Cryptology - LAB - 01

Luc Spachmann

Friedrich Schiller Universität

29.10.2021

Structure

- Sessions every Friday 12:15
- Other session not obligatory, only for questions/help
- Exercises every week
- Send your programs to me at luc.spachmann@uni-jena.de
- Alternatively, you can give me access to a repo
- Oral Exam: You will present your programs

Plans for the semester

- Implementations of different chiffres
  - Historical Chiffres (additive / Vigenère)
  - Modern symmetrical Chiffres (DES)
  - Asymmetrical Chiffres (RSA)
- Cryptoanalysis
  - Breaking historical chiffres
  - Attacking modern systems
- Write the programs in your favourite language

Today: Additive Cypher

1. Implement encryption and decryption for the additive Cypher
   - Alphabet: 7-bit ASCII Characters
   - Key: Number between 0 and 127
2. Write a tool, given an encrypted Lorem Ipsum text that automatically decrypts it
   - Read text from file
   - Find key with frequency analysis
   - Which character is the most common? (Hint: its not an 'e')
   - Automatically output the key and the decrypted text