Rätselserie 2

1) Gegeben sei ein Text, der mit einer Vigenère-Chiffre verschlüsselt wurde. Das Schlüsselwort ist unbekannt. Der Text ist eine bekannte Ballade von Johann Wolfgang von Goethe aus dem Jahr 1797.
   Die Leerzeichen im Text wurden entfernt und das Spacing im Kryptogramm hat nichts mit der Länge des Schlüsselworts zu tun. Diese Schlüssellänge ist aber mit dem in der Vorlesung beschriebenen Kasiski-Test zu ermitteln.
   Bei der Analyse geht bitte folgendermaßen vor:
   - Ermittelt die häufigsten Trigramme (3 Buchstaben). Wie viele ihr ermittelt, ist mir egal. Je mehr, umso besser! Ihr habt gesehen, dass es Ausreißer gibt. Längere Ketten sind besser, weil die Wahrscheinlichkeit, dass es sich um echte Kandidaten handelt, höher ist. Nutzt gegebenenfalls die n-Gramm-suche auf dem Kryptospielplatz
   - Ermittelt die Positionen der Trigramme und notiert sie euch.
   - Bildet die Differenzen zwischen den Trigrammpositionen und notiert sie euch.
   - Macht eine Zerlegung der Differenzen in ganzzahlige Teiler (hierfür schreibt ihr euch evtl. ein kleines Prográmmchen)
   - Entscheidet die Passwortlänge! Prüft euer Ergebnis mit geeigneten, in der Vorlesung gezeigten Mitteln. (z.B. Koinzidenzindex)
   - Wenn ihr es schafft, gebt das Schlüsselwort an. Wählt dazu ein geeignetes Verfahren.

```
GANEI ILPAV SMKKM MYJWK PVZZN PQUBH YJRDL PDVRJ RMDBY OYEOR BEDWY RDNMF
MEPKL ZDBRX ZUWIR RNLTV TVRSV IFMIE WIIVY AROME QPVKL YUUHM EQDMY SOKLM
JYFVQ JDNVS ELNLB EOUVZ FECTX VDWAR PZXKS UUJGY HYUUP ZNABH QBPCP AHCWM
ZGMCB FWKCI JBPLN YRZON DNPGR VHIFY DRZMM VDWLL YLZOS RYJGY PQCFW TRSRC
BXECW IGLOM ZHZDY TMTSI YXTMF YDUHE RLYOV DXLHG KTYSF VDIUE TUZJH EMDLC
PGOKP VYALP YOLLP PSVYJ VYSSW ISEWE UXPSA KBHNH INPWL EYCAK QFOFP CPQLZ
YMACH LFFRR FJGNP QOKHN YOWKP LLFMM AYDIY JRBZT MVTTR TTNOO HXPLL DTBQK
LWUTW VCXVG QENRK EQBPC PQHEN PRYSR YDOVO EZJKC ZFVEW LINLW ZVCNY ODSMF
YEOQP KCMVI GEGWS CWITJ NPJGK LYAYU PQIRO MFOBH YSKZP WZVDM UZDRF BILQX
GLXCS KQNCF HVCAH YCTVI GIMUW TSSUR YLRSE LOTWV FRKDT BORHT TFWJN LUVWT
RCHEX FVZDX LISQR XLINS EJNLL DRCFY DSWIS EKYTQ HMVZD NGBPV HMLUL AOKBK
YOWTS APCWB JODSC DLAPH LJNPN RDVIM PDTXD RDARX EUYMP KDXLY PAGKG EXFRE
HMYYL JRTCE COIIR EIVYD BRKGY NIJDI URNPV IGMYS ORPWD VSMJK GEBBF RTGOU
ZKUJZ SQPVK GIYXP AFKMA WIHRD AVIEE BXZUZ BQVYH LVCLN YVILE ARDIY XPERY
DNUDL VCPHV FNGAM DVSME RXIVS MAJDW UFVJE HBUZK UJDRU MXVMI ZVYQZ SDRHF
YVRYL JDMOX HNAUI IDGOE PTYND RYJRR NLBEO PHTCE LUJCF IZJPA GADRT FRRFJ
TZNPR OMNYJ RETGO KWIRT FELLE EYMJY LAYGR SYOAZ WPPYY NNYRE HEEJT WAKFM
PQDAW IRLYA PIOUV XHMGF VSLIU XPZJK KCBFQ ZPRLN PTPND BFJGB PSKLL CFMDB
OSXUP VOFPT YKZSI MPULW NRYHR NZUMF VJLYM VYARN ZIWIY VMIYA PLRYB HQFPC
PHVTS APNNN QBWJP VZKCW RSDLU VJVYI PEGME XTCBU IIMIZ VYLRX MIWIX YZIYV
YEVRK SNPGB OIYUF ORCDS YOWKP LKFNP JODDY SWKTP SNTTY YSAMB QVYHL XLZAO
BHNME JDIUN TTYJH CBGEJ DIUNT TYJHC BIECE IULYL QGRAF UIYZP GSPPR TCEGJ
XUPQZ TSIEL DNVFM CPWWR WBRTR EBUHR VSTDE MEYBH FFTGP RKNTM QKQWC FMTSQ
PTSVH TZUZE MTSAL IQMTR DIWIS BZFVC OTVKF SNEYE TIKVC SEGBH YOHKC MMWEL
VKFLU UXVDG ORPZS KVABS PZNLI ILDTK SRIGJ VYWLY ELRXH SNFRK KALZF VQTTN
EBRET GOYZN SKMUH EMTSE ADPNE KHWYI INPLL SPQQK SECMI JEIOE TVROK EMDLF
YESJV VRIGT YWSVW PPXQM EZHGC OHZPL VVSMU KKFNN MILGO ZSZUU GEHNE VNLAV
FVQYH EFBYW PRURD AHTCN UFWJP VDZCL NYHMM BECFR KRFNQ KMSNV JVYAL CNPRT
SSYUD CTGOV DORCZ EMTII SIYIF VQSDI MUIIS SLILU VIGRO GIELG OULSB SLTXF
VDPMZ KPZUK QRXJI EZXPJ EOEUR SXJIZ NLYZP NQODG YJWKP VDVCL NOBHH VRETG
OKWWF GHNXJ IVNOL SPART AEMFR JPMKR DORCD SYOHV YRHCD ORORT YSVLQ XLLNP
AAQZO TIZYI TQHMP QDELT XYPVC FCLRX ZLNFQ VTWAV CI
```

