

26. Oktober 2004

1. Übungsblatt Kryptologie

Aufgabe 1: (15 Punkte)

In jedem der folgenden vier Kryptogramme wurde deutscher Klartext auf der Basis von 26 Buchstaben mit einem der folgenden Verfahren verschlüsselt:

- CAESAR-Chiffre
- VIGENÈRE-Chiffre
- Allgemeine monoalphabetische Substitution
- Permutationschiffre mit einer Blocklänge zwischen fünf und zehn

Entscheiden Sie zunächst auf Grund der Häufigkeitsdiagramme, welche der vier Methoden in Frage kommt, und entschlüsseln Sie dann das Kryptogramm!

- a) CSHSI EUNUE EERRQ VNGDB EUINW HINES ZCUTE NELQL UHNXI DTCRX EFTTF ESLSD TOALI
TEESE DNLSUC EEHSN RGLEV UEFEA INCNH
- b) VRVFK ULHEV FKRQF DHVDU DQFLF HURXP VHLQH SODHQ HYRUD VWHUL AXQGR EHOLA CXYHU
KHLPO LFKHQ
- c) QQBUG EPKWZ KLUVZ EZSVS RRQKS RAKLP AOMGL YKPQZ KKSLU OQTQR PZVWZ EZSVS RRQKK
KSLUO QTQRU BUPQT OQCVQ GQKVD UZLNP KBGLP WDIYZ DRAHY CTNDP UVJAZ OLRHQ YVOOR
PJKPZ KBRLP QLTYC DPUVN PCKDJ OVEY QKPLG MMONT TTHYA IRKBL VDMRX HZAGP ZHORA
LDWOU BHAOP FASKB OAOZA
- d) KHTCD HKGCG EBAQQ ANHUF CHBQG AMABK ADPDY FCEMD HFNGA GTCKG AVADT JNQUA TTAQQ
UBMVE BBHJN DGJNC ABTEK HTTKG ATUA IADUB TGJNA DAQAG CUBMA BFADL UBPEK ADMHD
KUDJN KHTGB CADBA CVEBA GBART ABKAD ZUAGB ARARF LHABM ADMAT JNGJP CWADK ABPEA
BBABE NBAKH TTAGB QHUTJ NADRG CKADV ADTJN UAUTT AQCAB BHJND GJNCA CWHTH BLHBM
ABPHB BKHZU MANEA DCGBT IATEB KADAK HTTAD KGABH JNDGJ NCWAK ADQAT ABBEJ NUBIA
RADPC VADLH AQTJN ABPHB B

Aufgabe 2: (5 Punkte)

Wählen Sie einen deutschen Klartext von mindestens 30 000 Buchstaben und berechnen Sie die Zahlen für den FRIEDMANNschen κ -Test bezüglich der folgenden Alphabete:

- Nur 26 Buchstaben
- 26 Buchstaben und Leerzeichen
- Groß- und Kleinbuchstaben, Umlaute, Satzzeichen, Leerzeichen
- ASCII-Zeichen

Interpretieren Sie das Ergebnis in Hinblick auf die Abhängigkeit der Sicherheit des VIGENÈRE-Verfahrens vom Alphabet!