IT-Sicherheit

Praktikumsaufgabe 2: Brechen von Vigenere-Chiffren

Aufgabenstellung

In der Datei `interessantesDokument.txt.enc` befindet sich ein mit dem Vigenère-Chiffre verschlüsseltes Dokument.

❖Entschlüsseln Sie das Dokument!

❖Wie lautet das Verschlüsselungspasswort?

Hinweise:

- Das zum Verschlüsseln verwendete Programm finden Sie als Hilfestellung in `encrypt.py`.
- Ein kleines Tool zum Finden von identischen Ciphertext finden Sie in `helper.py`

Überlegungen

Beantworten Sie zur bzw. nach Bearbeitung der Praktikumsaufgabe folgende Fragen:

1. Wie können mögliche Schlüssellängen beim Vigenère-Chiffre ermittelt werden?
2. Warum kann der Vigenère-Chiffre trotz eines großen Schlüsselraums gebrochen werden?
3. Wie könnte der Vigenère-Chiffre gegen den von Ihnen genutzten Angriff gehärtet werden?