Kryptologie LAB

Summer Semester 2020

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena

Goals

- Implemenatation of cryptosystems
  (a) classical cyphers (additive, Vigenère, ..)
  (b) modern cyphers (DES, AES, RSA)

- Experiments with cryptanalysis
  - breaking classical cyphers
  - attacking modern cyphers

- Practical programming experience
  - use your favourite language (Python, C, C++, Java, ..)
  - if in doubt, recommended: Python

Today's Task – Additive Cypher

$$\begin{array}{cccc} x_1 & x_2 & \cdots & x_k \\ k & k & \cdots & k \\ \hline y_1 & y_2 & \cdots & y_k \end{array}$$

1. Implement the encryption and decryption functions of the additive cypher
   - alphabet: letters A to Z, spaces ' ' and newlines '\n'
   - spaces and newlines should not be encrypted
   - plaintext: github.com/JoshuaBlinkhorn/Kryptologie-LAB

2. Break the additive cypher by brute force
   - cryptotext: github.com/JoshuaBlinkhorn/Kryptologie-LAB
   - the plaintext is your final instruction

(3) Send me your code for part 1
<joshua.blinkhorn@uni-jena.de>