chiffre	**Kryptoanalyse**
Additive Chiffre	- Brute-Force - Häufigkeitsverteilung von Buchstaben und Buchstabenkombinationen
Substitutionschiffre	- Häufigkeitsverteilung von Buchstaben und Buchstabenkombinationen
Permutationschiffre	- Häufigkeitsverteilung von Buchstabenkombinationen - Rekonstruieren häufiger Wörter
Vigenère-Chiffre	1. Schritt: Rekonstruieren der Schlüssellänge (Kasiski-Test oder Koinzidenzindex) 2. Schritt: Für jedes Schlüsselelement: Häufigkeitsverteilung von Buchstaben und Buchstabenkombinationen.

Die Chiffriermaschine ENIGMA



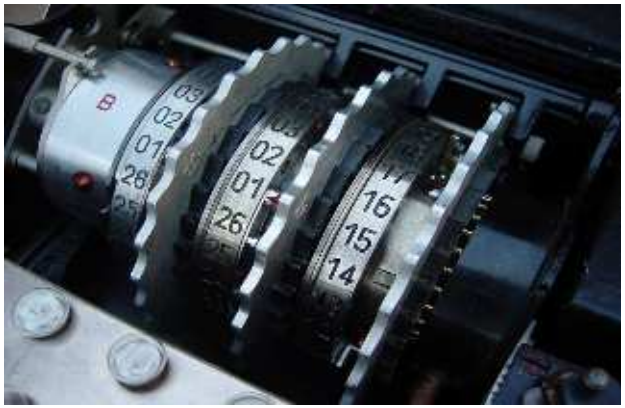
Quelle: http://www.pbs.org/wgbh/nova/decoding/enigma.html

Konstruktionsdetails der Chiffriermaschine ENIGMA



Quelle: Wikipedia

Skizze: Prinzipieller Aufbau der ENIGMA aus
Batterie (1),
Tastatur (2),
Steckerbrett (3, 7) mit
Steckkabel (8),
Walzensatz (5) mit
Eintrittswalze (4) und
Umkehrwalze (6) sowie
dem Lampenfeld (9)



Die Chiffriermaschine ENIGMA

Eigenschaften

- polyalphabetische Substitutionschiffre mit Periode 16900=26*25*26.
- Die Verschlüsselung hat keinen Fixpunkt, d.h. bei einer Verschlüsselung wird nie ein Zeichen des Klartexts auf sich selbst abgebildet (Schwachstelle!).
- Die Entschlüsselungsfunktion ist identisch zu der Verschlüsselungsfunktion: die Enigma hat involutorische Schlüssel.

Mathematische Beschreibung der Verschlüsselung

$$y_i = \sigma^{-1} \circ \alpha_{i_1}^{-1} \circ \beta_{i_2}^{-1} \circ \gamma_{i_3}^{-1} \circ \pi \circ \gamma_{i_3} \circ \beta_{i_2} \circ \alpha_{i_1} \circ \sigma(x_i)$$

α, β, γ: Substitution durch Rotoren, π: feste Permutation durch Umkehrwalze, σ: variable Konfiguration von Steckerverbindungen.

Die Chiffriermaschine ENIGMA

Schlüssel einer ENIGMA

- Auswahl der Rotoren und Anordnung der Rotoren
- Stellung der Ringe (Zuordnung der Rotorkontakte zu den Zeichen des Alphabets)
- Anfangsstellung jedes Rotors
- Verdrahtung des Steckerbretts

Der Schlüsselraum bei drei Rotoren ist ca. 2^{67}.

Geheim! **Sonder - Maschinenschlüssel BGT**

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT DW SK UY DF GV LJ BO MX	vyj
30.	III V II	Y V P	OR KI JV OM ZK MU BF YC DS GP	cqr
29.	V IV I	O H R	UX JC PB BK TA ED ST DS LU FI	vhf

Quelle: http://www.codesandciphers.org.uk

Kryptoanalyse der ENIGMA

Idee der Kryptoanalyse

- Hintereinanderschaltung mehrerer Enigma-Maschinen zur Elimination des Steckerbretts aus dem Schlüsselsuchraum.
- Raten eines wahrscheinlichen Klartextwortes in einer kodierten Nachricht, z.B. “WETTERVORHERSAGEBISKAYA”
- Brute Force zur Bestimmung von Tagesschlüsseln:
  - Verwerfen von Schlüsseln, bei denen Fixpunkte auftreten.
  - Verwerfen von Schlüsseln, bei denen bestimmte Grapheneigenschaften bei Klartext-Geheimtext-Paaren nicht erfüllt sind.

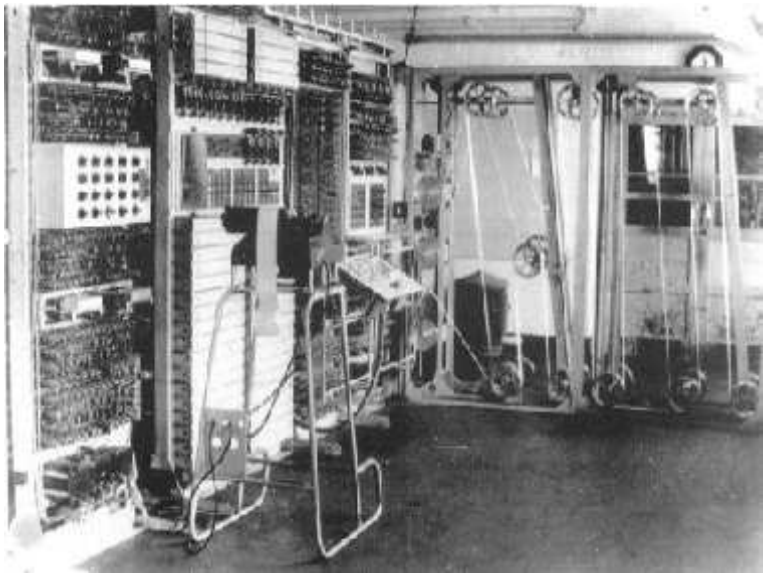
Maschinen zur Kryptoanalyse

- Bomba: Elektromechanische Maschine von Marian Rejewski
- Turing Bombe: Weiterentwicklung von Alan Turing in England (Bletchley Park).

Die Kryptoanalyse-Maschine COLOSSOS

Eigenschaften

- Design Start im März 1943 (Ziel: Kryptoanalyse des Lorenz Chiffre)
- Start des operationellen Betriebs: im Januar 1944.
- Erster programmierbarer, elektronischer Computer!



Original

Nachbau

Quelle: http://www.codesandciphers.org.uk