

1. Übungsblatt Kryptographie (SS 2006)

Stefan Lucks, Emin Islam Tatli

Besprechung: Mittwoch, 03. Mai 2006

BEMERKUNG: Dieses Blatt enthält nur drei Aufgaben, da in der Übung am 3. 5. auch die restlichen Aufgaben des 0. Übungsblattes besprochen werden.

Aufgaben

Aufgabe 1 Implementiere ein einfaches Programm, das als Eingabe ein Zeitlimit erwartet und als Ausgabe angibt, wie viele Schleifendurchläufe einer leeren Schleife das Programm innerhalb des Zeitlimits geschafft hat.

- Wie viele Durchläufe schafft dein Programm innerhalb von 10 Minuten?
- Rechne hoch, wie viele Durchläufe dein Programm innerhalb von 1 Stunde, 1 Tag, 1 Woche, 1 Monat und 1 Jahr schaffen würde.
- Unter einem "Brute-Force"-Angriff auf eine Chiffre versteht man das vollständige Ausprobieren aller denkbaren Schlüssel. Wenn man annimmt, dass dein Programm in jedem Schleifendurchlauf einen Schlüssel getestet hätte, welche maximale Schlüssellänge kann dein Rechner dann innerhalb von 1 Stunde, 1 Tag usw. durch einen Brute-Force-Angriff knacken?
- Wie lange bräuchte dein Programm unter der Annahme aus Teil c), um eine Chiffre mit Schlüssellänge 40, 64 bzw. 128 Bit zu knacken?

Aufgabe 2 Die folgenden beiden Kryptogramme sind mit einer Substitutionschiffre chiffriert worden; für beide wurde der gleichen Schlüssel verwendet.

Erstes Kryptogramm:

UAINR UDDCE CNTDD QLLRD PRFRE YRCFT DDUAI DQTZG TRYDR LCPUC RUCRA
IUXXG RTEDE GTLYR CVRUY RCFUR ORIYZ UGCUA IYTED FRZDU CC

Zweites Kryptogramm:

BLEOR LREYR OLTEP RCVEZ TAIRC ZTCDR UNTDZ TCCUA IYUDY UDYUC FRCZR
UDYRC XTRLL RCD AI NRGRG TLDNU GBLUA IVENR GFRCN TDZTC DAIRU CRCNU
LL

- Ermittle (z.B. durch Zählen oder mit einem kleinen Computerprogramm) die relativen Häufigkeiten der einzelnen Buchstaben in diesen Kryptogrammen. Welches ist der häufigste, welches der zweit- bzw. dritthäufigste Buchstabe?

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

Tabelle 1: Relative Buchstabenhäufigkeiten in der deutschen Sprache (Quelle: Beutelspacher, Kryptologie, S. 18)

- b) Entschlüssele die beiden Kryptogramme. Als Hinweis sei verraten, dass eines von ihnen mit dem Klartext-Fragment "ich" beginnt.
- c) Schreibe ein Programm, das alle Buchstaben außer den ersten acht im Deutschen am häufigsten benutzten Buchstaben (a, d, e, i, n, r, s, t) in dem Satz "Warum kann ich diesen Text lesen" mit * ersetzt. Was fällt dir auf?

Aufgabe 3 *Cryptool* ist ein eLearning-Programm für Kryptologie. Lade das Tool von <http://www.cryptool.de/download.de.html> (für Windows und mit wine auch für Linux) herunter, installiere es und mache dich mit seinen Eigenschaften und Funktionalitäten vertraut. Versuche, die Kryptogramme aus Aufgabe 2 mit diesem Tool zu entschlüsseln.