Rätselserie 3

1) Gegeben ist ein deutscher Text. Dieser ist mit der Vigenère-Chiffre mit beliebigen Passwörtern verschiedener Längen zu verschlüsseln. (Länge 1, 4, 7, 10 Buchstaben)
Mögliche Passwörter sind also z.B.: Z, ZWEI, ZWEIGER, ZWERGHASEN
Wie verändern sich der Koinzidenzindex *I* aus der folgenden Formel
und die Entropie?

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

Die Entropie und die absoluten Häufigkeiten der Buchstaben könnt ihr mit dem Kryptospielplatz ermitteln. Wer möchte kann das aber auch per Hand machen. ;)

Stellt die Kurvenverläufe in Abhängigkeit von der Passwortlänge dar! Was fällt auf?

```
ICHHA BEMIT DEMAL TENVI GENER ESKRI PTRUM GESPI ELTUM MICHI NSPIR IEREN
ZULAS SENEI NIGER ECHER CHENI MINTE RNETL IEFER TEMIR EINEG UTEID EEWAS
VONMI RERWA RTETW URDEE INUEB ERBLI CKUEB ERDIE VERSC HIEBE MULTI PLIKA
TIVEU NDTAU SCHCH IFFRE EINBI SSCHE NGESC HICHT EDANN ETWAS VIGEN ÈREUN
DZUMS CHLUS SNOCH ENIGM ADASH ABICH DANNA UCHGE MACHT ABERE SWARM IRZUD
UENNJ EDERV ONDEM ICHWA SGEFU NDENH ABEHA TTEVO NDEMA NDERN ABGES CHRIE
BENDI EORIG INELL STENQ UELLE NHABE ICHUN TERDE NLINK SZUSA MMENG EFASS
TESSI NDNIC HTVIE LESEI TEINI GENWO CHENG RUEBE LEICH UEBER DIESE RSITU
ATION ICHBE SCHLI ESSED ASPFE RDVON HINTE NAUFZ UZAEU MENAN STATT ALLES
NOCHM ALZUS AMMEN ZUFAS SENWI EDASS OVIEL EGEMA CHTHA BENGR EIFEI CHDIE
IDEEV ONPRO FESSO RMUMM WIEDE RAUFI CHSUC HEMEI NALTE SJAVA PROGR AMMVK
NACKE RJAVA UNDUE BERLE GEICH BESCH LIESS EMEIN ENVOR TRAGU NDMEI NEAUS
ARBEI TUNGA USDER SICHT EINES KRYPT OANAL YSTEN ZUSCH REIBE NICHA NALYS
IERED IEEIN FACHE NKLAS SISCH ENCHI FFREN UNDKO MMEZU DEMSC HLUSS DASSS
ICHAL LEEIN FACHE NMONO ALPHA BETIS CHENC HIFFR ENAUF LINEA REREC HENOP
ERATI ONENZ URUEC KFUEH RENLA SSEND ASIST DIEER STEGR OSSEE RKENT NIS
```

2) Folgendes Kryptogramm ist gegeben:

87	24	38	80	59	49	46	54	55	59	60	88
29	56	86	33	30	77	95	49	54	58	45	39
89	89	29	56	58	55	30	79	89	30	85	88
66	66	60	78	60	76	56	34	47	96	59	59
76	58	43	49								

In der Vorlesung haben wir die Nihilist-Substitution (5x5) behandelt. Im Beispiel auf den Folien sind 2 Passwörter verwendet worden. Das erste Passwort lautet ABC und das zweite Passwort lautet RAETSEL.

Welche Nachricht habe ich verschlüsselt.

Hinweis: Die Chiffre baut auf dem Polybios-Quadrat auf! Ersetzungsvorschrift für den 26. Buchstaben ist W=VV

3) Ich habe euch eine Nachricht mit der Bifid-Chiffre verschlüsselt. Das Passwort ist JUHU es gilt dieselbe Ersetzungsvorschrift wie bei Aufgabe 2.

KJLSQ TUECZ EVROJ NBTHY FCHDI HSJ