Angewandte Kryptographie 1 Prof. Dr.-Ing. Kerstin Lemke-Rust
SoSe 2023 Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 1

C.1 In LEA befindet sich ein verschlüsselter, englischsprachiger Text in der Datei "chiffrat.txt", der mit einer einfachen Substitutionschiffre verschlüsselt wurde. Ziel dieser Aufgabe ist es, den Klartext wiederzugewinnen, d.h., das Chiffrat zu entschlüsseln. Gehen Sie dabei wie folgt vor:

(a) Geben Sie die relative Häufigkeit der Buchstaben `A` bis `Z` des Chiffrates an.

(b) Entschlüsseln Sie den Text "chiffrat.txt" mit Hilfe einer Buchstabenhäufigkeitsverteilung der englischen Sprache (z.B. aus Wikipedia).

(c) Wie lautet der Schlüssel?

(d) Wer hat den Text wann und wo geschrieben?

Hinweise: Leerzeichen, Satzzeichen, Anführungszeichen etc. sind im Chiffrattext erhalten geblieben und helfen so bei der Dechiffrierung.

C.2 In LEA befindet sich ein verschlüsselter Text in der Datei "chiffrat2.txt", der mit der Vigenère-Chiffre verschlüsselt wurde. Die Sprache des Texts ist unbekannt. Ziel dieser Aufgabe ist es, den verwendeten Schlüssel zu bestimmen und das Chiffrat zu entschlüsseln. Gehen Sie dabei beispielsweise wie folgt vor:

(a) Geben Sie die relative Häufigkeit der Buchstaben `A` bis `Z` des Chiffrates an.

(b) Prüfen Sie z.B. durch Berechnung des Koinzidenzindex oder den Kasiski-Test, wie lang das verwendete Schlüsselwort ist.

(c) Bestimmen Sie den Schlüssel z.B. durch Berechnung des speziellen Koinzidenzindex M_g aus der Vorlesung.

(d) Entschlüsseln Sie das Chiffrat.

(e) Aus welcher Quelle stammt der Text?