

Computerpraktikum: Aufgabenblatt 1

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

- (a) Geben Sie die absolute und relative Häufigkeit der Buchstaben A bis Z des Chiffrates an.
- (b) Entschlüsseln Sie den Text “chiffprat.txt” mit Hilfe einer Buchstabenhäufigkeitsverteilung der deutschen Sprache (z.B. aus Wikipedia).
- (c) Wie lautet der Schlüssel?
- (d) Wer hat den Text wann im Original geschrieben? Worin unterscheidet sich der Originaltext von dem chiffrierten Text im Praktikum?

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

C.2 In LEA befindet sich ein verschlüsselter Text in der Datei “chiffprat2.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 Chiffprat zu entschlüsseln. Gehen Sie dabei beispielsweise wie folgt vor:

- (a) Geben Sie die absolute und 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 Chiffprat.
- (e) Aus welcher Quelle stammt der Text?

Hinweise: Leerzeichen, Satzzeichen, Anführungszeichen etc. sind im Chiffprattext entfernt worden.