

Security
SoSe 23
LV 4120, 7240
Übungsblatt 5

Aufgabe 5.1 (Angreifermodelle und Kerckhoffs Prinzip):

- a) Nennen Sie die vier gängigsten Angreifermodelle im Kontext von kryptoanalytischen Angriffen. Beschreiben Sie kurz die Modelle.
- b) Erläutern Sie das Kerckhoffs Prinzip.
- c) Welches Kriterium muss eine Chiffre erfüllen, damit es nach dem Prinzip von Kerckhoff erfüllt sein muss im Bezug auf Angreifermodelle.

Aufgabe 5.2 (Monoalphabetische und Polyalphabetische Substitution):

- a) Wieviele mögliche Schlüssel gibt es für eine monoalphabetische Substitution?
- b) Schreiben Sie ein Programm in einer beliebigen Programmiersprache zum Ver- und Entschlüsseln einer beliebigen Zeichenkette mit einer Vigenère-Chiffre.

Aufgabe 5.3 (Algebra):

Welche der folgenden Mengen sind Gruppen? Begründen Sie Ihre Aussage:

- a) $\langle \mathbb{Z}, - \rangle$ ist eine Gruppe
- b) $\langle \mathbb{N}, + \rangle$ ist keine Gruppe. Operationen sind zwar assoziativ aber nicht umkehrbar. Bsp: $2 + x = 1$ (unlösbar)
- c) $\langle \mathbb{N}_0, + \rangle$ siehe b)
- d) $\langle \mathbb{Z}, + \rangle$ ist eine Gruppe

Eine nichtleere Menge G von Elementen a, b, c, \dots heißt Gruppe, wenn in ihr eine Operation \circ erklärt ist, die folgenden Axiomen genügt:

1. Die Operation \circ ist assoziativ, d.h. für alle Elemente $a, b, c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$.
2. Die Operation \circ ist umkehrbar, d.h. zu beliebigen Elementen $a, b \in G$ sind die Gleichungen $a \circ x = b$ und $y \circ a = b$ (mit $x \in G$ und $y \in G$) lösbar.

Man nennt G eine abelsche Gruppe, wenn zusätzlich noch gilt:

3. Die Operation \circ ist kommutativ, d.h. für alle $a, b \in G$ gilt $a \circ b = b \circ a$.

Aufgabe 5.4 (Inverse Elemente eines Körpers):

Berechnen Sie die Inversen Elemente mit Hilfe des erweiterten euklidische Algorithmus. **Tipp:** Lesen Sie sich hierzu Kapitel 6.3.2 Der erweiterte euklidische Algorithmus in *Christoph Paar, Jan Pelz: Kryptografie verständlich, 2016, Springer* durch.

a) Berechnen Sie $a = 7^{-1} \mod 29$.

b) Berechnen Sie $a = 23^{-1} \mod 29$.

c) Berechnen Sie $a = 7^{-3} \mod 29$.

Aufgabe 5.5 (Hill-Chiffre):

Ein affine Hill-Chiffre möge für die Schlüsselmatrix K die Blocklänge 2 sowie für die Berechnung den Modulus $n = 26$ verwenden:

$$c = (K \cdot p) \mod n$$

Darin bezeichnet der Vektor p den Klartext und der Vektor c den Ciphertext. Die folgende Botschaft:

UHUSQHKX

sei mit einem Hill-Kryptosystem und der Schlüsselmatrix K

$$K = \begin{pmatrix} -8 & -9 \\ -9 & -8 \end{pmatrix}$$

verschlüsselt. Die Zeichencodierung erfolge anhand nachstehender Codierungstabelle:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

a) Wie lautet die zugehörige Entschlüsselungsfunktion $D : c \rightarrow p$?

b) An welche Bedingung ist die Entschlüsselungsvorschrift D geknüpft und warum?

c) Wie lautet der Klartext?