Institut für Angewandte und Numerische Mathematik
Sommersemester 2019
Dr. Daniel Weiß

Schnupperkurs Mathematik 2019
Verschlüsselung - Von Caesar bis zum TXDQWHQFRPSXWHU
Übungsblatt 2

Aufgabe 1 (Kasiski- und Friedman-Test) (3+3+2 Punkte)
Wir betrachten den folgenden Geheimtext mit $N = 368$ Zeichen, der durch die polyalphabetische Methode von Vigenère verschlüsselt wurde (siehe [1]).

EYRYC FWLJH FHSIU BHMJO UCSEG
TNEER FLJLV SXMVY SSTKC MIKZS
JHZVB FXMXK PMMVW OZSIA FCRVF
TNERH MCGYS OVYVF PNEVH JAOVW
UUYJU FOISH XOVUS FMKRP TWLCI

FMWVZ TYOIS UUIIS ECIZV SVYVF
PCQUC HYRGO MUWKV BNXVB VHHWI
FLMYF FNEVH JAOVW ULYER AYLER
VEEKS OCQDC OUXSS LUQVB FMALF
EYHRT VYVXS TIVXH EUWJG JYARS

ILIER JBVVF BLFVW UHMTV UAIJH
PYVKK VLHVB TCIUI SZXVB JBVVP
VYVFG BVIIO VWLEW DBXMS SFEJG
FHFVJ PLWZS FCRVU FMXVZ MNIRI
GAESS HYPFS TNLRH UYR

(a) Berechne zunächst den zugehörigen Koinzidenzindex I, um die Vigenère-Verschlüsselung zu bestätigen. Nutze dazu die Tabelle 1.

(b) Führe den Kasiski-Test durch, um die Länge des Schlüsselwortes einschätzen zu können.

Hinweis: Hilfreich sind hier die Zeichenfolgen **TNE**, **FCRV**, **NEVHJAOVWU** und **VWU**.

(c) Führe den Friedman-Test durch, um die Länge des Schlüsselwortes einschätzen zu können.

A	B	C	D	E	F	G	H	I	J	K	L	M
8	12	13	0	18	25	7	19	20	14	8	15	16

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	12	8	3	15	25	10	19	41	13	11	19	8

Tabelle 1: Anzahl der einzelnen Buchstaben im Geheimtext oben.

Aufgabe 2 (ADFGVX-Verschlüsselung) (5+3 Punkte)
Der ADFGVX-Verschlüsselungsalgorithmus ist eine zweistufige Verschlüsselung, bei dem neben einer monoalphabetischen Substitution eine Transposition durchgeführt wird. Dabei wird im ersten Schritt das Klartextalphabet $\{a, b, \ldots, y, z, 0, 1, \ldots, 9\}$ durch das Geheimtextalphabet substituiert, welches aus Paaren der Buchstaben A,D,F,G,V und X besteht, z. B. AA, AX, VX. Insgesamt stehen also $6 \cdot 6 = 36$ Geheimtextbuchstaben für die $26 + 10 = 36$ Klartextbuchstaben zur Verfügung. Ein Schlüssel ist zum Beispiel durch folgende Tabelle gegeben

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

wobei zum Beispiel die Zahl 8 durch AA und g durch GV ersetzt wird.

In einem zweiten Schritt wird der durch die Substitution entstandene Text spaltenweise unter ein Schlüsselwort geschrieben und die Spalten entsprechend der alphabetischen Anordnung des Schlüsselwortes vertauscht. Wir wählen z. B. das Schlüsselwort „KRYPTO“ und verschlüsseln im zweiten Schritt den (völlig willkürlich gewählten) Text AFDVXDDGVXDFAGXVFDGVXADF

K	**R**	**Y**	**P**	**T**	**O**
A	F	D	V	X	D
D	G	V	X	D	F
A	G	X	V	F	D
G	V	X	A	D	F

K	**O**	**P**	**R**	**T**	**Y**
A	D	V	F	X	D
D	F	X	G	D	V
A	D	V	G	F	X
G	F	A	V	D	X

und erhalten als Geheimtext ADVFXDDFXGDVADVGFXGFAVDX.

(a) Verschlüssele den Klartext *verschluesselnmachtspass* durch das ADFGVX-Verschlüsselungsverfahren mit den oben beschriebenen Schlüsseln.

(b) Diskutiere dieses Verschlüsselungsverfahren anhand des Kerckhoffsschen-Prinzips, welches aussagt, dass die Sicherheit eines Verschlüsselungsverfahrens nicht von der Geheimhaltung des Algorithmus abhängen darf.

Hinweis: Die Deutschen setzten dieses Verschlüsselungsverfahren im 1. Weltkrieg ein. Die Buchstaben A,D,F,G,V und X wurden gewählt, da sich ihre Morsecodes stark voneinander unterscheiden. Der Franzose Georges Painvin knackte noch vor einer deutschen Offensive die Verschlüsselung.

Aufgabe 3 (Vigenère-Verschlüsselung) (4 Punkte)

Verschlüssele den Klartext *verschluesselnmachtspass* durch die Methode von Vigenère mit Schlüsselwort KRYPTO, indem du sowohl den Klartext als auch das Schlüsselwort durch Zahlen repräsentierst (a mit 0, b mit 1 usw.) und bei der Verschlüsselung modulo 26 rechnest. Der Klartext lautet

21 4 17 18 2 7 11 20 4 18 18 4 11 13 12 0 2 7 19 18 15 0 18 18

und das Schlüsselwort lautet 10 17 24 15 19 14.

Literatur

[1] A. Beutelspacher: Kryptologie, Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, Springer Spektrum, Wiesbaden, 2015[10].

Beachte: Wir besprechen die Aufgaben in der nächsten Vorlesung.
Infos: http://www.math.kit.edu/ianm3/~dweiss/seite/schnuppernmathe2019/