Übungsaufgaben zur Vorlesung Kryptologie

Helmut-Schmidt-Universität — Universität der Bundeswehr Hamburg
Professur für Allgemeine Nachrichtentechnik — Prof. Dr.-Ing. Udo Zölzer
Dr.-Ing. Martin Holters, Raum: H3 - R115, Tel.: 040 / 6541 - 3468

M.Sc. Patrick Nowak, Raum: H3 - R116, Tel.: 040 / 6541 - 3650

Übungsaufgaben zu Kap. 3: Monographische, polyalphabetische Substitution

---

Aufgabe 1 — Verschlüsselung mit begleitenden Alphabeten und periodischem Schlüssel

Im Folgenden sei

- ρ der Zyklus des Standardalphabets

$$(abcdefghijklmnopqrstuvwxyz)$$

- P die Permutation

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

- R die Permutation

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

Es soll nun der Klartext `klartext` mit dem periodisch wiederholten Schlüssel `abcd` verschlüsselt werden mit

a) den verschobenen Standardalphabeten (VIGENÈRE-Verfahren) $\chi_j = \rho^j$

b) den horizontal verschobenen P-Alphabeten (ALBERTI-Verfahren) $\chi_j = \rho^j P$

c) den vertikal verschobenen P-Alphabeten $\chi_j = P\rho^j$

d) den R-rotierten Standardalphabeten $\chi_j = \rho^{-j} R \rho^j$

e) den R-rotierten P-Alphabeten $\chi_j = P\rho^{-j} R \rho^j P^{-1}$

Aufgabe 2 — Inversion der Verfahren mit begleitenden Alphabeten

Wie lauten zu den fünf Verfahren aus Aufgabe 1 jeweils die Inversen Schritte χ_j^{-1}?

Aufgabe 3 — Zyklen rotierter Alphabete

Es sei R die Permutation

a	b	c	d	e	f
C	F	A	E	B	D

über $\{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}\}$. Bilden Sie die Zyklendarstellung von $\rho^{-j} R \rho^j$ (mit $\rho = (abcdef)$) für $j = 0, \ldots, 5$.

Aufgabe 4 — Verschlüsselung mit einer Rotormaschine

Es sei vereinfacht eine Rotormaschine mit nur einem Rotor

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

und einer festen Umkehrwalze

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

betrachtet. Chiffrieren Sie den Klartext `geheim` mit der Ausgangsposition $i = 24$.

Aufgabe 5 — Angriff mit der Isomorphie-Methode

Es sei eine mit einer kommerziellen Enigma verschlüsselte Nachricht abgefangen worden, die mit

`OXSIS HWULE Q...`

beginnt. Wir vermuten, dass der zugehörige Klartext mit `sehrgeehrte` beginnt. Angenommen, der schnelle Rotor wird durch die Substitution

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

beschrieben, welche der Anfangsstellungen $i_1 \in \{0,1,2,3\}$ ist möglich?