

Steganografie

Referentin: Sarah Jäckels

Universität des Saarlandes

Fachrichtung 6.1 Mathematik

Seminar: Kryptologie

Dozent: Prof. Dr. Decker

WS 2007/2008

09.04.2008

Gliederung

1. Kryptologie

1.1 Kryptoanalyse

1.2 Kryptografie

a) Verschlüsselung

a1) symmetrische Verschlüsselung

a2) asymmetrische Verschlüsselung

b) Transposition

c) Substitution

c1) monoalphabetische Substitution

c2) polyalphabetische Substitution

Gliederung

2. Steganografie

2.1 Technische Steganografie

- a) Computergestützte Steganografie

2.2 Linguistische Steganografie

- a) Semagramme

- b) Open code

- b1) Maskierung

- Stichwort

- b2) Verschleierung

- Würfel

- Raster

1. Kryptologie

Kryptologie (griech. *kryptós* = verborgen, *logos* = Lehre) ist die Wissenschaft der Verheimlichung von Informationen durch Transformation der Daten, die Lehre vom Geheimen.

Kryptologie ist eine Jahrtausende alte Wissenschaft, die u.a. folgende mathematische Disziplinen umfasst:

- Zahlentheorie
- Gruppentheorie
- Kombinatorik
- Relationstheorie
- Komplexitätstheorie
- Informationstheorie

1. Kryptologie

Kryptografie und Kryptoanalyse sind zwei Teilgebiete der Kryptologie.

1.1 Kryptografie

- Entwicklung von Algorithmen zur Verschlüsselung von Informationen
- Aufgabe: eine Nachricht oder eine Aufzeichnung für den Unbefugten unverständlich, unlesbar machen.

1.2 Kryptoanalyse

- Analyse von kryptografischen Verfahren
- Stärken und Schwächen der kryptografischen Verfahren werden untersucht

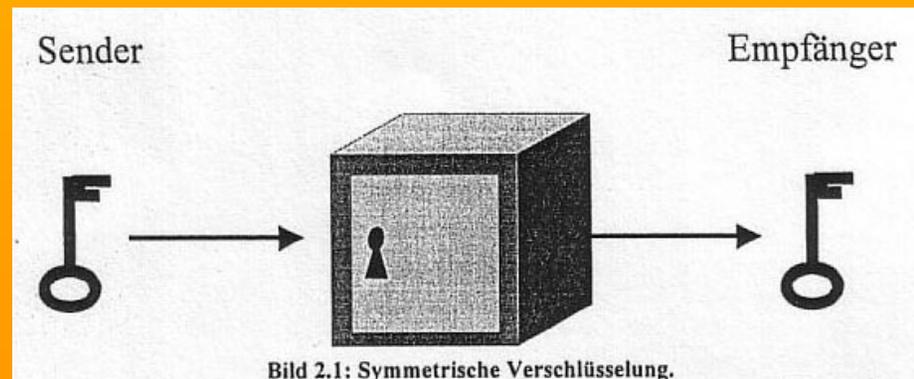
1. Kryptologie

a) Verschlüsselung:

a1) symmetrische Verschlüsselung:

Sender und Empfänger besitzen beide den gleichen, geheimen Schlüssel zur Ver- und Entschlüsselung der Nachrichten.

Problem: Schlüsselübergabe vor Botschaft, Geheimhaltung des Schlüssels



(aus Beutelspacher, A.;Schwenk, J.; Wolfenstetter, K.D.: *Moderne Verfahren der Kryptographie*, S. 6)

1. Kryptologie

a) Verschlüsselung:

a2) asymmetrische Verschlüsselung:

Sender und Empfänger besitzen nicht den gleichen Schlüssel. Sondern der Schlüssel wird aus 2 Schlüsseln gebildet, durch einen öffentlichen und einen geheimen.

