Geheime Botschaften

Sommersemester 2017

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527

Technische Universität Braunschweig

Übungsblatt 3

Aufgabe 1. (Evaluation)
Füllen Sie den beiliegenden Bogen zur Evaluation der Lehrveranstaltung gewissenhaft aus.

Aufgabe 2. (Enigma - Verschlüsselung)
Sie haben Ihre Enigma I in die Walzenlage **B III I II** gebracht und die Walzen in die Stellung **AAC** gedreht. Der Einfachheit halber sind die Ringe nicht verdreht und es sind keine Steckverbindungen gesteckt. Verschlüsseln Sie nun (ohne Verdoppelung) den Spruchschlüssel **RTZ**. Beachten Sie, dass sich bei einem Verschlüsselungsschritt erst die Walzen drehen und dann der Strom durch die Enigma fließt.

Verschlüsselung von **R**:

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

Verschlüsselung von **T**:

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

Verschlüsselung von **Z**:

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

Aufgabe 3. (Enigma & Cribs)
Wir wollen eine vereinfachte Version von Turings Ansatz zum Brechen der Enigma betrachten. Insbesondere wollen wir einsehen, wie **Cribs** uns dabei helfen können, bestimmte Einstellungen der Enigma auszuschließen.

• **Crib-dragging:**
Sie vermuten, dass der Crib

ATTACKATDAWN

sich im Geheimtext

AAWSNPNLKLSTCSQPN

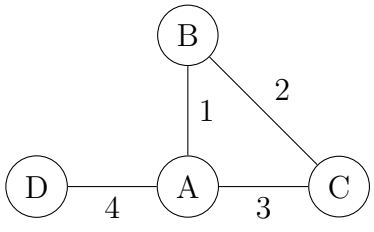
befindet. Benutzen Sie das sogenannte **Crib-dragging** um eine mögliche Position des Cribs im Geheimtext zu bestimmen.

• **Matching:**
Stellen Sie in folgender Tabelle den Zusammenhang zwischen Geheimtext und Crib dar:

Geheimtext												
Crib	A	T	T	A	C	K	A	T	D	A	W	N
Position	1	2	3	4	5	6	7	8	9	10	11	12

• **Menu:**
Erstellen Sie aus dem **Matching** das sogenannte **Menu**. Dies ist ein Graph, der als Ecken die Buchstaben aus Geheimtext und Crib enthält. Eine Kante zwischen zwei Buchstaben gibt es, wenn diese zwei Buchstaben im Matching verbunden sind. Die Kante wird mit der Position aus dem Matching gekennzeichnet. Beispiel:

Geheimtext	B	C	A	A
Crib	A	B	C	D
Position	1	2	3	4



• **Logical contradictions:**
Betrachte nun die drei Walzen und die Umkehrwalze als eine Einheit und sei $\boldsymbol{S_i}$ die Permutation der Buchstaben $A - Z$, die diese Einheit beim i-ten Verschlüsselungsvorgang (startend beim ersten Buchstaben des Cribs) durchführt. Weiter bezeichne $\boldsymbol{P}$ die Permutation der Buchstaben $A - Z$, die durch das Steckerbrett erzeugt wird.

Im i-ten Verschlüsselungsschritt kann die Verschlüsselung eines Buchstaben $*$ also beschrieben werden als

$$P(S_i(P(*)).$$

Nehmen Sie an, dass $S_6(G) = F$, $S_7(F) = N$, $S_8(Q) = G$ und $S_{10}(Y) = Q$ gilt. Erinnern Sie sich daran, dass das Steckerbrett, d.h. die Permutation $\boldsymbol{P}$, selbstinvers ist. Es gilt also $P(P(*)) = *$ für jeden Buchstaben $*$.

Benutzen Sie das **Menu** (insbesondere den Zykel **ATLK**) um zu zeigen, dass unter diesen Annahmen die Buchstaben A und Y kein Steckerpaar bilden können, d.h. es gilt $P(A) \neq Y$.