IT-Sicherheit Übung 3

Gruppe: Herr Herden (10045920), Herr Lienenkamp (10038452), Herr Döhring (10052723)

8. Juni 2020

# **Aufgabe 1 Entschlüsselung eines Vigenére-Chiffrats ohne Schlüssel**

**In der Aufgabe Verschlüsselter Text:**

kjegimoeugcmoemgcbkxmojlovpgkbkjqksmtactxmmvqycmoectupgkbkjqkcqkseovmoemslbzvzoyzkbqtumxcqkspgkmoemykimvacftrkmyzmoelkeegclaelllbzvznftkelgiqkwaovircmyzmhvvnvzhvqaelygzgtprzmhvsoelkiqiyeoctnzvglaoelkeegclyvqjrclvcxvznlbbfzjvucftlnmtemxymxvqtbwsdbyfnxzaykmxvciyircmszbnrczlvjyigimxmmxjbkctzjqiywlkihvzgeakzvkizglpkeazzusvctuitjmoemtjknnixqmtwckjakeekilkkqniqnemxbmtemtuqkxmojtkzvyrozvvrzmhvuakbkieoieuctkectjaiywtzvgtpzemndmtzpxbwkevzfptvauiokwwxkokymtuisvkqvzzvlovirkmaelsrknkmyzknxmziwykiawlkeekx

**Zur Lösung dieser Aufgabe wurde ein Python-Skript „Vigenére.py“, welches mit dem Friedman-Test arbeitet.**

**Lösung zu a) + b) + c)**

Konistenzindex lautet: 4.98%

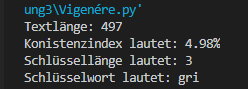
Schlüssellänge lautet: 3

Schlüsselwort lautet: gri

**Lösungstext:**

eswareinmaleinealtegeisdiehattesiebenjungegeisleinundhattesieliebwieeinemutterihrekinderliebhateinestageswolltesieindenwaldundfutterholendariefsieallesiebenherbeiundsprachliebekinderichwillhinausindenwaldseidaufeurerhutvordemwolfwennerhereinkommtsofrisstereuchallemithautundhaarerverstelltsichoftaberanseinerrauhenstimmeundanseinensschwarzenfuessenwerdetihrihnerkennendiegeisleinsagtenliebemutterwirwollenunsschoninachtnehmenihrkoenntohnesorgefortgehendameckertediealteundmachtesichgetrostaufdenweg

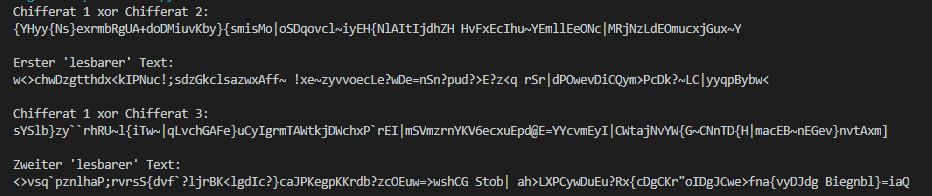
In der Konsole gab es folgende Ausgabe:



# **Aufgabe 2 Entschlüsselung von Multiple-Time-Pad-Chiffraten**

**Zudem wurde wieder ein Python-Skript „Multiple Time Pad“ geschrieben.**

Lösung wäre bei uns:



Man sieht hier, dass nicht der richtige Klartext rauskommt. Wir haben versucht mit dem „Pad“ „seven“ zu arbeiten oder „that“ aber da kam jedes Mal was noch Kryptischeres raus. Die XOR-Verknüpfungen wurden richtig gesetzt. Wir haben sehr lange danach gesucht wo der Fehler sein könnte, aber finden diesen nicht. Die XOR-Verknüpfungen liefen auch Bitweise & hatten es auch versucht den ASCII-Bereich einzuschränken, damit dieser nur Buchstaben enthält, aber vergeblich.