2) Gegeben sei die Ballade „Der Handschuh“ von Friedrich Schiller (1797).
In der Vorlesung haben wir den Koinzidenzindex(KI) von William F. Friedman kennen gelernt

$$I = \frac{\sum(n_i * (n_i - 1)}{n * (n - 1)} \quad i = 1..26$$

Wir haben gelernt, dass der KI für deutsche Texte etwa bei 0,0762 liegen soll. Beweist mir, dass Schiller den Handschuh in Deutsch geschrieben hat. Wenn es Abweichungen gibt, warum?
Bei der Analyse sind folgende Konventionen zulässig Ä, Ö, Ü, ß dürfen durch AE, OE, UE, SS ersetzt werden. Alle anderen Zeichen außer A-Z werden weggelassen und Groß-Klein-Schreibung wird ignoriert.

Der Handschuh

Vor seinem Löwengarten,
Das Kampfspiel zu erwarten,
Saß König Franz,
Und um ihn die Großen der Krone,
Und rings auf hohem Balkone
Die Damen in schönem Kranz.

Und wie er winkt mit dem Finger,
Auf tut sich der weite Zwinger,
Und hinein mit bedächtigem Schritt
Ein Löwe tritt
Und sieht sich stumm
Rings um,
Mit langem Gähnen,
Und schüttelt die Mähnen
Und streckt die Glieder
Und legt sich nieder.

Und der König winkt wieder,
Da öffnet sich behend
Ein zweites Tor,
Daraus rennt
Mit wildem Sprunge
Ein Tiger hervor.

Wie der den Löwen erschaut,
Brüllt er laut,
Schlägt mit dem Schweif
Einen furchtbaren Reif,
Und recket die Zunge,
Und im Kreise scheu
Umgeht er den Leu
Grimmig schnurrend,
Drauf streckt er sich murrend
Zur Seite nieder.

