Kryptologie LAB 01 - Additive Chiffre

Luc Spachmann

FSU Jena

26.10.2023

Organisatorisches

- Nur ein fester Termin: Donnerstag 14:15
- Falls nötig: zweiter Termin für Fragen etc. Wann?
- Jede Woche Programmieraufgaben
- Prüfungsleistung: Einsenden der dokumentierten Programme
  - Wie lässt sich das Programm ausführen?
  - Wie wurde die Korrektheit getestet?
  - Leichte Dokumentation des Quellcodes:
  - Was macht diese Funktion
  - Nicht nötig: Jede Zeile kommentieren

Plan für das Semester

- Implementierung verschiedener Verschlüsselungsalgorithmen
  - Historische (Additiv/Vigenère)
  - Moderne symmetrische (AES)
  - Moderne asymmetrische (RSA)
  - Je nach Zeit: Quantenalgorithmen
- Kryptoanalyse:
  - Brechen historischer Systeme
  - Attackieren moderner Systeme
- Programme in beliebiger üblicher Sprache

Heute: Additive Chiffre

- Implementiert jeweils ein Programm zur Ver- und Entschlüsselung der Additiven Chiffre
  - Alphabet: Großbuchstaben A-Z
  - Alle anderen Zeichen: Unverändert lassen
  - Schlüssel: Zahl 0-25
  - In- und Output in txt Dateien
  - Kommandozeilenargumente: [input.txt] [Schlüssel] [output.txt]
- Implementiert ein Programm zur automatischen Entschlüsselung deutscher Texte
  - Schlüssel über Häufigkeitsanalyse
  - Input: txt Datei
  - Output: txt Datei, erste Zeile Schlüssel, danach entschlüsselter Text
  - Kommandozeilenargumente: [input.txt]