Klassische Kryptosysteme

Dr. Lorenz Müller

BFH, HTI

Klassische Kryptosysteme

Grundalgorithmen

1.1. Einfache Substitutionschiffren

1.2. Transpositionschiffren

Verallgemeinerte Substitutionen

2.1. Homophone Substitution

2.2. Polyalphabetische Substitution

2.3. Vernam Chiffre, One-time pad

2.4. Polygraphische Blockchiffren

Produktchiffren

3.1. Historische Chiffriergeräte

3.2. Rotormaschinen

3.3. Moderne Produktchiffren

Grundalgorithmen der Chiffrierung

Transposition $\varphi: m_n \rightarrow C$

$$m_n \rightarrow C_n = \varphi(m_n)$$

Substitution $S: A \rightarrow A'$

$$m \rightarrow C = S(m)$$

Produkt

$$m \rightarrow C = S \circ \varphi(m)$$

Potenz- und Exponentialchiffre

$$m \rightarrow C = m^k$$

Kryptographische Grundoperationen

Transposition

Vertauschen der Zeichenpositionen

Klartext		**Schüsseltext**
(m1,m2,m3,m4,m5)	**======>**	**C=(m3,m2,m5,m1,m4)**
m i l c h		**L I H M C**

Permutation der n Positionszahlen in Textblock der Länge n:

Anzahl: $|\varphi(n)| = n!$

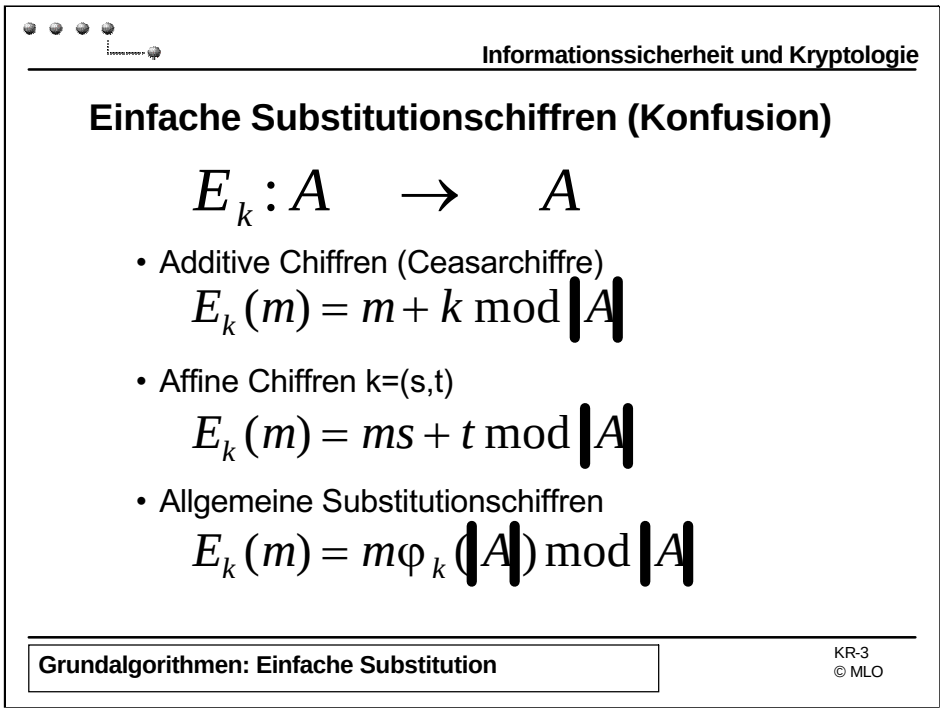
Substitution

Ersetzen der Zeichen durch andere Zeichen

Klartext		**Schüsseltext**
(m1,m2,m3,m4,m5)	**======>**	**C=(m1',m2',m3',m4',m5')**
m i l c h		**L H K B G**

Injektive Abbildung S des Alphabets A auf Alphabet A':

Anzahl: $|S| = \frac{|A'|!}{|A'-A|!}$



Einfache Substitutionen

Substitutionen dienen der Konfusion, d.h. der Erzeugung eines möglichst komplexen Zusammenhangs zwischen Klartext- und Schlüsseltext. Die Komplexität hängt direkt mit der Grösse des Schlüsselraums und dem Algorithmus zusammen.

