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. 2: Monographische, monoalphabetische Substitution

---

Aufgabe 1 — CAESAR-Verschlüsselung

a) Verwenden Sie eine CAESAR-Verschlüsselung mit $t = 8$, um folgenden Text zu verschlüsseln:
`einku rzert ext`

b) Für welchen Wert von t erreicht man eine Entschlüsselung des so gewonnenen Chiffrats?

c) Entschlüsseln Sie die mit $t = 8$ nach dem CAESAR-Verfahren verschlüsselte Nachricht
`ZQKPB QOOMU IKPB`

Aufgabe 2 — Chi-Analyse

Es sei der Geheimtext
`ADCCD CDCED CEDDC CECAC`
über dem Geheimtextalphabet $W = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}\}$ abgefangen worden. Es sei bekannt, dass dieser durch lineare Substitution entstanden ist und der Klartext die folgenden Auftrittswahrscheinlichkeiten aufweist:

x	a	b	c	d	e
$p(x)$	0,5	0,25	0,125	0,0625	0,0625

Bestimmen Sie die wahrscheinlichste Verschiebung t mittels der Chi-Analyse!

Aufgabe 3 — Zyklenschreibweise

a) Geben Sie die Substitutionsvorschrift der CAESAR-Verschlüsselung mit $t = 1, 2, 3, 4$ in Zyklenschreibweise an.

b) Welcher Zusammenhang besteht zwischen t und den sich ergebenden Zyklenlängen?

Aufgabe 4

Entschlüsseln Sie die geheime Nachricht

`GNTFU LVVLW AFQEW IHQFL DGTFF ACFBF QONQB FOFLB FQFNA OFLVM AHFA`

unter der Annahme, dass ein echt involutorisches Substitutionsverfahren zur Anwendung gekommen ist und der Klartext das Wort `mission` enthält.