Humboldt Universität zu Berlin
Institut für Informatik
Seminar: „Geschichte der Verschlüsselung“

Vortrag zum Thema:

„Kryptographie in der Antike und in der Renaissance“

Radin Hristov

Gliederung

- Überblick über die Antike und die Renaissance als historische Epochen
- Kurze Einführung in die Kryptologie
- Kryptographie in der Antike
- Kryptoanalyse der antiken Verfahren
- Kryptographie in der Renaissance
- Kryptoanalyse der Verfahren
- Zusammenfassung

Historische Übersicht

- Antike (1200 v. Chr. – 600 n. Chr.)
  - Geschichte des archaischen und klassischen Griechenland
  - Geschichte des Hellenismus
  - Geschichte des Römischen Reiches
- Renaissance (1400 n. Chr. – 1600 n. Chr.)
  - Die Renaissance als geistige Bewegung (Wiedergeburt des antiken Geistes)
  - Übergang vom Mittelalter zur Neuzeit

Einführung in die Kryptologie

- Die **Kryptologie** ist die Gesamtheit folgender Wissenschaften/Künsten:
  - **Kryptographie** (*κρυπτοσ* – geheim; *γραφειν* – schreiben)**:** Entwicklung von Methoden zur Verheimlichung von Nachrichten
  - **Kryptoanalyse:** Die Kunst Geheimschriften zu entziffern
- **Kryptographie** vs. **Steganographie** (*στεγανοσ – bedeckt)*

Einführung in die Kryptographie

- ***V*** – Zeichenvorrat, mit dessen Hilfe der Klartext formuliert wird (***Klartextalphabet***)
- ***W*** – Zeichenvorrat, mit dessen Hilfe der Geheimtext formuliert wird (***Geheimtextalphabet***)
- $\mathbf{X}_i : V^{(n_i)} \rightarrow W^{(m_i)}$ (***Chiffrierschritt***)
- $\{\mathbf{X}_0, \mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_{\theta-1}\}$ (***Chiffriersystem***)

Einführung in die Kryptographie

- $\mathbf{X}_i : \boldsymbol{V}^{(n_i)} \rightarrow \boldsymbol{W}^{(m_i)}$ (***Chiffrierschritt***)
- $\{\mathbf{X}_0, \mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_{i-1}\}$ (***Chiffriersystem***)
  - Monoalphabetische Chiffrierung (i=1)
  - Polyalphabetische Chiffrierung (i>1)
  - Monographische Chiffrierung (n=1)
  - Polygraphische Chiffrierung (n>1)
  - Monopartite Chiffrierung (m=1)
  - Multiparitite Chiffrierung (m>1)

Anfänge der Kryptographie I

- Ägypten (1900 v. Chr.) – absichtliche Veränderung des Geschriebenen

- Mesopotamien (1500 v.Chr.) - erste nachgewiesene Chiffrierung

Anfänge der Kryptographie II

- ***Atbash*** (600 v. Chr.) – die Geheimschrift der Hebräer

  Klartextalphabet: A B C D E F . . . .

  Geheimtextalphabet: Z Y X W V U . . . .

- ***Mlecchita – vikalpa*** (400 v. Chr.) – die Geheimschrift des *Kamasutra*

  A D H I K M O R S U W Y Z

  V X B G J C Q L N E F P T

Kryptographie in der Antike I

- Die ***Skytala*** von Sparta (487 v. Chr.) – die erste und die einzige Transposition-verschlüsselung

Beispiel 1

Geheimtext: W I A I N P R D S S P T

Klartext (u=3):

W	**I**	**R**	**S**
I	**N**	**D**	**P**
A	**P**	**S**	**T**

Kryptographie in der Antike II

- **Tafel des Polybius** (200 v. Chr.)

  Beispiel 2
  Geheimtext: 22 54 42 34 43
  Klartext: ???

	1	2	3	4	5
1	A	B	C	D	E
2	F	**G**	H	I/J	K
3	L	M	N	**O**	P
4	Q	**R**	**S**	T	U
5	V	W	X	**Y**	Z

- **Die *Caesar – Verschiebung*** (50 v. Chr.)

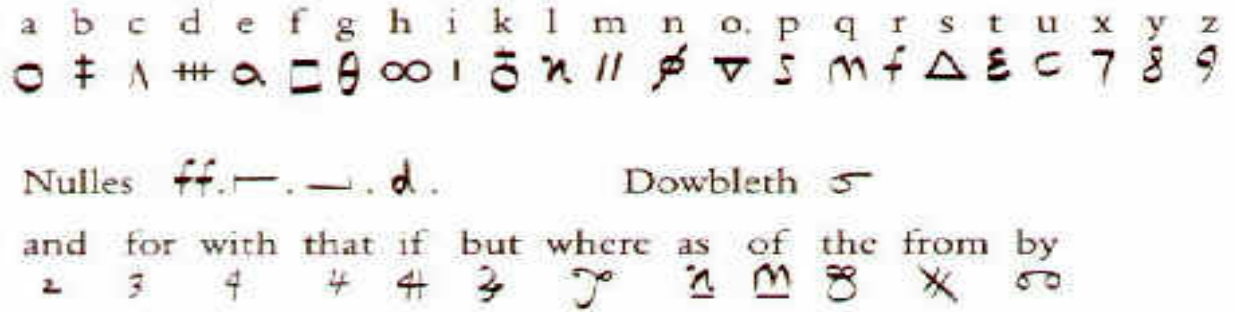
  Beispiel 3
  Geheimtext: Y H Q L, Y L G L, Y L F L
  Klartext: **V E N I**, **V I D I**, **V I C I**