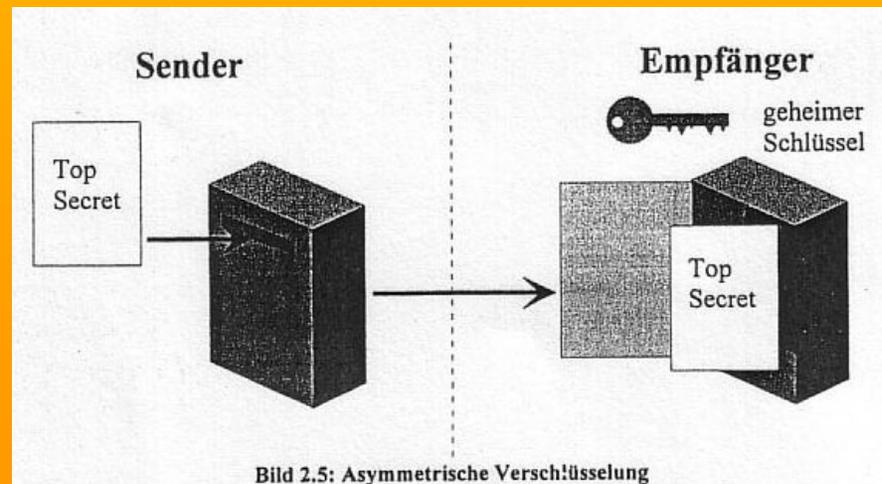


Bild 2.5: Asymmetrische Verschlüsselung

1. Kryptologie

Methoden der Kryptografie:

b) Transposition:

Die Zeichen eines Textes werden umsortiert, entweder wahrlos oder nach einem bestimmten Schema. Dies kann z.B. die Gartenzaunmethode sein.

Beispiel wahrlos, Anfangs- und Endbuchstabe richtig:

Luat einr Stduie der Cambrdige Unievrstiät speilt es kenie Rlloe, in welcehr Reiehnfogle die Buhcstbaen in eniem Wrot vorkmomen, die eingzie whctige Sahce ist, dsas der ertse und der letzte Buhcstbaen stmimt. Der Rset knan in eienm vöillegen Duchrienanedr sein und knan trtozedm prboelmols gelseen wreden. Das ist, wiel das menchsilche Ague nicht jeedn Buhcstbaen liset.

1. Kryptologie

Methoden der Kryptografie:

b) Transposition:

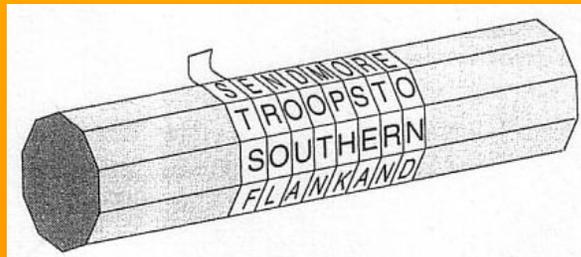
Beispiel Gartenzaunmethode:

Heute beginnt das Blockseminar zum Thema Kryptologie.

↓
h u e e i n d s l c s m n r u t e a r p o o i
e t b g n t a b o k e i a z m h m k y t l g e
↓

h u e e i n d s l c s m n r u t e a r p o o i e t b g n t a b o k e i a z m h m k y t l g e

Beispiel Skytale:



(aus Simon, S.: *Geheime Botschaften*, S. 23)

Send more troops to southern flank and

1. Kryptologie

Methoden der Kryptografie:

c) Substitution:

Die Zeichen eines Textes werden durch andere Zeichen oder Buchstaben ersetzt.

c1) monoalphabetische Substitution:

Jedem Buchstaben wird genau ein anderes Zeichen zugeordnet, dadurch entsteht ein Geheimalphabet.

Beispiel:

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
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Seminar → 19051309140118

1. Kryptologie

Methoden der Kryptografie:

c) **Substitution:**

c2) polyalphabetische Substitution:

Jedem Buchstaben wird ein anderes Zeichen zugeordnet, allerdings werden hier mehrere Geheimalphabete verwendet.

Beispiel Vigenère-Verschlüsselung:

