Bernd Borchert

Univ. Tübingen WS 13/14

Vorlesung

Kryptographie

Teil 1

18.10.13

Kryptologie – der Umgang mit Geheimnissen

Geheimnisse müssen nichts romantisches oder kriminelles sein, sondern es gibt ganz seriöse wirtschaftliche Anwendungen, z.B. Geschäftsgeheimnisse.

Es geht in diesem Kurs vor allem um Ver- und Entschlüsselung, zum Zweck der **Vertraulichkeit**.

Es gibt aber andere zu erreichende Ziele, die Thema der Kryptologie sind:
- **Authentisierung** (Passwörter etc.)
- **Integrität**, d.h. Nicht-Fälschbarkeit, Stichwort Signatur

Erstes Szenario: Ein Sender A will einen Empfänger B in der Zukunft eine Nachrichten zuschicken, die nicht von jemand anders gelesen werden kann.

Zu dem Zweck dürfen sich A und B, solange sie noch am gleichen Ort sind, ein gemeinsames Geheimnis erzeugen, sagen wir auf Papier (oder USB Stick).

Die Nachricht wird dann von A mithilfe des Geheimnisses kodiert, Nach Empfang dekodiert von B die Nachricht ebenfalls mithilfe des Geheimnisses.

Anwendungen z.B.:
- Militär: A Befehlender, B Befehlsempfänger
- Geschäft: A Chef, B Mitarbeiter

Cäsar Chiffren

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
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

HALLOWELT wird zu OHSSVELSB

Zyklus der Buchstaben. Leicht zu knacken (nur n=26 Möglichkeiten).

Besser ist “monoalphabetische Chiffre”, also eine Bijektion der Buchstaben:

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

HALLOWELT wird zu NIAABGLAK

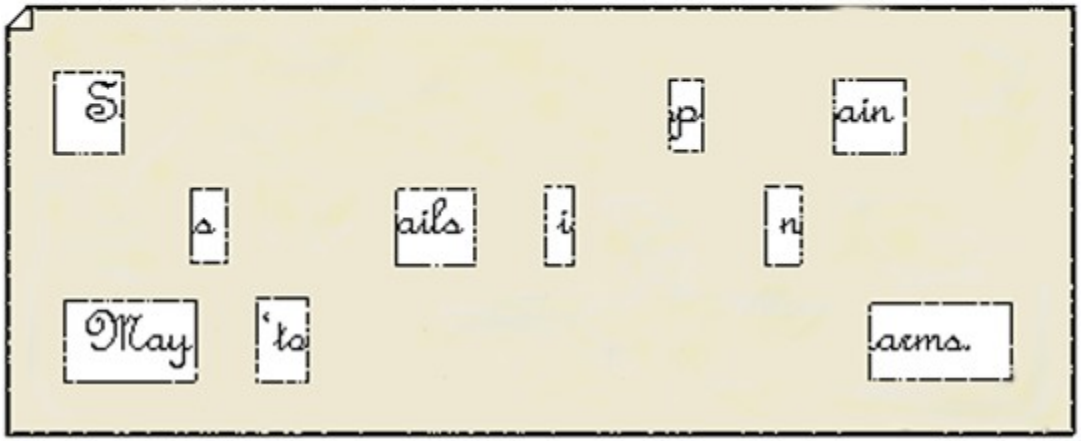
Nicht sicher: Zählung häufigster Buchstaben, Doppelbuchstaben, etc.

Cardano Gitter

Nachricht →

Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.

Geheimnis →
(die Lochkarte)



(hier in der Steganographie Version, d.h. die Nachricht erscheint harmlos)

One-Time Pad

Das One-Time Pad ist die einzige Verschlüsselung, die nachweislich sicher ist, und nicht nur sicher aufgrund von Annahmen ist.

Einzige Annahme (realistisch):

Es gibt gleichverteilten Zufall (Münze, Würfel)

Erfinder: Vernam + Mauborgne (USA, ca. 1918)

Beweis der 100% Sicherheit: Shannon (USA, 1948)

Beispiel One-Time Pad

Alphabet: A-Z plus ein paar extra Zeichen (insgesamt 30 Zeichen)

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		.	,	?	!
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Schlüssel: Gleichverteilter Zufallsstring aus diesen Zeichen:

K	,	W	R	L		D	H	H	P	B	J	A	F	Z	I

Zu codierende Nachricht:

A	N	G	R	I	F	F		M	O	R	G	E	N	!	

Codierte Nachricht:

K	K	?	E	S	A	I	C	T	!	S	P	E	S	Y	D

Decodierte Nachricht:

A	N	G	R	I	F	F		M	O	R	G	E	N	!	

