Kryptologie

Friedman-Analyse eines polyalphabetisch verschlüsselten Textes

```
a7Hzq .#5r<
kÜ\as TâÆK$
ûj(Ö2 ñw%h:
Úk{4R f~`z8
¤˜Æ+Ô „&¢Dø
```

Das Kryptogramm

... ist das bereits mit Hilfe der KASISKI-Analyse gebrochene:

```
      00    05    10    15    20    25    30    35    40    45

0000  AOWBK NLRMG EAMYC ZSFJO IYYVS HYQPY KSONE MDUKE MVEMP JBBOA
0050  YUHCB HZPYW MOOKQ VZEAH RMVVP JOWHR JRMWK MHCMM OHFSE GOWZK
0100  IKCRV LAQDX MWRMH XGTHX MXNBY RTAHJ UALRA PCOBJ TCYJA BBMDU
0150  HCQNY NGKLA WYNRJ BRVRZ IDXTV LPUEL AIMIK MKAQT MVBCB WVYUX
0200  KQXYZ NFPGL CHOSO NTMCM JPMLR JIKPO RBSIA OZZZC YPOBJ ZNNJP
0250  UBKCO WAHOO JUWOB CLQAW CYTKM HFPGL KMGKH AHTYG VKBSK LRVOQ
0300  VOEQW EALTM HKOBN CMVKO BJUPA XFAVK NKJAB VKNXX IJVOP YWMWQ
0350  MZRFB UEVYU ZOORB SIAOV VLNUK EMVYY VMSNT UHIWZ WSYPG KAAIY
0400  NQKLZ ZZMGK OYXAO KJBZV LAQZQ AIRMV UKVJO CUKCW YEALJ ZCVKJ
0450  GJOVV WMVCO ZZZPY WMWQM ZUKRE IWIPX BAHZV NHJSJ ZNSXP YHRMG
0500  KUOMY PUELA IZAMC AEWOD QCHEW OAQZQ OETHG ZHAWU NRIAA QYKWX
0550  EJVUF UZSBL RNYDX QZMNY AONYT AUDXA WYHUH OBOYN QJFVH SVGZH
0600  RVOFQ JISVZ JGJME VEHGD XSVKF UKXMV LXQEO NWYNK VOMWV YUZON
0650  JUPAX FANYN VJPOR BSIAO XIYYA JETJT FQKUZ ZZMGK UOMYK IZGAW
0700  KNRJP AIOFU KFAHV MVXKD BMDUK XOMYN KVOXH YPYWM WQMZU EOYVZ
0750  FUJAB YMGDV BGVZJ WNCWY VMHZO MOYVU WKYLR MDJPV JOCUK QELKM
0800  AJBOS YXQMC AQTYA SABBY ZICOB XMZUK POOUM HEAUE WQUDX TVZCG
0850  JJMVP MHJAB VZSUM CAQTY AJPRV ZINUO NYLMQ KLVHS VUKCW YPAQJ
0900  ABVLM GKUOM YKIZG AVLZU VIJVZ OGJMO WVAKH CUEYN MXPBQ YZVJP
0950  QHYVG JBORB SIAOZ HYZUV PASMF UKFOW QKIZG ASMMK ZAUEW YNJAB
1000  VWEYK GNVRM VUAAQ XQHXK GVZHU VIJOY ZPJBB OOQPE OBLKM DVONV
1050  KNUJA BBMDU HCQNY PQJBA HZMIB HWVTH UGCTV ZDIKG OWAMV GKBBK
1100  KMEAB HQISG ODHZY UWOBR ZJAJE TJTFU K
```