Beispiele:

Additive Chiffre, Caesarchiffre: k=2

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 >
A'= <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 >

Affine Substitution: s=2, t=0 (nicht surjektiv, ungeeignet als Chiffre)

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 >
A'= <A C E G I K M O Q S U W Y A C E G I K M O Q S U W Y >

Shift: **key = 3**

A B C D E F G H I J ... R S ... Z
D E F G H I J K L M ... U V ... C

F H D V D U = C E A ? S A R

Einfache Substitution - Beispiele: Ceasar's cipher

KR-4
© MLO

Mono-alphabetische Substitution

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

G P U Y R B = ? C R Y P T O

Mono-alphabetische Substitution

Key = **HISTORICAL**

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

S N Y K Q J = **?** **C R Y P T O**

Poly-alphabetische Substitution

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

V U G R I M V = ? S U C C E S S

Einfache Substitution - Beispiele: Poly-alphabetische Substitution (1)

Kryptoanalyse von einfachen Substitutionen

- Schlüsseltextangriff
  - Häufigkeitsanalyse
    - ==> Einzelzeichen, Di-, Tri- bis n-Gramme
- Klartextangriff
  - Additive, affine und polynomiale Chiffren
    - ==> Gleichungssystem
  - Allgemeine Substitution
    - ==> Schlüsseltabelle

Statistische Kryptoanalyse

Eindeutigkeitsdistanz für allgemeine Substitution |K| = 4 x 10^{26}

Analyse bis zu	Zeichen	Bigramme	Trigramme	Theoret. N-Gramme
# Zeichen (Eindeutigkeitsdist.)	167	81	58	28

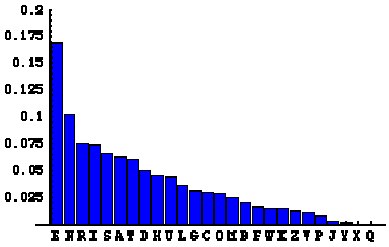
Beispiel: Strukturierter englischer Text mit 52 Zeichen

EUMGKJIDF TDI KBDINWTHNI HKJ LKMTBF TDI IPIB MUDI KBDINWTHNI

Statistische Analyse ergibt: (Vergleiche mit Häufigkeitstabelle im Anhang)

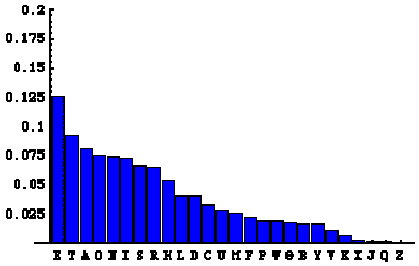
D

Lettre	Fréquence	Lettre	Fréquence
A	6.28 %	N	10.20 %
B	1.99 %	O	2.87 %
C	2.98 %	P	0.77 %
D	5.04 %	Q	0.02 %
E	16.92 %	R	7.44 %
F	1.62 %	S	6.62 %
G	3.12 %	T	5.95 %
H	4.51 %	U	4.39 %
I	7.42 %	V	1.07 %
J	0.30 %	W	1.52 %
K	1.46 %	X	0.03 %
L	3.56 %	Y	0.10 %
M	2.54 %	Z	1.24 %



