

Grundlagen der Kryptologie

Kryptographie, Kryptoanalyse, klassische und moderne Verfahren

Tom Gries



Dokumenten URL:

<http://docs.tx7.de/TT-TK6>

Autor:

Tom Gries <TT-TK6@tx7.de>
@tomo@chaos.social

Lizenz:

Creative Commons BY-NC-ND

Version:

7.2.1 vom 16.01.2025



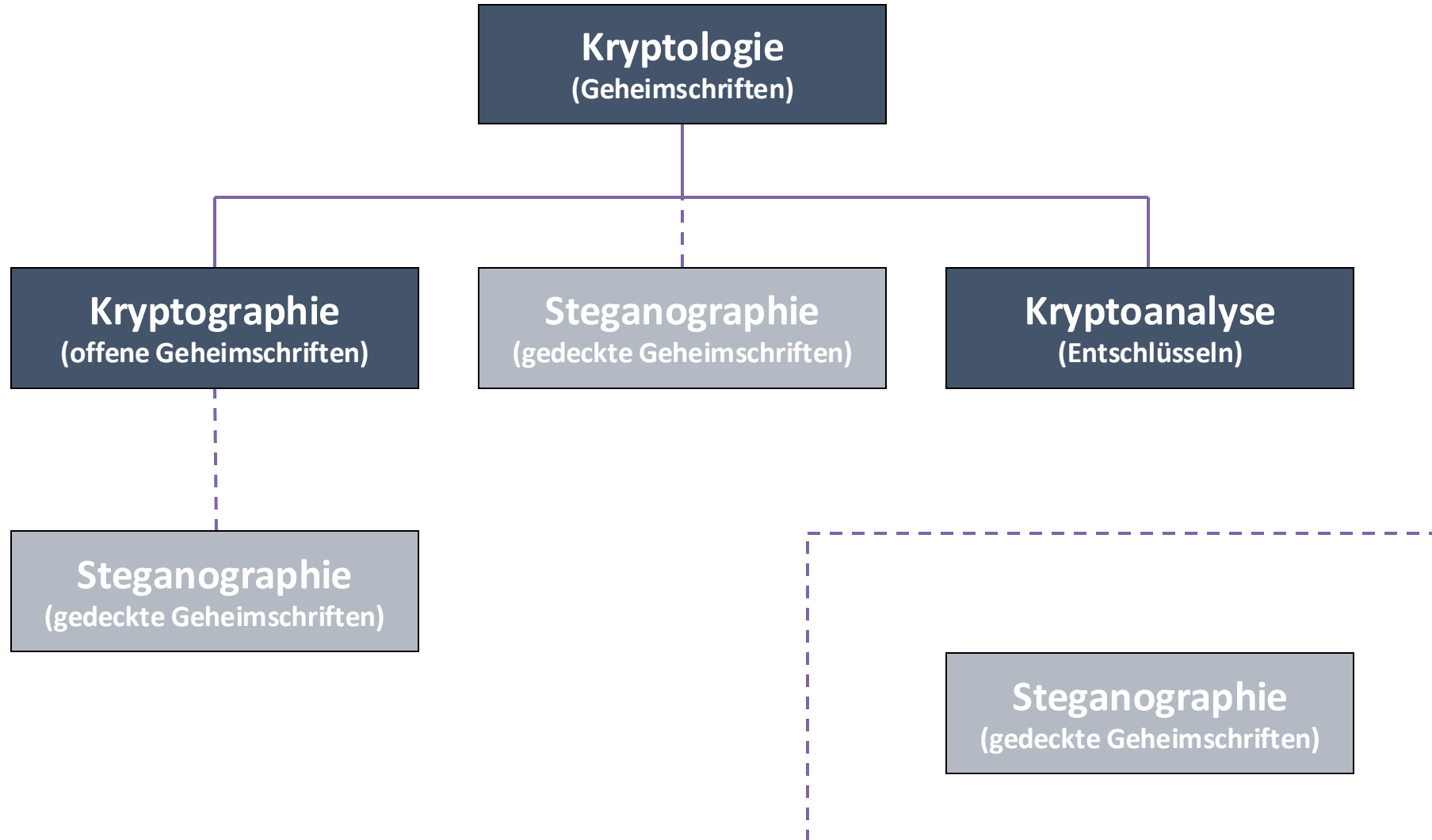


Die Kryptologie ist die Wissenschaft der Verschlüsselung und Entschlüsselung von Informationen.