Schlüssel: code

Text: Seminar

Geheimtext: uspmpos

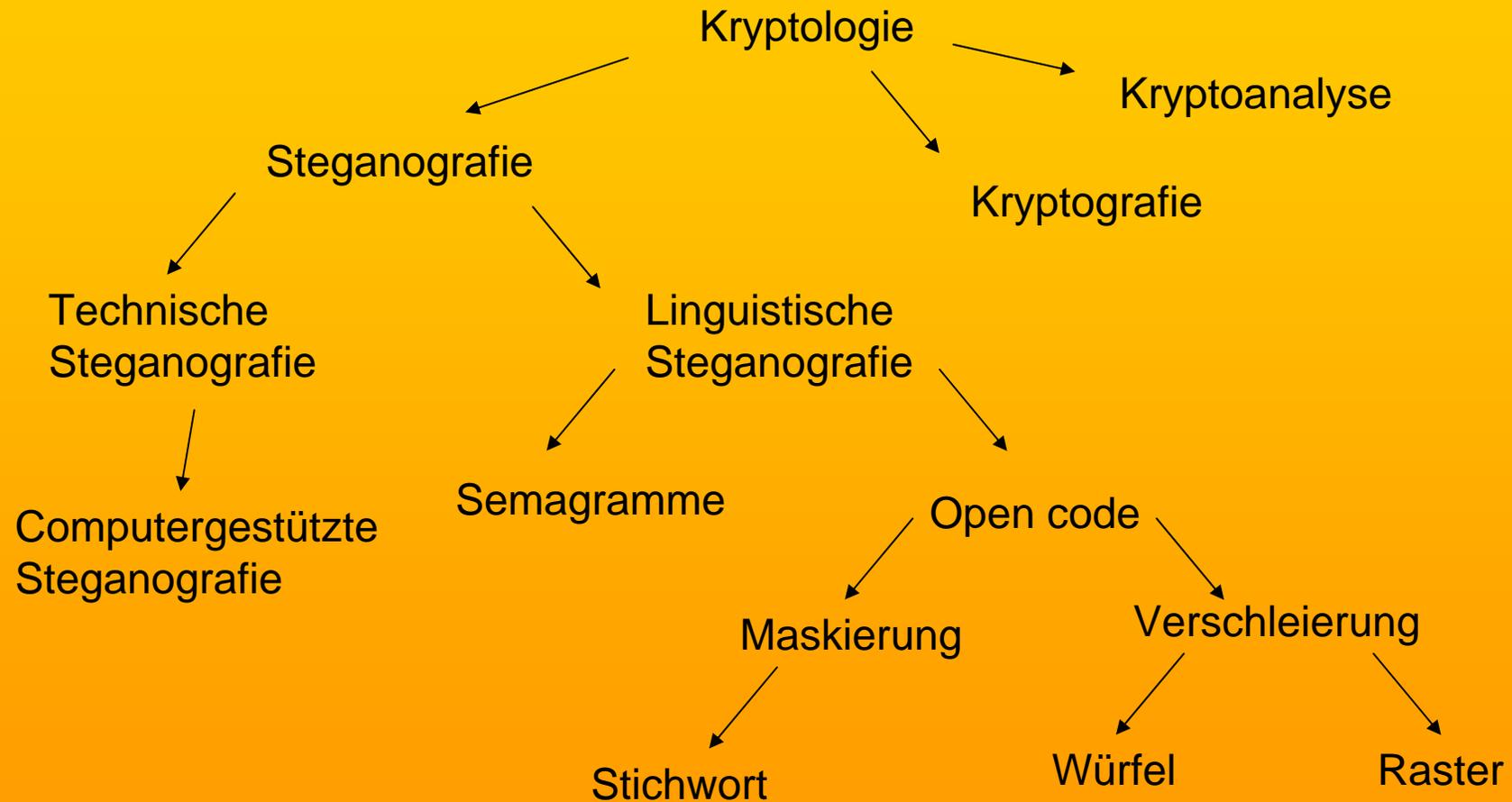
1. Kryptologie

Vigenère-Quadrat

		Text																									
		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
S c h ü s s e l	1	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
	2	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
	3	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
	4	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
	5	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
	6	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
	7	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
	8	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
	9	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
	10	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
	11	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
	12	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
	13	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
	14	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
	15	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
	16	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
	17	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
	18	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
	19	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
	20	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
	21	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
	22	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
	23	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
	24	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
	25	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
	26	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

**G
e
h
e
i
m
t
e
x
t**

Überblick Kryptologie



2. Steganografie

Übermittlung von geheimen Nachrichten, bei der verborgen wird, dass überhaupt eine Botschaft existiert (gedeckte Geheimschrift).

griech.: steganos = bedeckt

graphein = schreiben

Allerdings ist die Botschaft lesbar, wenn das Versteck erkannt wurde.

Da die geheime Nachricht zwar verschlüsselt sein kann, aber nicht muss, wird die Steganografie als Randgebiet der Kryptologie betrachtet.