Binäres
One-Time Pad

ASCII TABLE

Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]	48	30	110000	60	0	96	60	1100000	140	`
1	1	1	1	[START OF HEADING]	49	31	110001	61	1	97	61	1100001	141	a
2	2	10	2	[START OF TEXT]	50	32	110010	62	2	98	62	1100010	142	b
3	3	11	3	[END OF TEXT]	51	33	110011	63	3	99	63	1100011	143	c
4	4	100	4	[END OF TRANSMISSION]	52	34	110100	64	4	100	64	1100100	144	d
5	5	101	5	[ENQUIRY]	53	35	110101	65	5	101	65	1100101	145	e
6	6	110	6	[ACKNOWLEDGE]	54	36	110110	66	6	102	66	1100110	146	f
7	7	111	7	[BELL]	55	37	110111	67	7	103	67	1100111	147	g
8	8	1000	10	[BACKSPACE]	56	38	111000	70	8	104	68	1101000	150	h
9	9	1001	11	[HORIZONTAL TAB]	57	39	111001	71	9	105	69	1101001	151	i
10	A	1010	12	[LINE FEED]	58	3A	111010	72	:	106	6A	1101010	152	j
11	B	1011	13	[VERTICAL TAB]	59	3B	111011	73	;	107	6B	1101011	153	k
12	C	1100	14	[FORM FEED]	60	3C	111100	74	<	108	6C	1101100	154	l
13	D	1101	15	[CARRIAGE RETURN]	61	3D	111101	75	=	109	6D	1101101	155	m
14	E	1110	16	[SHIFT OUT]	62	3E	111110	76	>	110	6E	1101110	156	n
15	F	1111	17	[SHIFT IN]	63	3F	111111	77	?	111	6F	1101111	157	o
16	10	10000	20	[DATA LINK ESCAPE]	64	40	1000000	100	@	112	70	1110000	160	p
17	11	10001	21	[DEVICE CONTROL 1]	65	41	1000001	101	A	113	71	1110001	161	q
18	12	10010	22	[DEVICE CONTROL 2]	66	42	1000010	102	B	114	72	1110010	162	r
19	13	10011	23	[DEVICE CONTROL 3]	67	43	1000011	103	C	115	73	1110011	163	s
20	14	10100	24	[DEVICE CONTROL 4]	68	44	1000100	104	D	116	74	1110100	164	t
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]	69	45	1000101	105	E	117	75	1110101	165	u
22	16	10110	26	[SYNCHRONOUS IDLE]	70	46	1000110	106	F	118	76	1110110	166	v
23	17	10111	27	[ENG OF TRANS. BLOCK]	71	47	1000111	107	G	119	77	1110111	167	w
24	18	11000	30	[CANCEL]	72	48	1001000	110	H	120	78	1111000	170	x
25	19	11001	31	[END OF MEDIUM]	73	49	1001001	111	I	121	79	1111001	171	y
26	1A	11010	32	[SUBSTITUTE]	74	4A	1001010	112	J	122	7A	1111010	172	z
27	1B	11011	33	[ESCAPE]	75	4B	1001011	113	K	123	7B	1111011	173	{
28	1C	11100	34	[FILE SEPARATOR]	76	4C	1001100	114	L	124	7C	1111100	174	|
29	1D	11101	35	[GROUP SEPARATOR]	77	4D	1001101	115	M	125	7D	1111101	175	}
30	1E	11110	36	[RECORD SEPARATOR]	78	4E	1001110	116	N	126	7E	1111110	176	~
31	1F	11111	37	[UNIT SEPARATOR]	79	4F	1001111	117	O	127	7F	1111111	177	[DEL]
32	20	100000	40	[SPACE]	80	50	1010000	120	P					
33	21	100001	41	!	81	51	1010001	121	Q					
34	22	100010	42	"	82	52	1010010	122	R					
35	23	100011	43	#	83	53	1010011	123	S					
36	24	100100	44	$	84	54	1010100	124	T					
37	25	100101	45	%	85	55	1010101	125	U					
38	26	100110	46	&	86	56	1010110	126	V					
39	27	100111	47	'	87	57	1010111	127	W					
40	28	101000	50	(	88	58	1011000	130	X					
41	29	101001	51	)	89	59	1011001	131	Y					
42	2A	101010	52	*	90	5A	1011010	132	Z					
43	2B	101011	53	+	91	5B	1011011	133	[					
44	2C	101100	54	,	92	5C	1011100	134	\					
45	2D	101101	55	-	93	5D	1011101	135	]					
46	2E	101110	56	.	94	5E	1011110	136	^					
47	2F	101111	57	/	95	5F	1011111	137	_					

1	0	0	1	0	0	0	1	1	0	1	0	0	1
H							i						

Beweis der perfekten Sicherheit der One-Time Pads.

