Wolfgang K. Seiler
Tel. 2515

A5, C201

11. September 2007

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) AQGNE EULLL EMTXE CAEHT UASND LSBEN NCELI THBAE RZUKR QEEUE LTETX MECAL ESUNN ADLSH BCNES WHREE

b) XTAJW XHMQZ JXXJQ SMJZY JSZWS THMRF KNFGT XXJNM WJSFH MWNHM YJS

c) XYODE FFHUP DNNXG FUNDU GYMVC TVDIZ WRNEY HPHNE UIHUG EAMTU BDSCZ DQZUG WYBFD NTSCP HPYTJ SDZDS CHYZC YBVUD EUIDS CYUGW UIEIX SBPPI NPBWL H

d) KHTCD HKGCG EBAQQ ANHUF CHBQG AMABK ADPDY FCEMD HFNGA GTCKG AVADT JNQUA TTAQQ UBMVE BBHJN DGJNC ABTEK HTTKG ATAUA 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

(Die Kryptogramme sind auch auf der home page der Vorlesung zu finden; falls sie zur Lösung einen Computer benutzen, müssen sie sie also nicht abtippen.)

Aufgabe 2: (*5 Punkte)*

Der Aufwand für die Faktorisierung einer n-stelligen Zahl mit dem Zahlkörpersieb liegt bei ungefähr $e^{1,6n^{1/3}\ln(n)^{2/3}}$.

a) Angenommen, es gäbe ein Verfahren, das eine n-stellige Zahl mit Aufwand n^m für eine feste Zahl m faktorisieren kann. Wie groß dürfte m höchstens sein, damit dieses Verfahren für 150-stellige Zahlen schneller wäre als das Zahlkörpersieb?

b) Wie groß dürfte m höchstens sein, damit der Aufwand mit diesem Verfahren langsamer wächst als beim Zahlkörpersieb, wenn man die Stellenzahl 150 leicht erhöht?

Abgabe bis zum Dienstag, dem 18. September 2007, um 12.00 Uhr