2.1 Technische Steganografie

Seit Plinius (1. Jh. n. Chr.):

- Geheimtinte (z.B. Zwiebelsaft, Milch -> sichtbar durch Erwärmen)
- doppelte Böden bei Briefumschlägen, Paketen
- hohle Absätze von Schuhen

In der Moderne:

- Morsecode
- Frequenzbandpermutationen beim Sprechfunk
- Mikrofotografie (z.B. Macrodot (Botschaft auf Kopf eines Sklaven), später Micridot (Größe des Schreibmaschinenpunktes))
- versteckte Botschaften in Datenmaterial (z.B. Musikdateien und Bildern)

a) Computergestützte Steganografie

Durch spezielle Software ist es möglich, Informationen in digitalen Bild- oder Tondateien zu verstecken.

Hierbei werden unbedeutende Daten durch geheime Informationen ersetzt. Die Informationen werden in das Least Significant Bit (LSB) hineingeschrieben.

Beispiel: 3 Bildpunkte eines 24Bit-Bildes (je 8 Bit für rot, grün, blau)

	Rot	Grün	Blau
1	(00100111	11101001	11001000)
2	(00100111	11001000	11101001)
3	(11001000	00100111	11101001)

Darin das ASCII Zeichen A (65 = 1000001) versteckt, ergibt:

Rot	Grün	Blau
(00100111	11101000	11001000)
(00100110	11001000	11101000)
(11001001	00100111	11101001)

a) Computergestützte Steganografie

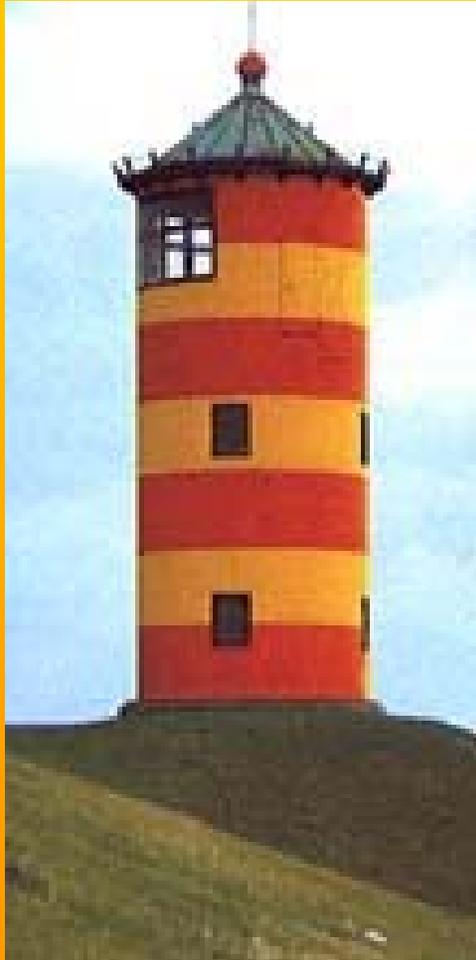
Speichern von Daten in eine .wav-Datei:

- Maximale Größe der Daten $1/8$ der .wav-Datei, da sonst ein hörbares Rauschen entsteht

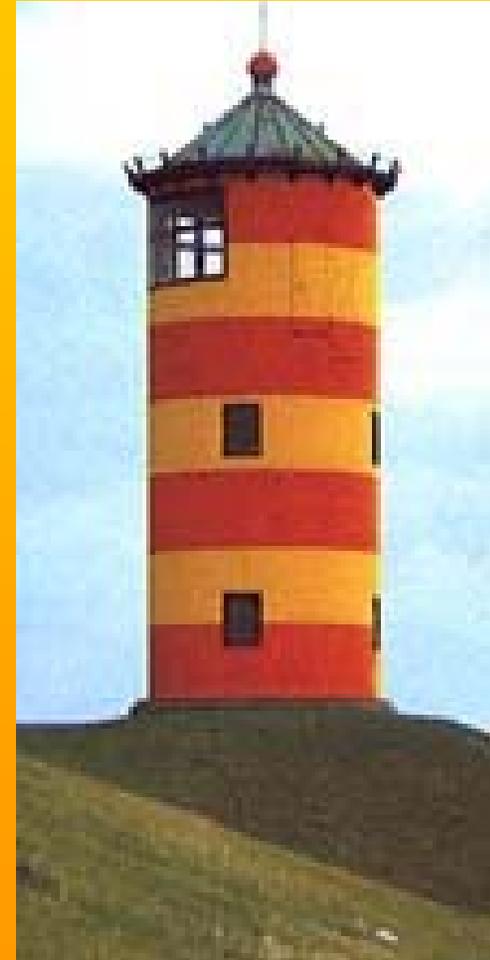
Speichern von Daten in einer .bmp-Datei:

