Datensicherheit, Übung 6

Henry Haustein

Aufgabe 1

$c = m \oplus k = 111000100110$

Aufgabe 2

Ja, der Angreifer ändert einfach das letzte Bit von c.

Aufgabe 3

Weil sie das einzige informationstheoretisch perfekte Verfahren ist. Ein Schlüsseltext kann zu jedem Klartext entschlüsselt werden, wenn der Schlüssel unbekannt ist.

Aufgabe 4

Da jeder Schlüssel nur einmal verwendet wird, kann mit der Herausgabe eines Schlüssels nur eine Nachricht entschlüsselt werden.

Aufgabe 5

Nein, gibt es nicht. Asymmetrische Signaturen können von Computern geknackt werden (dauert lange), allerdings haben symmetrische Signatursysteme das Problem, dass diese nur sicher sind, wenn diese nur einmal verwendet werden. Man müsste also jede Nachricht mit einem anderen Schlüssel unterschreiben. Das ist nicht praktikabel.

Aufgabe 6

$$\begin{pmatrix} H & O & M & O & P & H & O \\ N & E & V & E & R & S & C \\ H & L & U & E & S & S & E \\ L & U & N & G & E & R & S \\ C & H & W & E & R & T & S \\ T & A & T & I & S & T & I \\ S & C & H & E & A & N & A \\ L & Y & S & E & N & X & Y \end{pmatrix}$$

Homophone Verschlüsselung erschwert statistische Analysen.

Aufgabe 7

Mit diversen online Tools findet man recht schnell die Verschiebung von 9. Dann ist der Klartext *Affine Chiffren sind ein weiteres Beispiel für einfache Substitutionen.*

Aufgabe 8

m_1	0	0	1	1	0	1	0	1	0	1	1	1
k_1	1	0	0	1	1	1	0	0	1	1	0	0
c	1	0	1	0	1	0	0	1	1	0	1	1
k_2	0	0	1	1	0	1	0	0	1	1	0	1
m_2	1	0	0	1	1	1	0	1	0	1	1	0

Aufgabe 9

Histogramm der Buchstabenverteilung von der Zielsprache und des Schlüsseltextes. Dann gibt es 3 Möglichkeiten:

- Häufigkeiten der Buchstaben stimmen komplett überein → Transposition
- Häufigkeiten sind die selben, aber für verschiedene Buchstaben → MM-Substitution
- sonst → PM-Substitution

Aufgabe 10

Z.B. diese Seite hier https://www.dcode.fr/monoalphabetic-substitution löst das fast vollautomatisch.

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

ergibt: *Auch längere Texte können durchaus von den charakteristischen Eigenschaften der verwendeten Sprache abweichen, allerdings ist es im Allgemeinen nicht möglich, jede charakteristische Eigenschaft einer Sprache zu vermeiden und sich dennoch in dieser Sprache auszudrücken.*