# Kryptologie LAB - 2

## Summer Semester 2020

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena

# Good practices

- formatting – use of whitespace and indenting
- descriptive variable names
- commenting – more is always better
- command line tools require a README file

# Vigenére and Rauheitsgrad

$$\begin{array}{c|cccccccl} & x_1 & x_2 & \cdots & x_d & x_{d+1} & x_{d+2} & \cdots & \text{plaintext} \\ + & k_1 & k_2 & \cdots & k_d & k_1 & k_2 & \cdots & \text{key} \\ \hline & y_1 & y_2 & \cdots & y_d & y_{d+1} & y_{d+2} & \cdots & \text{cryptotext} \end{array}$$

$$\text{Rauheitsgrad}: \quad MR_L = \left( \sum_{a \in A} p(a)^2 \right) - \frac{1}{||A||}$$

- block size: $1 \leq d \leq 100$
- alphabet $A$: the first 128 ASCII characters (integers 0 to 127)
- $p(a)$ is the frequency of occurrence of character $a$

# Preliminary Exercises

Materials: github.com/JoshuaBlinkhorn/Kryptologie-LAB

1 Let $C$ be a constant language, $R$ a random language, $L$ the Lorum Ipsum language. Using the sample texts, confirm that

- $RH_C \approx 1$
- $RH_R \approx 0$
- $RH_L \approx 0.6$

2 Confirm that `encrypted-lorem-1.txt` was encrypted with key length $d = 3$.

3 Determine the key lengths of the other three cryptotexts

4 Determine the keys themselves (they are ASCII strings)
hint: what is the most common character in Lorem Ipsum?

# Task 2

- Design and implement a command line tool that breaks the Vigenère cypher.
  - The tool takes an encrypted Lorem Ipsum text as input and outputs the plaintext automatically
  - use the encrypted texts to test your tool
  - the tool should be documented with a README
  - send me a .zip file (source code and README)