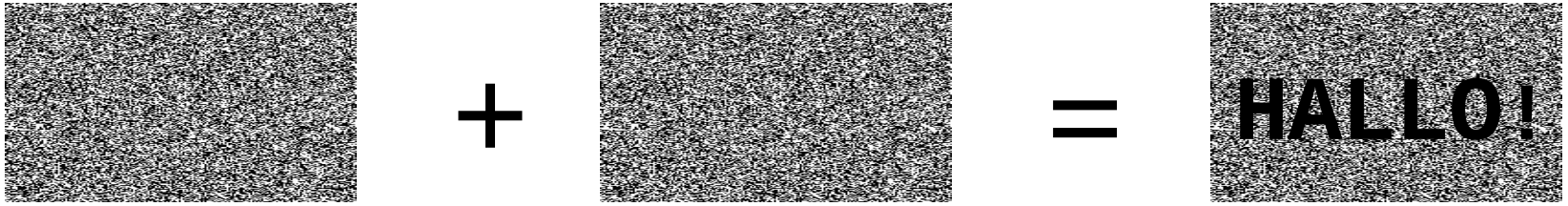
Es reicht zu zeigen: egal wie die zu kodierende Nachricht aussieht, die kodierten Nachrichten sind gleichverteilt zufällig. Denn daraus ergibt sich, dass die kodierten Nachrichten immer gleichverteilt zufällig sind.

Und dass für eine beliebige, aber feste, zu kodierende Nachricht N die zu codierenden Nachrichten gleichverteilt zufällig sind (auch wenn das Zufallsexperiment der Schlüsselerzeugung schon vor der Nachricht-Formulierung stattgefunden hat) ergibt sich direkt daraus, dass die Wahrscheinlichkeit, an einer Stelle i der codierten Nachricht einen Buchstaben a vorzufinden, 1/n ist (n = Anzahl Buchstaben), und zwar unabhängig von den anderen Stellen j <> i (das ist die Defintion von gleichverteilt zufällig). Das gilt deshalb, weil die Schlüssel gleichverteilt zufällig sind und die Buchstaben-Abbildungen bijektiv sind.

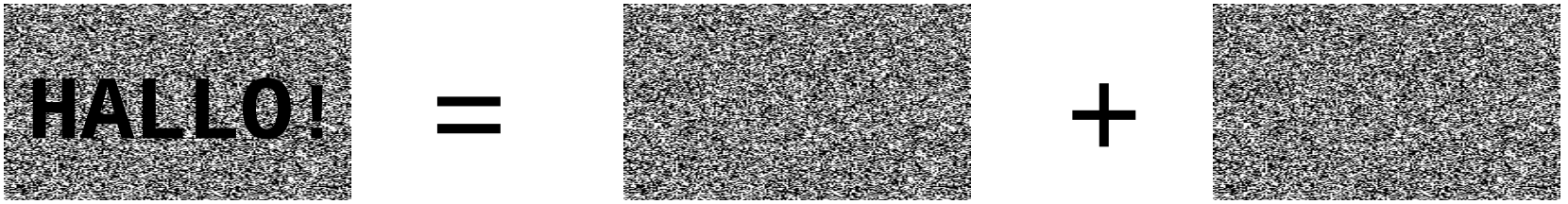
Dies ist ein kurzer Beweis, aber er ist vollständig.

Visuelle Kryptographie

Sie sehen an den mitgebrachten Folien:



Man kann es aber auch so sehen: die Information wird in zwei Teile zerlegt, die beide jeweils allein keine Information haben:



1. Wie kann man das anwenden?
   Idee: immer dann, wenn es um Geheimnisse geht. Geheimnisse müssen nichts kindisches, romantisches oder kriminelles sein, sondern es gibt ganz seriöse wirtschaftliche Anwendungen, z.B. Passwörter, oder Geschäftsgeheimnisse.
2. Wie funktioniert das?
   ist einfach: keine höhere Mathematik - gesunder Menschenverstand reicht!

