IT-Sicherheit

Praktikumsaufgabe 1: Brechen von Substitution-Chiffren

Aufgabenstellung

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

- ❖Entschlüsseln Sie das Dokument!
- ❖Wie lautet die Ersetzungstabelle?

Hinweise / Hilfestellungen:

1. Leerzeichen und Satzzeichen sind bei der Verschlüsselung erhalten geblieben.
2. Groß-/Kleinschreibung ist erhalten geblieben.
3. Es handelt sich um einen Text in deutscher Sprache.
   Tipp: https://de.wikipedia.org/wiki/Buchstabenh%C3%A4ufigkeit

Überlegungen

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

1. Wie können einfache Ersetz-Chiffren gebrochen werden?
2. Nennen Sie mindestens zwei Möglichkeiten den Verschlüsselungsalgorithmus gegen den von Ihnen verwendeten Angriff zu härten!
3. Ist die mehrfache Anwendung des Verschlüsselungsalgorithmus mit verschiedenen Schlüsseln eine Härtung gegen den von Ihnen verwendeten Angriff?