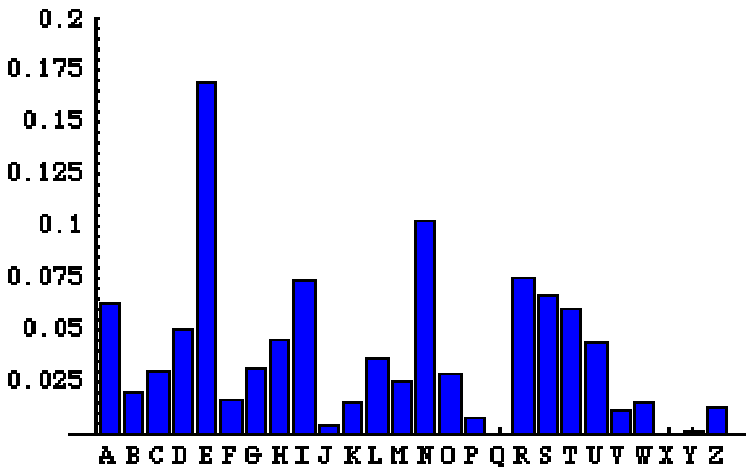
E

Lettre	Fréquence	Lettre	Fréquence
A	8.08 %	N	7.38 %
B	1.67 %	O	7.47 %
C	3.18 %	P	1.91 %
D	3.99 %	Q	0.09 %
E	12.56 %	R	6.42 %
F	2.17 %	S	6.59 %
G	1.80 %	T	9.15 %
H	5.27 %	U	2.79 %
I	7.24 %	V	1.00 %
J	0.14 %	W	1.89 %
K	0.63 %	X	0.21 %
L	4.04 %	Y	1.65 %
M	2.60 %	Z	0.07 %



Kryptoanalyse einfache Substitution: Häufigkeit der Buchstaben

KR-9
© MLO



Kryptoanalyse einfache Substitution: Häufigkeitsverteilung

KR-10
© MLO

Transpositionschiffren (Diffusion)

$$E_k : Z_n \rightarrow Z_n$$

Aufbrechen der n-Gramme

Bruchteil aller Permutationen erfüllt Anforderung

Darstellung von Transpositionen (Permutationen)

Angabe der Position des Urbildes im Klartext

$$\varphi_n(m) = [\varphi^{-1}(C_1), \varphi^{-1}(C_2)\varphi^{-1}(C_3), \ldots \varphi^{-1}(C_n)]$$

Angabe der Position des Bildes im Schlüsseltext

$$\varphi_n(m) = [\varphi(m_1), \varphi(m_2)\varphi(m_3), \ldots \varphi(m_n)]$$

Darstellung von Transpositionen (Permutationen)
Beispiel : Angabe der Position des Urbildzeichens

$$\varphi_n(m) = [\varphi^{-1}(C_1), \varphi^{-1}(C_2)\varphi^{-1}(C_3), \ldots \varphi^{-1}(C_n)]$$

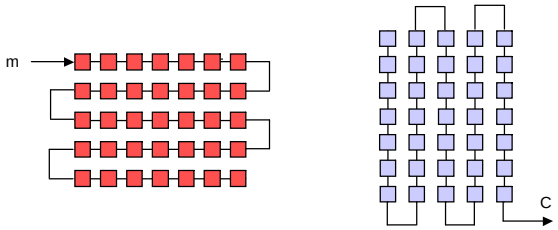
Beispiel: Angabe der Zielposition des Klartextzeichens

$$\varphi_n(m) = [\varphi(m_1), \varphi(m_2)\varphi(m_3), \ldots \varphi(m_n)]$$

Spezielle Transpositionen

Spalten Transposition

Matrixdarstellung mit fixer Breite d



Block Transposition mit Blocklänge b

Blocklänge definiert Anzahl Permutationen

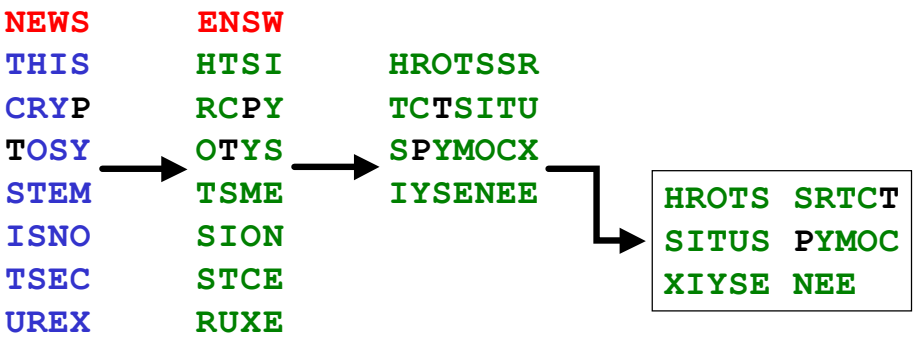
$$b! \cong \sqrt{2\pi b}\left(\frac{b}{e}\right)^{b}$$

