4

502470 - Einführung in Sicherheit und Privatheit
Übung: Angriffe/Kryptographie
— Diskussion der Lösung während der Übung: 06./07. Juni 2024 —

1 Kryptographie

Aufgabe 1. Verschlüsseln Sie das Wort `Computersicherheit` mit der Verschiebechiffre (Caesar-Verschlüsselung) und einem $k = 12$

2 Kryptoanalyse

Im Folgenden sind drei Aufgaben der Kryptoanalyse. Sie finden auf der letzten Seite des Übungsblattes Hinweise zur Lösung. Sie sollten die Aufgaben zunächst jedoch ohne Hilfestellungen in Angriff nehmen.

Aufgabe 2. Im Dateiverzeichnis zur Übung finden Sie eine Textdatei **enc_aufgabe2.txt**. Diese Textdatei beinhaltet einen verschlüsselten Text, der mit der Substitutionschiffre verschlüsselt wurde. Ihre Aufgabe ist es nun, das Chiffrat zu entschlüsseln, um damit den ursprünglichen Klartext zu erhalten.

Aufgabe 3. Entschlüsseln Sie das Chiffre `TVMZEXLIMX`

Aufgabe 4. Im Dateiverzeichnis zur Übung finden Sie eine Textdatei **enc_aufgabe4.txt**. Diese Textdatei beinhaltet einen verschlüsselten Text, der mit einem OTP verschlüsselt wurde. Das OTP wurde per Pseudo-Zufallszahlengenerator erzeugt. Folgendes ist bekannt:

- $s_1 = 1$, $s_2 = 3$, $s_3 = 7$. Die Berechnung ist: $s_{i+1} = s_i A + B \mod 9$.
- Die Verschlüsselungslogik war $k_i(x_i) = x_i + s_i$, wobei $k_i(x_i)$ das verschlüsselte Zeichen des Klarzeichens x_i ist und s_i der entsprechende Wert des OTP an dieser Stelle.
- Die Verschlüsselung erfolgte auf ASCII-Zeichen-Ebene.

3 Hinweise zur Kryptoanalyse

Die Hinweise in diesem Abschnitt sind iterativ zu verstehen. Lesen Sie zunächst Hinweis 1 und probieren Sie die Aufgabe zu lösen. Falls Sie weitere Hilfe brauchen, lesen Sie Hinweis 2, usw.

Aufgabe 2

1. Bestimmen Sie die relativen Häufigkeiten der Buchstaben im Chiffrat und recherchieren Sie Buchstabenhäufigkeiten im Deutschen
2. Programmieren Sie (nach Möglichkeit) eine Automatisierung für die relativen Häufigkeiten
3. Im Text geht es um eine bekannte Persönlichkeit.

Aufgabe 3

1. Es handelt sich um die Caesar-Verschlüsselung
2. Eine Möglichkeit, k herauszufinden, ist es ein Programm zu schreiben, das alle Möglichkeiten durchprobiert. Sie haben dann 25 Wörter, von denen nur eins sinnvoll ist.
3. Um nach Position 26 wieder zurück zu A zu kommen, benötigen Sie den Modulo.

Aufgabe 4

1. Gleichungssysteme mit Modulo löst man wie herkömmliche Gleichungssysteme (bis auf die Division, die Sie in unserem Fall nicht benötigen)
2. Der Schlüsselstrom started bei s_0
3. Die Entschlüsselung klappt ebenfalls nur auf der ASCII-Zeichen-Ebene
4. Leerzeichen wurden im Chiffrat gelöscht