Die Kryptologie wird unterteilt in:

- Kryptographie
- Kryptoanalyse
- Steganographie

Das Bild auf der nächsten Seite zeigt den Zusammenhang schematisch.





Hauptziele der Kryptographie

Die Kryptographie hat 4 Hauptziele:

1. Confidentiality (Wahrung der Vertraulichkeit)
2. Integrity (Sicherstellung der Datenintegrität)
3. Authenticity (Sicherstellung der Echtheit)
4. Non Repudiation (Nichtabstreitbarkeit)

Die allgemeine IT-Security hat darüber hinaus noch das Ziel der Availability (Sicherstellung der Verfügbarkeit). Der Geheimschutz kennt nur [1] und [2]. Bei Confidentiality, Integrity und Availability spricht man von der CIA-Triade.



Dein Auftrag

Entschlüssele den Text auf der folgenden Seite. Erkläre anschließend, wie Du auf die Lösung gekommen bist.

Du hast 20 Minuten Zeit.

Text unter <http://docs.tx7.de/TT-TUV>



Beispiele für Verschlüsselung (Textauszug)

FIMWTMIP GEIWEV GLMJJVI

HMI OVCTXSKVETLMI MWX HIV DAIMK HIV OVCTXSPSKMI, HIV WMGL QMX HIQ
ZIVWGLPYIWWIPR ZSR MRJSVQEXMSRIR FIJEWWX.

HMI OVCTXSEREPCWI MWX HMI AMWWIRWGLEJX, MRJSVQEXMSRIR EYW
ZIVWGLPYIWWIPXIR XIBXIR DY KIAMRRIR. HMIWI MRJSVQEXMSRIR OSIRIR WSASLP
HIV ZIVAIRHIXI WGLPYIWWIP EPW EYGL HIV SVMKMREPXIBX WIMR. AIWIRXPMGLI
DMIPI HIV OVCTXSEREPCWI WMRH HEW EYJLIFIR HIV WGLYXDJYROXMSR, HEW
YQKILIR HIV WGLYXDJYROXMSR WSAMI HIV REGLAIMW YRH UYERXMJMDMIVYRK
HIV WMGLIVLIMX IMRIW ZIVJELVIRW.



BEISPIEL CAESAR CHIFFRE

DIE KRYPTOGRAPHIE IST DER ZWEIG DER KRYPTOLOGIE, DER SICH MIT DEM VERSCHLUESSELN VON INFORMATIONEN BEFASST.

DIE KRYPTOANALYSE IST DIE WISSENSCHAFT, INFORMATIONEN AUS VERSCHLUESSELTEN TEXTEN ZU GEWINNEN. DIESE INFORMATIONEN KOENNEN SOWOHL DER VERWENDETE SCHLUESSEL ALS AUCH DER ORIGINALTEXT SEIN. WESENTLICHE ZIELE DER KRYPTOANALYSE SIND DAS AUFHEBEN DER SCHUTZFUNKTION, DAS UMGEHEN DER SCHUTZFUNKTION SOWIE DER NACHWEIS UND QUANTIFIZIERUNG DER SICHERHEIT EINES VERFAHRENS.

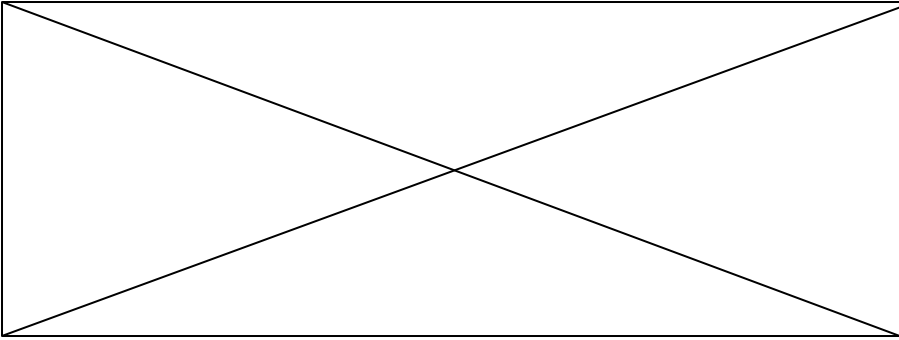


Beispiele für klassische und moderne Verschlüsselungsverfahren:

