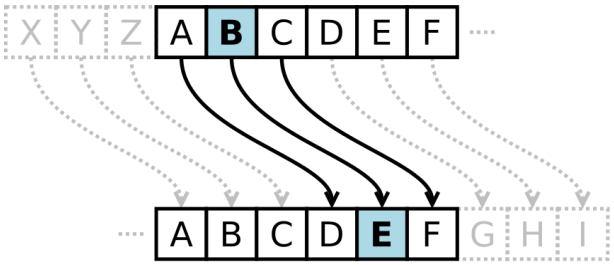
Einführung

1. Einführung

Um Daten im Internet sicher übertragen zu können, so dass sie von niemandem mitgelesen werden können müssen sie verschlüsselt werden.

2. Cäsar-Verschlüsselung

Die einfachste Verschlüsselungsart ist die Cäsar-Verschlüsselung. Hierbei werden sämtliche Buchstaben „verschoben“:



Der Verschlüsselungscode hierbei wird mittels dem Buchstabe angegeben, dem das „A“ zugeordnet wird, im Beispielbild also das „D“.
Am einfachsten lässt sich der Code mit einer *Cäsar-Scheibe* ver- und wieder entschlüsseln.

Aufgabe 1:

Schreibe deinem Nachbarn einen kurzen verschlüsselten Text, den dieser dann wieder entschlüsselt.

Aufgabe 2:

Entschlüssele den folgenden Text, er wurde mit dem Buchstaben „J“ verschlüsselt:
Odalqc odnqac id Fdc, Fdc odnqac id Qjbb. Qjbb odnqac id dwbjnpurlqnv Unrm. (Hxmj id Jwjtrw Bthfjutna, BcjaFjab)

Aufgabe 3:

Ist diese Verschlüsselung deiner Meinung nach *sicher*?
Was bedeutet „sicher“ im Zusammenhang mit einem Verschlüsselungsverfahren?
Wie könnte man ohne den Schlüsselbuchstaben versuchen, den Text zu entschlüsseln?

Diese Cäsar-Verschlüsselung ist eine sogenannte *monoalphabetische Verschlpsselung*, da jedem Buchstaben eindeutig ein anderer Buchstaben zugeordnet wird.

Aufgabe 4:

Eine geringfügig schwieriger zu knackende Verschlüsselungsmethode ist die *Vigenère-Verschlüsselung*, die auf der Cäsar-Verschlüsselung basiert.
Hierbei wird nicht nur ein einziger Schlüsselbuchstabe verwendet, sondern ein Schlüsselwort.
Enschlüssle folgenden Text mit dem Schlüsselwort „DHG“:
Lulrysdaon pyw auos!