Kryptografie und -analyse, Übung 2

Henry Haustein

Aufgabe 1: Analyse historischer Verfahren

Zuordnung zu den Histogrammen:

- Histogramm 1: PM-Substitution (Buchstabenverteilung ist relativ gleichverteilt)
- Histogramm 2: Transposition (Buchstabenverteilung ist genau so wie im Deutschen)
- Histogramm 3: MM-Substitution (J = e, S = n), Verschiebechiffre mit Verschiebung 5
- Histogramm 4: MM-Substitution (W = e, O = n)

Aufgabe 2: Permutation

Die Matrix ist

$$\begin{pmatrix} A & F & F & I & N & E \\ C & H & I & F & F & R \\ E & N & S & I & N & D \\ E & B & E & N & F & A \\ L & L & S & M & M & S \\ U & B & S & T & I & T \\ U & T & I & O & N & E \\ N & X & Y & Z & X & Z \end{pmatrix}$$

Affine Chiffren sind ebenfalls MM-Substitutionen.

Aufgabe 3: Verschiebechiffre

Durchprobieren aller Schlüssel führt zu einer Verschiebung von 7: *Einfache Substitutionen erhalten die Zeichenhaeufigkeiten.*

Aufgabe 4: MM-Substitution

Nahezu jedes Tool im Internet (z.B. dieses hier https://www.guballa.de/substitution-solver) kann das automatisch brechen

Klartext	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
Ciphertext	q	g	t	k	x	j	u	c	w	n	s	r	y	v	h	e	i	z	b	f	o	d	l	a	p	m

liefert *Auch laengere Texte koennen durchaus von den charakteristischen Eigenschaften der verwendeten Sprache abweichen, allerdings ist es im Allgemeinen nicht moeglich jede charakteristische Eigenschaft einer Sprache zu vermeiden und sich dennoch in dieser Sprache auszudruecken.*

Aufgabe 5: Vernam-Chiffre

(a) Der Schlüsseltext lautet

Klartext	0	1	0	0	1	1	1	0	1	0	1	0
Schlüssel $\oplus$	1	0	1	0	1	1	0	0	1	1	0	0
Schlüsseltext	1	1	1	0	0	0	1	0	0	1	1	0

(b) Ja kann er. Er muss einfach das letzte Bit des Schlüsseltextes verändern.

(c) Nein. Der Angreifer kann den Schlüssel berechnen, aber dieser wird ja nicht noch mal verwendet.

(d) Schlüsseltext

Klartext	G	E	H	E	I	M	E	S	T	R	E	F	F	E	N
Schlüssel	N	W	Y	P	R	C	I	K	S	E	N	F	O	L	Q
Schlüsseltext	T	A	F	T	Z	O	M	C	L	V	R	K	T	P	D
Schlüssel 2	G	A	D	M	I	G	K	V	S	V	E	K	I	E	Z
Klartext 2	N	A	C	H	R	I	C	H	T	A	N	A	L	L	E