

Hausübung Kryptographie

1. Verschlüsse die folgenden Wörter mit der Caesar-Verschlüsselung mit dem Schlüssel 6:

GEWITTER

SPIONAGE

2. Entschlüsse die Nachrichten, die mit der Caesar-Verschlüsselung mit dem Schlüssel 7 verschlüsselt wurden.

ZVTTLY

NLOLPT

3. Julius C. schlägt vor: "Wenn die Caesar-Verschlüsselung so einfach zu knacken ist, dann verschlüsse ich meinen Text einfach zweimal, dann ist er doppelt so gut geschützt!" Was meinst du dazu?
4. Wie könnte man die Caesar-Verschlüsselung etwas sicherer machen?
5. Verschlüsse das folgende Wort mit der Vigenère-Verschlüsselung.
Klartext: FEUERBALL
Schlüssel: CODE
6. Entschlüsse das folgende, mit dem Vigenère-Verfahren verschlüsselten Wort.
Geheimtext: OOWVJOQCAVZ
Schlüssel: MATRIX
7. Wie viele Versuche braucht ein Computer maximal um die folgende Verschlüsselung durch Ausprobieren (Brute-Force-Angriff) zu knacken?
 - Caesar-Verschlüsselung mit Groß- und Kleinbuchstaben.
 - Vigenère-Verschlüsselung mit einem 1 Zeichen langen Schlüssel.
 - Vigenère-Verschlüsselung mit einem 6 Zeichen langen Schlüssel.