Und der König winkt wieder;
Da speit das doppelt geöffnete Haus
Zwei Leoparden auf einmal aus,
Die stürzen mit mutiger Kampfbegier
Auf das Tigertier;
Das packt sie mit seinen grimmigen Tatzen,
Und der Leu mit Gebrüll
Richtet sich auf - da wird's still;
Und herum im Kreis,
Von Mordsucht heiß,
Lagern sich die greulichen Katzen.

Da fällt von des Altans Rand
Ein Handschuh von schöner Hand
Zwischen den Tiger und den Leun
Mitten hinein.

Und zu Ritter Delorges spottender Weis',
Wendet sich Fräulein Kunigund:
"Herr Ritter, ist Eure Lieb' so heiß,
Wie Ihr mir's schwört zu jeder Stund,
Ei, so hebt mir den Handschuh auf."

Und der Ritter in schnellem Lauf
Steigt hinab in den furchtbarn Zwinger
Mit festem Schritte,
Und aus der Ungeheuer Mitte
Nimmt er den Handschuh mit keckem Finger.

Und mit Erstaunen und mit Grauen
Sehen's die Ritter und Edelfrauen,
Und gelassen bringt er den Handschuh zurück.
Da schallt ihm sein Lob aus jedem Munde,
Aber mit zärtlichem Liebesblick -
Er verheißt ihm sein nahes Glück -
Empfängt ihn Fräulein Kunigunde.
Und er wirft ihr den Handschuh ins Gesicht:
"Den Dank, Dame, begehr ich nicht!"
Und verläßt sie zur selben Stunde.

3) Der folgende Text ist erst binär kodiert worden (auf dem Kryptospielplatz) und dann mit einem binären Passwort XOR-verschlüsselt (Vigenère mit dem Zeichensatz {0,1}) worden.
   Ermittelt mittels Autokorrelation die Passwortlänge. Versucht weiterhin, mit geeigneten Mittel (alles ist erlaubt), das Passwort und die Nachricht zu ermitteln. Nutzt gegebenenfalls das CrypTool (http://www.cryptool.de) von Herrn Esslinger.

   Hinweise:
   - Hierzu ist es nicht nötig, den gesamten Text zu verwenden, dann geht es manuell mit einem Texteditor und nachzählen. Das sieht dann so aus:

     ```
     1111011011011001110000011000110011001111011001001110111111101111111001
      11110110110110011100000110001100110011
      111  1  1  1 1 11 1111 1 11 1 1 1 1 11              21
     ```

     Das ist natürlich nur ein Vorschlag, ich habe es auch in Excel versucht… geht wunderbar. (Beachtet: Excel hat nur 256 Spalten)
   - Fragt mich und diskutiert die Ansätze in StudIP!

Nachricht

```
1111011011011001110000011000110011001111011001001110111111101111111001
0011101111011001001110000010100011001111101011001001110111110110111111
0110000100100011000001011001000110000101100010111011111100011001100100
1110000011101110011001010110001011100100111000000110110001000110011100
1001110111111000110011011111110001011100111111000100100000001000110011
1001101110110011100111111000100100011001100100011000101110010011000011
0011101101110011101101111111001111110001001100001011000101110110001100
1100011001001100011001100111011001001110101100101000011001011110000000
1100010111001111110001001000110011100100110001011100001011011000110011
0011101111011001011110111101101100111000010110010001101101111000101111
0111111101111111001001110000101000110011010110110110011000110011011111
1110110001101100111001000110001011100100111011111011001001110000101000
0010100011001110100111000101110000101100010111001011110010011000110011
1111010110010011101111011001010110011011100010011011110110010011100000
1010001100110010011101111011000111110000000100100011011110110010011110
0001010001100110111111100010111001111110001001000110011001101110110011
1100101010001100110010001100010111001001110111111100100110001100111111
0111100100111000101110111111110010011000110011001011110011011100001011
0101101000110011011010110000111100001010001100110111111100100111000000
0110011101101111111011000100000101000110 0
```

Viel Spaß und Erfolg!