Kryptographie in der Antike und in der Renaissance

Markus Mahrla

31.10.2006

Gliederung

1. Definitionen
2. Kryptographie in der Antike
   - Steganographie
   - Monoalphabetische Verschlüsselung
   - Häufigkeitsanalyse
3. Kryptographie in der Renaissance
   - Anwendungsgebiete der Kryptographie
   - Verbesserungen der monoalphabetischen Verschlüsselung
   - Vigenere-Verschlüsselung
4. Zusammenfassung

Definitionen

- Steganographie
  - steganos (gr.) = bedeckt, versteckt
  - graphein (gr.) = schreiben
  - Wie kann eine Mitteilung versteckt werden ?
- Kryptographie
  - kryptos (gr.) = verborgen
  - Wie kann eine Mitteilung verschlüsselt werden ?
- Kryptoanalyse
  - Entschlüsselung ohne Kenntnis des Schlüssels

Definitionen

- Code
  - Substitution auf der Ebene der Wörter oder Sätze
  - Klartext wird durch andere Wörter oder Buchstabenfolgen ersetzt
- Chiffre
  - Substitution auf der Ebene der Buchstaben
  - Ersetzung durch Buchstabe, Zahl oder Symbol
- Verschlüsseln: Codieren, Chiffrieren
- Entschlüsselung: Decodieren, Dechiffrieren

Kryptographie in der Antike

- Antike
  - Herausbildung der griechischen Staatenwelt bis zum Ende des weströmischen Reiches
  - 800 v.Chr. bis 500 n.Chr.

- Herodots Beschreibungen über die Kriege zwischen Griechenland und Persien 500 v.Chr. dienen als Quelle

- Steganographie in der Antike

Kryptographie in der Antike

Kryptographie:

Transposition

truppenabzug nach osten

t u p n b u n c o t n
r p e a z g a h s e

tupnbuncotnrpeazgahse

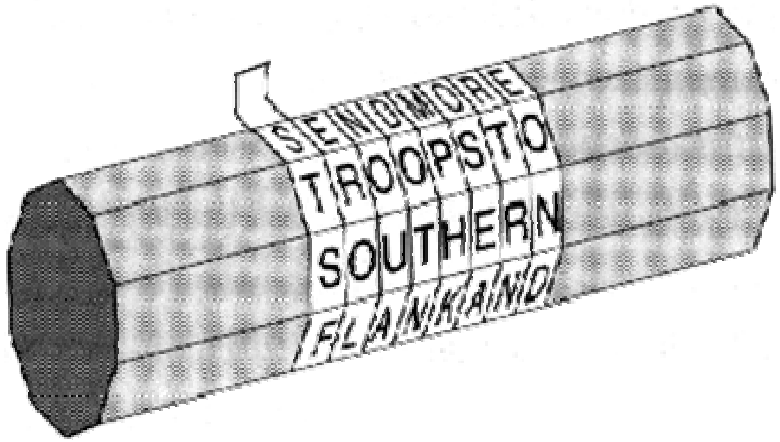
Substitution

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

→ truppen
44424535351533

Kryptographie in der Antike

- Skytale
  - Erste militärische Kryptographie-Verfahren
  - Von den Spartanern 500 v.Chr. errichtet



- S,T,S,F,…,E,R,O,L,…

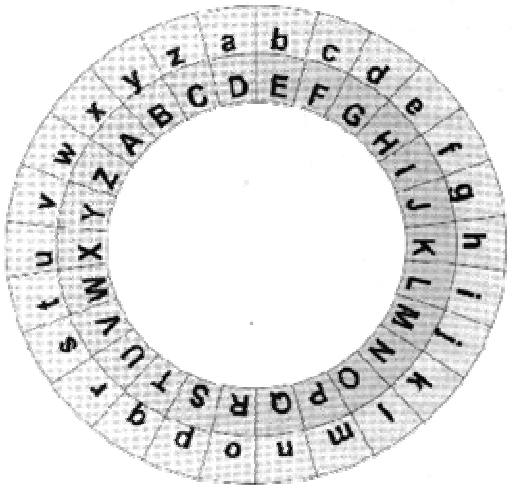
Kryptographie in der Antike

- Eine der frühesten Beschreibungen von Substitution im Kamasutra 400 v.Chr.

```
d w m x i a s b c p q z u
r t y j e f o g h k l v n
```

- Substitution für militärische Zwecke erstmals eingesetzt von Julius Caesar

- Caesar-Verschiebung



Kryptographie in der Antike

- Relativ schwach, da 25 mögliche Schlüssel
- Bei einer beliebigen Ordnung sehr stark
- Zur Vereinfachung kann Schlüsselwort oder Schlüsselsatz verwendet werden

```
abcdefghijklmnopqrstuvwxyz
KRYPTOGAHIEFJLMNQSUVWXZBCD
```

- Monoalphabetische Verschlüsselung

Kryptographie in der Antike

- Überwindung der monoalphabetischen Verschlüsselung von Al-Kandi ca. 900 n.Chr.
- Grundlage waren Koranstudien
- Häufigkeitsanalyse ist ein Werkzeug, kein vollständiger Lösungsweg

	Englisch	Deutsch	Französisch	Italienisch	Spanisch	Portugiesisch
A	7,81	5	9,42	11,74	12,69	13,5
…			…			
E	13,05	18,5	15,87	11,79	13,15	13
…			…			
N	7,28	11,5	7,15	6,88	6,95	5,5

Häufigkeitsanalyse

- Häufigkeit der Buchstaben, Bigramme und Trigramme feststellen
- Erkannte Buchstaben einsetzen und Wörter erraten
- Eigenheiten der Sprache benutzen
  - z.B. erscheint im Deutschen nach c häufig h oder k oder nach q folgt immer u
  - Häufigsten Wörter der Sprache kennen
- Eventuell Schlüsselwort erraten