Transpositionen bewirken Diffusion innerhalb des Blocks

Transposition

Message: **This cryptosystem is not secure**

Key = **NEWS**



Transposition - Beispiel: Kolonnentransposition

KR-13
© MLO

During the **Civil War** the **Federal Army** made extensive use of **transposition ciphers**, in which a key word indicated the order in which columns of the array were to be read and in which the elements were either plaintext words or code word replacements for plaintext. The **Confederate Army** primarily used the **Vigenère** cipher and on occasion monoalphabetic substitution. While the Union cryptanalysts solved most of the intercepted Confederate ciphers, the Confederacy in desperation sometimes published Union ciphers in newspapers, appealing for help from readers in cryptanalyzing them.

Encyclopædia Britannica

Transposition - Beispiel: Anwendung

Kryptoanalyse von Transpositionen

Schlüsseltextangriff

Blockgrösse, Spaltenhöhe

==> Bigrammperioden, Kasiskitest

==> Grosse Eindeutigkeitsdistanz

Klartextangriff

Bekannte Blockierung

==> Permutationstabelle

Unbekannte Blockierung

==> Bi- und Trigrammanalyse

	_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_	53	316	320	150	17	129	282	297	28	16	40	571	244	1217	4	32	0	658	552	416	878	20	7	2	2	31
B_	181	3	2	22	1101	4	17	11	157	10	3	81	3	23	69	2	0	107	77	33	57	6	17	0	2	3
C_	23	2	2	2	18	0	2	2647	30	0	200	5	10	14	15	1	0	4	2	3	0	2	0	0	0	0
D_	508	44	9	160	2386	27	32	25	959	11	30	105	47	39	102	13	1	79	116	37	181	55	47	0	0	23
E_	319	337	151	561	336	235	400	388	1935	27	220	652	540	3956	69	110	9	3818	1443	547	317	170	218	15	7	143
F_	219	9	0	83	277	102	31	18	57	2	16	69	7	29	126	2	0	166	23	118	234	5	18	0	0	13
G_	195	26	3	156	1521	21	28	21	109	4	41	116	18	43	17	3	0	194	136	229	143	31	39	0	1	29
H_	529	38	1	181	954	21	40	37	293	6	52	275	123	304	195	11	1	447	124	529	131	45	136	0	4	33
I_	35	52	1038	117	1702	42	470	201	21	32	99	242	207	1579	77	19	1	153	488	684	23	98	7	0	1	36
J_	121	2	0	3	78	8	1	0	4	0	1	1	1	1	27	0	0	1	7	0	45	0	1	0	0	0
K_	190	14	3	17	277	2	20	13	88	1	11	95	21	17	221	3	0	108	46	157	116	11	27	0	0	5
L_	492	73	27	150	622	52	72	17	616	1	26	406	33	28	194	9	0	10	240	283	136	22	17	1	12	25
M_	432	62	6	90	524	40	49	33	323	20	23	52	222	42	106	49	0	16	157	90	109	19	48	0	6	26
N_	636	235	42	1990	1317	216	971	179	594	55	284	125	188	459	218	94	2	83	729	559	453	195	284	3	2	292
O_	6	166	158	87	10	71	75	99	18	26	28	239	190	613	5	87	1	479	277	101	20	46	50	2	4	17
P_	70	1	0	1	114	67	1	41	45	0	2	117	0	0	56	52	0	114	5	56	25	1	0	0	0	0
Q_	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20	0	0	0	0	0
R_	739	248	113	607	1098	171	247	173	531	44	189	170	235	321	282	67	3	128	607	460	459	151	206	1	32	162
S_	361	88	834	205	1045	64	131	86	675	21	133	66	84	82	268	130	1	45	778	1075	152	71	116	0	18	91
T_	504	59	14	333	2167	59	105	108	424	14	39	104	73	64	198	18	0	281	299	234	306	78	177	4	4	281
U_	29	190	256	82	154	285	139	110	21	6	23	53	284	1360	4	55	1	548	470	252	15	24	16	0	1	19
V_	85	8	0	5	403	4	6	0	80	1	0	6	2	3	439	2	0	2	11	0	8	0	1	0	2	1
W_	452	0	2	0	501	0	0	0	318	2	0	1	0	0	134	1	0	0	0	5	103	0	0	0	0	0
X_	4	0	0	0	4	1	0	0	10	0	0	0	0	0	1	0	0	0	0	1	0	2	2	0	0	3
Y_	8	2	1	5	3	0	2	0	4	2	1	1	8	9	3	4	0	2	24	6	5	3	3	0	0	2
Z_	91	16	0	29	294	3	3	6	84	1	1	13	4	2	45	4	0	1	9	72	461	14	82	0	0	5