- ⇒ Caesar
- ⇒ Skytale
- ⇒ Fleißnersche Schablone
- ⇒ Homophone Verschlüsselung
- ⇒ Vigenère-Verschlüsselung
- ⇒ ENIGMA
- ⇒ Blockchiffre



Klassische Verfahren der Kryptographie

	Symmetrische Chiffre	Asymmetrische Chiffre
Klassisch	<ul style="list-style-type: none">⇒ Transposition⇒ Substitution<ul style="list-style-type: none">▪ Monoalphabetische Substitution▪ Polyalphabetische Substitution	
Modern (IT)	<ul style="list-style-type: none">⇒ Blockchiffre⇒ Stromchiffre	<ul style="list-style-type: none">⇒ Public-Key Verfahren
	Schlüssel ≤ 512 Bit	Schlüssel ≥ 1.024 Bit



Transpositionsverfahren:

Bei den Transpositionsverfahren werden die Buchstaben des Klartextes vertauscht (permutiert). Die Zeichen selber und die Anzahl jedes einzelnen Zeichens werden nicht verändert.

Beispiel:

Klartext: FRIKADELLE

Geheimtext: LEKADEFRIIL



Frage:

Wie viele Permutationen und mögliche Geheimtexte gibt es bei dem Klartextwort ZOO?

Antwort:

3 Permutationen (6, wenn unterscheidbar):

$ZO_1O_2 - ZO_2O_1 - O_1ZO_2 - O_2ZO_1 - O_1O_2Z - O_2O_1Z$

und 2 Geheimtexte:

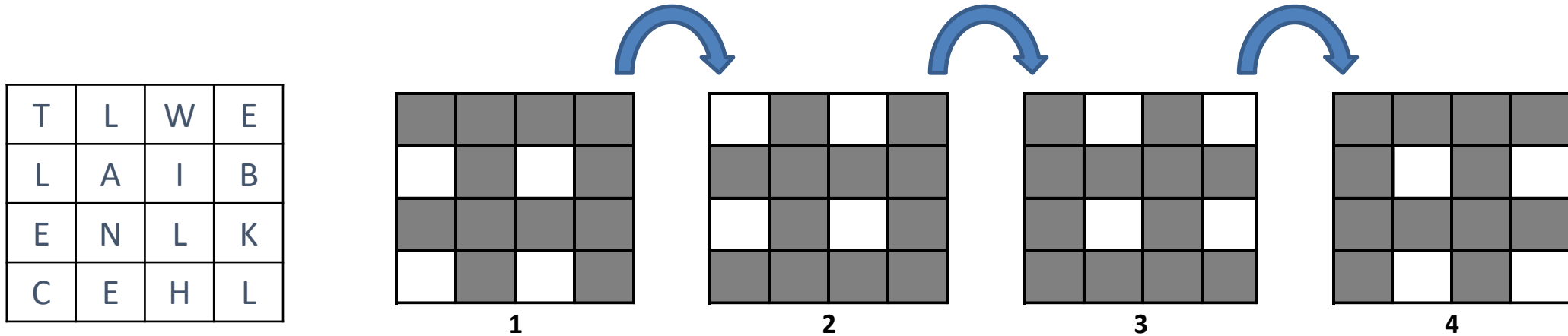
$OZO - OOZ$



Die Skytale:



Die Fleißnersche Schablone:



Die monoalphabetische Substitution:

Caesar - Verschiebung um 5	
Klartextalphabet	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
Geheimtextalphabet	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

ROT 13	
Klartextalphabet	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
Geheimtextalphabet	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

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

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



Bei der Substitution können anstatt Buchstaben natürlich auch Zahlen verwendet werden.

Es können auch beliebig andere Zeichen verwendet werden. Zum Beispiel selbstausgedachte Zeichen.