- Maximale Größe der Daten $1/8$ der .bmp-Datei
- Daten leicht durch Programme auslesbar
- Farbbilder können verpixeln, deshalb sind schwarz/weiß-Bilder besser als Versteck geeignet

a) Computergestützte Steganografie



bmp-Datei ohne versteckte Nachricht



bmp-Datei mit versteckter Nachricht

a) Computergestützte Steganografie

Mit Hilfe von dem Programm *ID Image Protector* entstand das Bild mit der versteckten Nachricht:

Entschlüsselung der Nachricht mit Hilfe von

[IDImageProtector.exe](#)

2.2 Linguistische Steganografie

Die linguistische Steganografie lässt sich in Semagramme und in open code unterteilen.

Hierbei geht es darum, ob eine geheime Nachricht als unverfängliche, offen verständliche Nachricht erscheinen soll (open code) oder ob sie in sichtbaren, grafischen Details einer Schrift oder Zeichnung ausgedrückt wird (Semagramm).

a) Semagramme

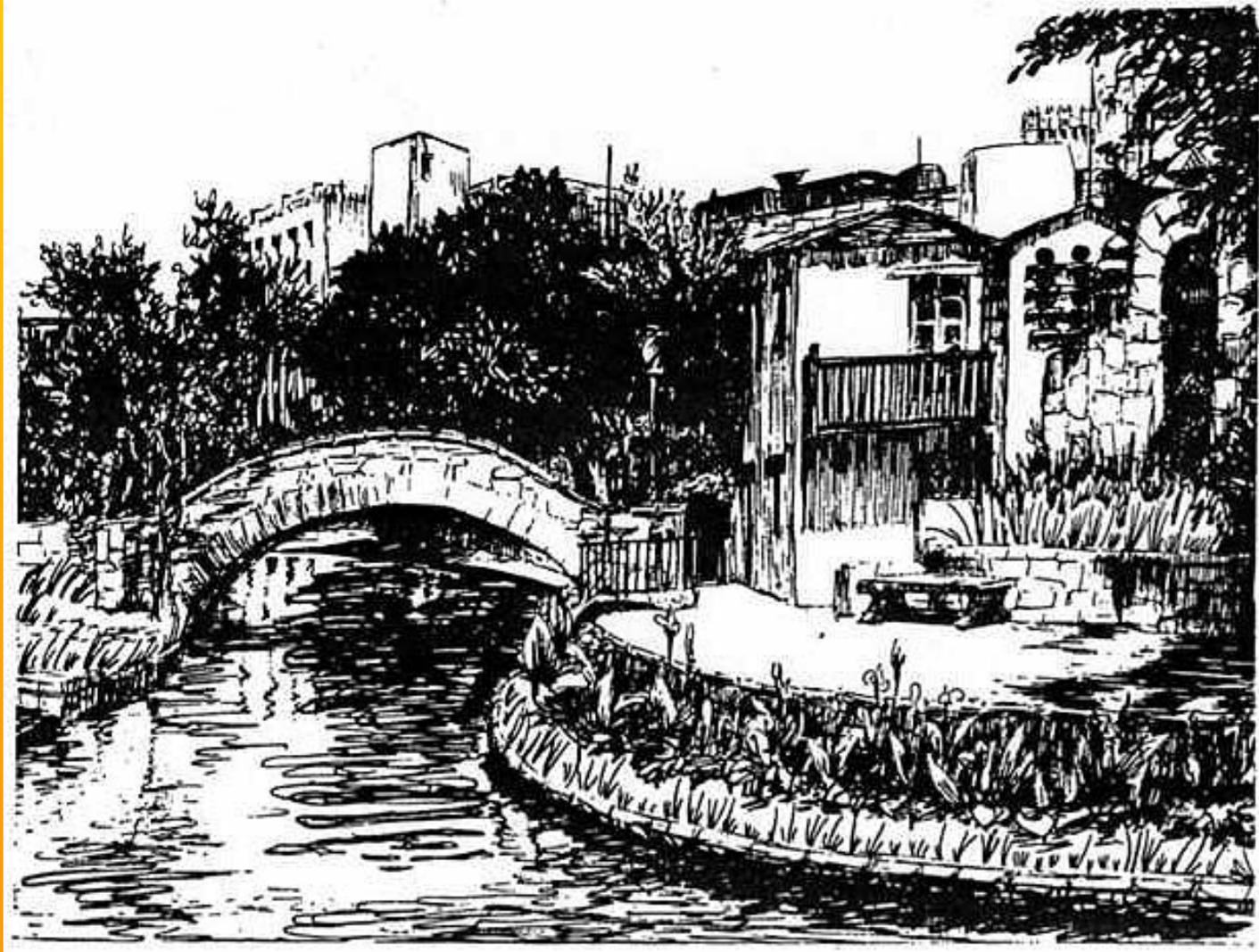
Verstecken der Botschaft in sichtbaren, grafischen Details einer Schrift oder Zeichnung.

