



Prof. Dr. Bernd E. Wolfinger/  
 Prof. Dr. em. Klaus Brunnstein/  
 Dipl.-Inform. Bastian Braun/  
 Dipl.-Inform. Andrey Kolesnikov

Übungsblatt 7  
 SS 2008  
 Abgabetermin: **Mi., 02.07.2008**

## Übung 7 zu Grundlagen der Systemsoftware (GSS)

**Aufgabe 26:** (Vigenère, 30 Punkte)

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

Beispiel: Der Klartext "HALLO" würde mit dem Schlüsselwort "GSS" zu "NSDRG".

1. Gibt es irgendwelche Einschränkungen für die Wahl des Schlüsselwortes?
2. Wenn Sie zwischen den Schlüsselworten "TOR" und "DEUTSCHLANDWIRDEEUROPAMEISTER" wählen könnten, für welches würden Sie sich entscheiden und warum?
3. Das Kryptogramm KMJWWNKCPF entstand durch die Verschlüsselung eines deutschen Satzes mit dem Vigenère-Verfahren. Was sagt Ihnen das über das verwendete Schlüsselwort?
4. (Fortsetzung von 3.) Nehmen Sie an, Sie hätten herausgefunden, dass ein Buchstabe des Schlüsselwortes E ist, dass das Schlüsselwort nur unterschiedliche Buchstaben enthält, dass im Klartext ein S an dritter und ein I an vierter Position steht sowie der zweite und fünfte Buchstabe gleich sind, und dass der fünfte und der neunte Buchstabe mit dem gleichen Schlüssel verschlüsselt wurden. Finden Sie den Klartext und das Schlüsselwort, und erklären Sie Ihren Lösungsweg! (ohne Brute-Force!)

**Aufgabe 27:** (Symmetrische Verschlüsselung, 25 Punkte)

1. Symmetrische Verschlüsselung basiert im Wesentlichen auf zwei unterschiedlichen Operationen. Erklären Sie kurz die beiden Operationen.
2. Welche Operation(en) wird/werden bei der Vigenère-Chiffre verwendet?
3. Inwiefern unterscheidet sich die Vigenère-Chiffre von der Cäsar-Chiffre?
4. Sollte die Sicherheit eines Kryptoverfahrens auf dessen Geheimhaltung basieren? Geben Sie mindestens ein Beispiel aus der Geschichte, um Ihre Antwort zu begründen.

**Aufgabe 28:** (Authentifikation, 25 Punkte)

1. Erklären Sie kurz in eigenen Worten die Unterschiede zwischen Authentifikation und Identifikation. Geben Sie je zwei Beispiele.
2. Geben Sie mindestens drei Authentifikationsgrundlagen und zugehörige Beispiele (d.h. was kann als Basis für eine Authentifikation dienen?).
3. Welche Angriffe können üblicherweise auf Authentifikationsprotokolle angewendet werden? Geben Sie je eine kurze Beschreibung.
4. Nehmen Sie an, eine Hash-Funktion werde verwendet, um Passwörter lokal auf einem PC zu speichern. Würden Sie eine "gewöhnliche Hash-Funktion" (wie md5), eine CRC oder eine MAC-Funktion bevorzugen? Erläutern Sie Ihre Antwort, indem Sie die wichtigsten Merkmale herausstellen.

**Aufgabe 29:** (Nachrichtenverschlüsselung, 20 Punkte)

Alice möchte eine lange Nachricht an Bob und Caroline schicken. Jeder der drei kennt alle öffentlichen Schlüssel  $Pub_A$ ,  $Pub_B$  und  $Pub_C$  sowie jeweils den eigenen privaten Schlüssel  $Priv_A$ ,  $Priv_B$  bzw.  $Priv_C$ . Wie kann Alice eine einzige verschlüsselte Nachricht an beide Empfänger schicken? Gibt es eine Möglichkeit, dass die gesamte Nachrichtenlänge nicht wesentlich mit der Anzahl der Empfänger steigt?