Kryptographie in der Renaissance

- Renaissance
  - Epoche Europas während des Überganges vom Mittelalter zur Neuzeit
  - Etwa 14./15. Jahrhundert

- Von 500 bis 1400 n.Chr. überwiegend Stagnation in der westlichen Welt

- Im 14. Jahrhundert Geheimhaltung der Entdeckungen von Wissenschaftlern

Kryptographie in der Renaissance

- Im 15. Jahrhundert überwiegend für diplomatische Zwecke benutzt
- Möglichkeit der Entschlüsselung war noch nicht hinreichend bekannt
- Verbesserung der monoalphabetischen Verschlüsselung
  - Füllzeichen
  - Absichtliche Rechtschreibfehler
  - Codes (Nomenklatur)

Kryptographie in der Renaissance

- Leon Battista Alberti schlug erstmal vor, mehrere Geheimtextalphabete zu verwenden und zwischen diesen zu springen
- Idee weiterentwickelt von Trithemius, Porta und schließlich Vigenere
- Vigenere-Verschlüsselung

Kryptographie in der Renaissance

LICHTLICHTLICHTLICHTL

truppenabzugnachosten

EZWWIPVCISFOEHVSWUAXY

	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

Vigenere-Quadrat

Kryptographie in der Renaissance

- Polyalphabetische Verschlüsselung
- Erstaunlicher Weise wurde die Vigenere-Verschlüsselung kaum benutzt
- Mittelweg war die homophone Verschlüsselung
  - homo (gr.) = gleich
  - phone (gr.) = Klang
- Im Prinzip aber auch monoalphabetische Verschlüsselung

Kryptographie in der Renaissance

- Vigenere-Verschlüsselung galt als unüberwindbar
- Babbage (bzw. Kasiski) erkannte wie man die Vigenere-Verschlüsselung knackte
- Wiederholungen suchen und Abstände zählen
- Über gemeinsamen Teiler gelangt man zu der Länge des Schlüsselwortes
- Reduktion der polyalphabetischen Verschlüsselung auf mehrere monoalphabetische Verschlüsselungen

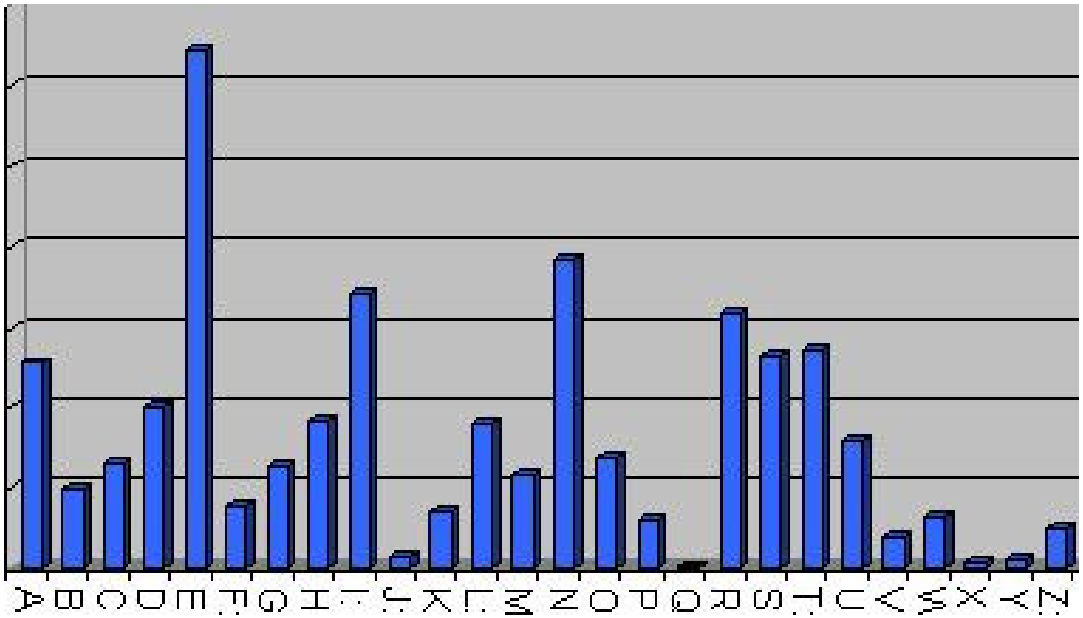
Kryptographie in der Renaissance

WUBEFIQLZURMVOFEHMYMWT

IXCGTMEFIQPIUPMVOIRQMM

WOQMMZMPBNYVQQQMVMVJLE

YMHFEFNZPSDLPPSDLPEVQM



Zusammenfassung

- Monoalphabetische Verschlüsselung in der Antike (erstmals 400 v.Chr. beschrieben)
- Entschlüsselung durch islamische Gelehrte (900 n.Chr.)
- 500 n.Chr. bis 1400 n.Chr. Stagnation im Westen
- Benutzung der monoalphabetischen Verschlüsselung und Erfindung der Vigenere-Verschlüsselung in der Renaissance
- Entschlüsselung durch Babbage im Jahr 1854

Literatur

- Kahn, David: The Codebreakers. The Story of Secret Writing. 2. Auflage. New York: Scribner, 1996.
- Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München: Hanser, 2000.
- Gaines, Helen Fouche: Cryptanalysis. A study of ciphers and their solutions. New York: Dover, 1956.
- Sinkov, Abraham: Elementary Cryptanalysis. A mathematical approach. 1. Auflage. New York: Random House, 1968.
- Beker, Henry/Piper, Fred: Cipher Systems. The Protection of Communication. London: Northwood Publication, 1982.