Kryptoanalyse Transposition: Häufigkeit der Bi- bis n-Gramme

KR-16

Homophone Alphabetserweiterung

$$E_k : A \rightarrow A'$$

Uniforme Zeichenhäufigkeit im Schlüsselalphabet *A'*

$$m_i \rightarrow H_{m_i} = \{C_1(m_i), C_2(m_i) \ldots C_h(m_i)\}$$

mit $\left|H_{m_i}\right| \propto r(m_i)$

Homophone Verschlüsselung von m H_{m_i}

Zufällige Wahl eines Homophones aus

==> Statistische Einzelhäufigkeiten uniform

==> Bi- und Trigramm weiterhin vorhanden

Lettres	Fréquence	Symboles de substitution	Scrabble
a	8.40 %	15, 33, 37, 55, 57, 72, 91, 96	9 %
b	1.06 %	24	2 %
c	3.03 %	03, 39, 67	2 %
d	4.18 %	04, 43, 61, 88	3 %
e	17.26 %	08, 12, 20, 46, 47, 48, 53, 59, 64, 76, 79, 80, 81, 85, 90, 94, 97	15 %
f	1.12 %	40	2 %
g	1.27 %	29	2 %
h	0.92 %	05	2 %
i	7.34 %	14, 45, 50, 73, 82, 93, 99	8 %
j	0.31 %	11	1 %
k	0.05 %	77	1 %
l	6.01 %	01, 16, 26, 60, 71, 98	5 %
m	2.96 %	34, 87	3 %
n	7.13 %	06, 17, 22, 30, 31, 49, 58	6 %
o	5.26 %	02, 10, 41, 66, 89	6 %
p	3.01 %	13, 18, 83	2 %
q	0.99 %	36	1 %
r	6.55 %	21, 25, 65, 68, 92, 95	6 %
s	8.08 %	00, 28, 51, 52, 63, 74, 78, 84	6 %
t	7.07 %	07, 19, 23, 35, 38, 54, 70	6 %
u	5.74 %	09, 32, 42, 69, 75	6 %
v	1.32 %	44	2 %
w	0.04 %	56	1 %
x	0.45 %	86	1 %
y	0.30 %	62	1 %
z	0.12 %	27	1 %

Homophone Substitution Beispiel: Zahlcodierung

KR-18

Polyalphabetische Substitutionssequenz

$$E_k = (E_{k_1}, E_{k_2}, \ldots E_{k_d}) : A^d \quad \rightarrow \quad A^d$$

Periodische Folge von *d* einfachen Substitutionen

==> **Grosser Schlüsselraum** $|K_i|^d = (n!)^d = \left[\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right]^d$

Verschlüsselung erfolgt oft mit Schlüsselwort k^d

Vigenère-Chiffre $C_i = (m_i + k_i) \bmod n$

Klartext	d	a	s	i	s	t	e	i	n	b	e	i	s	p	i	e	l
Schlüssel	m	u	s	t	e	r	m	u	s	t	e	r	m	u	s	t	e
Schlüsseltext	P	U	L	P	W	K	Q	C	F	U	I	Z	E	J	A	X	P

==> **Statistische Häufigkeiten uniform**

==> **Periodische Sequenzwiederholungen**

Poly-alphabetic substitution

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

V U G R I M V = ? S U C C E S S

Polyalphabetische Substitution: Beispiel

KR-20

Vigenère cipher

Message: **This cryptosystem is not secure**

Key = **BERN**

```
THISC RYPTO SYSTE MISNO TSECU REXXX
BERNB ERNBE RNBER NBERN BERNB ERNBE
ULZFD VPCUS JLTXV ZJWEB UWVPV VVKYB
```

Vigenère Tabelle

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Polyalphabetische Substitution - Beispiel: Vigenère Tabelle