Ein Brief von Ihrer Bank, Inhalt: eine bedruckte Klarsichtfolie

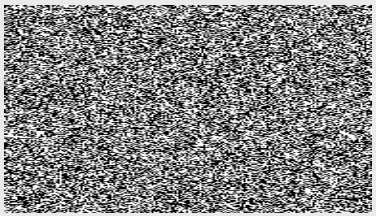
XY Bank
70333 Stuttgart
Postfach 1111

15.3.2007

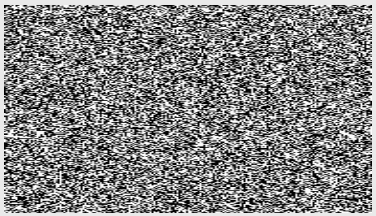
Verschlüsselungs-Folie Nr.1

Sehr geehrter Kunde Z,
bitte bewahren Sie diese Klarsichtfolie in Ihren Unterlagen auf, sie wird zur Entschlüsselung von verschlüsselten Nachrichten an Sie dienen.

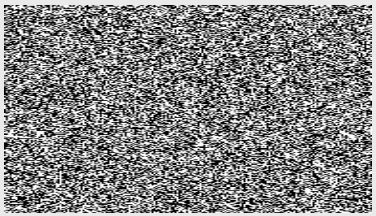
Feld 1



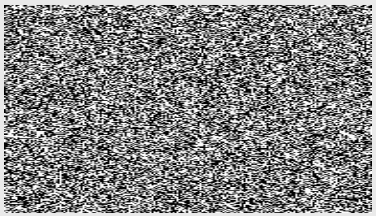
Feld 2



Feld 3



Feld 4



Zwei Monate später: ein anderer Brief (Papier)

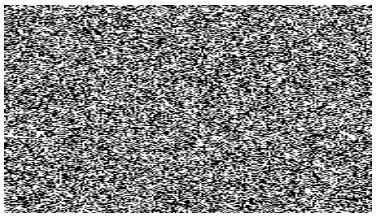
XY Bank
70333 Stuttgart
Postfach 1111

10.5.2007

Betr.: Ihr neues Online-Passwort

Sehr geehrter Kunde Z,
Ihr Online-Passwort wird sich zum 1.6.2007 ändern. Das neue Passwort ist im Feld 1 unten zu lesen, wenn Sie die Verschlüsselungs-Folie Nr.1 auf diesen Brief legen.

Feld 1



Übereinandergelegt ergibt sich:

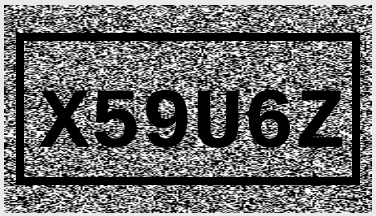
XY Bank
70333 Stuttgart
Postfach 1111

10.5.2007

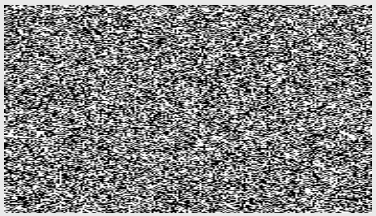
Betr.: Ihr neues Online-Passwort

Sehr geehrter Kunde Z,
Ihr Online-Passwort wird sich zum 1.6.2007 ändern. Das neue Passwort ist im Feld 1 unten zu lesen, wenn Sie die Verschlüsselungs-Folie Nr.1 auf diesen Brief legen.

