

# Kryptologie LAB - 02

## Vigenère

Luc Spachmann

Friedrich-Schiller-Universität Jena

05.11.2021

# Vigenère - Verschlüsselung

$$\begin{array}{cccccccccc} & x_1 & x_2 & x_3 & \cdots & x_n & x_{n+1} & x_{n+2} & \cdots & x_{mn+i} \\ + & k_1 & k_2 & k_3 & \cdots & k_n & k_1 & k_2 & \cdots & k_i \\ \hline y_1 & y_2 & y_3 & \cdots & y_n & y_{n+1} & y_{n+2} & \cdots & y_{mn+i} \end{array}$$

- Additive Verschlüsselung mit  $n$  zyklisch verwendeten Schlüsseln
- Schlüssellänge nicht konstant, teil des Schlüssels
- Wie letzte Woche:
  - Klartextalphabet und Kryptotextalphabet 7-bit ASCII
  - Schlüsselraum:  $\{ i \mid 0 \leq i \leq 127 \}^*$

# Kryptoanalytische Betrachtungen

- Falls Schlüssellänge  $n$  bekannt:
  - Aufteilung des Texts in  $n$  Teiltexte mit jeweils gleichem Schlüssel
  - Schlüsselbestimmung über Häufigkeitsanalyse
- Schlüssellänge über Koinzidenzindizes bestimmen

# Koinzidenzindex einer Sprache $L$

- Sei  $\Sigma$  Alphabet der Sprache  $L$
- Sei  $p(a)$ ,  $a \in \Sigma$  die Häufigkeit des Zeichen  $a$
- Dann ist der Koinzidenzindex definiert als

$$IC_L = \sum_{a \in \Sigma} p(a)^2.$$

- $IC_L \approx 0.06$
- $IC_{random} = \frac{1}{26}$

# Konizidenzindex eines Texts

- Sei  $y$  ein Text über  $\Sigma$  der Länge  $n$
- Sei  $H(a)$  die absolute Häufigkeit von  $a$
- Dann ist der Koinzidenzindex definiert als

$$IC(y) = \frac{1}{n(n-1)} \sum_{a \in \Sigma} H(a)(H(a) - 1).$$

- Beschreibt die Ungleichmäßigkeit der Buchstaben eines Textes

# Bestimmung der Schlüssellänge

- Für  $i = 1, \dots, 100$
- Aufteilung des Textes in  $i$  Teiltex te sodass
- Text 1:  $x_1, x_{i+1}, \dots$
- Berechnung des Koinzidenzindex der Teiltex te
- Hohe Koinzidenz  $\rightarrow$  Wahrscheinlicher Schlüssel
- Vielfache des Schlüssels haben ebenfalls eine hohe Koinzidenz

- Schreibt ein Programm zur automatische Entschlüsselung von Vigenère
- Input: Verschlüsselter Lorem Ipsum Text
- Gebt den Schlüssel und die Schlüssellänge aus
- Beispieltex te in Moodle
- Als Referenz: Lorem1.txt hat Schlüssellänge 3