KR-22

Kryptoanalyse polyalphabetischer Chiffren

Schlüsseltextangriff

Periodenbestimmung

==> **Kasiskitest (analytisch)**

$d = Max[ggt(\text{häufigste Abstände von n-Grammen})]$

==> **Koinzidenzindex (statistisch)**

$$IC = \frac{1}{d}\sum_i p_i^2 + \frac{d-1}{d \cdot N} = \sum_i \frac{H_i(H_i-1)}{N(N-1)}$$

H: Zeichenhäufigkeit

N: Schlüsseltextlänge

Bestimmung der additiven Verschiebung (pro Kolonne)

==> **Koinzidenzindex mit Verschiebung (MIC)**

The Vigenère cipher (an example)

Message: **This cryptosystem is not secure**

Key = **BERN**

```
THISC RYPTO SYSTE MISNO TSECU REXXX
BERNB ERNBE RNBER NBERN BERNB ERNBE
ULZFD VPCUS JLTXV ZJWEB UWVPV VVKYB
```

BERN	B E R N
THIS	U L Z F
CRYP	D V P C
TOSY	U S J L
STEM	T X V Z
ISNO	J W E B
TSEC	U W V P
UREX	V V V K
XX	Y B

Polyalphabetische Substitution: Vigenère Angriff

KR-25

Ciphertext

```
KFRPGRYLRVGWURRVULFJBRGRTEEBHXMVWBTPIJMBUXNDP
BTXFETNPHFKTECGYZVREMYZEFKXNJACRVJTINVIIWOEVL
JFPCQVYLNVVMJJIGQJKVRFHSWSUFKRJJSNPHHFMZGVHVF
BTWYLDLHSWTUYVYWVAAFJTIEAVIWKAVPQJETVVWLRSGTS
SFMLJEZKEPQYYLRRRENETVPKQZTRTEYLRRCRIZNGGPQVC
GWEQTOZOYSZTLGWUVCVCPQPEALSDRNRPZNRBYGVJGUGCX
NFNVVWXFBEKUZVTGJIHZTLQJQZGUVIFINRFHZIIAIXMVE
ANMLYTRPQJETEGQFZNFCTUIOCTMFKESQVURRVULFJRRVE
NEEQKXXZMCQVYRNPGEXRCRPXWVFBTIILCNVMTEAAFMSKE
YNIHKUNNTZISHKXXGAEKWXZTRCXFTRBUWWFAQUSKSOGJA
FKEECRICAAFVTLTRUWNXNVHMHRNGVSJLRBRIFJWRNPFJT
BHVFECRJEXYAQCGTETVPYNEGVPJQLEAEITEIGUKWFWGJ
```

Strategie

- Finde Schlüssellänge

  Kasiski test, index of coincidence

- Finde relativen Abstand der einzelnen Elemente zwischen Positionen (transformiert Vigenère Chiffre an jeder Stelle in einfache Caesar Substitution)

  Mutual index of coincidence

- Finde Schlüssel (Verschiebung an jeder Stelle)

  Mutual index of coincidence

Vernam Chiffre, one-time pad

$$E_k = (\ldots E_{k_{i+1}}, E_{k_i}, E_{k_{i+1}}, \ldots): A^\infty \quad \rightarrow \quad A^\infty$$

Nichtperiodische Folge von einfachen Substitutionen

==> Unbeschränkter Schlüsselraum

Schlüsseltext in natürlicher Sprache

==> Angriff evt. möglich (Zeichenkoinzidenz)

Schlüsseltext Zufallsfolge (one time pad)

==> Theoretisch unbrechbar

==> Perfekte Sicherheit

White House

1001101001111010110001010100001110100101101010 1

Kremlin

Vernam Chiffre, One time pad – Beispiel: rotes Telefon

KR-29
© MLO

One-time pad

Plaintext : 1 1 0 0 1 1 0 1 1 1 1 0 1 1 1 ...

Secret key : 1 0 0 1 0 1 1 1 0 1 1 0 0 1 1 ...

Ciphertext : 0 1 0 1 1 0 1 0 1 0 0 0 1 0 0 ...

