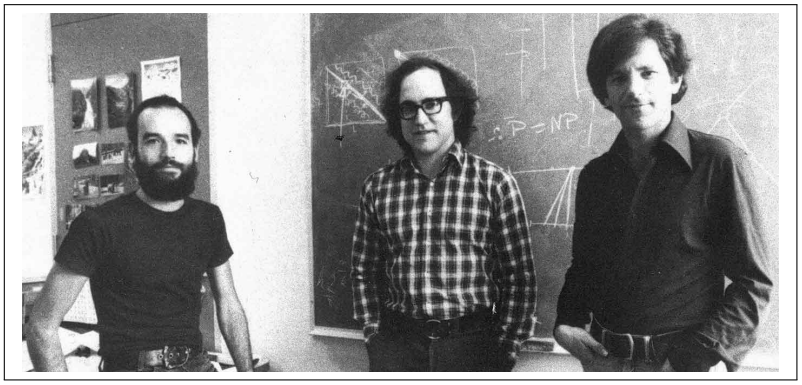
Übungsaufgaben zur Vorlesung *Panorama der Mathematik (LWB)*

Dr. Jonathan Spreer, Dr. Daniel Pitteloud

Sommersemester 2018

Blatt 12 Freitag, 1. VI. 2018



Shamir, Rivest und Adleman

Aufgabe 34 (Verschlüsselungsverfahren)

- Was ist der Unterschied zwischen Substitutions- und Transpositionschiffren?
- Was ist der Unterschied zwischen monoalphabetischen und polyalphabetischen Chiffren? Warum sind Letztere schwerer zu entschlüsseln?
- Beschreiben Sie den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren.

Aufgabe 35 (Cäsar-Verschlüsselung)

Entschlüsseln sie folgenden Text, der mithilfe der Cäsar-Verschlüsselung verschlüsselt wurde:

```
Tnam Tnyyvra vfg iba qra Eözrea orfrgmg...
 Tnam Tnyyvra? Arva! Rva iba haorhtfnzra
Tnyyvrea oriöyxregrf Qbes uöeg avpug nhs,
 qrz Rvaqevatyvat Jvqrefgnaq mh yrvfgra.
```

Aufgabe 36 (Faktorisieren ist schwerer als Multiplizieren)

Lösen Sie folgenden Aufgaben ohne Taschenrechner und stoppen Sie, wieviel Zeit sie jeweils benötigen:

- Multplizieren Sie 31 mit 67.
- Finden Sie einen Faktor von 1961 oder zeigen Sie, dass 1961 prim ist.

Diskutieren Sie das Ergebnis.

Zusatzaufgabe (Vigenère Chiffre)

Entschlüsseln Sie folgende Botschaft, die mit der Vigenère Chiffre und mit Schlüssel `klausur` verschlüsselt wurde.

```
ntem wulp ravw qzbo ncub ksyd yjec kfso jvvr lnxw fkgp rxwh
```

Klartext / Schlüssel	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

Das “Vigenère-Quadrat” zur Ver- und Entschlüsselung mittels der Vigenère Chiffre.