Beispiele:

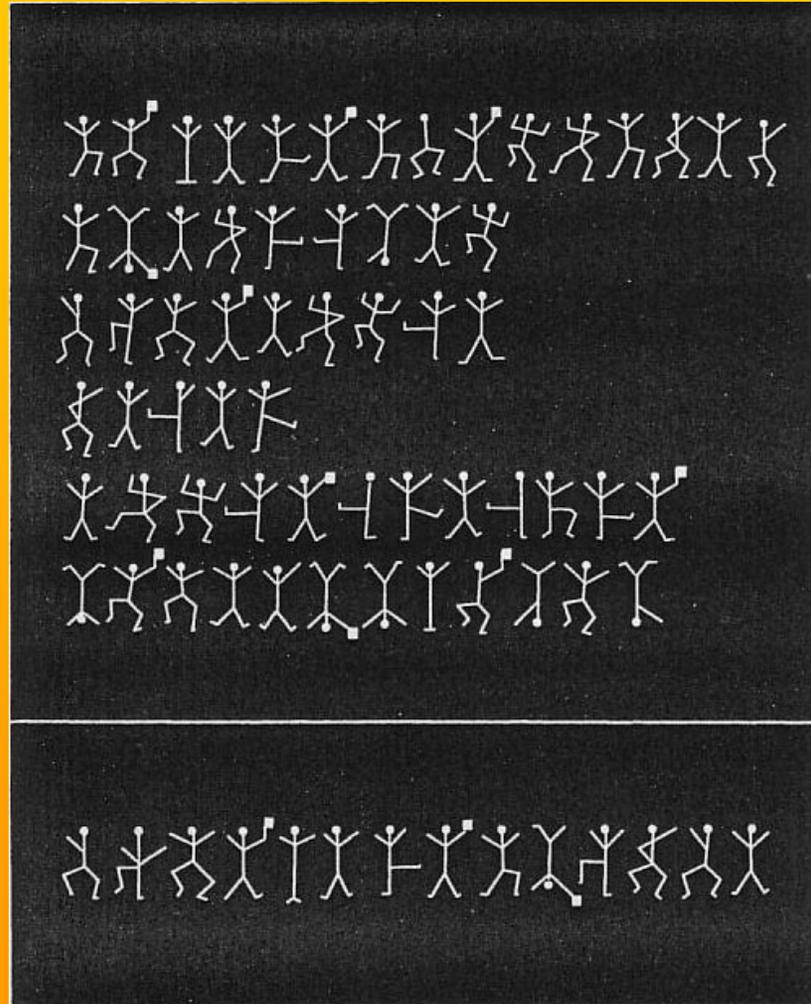
- Verwendung von zwei Schriftarten
- Punktierung ausgewählter Zeichen (auch zusätzlich durch Geheimtinte möglich)
- Kennzeichnung durch Absetzungen im Wort
- Stellung der Zeiger bei mehreren Uhren
- Stellung der Steine bei einem Paket Dominosteine
- tanzende Männchen bei Sherlock Holmes
- versteckter Morsecode in Bildern

Problem: leicht zu entdecken, auch von ungeschulten Beobachtern

a) Semagramme



a) Semagramme



Come here at once

b) Open code

Botschaft erscheint als unverfängliche, offen verständliche Nachricht, durch den Gebrauch von ‚unersichtlich getarnten Geheimschriften und -sprachen‘. Dadurch ist eine Absprache zwischen Sender und Empfänger nötig.

