Übungsaufgaben zur Vorlesung Kryptologie

Helmut-Schmidt-Universität — Universität der Bundeswehr Hamburg
Professur für Allgemeine Nachrichtentechnik — Prof. Dr.-Ing. Udo Zölzer
Dr.-Ing. Martin Holters, Raum: H3 - R115, Tel.: 040 / 6541 - 3468

M.Sc. Patrick Nowak, Raum: H3 - R116, Tel.: 040 / 6541 - 3650

Übungsaufgaben zu Kap. 3, Kap. 4, Kap. 5, Kap. 6 und Kap. 7

Aufgabe 1 — Angriff mit der Turing-Bombe

Es sei eine mit einer Wehrmachts-Enigma verschlüsselte Nachricht aufgefangen worden, die mit

`HUPTV TYXUP AOVJO ...`

beginnt. Wir vermuten, der zugehörige Klartext beginnt mit `angeneraloberst`. Wie ist die Turing-Bombe zu verschalten, um die möglichen Konfigurationen zu ermitteln?

Aufgabe 2 — Inversion in $\mathbb{Z}_{13}$

Bestimmen Sie für alle Zahlen $x = 1, \ldots, 12$ das Inverse in $\mathbb{Z}_{13}$.

Aufgabe 3 — Rekonstruktion eines linearen Schieberegisters

Wir vermuten (auf Basis eines Angriffs mittels wahrscheinlichen Wortes), dass ein lineares Schieberegister die folgende Ausgabe geliefert hat (Berechnungen in $\mathbb{Z}_{26}$):

n	1	2	3	4	5	6	7
$c(n)$	7	6	21	20	15	0	23

Rekonstruieren Sie das Schieberegister minimaler Länge, das diese Ausgabe produziert haben könnte.

Aufgabe 4 — Drehraster

Wie viele verschiedene Drehraster der Größe $n \times n$ (n gerade) gibt es?

Aufgabe 5 — Komposition von Chiffrierverfahren

Beurteilen Sie folgende Kompositionen von Chiffrierverfahren hinsichtlich der Sicherheit:

a) Hintereinanderausführung zweier VIGENÈRE-Verfahren, wobei die Schlüssellänge des ersten $d_1 = 8$, die des zweiten

(I) $d_2 = 6$

(II) $d_2 = 7$

(III) $d_2 = 8$

beträgt.

b) Hintereinanderausführung zweier gemischter Zeilen-Block-Transpositionen der gleichen Länge.

c) Hintereinanderausführung einer Block-Transposition und einer VIGENÈRE-Verschlüsselung mit

(I) gleicher Perioden- und Blocklänge

(II) unterschiedlicher Perioden- und Blocklänge.