Kryptoanalyse

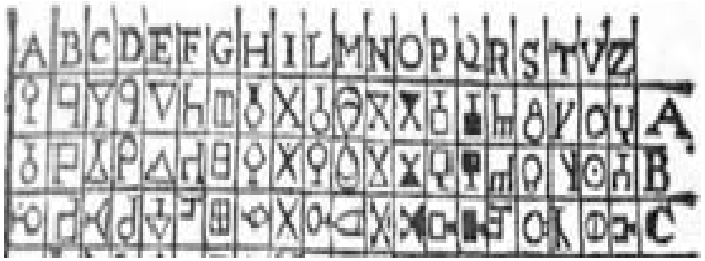
- Schwachstelle der antiken Chiffrierverfahren
- Was hat Religion mit Kryptoanalyse zu tun?
- Al-Kindi und die Häufigkeitsanalyse

Kryptographie in der Renaissance I

- „**Füller**" und absichtliche Schreibfehler
- ***Nomenklator*** = monoalphabetische Verschlüsselung + Codewörter



- **Bigramm – Substitution** (G.B. Porta, 1563)



Kryptographie in der Renaissance II

- ***Homophone Verschlüsselung*** (Matteo Argenti, 1590)
  - Jede Buchstabe wird durch mehrere Stellvertreter ersetzt
  - Die Zahl der möglichen Stellvertreter steht im Verhältnis zur Häufigkeit der Buchstaben
    - k – 84
    - u – 61,63,34,60
    - c – 48,81

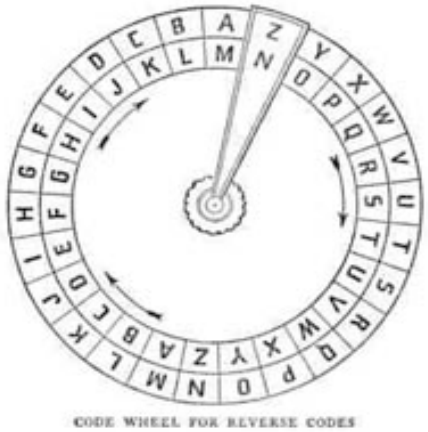
    Beispiel 4

    Klartext: Kuckuck

    Geheimtext: 84 61 48 84 63 81 84

Renaissance der Kryptographie I

- ***Chiffrierscheibe*** (L.B. Alberti, 1460)



Ersetzungstabelle:

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

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
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

Beispiel 5

Klartext: DIE WELT DER GEHEIMEN ZEICHEN

Geheimtext: JUK I KXZ VKD MQNQOYKZ FQOONQT

Renaissance der Kryptographie II

- ***Die Vigenere - Chiffre***
  (Blaise de Vigenere, um 1580)

Beispiel 6

Schlüsselwort: TORATORATOR
Klartext: PEARLHARBOR
Geheimtext: ISRAEVRRUCI

Klar	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	J	K	L	M	N	O	P	Q	R	S	T	J	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Zusammenfassung

- $\mathbf{X}_i : \boldsymbol{V}^{(n_i)} \rightarrow \boldsymbol{W}^{(m_i)}$ (***Chiffrierschritt***)
  - i=1 monoalphabetisch, polyalphabetisch sonst
  - n=1 monographisch, polygraphisch sonst
  - m=1 monopartit, multipartit sonst

- **Antike**
  - Monoalphabetische Chiffrierverfahren
  - Anfänge der Kryptoanalyse (Häufigkeitsanalyse)

- **Renaissance**
  - Verbesserung der monoalphabetischen Verschlüsselung (Homophone, Nomenklatoren, Füller)
  - Vigenere – Chiffre (erste ausgereifte polyalphabetische

Quellenverzeichnis

- Bauer, Friedrich L.: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. 2 Auflage. Springer-Verlag 1995
- Beutelspacher, Albrecht: Kryptologie. Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. 6 Auflage. Vieweg 2002
- Kahn, David: The Codebreakers. Überarbeitete Auflage, Scribner Book Company 1996
- Schmeh, Klaus: Die Welt der geheimen Zeichen - Die faszinierende Geschichte der Verschlьsselung. W3L 2004
- Singh, Simon: Geheime Botschaften. dtv 2001