Diesen Bereich der Steganografie lässt sich unterteilen in:

- Maskierung
 - Stichwörter
- Verschleierung
 - Würfel
 - Raster

b1) Maskierung

- vorher Absprache über die wahre Bedeutung unverfänglicher Floskeln nötig
- in allen Kulturen verwendet
- auch in kriminellen Kreisen und bei Kartenspielern

Problem: führt häufig zu auffallenden Formulierungen und kann somit leicht durchschaut werden

Beispiele:

- Jargon (Sondersprachen beruflicher und gesellschaftlicher Art)
- Gebrauch von Zinken (Geheimzeichen)

b1) Maskierung

Beispiel Zinken

aus dem Mittelwesten der Vereinigten Staaten, erste Hälfte des 20. Jh:



(aus Bauer, F.L.: *Entzifferte Geheimnisse – Methoden und Maxime der Kryptologie*, S. 15)

Stichwort

- Spezialfall der Maskierung
- Verwendung eines Stichwortes, Satzes, Verses mit einer einzigen vorher bestimmten Bedeutung
- Wichtigkeit der Nachricht an Zeitpunkt der Aussendung gebunden

Beispiel:

1941 von den Japanern:

HIGASHI NO KAZE AME (= Ostwind, Regen) sollte, wenn es 2mal hintereinander im Wetterbericht gesagt wurde, bedeuten ‚Krieg mit USA‘.

b2) Verschleierung

- Nachricht in die zu übermittelnde, unverfängliche offene Nachricht eingebettet, durch Hinzufügen von Blendern, Nieten, Füllzeichen, Nullen
- Platz an dem die eigentliche Nachricht steht, muss verabredet sein
- hierzu gibt es 2 Möglichkeiten
 - Regeln angeben, Würfel
 - Benutzung eines Rasters

Würfel

Regeln von der Art ‚Das x-te Zeichen nach einem bestimmten Zeichen‘.

Problem: Kann schnell von einem Zensor erkannt werden.

Beispiel:

„Noch einmal tiefempfundene Anteilnahme. Rasche Rückkehr erforderlich. Von Norbert alles Liebe. Paula.“

Botschaft: Plan verraten.

Raster

- Verwendung einer Schablone, die nur die geheime Botschaft erscheinen lässt.
- Sender und Empfänger besitzen die gleiche Schablone.

Problem: Sehr umständlich (sauberes Schriftbild, Ideen für den Text)
Geheimhaltung des Rasters
Formulierungen oft auffällig

Raster

*And there was mounting in hot haste the steed,
The mustering squadron and the clattering car,
And swiftly forming in the ranks of war;
And deep the thunder peal on peal afar;
And near, the beat of the alarming drum
Roused up the soldier ere the morning star
While thronged the citizens with terror dumb
Or whispering, with white lips, — 'the
foe! they come, they come!'*

mustering squadron
forming *ranks* *war*

near

Abb. 16. Lord Byrons hypothetische Nachricht

Aufgabe

Schreibe eine Nachricht, nach dem Prinzip der Verschleierung (Würfel), in der die Botschaft „Ende“ zu finden ist.

Literatur

- Bauer, F.L.: *Entzifferte Geheimnisse – Methoden und Maxime der Kryptologie*. Berlin; Heidelberg; New York; Barcelona; Hongkong; London; Mailand; Paris; Singapur; Tokio: Springer, 2000.
- Beutelspacher, A.; Schwenk, J.; Wolfenstetter, K.D.: *Moderne Verfahren der Kryptographie*. Braunschweig; Wiesbaden: Vieweg, 1998.
- Kippenhan, R.: *Verschlüsselte Botschaften – Die Geheimschrift des Julius Caesar – Geheimschriften im I. und II. Weltkrieg – Das Codebuch des Papstes Enigma*. Hamburg: Nikol, 2006.
- Simon, S.: *Geheime Botschaften*. München; Wien: Carl Hanser, 2000.

**Vielen Dank für eure
Aufmerksamkeit!**