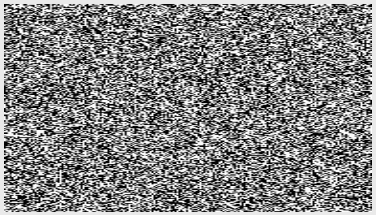
Feld 1



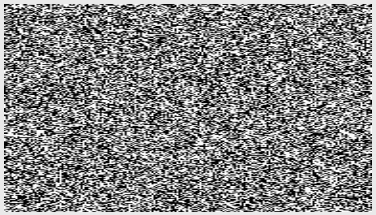
Feld 2



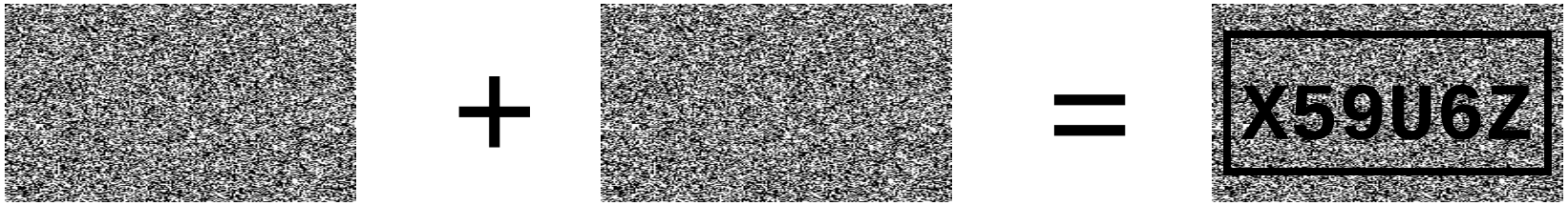
Feld 3



Feld 4



Eigenschaften



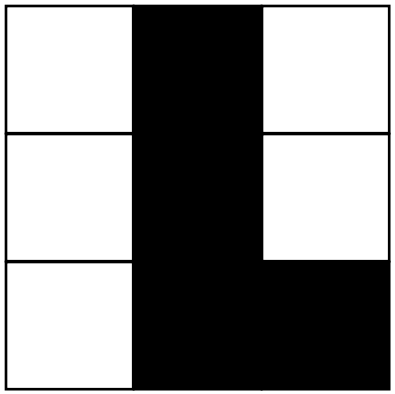
Eigenschaften:

- eine Folie allein hat keine Information
- beide Folien zusammen (bzw. Folie + Papier) ergeben die gesamte Information

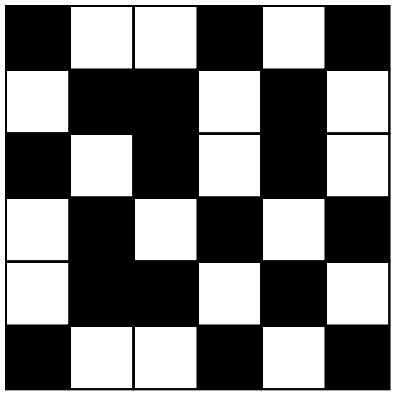
Wie funktioniert‘s?

Wie funktioniert‘s?

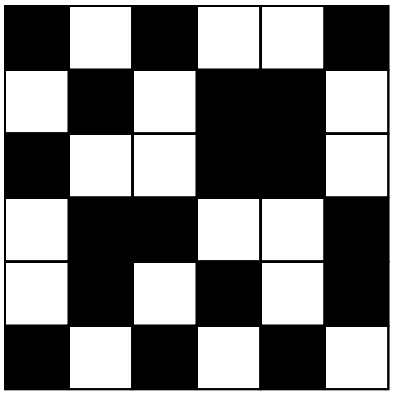
Original-Bild



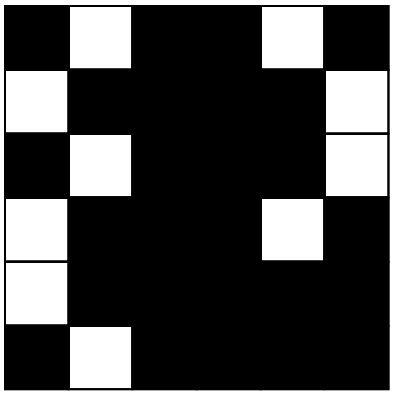
1.Folie

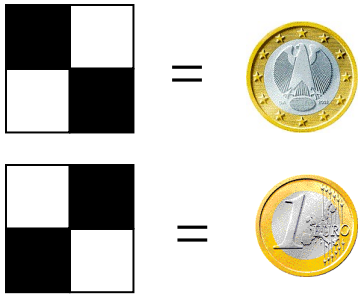


2.Folie



1.+ 2. Folie





Vor- und Nachteile

- Vorteile der Visuellen Kryptographie:
  - Die Dekodierung ist einfach: das menschliche Auge reicht (daher der Name)
  - Die Handhabung ist einfach: keine Computer-Kenntnisse notwendig, es reichen Folien, Papier, Fax, etc.
  - Die Verschlüsselung ist im folgenden Sinne sicher: wenn ein Angreifer nicht beide Folien hat, kann er keinerlei Information gewinnen
  - Die Verschlüsselung ist verlustfrei: Information kann 100% zurückgewonnen werden

- Nachteile:
  - der Kontrastverlust (weiß wird grau)
  - Für jede neue Verschlüsselung braucht man einen neuen Schlüssel. Das ist sehr großer Nachteil! (wenn man Schlüssel doppelt benutzt, läuft man sofort Gefahr, abgehört zu werden)

Zusammenfassung

Einfache Verschlüsselungsverfahren für das einfachste Szenario

„A will B eine geheime Nachricht senden“

vorgestellt:

- Cäsar
- Cardano
- One time Pad
- Visuelle Kryptographie als Variante des One-time Pad (und Variante von Cardano)