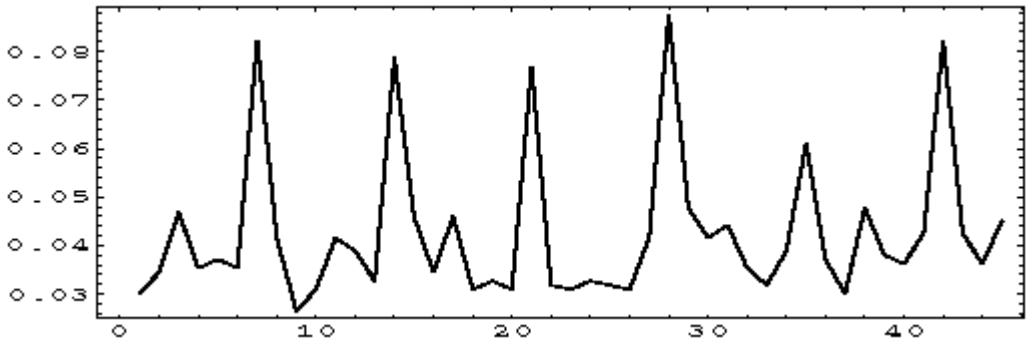
Die Autokoinzidenzindizes

`kappa[q]` ist der *q*-te Autokoinzidenz-Index, d. h. der Koinzidenzindex des Textes mit sich selbst um *q* Stellen (zyklisch) verschoben. Die Folge der Autokoinzidenzindizes des obigen Geheimtextes sieht so aus:

```
kappa[1]  = 0.0301
kappa[2]  = 0.0345
kappa[3]  = 0.0469
kappa[4]  = 0.0354
kappa[5]  = 0.0371
kappa[6]  = 0.0354
kappa[7]  = 0.0822 <---
kappa[8]  = 0.0416
kappa[9]  = 0.0265
kappa[10] = 0.0309
kappa[11] = 0.0416
kappa[12] = 0.0389
kappa[13] = 0.0327
kappa[14] = 0.0787 <---
kappa[15] = 0.0460
kappa[16] = 0.0345
kappa[17] = 0.0460
kappa[18] = 0.0309
kappa[19] = 0.0327
kappa[20] = 0.0309
```

```
kappa[21] = 0.0769 <---
kappa[22] = 0.0318
kappa[23] = 0.0309
kappa[24] = 0.0327
kappa[25] = 0.0318
kappa[26] = 0.0309
kappa[27] = 0.0416
kappa[28] = 0.0875 <---
kappa[29] = 0.0477
kappa[30] = 0.0416
kappa[31] = 0.0442
kappa[32] = 0.0354
kappa[33] = 0.0318
kappa[34] = 0.0389
kappa[35] = 0.0610 <---
kappa[36] = 0.0371
kappa[37] = 0.0301
kappa[38] = 0.0477
kappa[39] = 0.0380
kappa[40] = 0.0363
...
```

Die aufgrund der KASISKI-Analyse vermutete Periode 7 hebt sich auch hier deutlich hervor. Auch die folgende Grafik zeigt das.



Die Werte für q außerhalb der Vielfachen von $l = 7$ schwanken, wie erwartet, um den Wert $1/26 \approx 0.0385$.

Der in den »Spitzen« zu erwartende Wert wird im Rest dieses Abschnitts mathematisch hergeleitet. (Dass er der typischen Zeichenkoinzidenz der Klartextsprache entspricht, ist schon klar. Wie groß dieser Wert ist - und ob er überhaupt sinnvoll definiert werden kann - ist aber schon noch einer Überlegung wert.)

Die Folge der Autokoinzidenzindizes $\kappa_1(a)$, ... $\kappa_{r-1}(a)$ eines Textes $a \in \Sigma^*$ der Länge r soll wegen ihrer offensichtlichen Bedeutung für die Kryptoanalyse als **Autokoinzidenzspektrum** von a bezeichnet werden. [Auch diese Bezeichnung ist nicht Standard in der Literatur.]

Übungsaufgaben.

1. Bestimme das Autokoinzidenzspektrum Deines bereits mit der KASISKI-Analyse gebrochenen Geheimtextes. Fertige eine grafische Darstellung davon mit Hilfe eines Programms Deiner Wahl an.
2. ```
   ECWUL MVKVR SCLKR IULXP FFXWL SMAEO HYKGA ANVGU GUDNP DBLCK
   MYEKJ IMGJH CCUJL SMLGU TXWPN FQAPU EUKUP DBKQO VYTUJ IVWUJ
   IYAFL OVAPG VGRYL JNWPK FHCGU TCUJK JYDGB UXWTT BHFKZ UFSWA
   FLJGK MCUJR FCLCB DBKEO OUHRP DBVTP UNWPZ ECWUL OVAUZ FHNQY
   XYYFL OUFFL SHCTP UCCWL TMWPB OXNKL SNWPZ IIXHP DBSWZ TYJFL
   NUMHD JXWTZ QLMEO EYJOP SAWPL IGKQR PGEVL TXWPU AODGA ANZGY
   BOKFH TMAEO FCFIH OTXCT PMWUO BOK
   ```

Autor: Klaus Pommerening, 14. Juli 1997; letzte Änderung: 13. November 2007.
   ```

E-Mail an Pommerening »AT« imbei.uni-mainz.de.