[15]

Homophone Verschlüsselung:

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
23	27	54	02	06	17	31	01	05	84	92	04	34	11	47	28	03	18	09	14	00	51	77	70	19	67
26	65	90	07	10	78	38	08	16			46	96	24	79			30	22	35	20					
36			41	12		64	13	21			87		29				45	32	43	57					
56			58	15			52	25					40				60	50	55	98					
82			88	33			62	44					49				68	66	75						
93				37				59					61				74	80	83						
				39				81					69				99	94							
				42				89					73												
				48									85												
				53									91												
				63																					
				71																					
				72																					
				76																					
				86																					
				95																					
				97																					

62251723581132102117764111111

=

100

Vigenère-Verschlüsselung:

Klartext:	R	H	A	B	A	R	B	E	R
Schlüssel:	B	E	R	L	I	N	B	E	R
Geheimtext:									

Klartext:	R	H	A	B	A	R	B	E	R
Schlüssel:	B	E	R	L	I	N	B	E	R
Geheimtext:	S	L	R	M	I	E	C	I	I

	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	Z
B	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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



Die ENIGMA (griechisch αἴνιγμα ainigma „Rätsel“) ist eine Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs des deutschen Militärs verwendet wurde.

Trotz mannigfaltiger Verbesserungen der Verschlüsselungsqualität der Maschine vor und während des Krieges gelang es den Alliierten mit hohem personellem und maschinellem Aufwand, die deutschen Funksprüche nahezu kontinuierlich zu entziffern.



Die ENIGMA



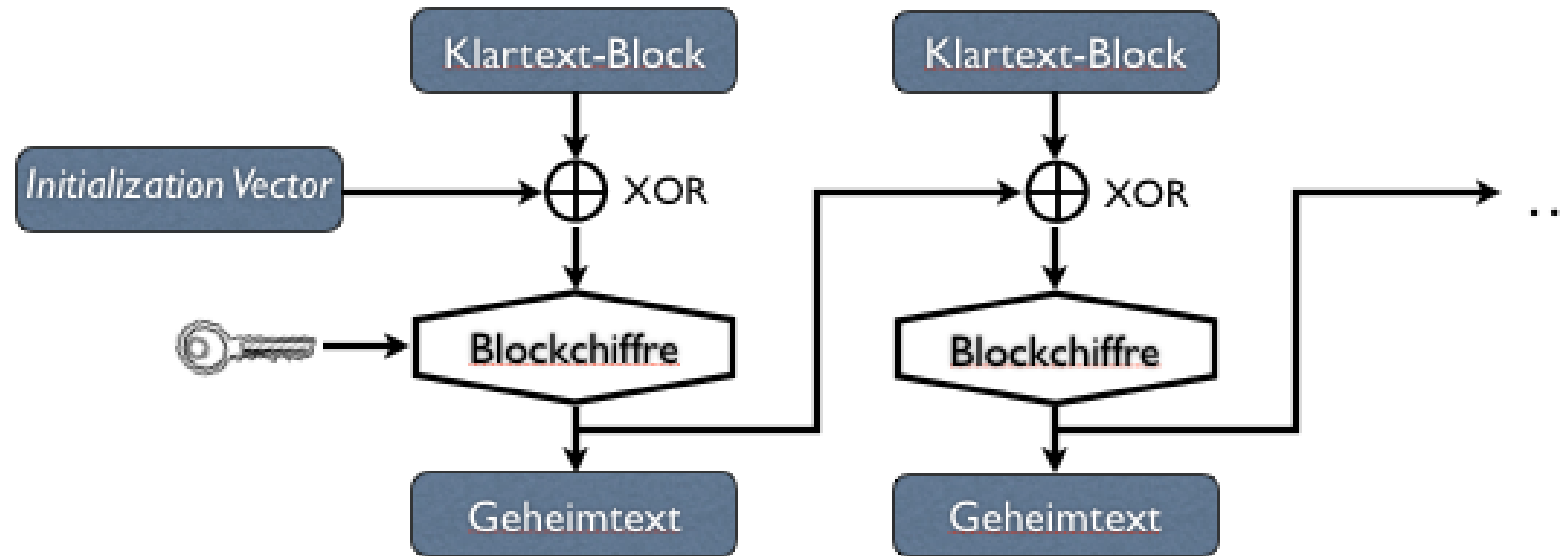
Blockchiffre:

Bei einer Blockchiffre werden nicht einzelne Zeichen verschlüsselt, sondern Blöcke. Die Blockgröße kann variieren - meistens beträgt sie aber 64 Bit.

In der Praxis bedeutet dies, dass ein Klartext zunächst binär umgewandelt werden muss. Diese Binärdarstellung wird dann in 64 Bit Blöcke aufgeteilt.



Blockchiffre (Beispiel Cypher Block Chaining = CBC):



00110001
00110010
00110011
00110100
01100001
01100010
01100011
01100100

Anmerkungen oder Fragen?