One time pad – Beispiel: unbrechbarer Code

KR-30
© MLO

Polygraphische Blockchiffren

$$E_k : A^d \rightarrow A^d$$

Neues Alphabet mit Mächtigkeit $|A|^d$

==> **Reduktion der statistischen Charakteristika**

==> **Moderne Blockchiffren sind Weiterentwicklungen**

z.B.: DES: $|A|^d = 2^{64}$

Transposition und Substitution kombiniert

$$E_k = S \circ T \circ \ldots \circ T \circ S : A \rightarrow A$$

Produktchiffren sehr rechenaufwendig

==> Maschinelle Verarbeitung E(m;k), D(C;k)

Maschinelle Verarbeitung

Historische Geräte (mechanisch, polyalphabetisch)

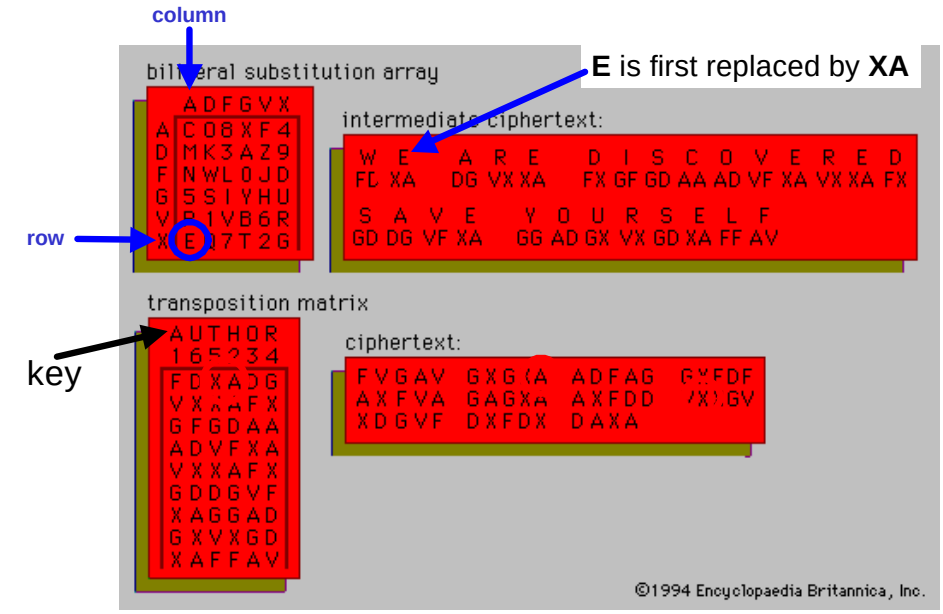
==> Jefferson Zylinder, Wheatstone Disk

Neuzeitliche Geräte (elektromechanisch, Rotoren)

==> ENIGMA, Hagelin C-48

Moderne Verarbeitung (elektronisch, Produktchiffren)

==> DES, IDEA etc



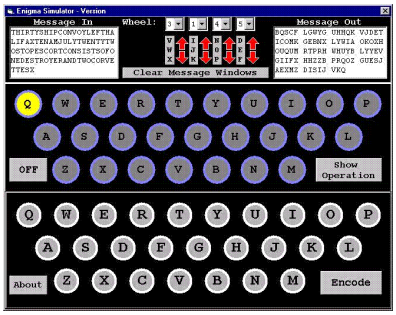
Produktchiffren - Beispiel: ADFGVX Chiffre

KR-33
© MLO

One of the most famous field ciphers of all time was a fractionation system called the ADFGVX cipher. The German Army used it during World War I. This system used first a substitution defined by a 6×6 matrix which contains the 26 letters and 10 digits. Each letter and each digit is replaced by a pair of the symbols A, D, F, G, V and X. The intermediate ciphertext was then encrypted using a substitution defined by a key word.

In 1918 the French cryptanalyst Georges J. Painvin's succeeded in cryptanalyzing important **ADFGVX** ciphertexts. The effect was devastating for the German army in the battle for Paris.

More recently, in 1984, the U.S. cryptanalyst Stephen M. Matyas presented new research on the cryptanalysis of **ADFGVX** ciphers.



http://www.myke.com/enigma1.htm

Produktchiffren – Beispiel Chiffriergerät: Enigma

KR-34
© MLO