

Übung zu Kryptographische Verfahren Übung 2

Christian Viergutz

Fachgruppe Kombinatorische Algorithmen
Fachbereich Mathematik / Informatik
Universität Osnabrück

WS 2006/07



In dieser Übung

- 1 Selbstinverse Schlüssel
- 2 Permutationschiffren
- 3 Vigenère-Kryptosystem
- 4 Umgang mit dem CrypTool



Selbstinverse Schlüssel

Definition 2.1 (Selbstinverser Schlüssel)

Ein Schlüssel $K \in \mathcal{K}$ heißt *selbstinvers*, wenn die Verschlüsselungsfunktion $E(x, K)$ und die Entschlüsselungsfunktion $D(x, K)$ identisch sind, also wenn $\forall x \in \mathcal{P} : E(x, K) = D(x, K)$.

Folgerung

Ist $K \in \mathcal{K}$ ein selbstinverser Schlüssel in einem Kryptosystem, dann gilt in diesem System $E(E(x, K), K) = x$.



Affine Chiffre

Zur Erinnerung: Bei der **affinen Chiffre** über einem Alphabet \mathcal{A} und mit Schlüssel $K = (a, b) \in \mathbb{Z}_{|\mathcal{A}|}^2$ ist die Verschlüsselungsfunktion gegeben durch:

$$E(x, K) = ax + b \bmod |\mathcal{A}|$$

Aufgabe

Sei $\mathcal{A} = \mathbb{Z}_{15}$ und $K = (5, 7) \in \mathbb{Z}_{15}^2$

- 1 Ist diese Chiffre selbstinvers?
- 2 Gibt es einen Schlüssel zum Entschlüsseln? Wenn ja, wie lautet er? Wenn nein, warum gibt es keinen?



Permutationschiffren

Permutationschiffren werden auch Transpositionschiffren genannt. Beim Verschlüsseln bleiben alle Zeichen des Klartextes erhalten, sie ändern nur ihre Positionen. Als Anwendungsbeispiel folgende Aufgabe:

Aufgabe

Der Schlüssel sei die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 1 & 3 \end{pmatrix}$$

- 1 Was ist die Verschlüsselung von `kryptografie`?
- 2 Was ist die Entschlüsselung von `LERTKATHUCXBTNBESA`?

Vigenère-Kryptosystem

- Polyalphabetische Chiffre, d.h. ein Klartextzeichen kann in verschiedene Chiffretextzeichen verschlüsselt werden (bei Vigenère abhängig von der Position im Text).
- Verfahren: Schlüsselwort wird wiederholt unter den Klartext geschrieben. Addition (entsprechende Verschiebung) der jeweils untereinanderstehenden Paare liefert den Chiffretext.

geheim

 SECRET

 YI JVMF

	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

Vigenère-Kryptosystem

	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



Ciphertext-only-Angriffe auf das Vigenère-Verfahren

Erster Schritt: Bestimmung der verwendeten Schlüssellänge

- **Autokorrelation:** Kennzahl für die Ähnlichkeit von Teilen des Dokuments. Beschreibt Übereinstimmungen zwischen einer Zeichenfolge und einer verschobenen Kopie davon. Hohe Autokorrelationswerte deuten auf Vielfache der Schlüssellänge hin.
- **Kasiski-Test:** Suche Folgen von 3 oder mehr gleichen Zeichen im Text und bestimme deren Abstand. Dieser ist (vermutlich) ein Vielfaches des Schlüsselwortlänge.
- **Friedman-Test:** Berechnung des Koinzidenzindex: Bezeichnet die W'keit, bei zufälliger Wahl zweier Zeichen die gleichen Buchstaben zu erhalten:

$$I = \frac{\sum_{i=1}^{26} \binom{n_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=1}^{26} n_i(n_i - 1)}{n(n - 1)} \approx \sum_{i=1}^{26} p_i^2$$

Dabei ist p_i die rel. Häufigkeit des i -ten Buchstabens.



Ciphertext-only-Angriffe auf das Vigenère-Verfahren

- Für deutsche Texte erhält man durch Einsetzen der bekannten Buchstaben-Häufigkeiten:

$$I_d \approx 0,0651^2 + 0,0189^2 + \dots + 0,0113^2 \approx 0,0762$$

- Bei zufällig gleichverteilten Buchstabenfolgen erhält man

$$I_r = \sum_{i=1}^{26} \left(\frac{1}{26} \right)^2 = \frac{1}{26} \approx 0,0385$$

- Näherung für Schlüssellänge ergibt sich als Umstellung der Gleichung für den Koinzidenzindex für ein festes k :

$$k \approx \frac{(I_d - I_r)n}{(n-1)I - I_r n + I_d}$$

