

# Verschlüsseln von Informationen

– Lösungshinweis –

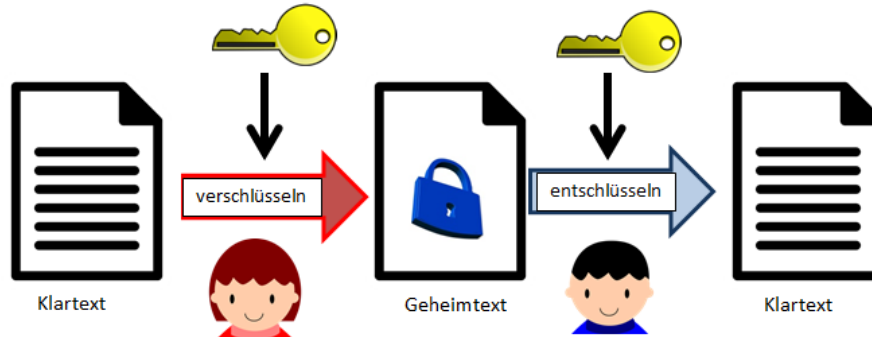


Abbildung 1: Schema eines Ver- und Entschlüsselungsprozesses

In manchen Situationen ist es nicht erwünscht, dass Dritte an Informationen gelangen (bspw. bei der Übertragung von persönlichen Daten). Um zu vermeiden, dass dies auf dem Kommunikationsweg (bspw. per Brief oder per Funk) passiert, können die Informationen verschlüsselt – also in eine Art Geheimsprache übersetzt – werden. Diese können dann bei Kenntnis über die Verschlüsselung vom Empfänger rückübersetzt werden (siehe Abbildung 1).



**Können Sie Informationen ver- und entschlüsseln?**

**Aufgabe:** Entwickeln Sie ein eigenes System zum Ver- und Entschlüsseln von Informationen. Probieren Sie es aus.

- Dokumentieren Sie Ihr Ver- und Entschlüsselungssystem auf einem extra Blatt Papier.  
Welche Parameter sind frei wählbar und wie können diese gewählt werden?
- Verschlüsseln Sie ein Wort oder einen kurzen Satz, den eine andere Gruppe entziffern soll. Notieren Sie die gewählten Parameter auf der Rückseite des Blattes aus a) und die verschlüsselte Information auf einem weiteren Blatt Papier.
- Versuchen Sie die verschlüsselte Nachricht einer anderen Gruppe zu entziffern. Tun Sie dies zunächst ohne Hinweise über das Ver-/Entschlüsselungssystem und beziehen diese nur ein, falls nötig.
- Was sind Stärken und Schwächen Ihres Verfahrens?  
Welche Anforderungen sollten an ein Verschlüsselungssystem gestellt werden?

**Lösungshinweise:**

Das Ver- und Entschlüsselungssystem kann auf unterschiedlichen Ideen fußen und auch Alltagsgegenstände einbeziehen. Denkbar wäre die Cäsar-Verschlüsselung:

- Zur Verschlüsselung der geheimen Informationen können die Buchstaben des Alphabets zyklisch angeordnet und die einzelnen Buchstaben der ursprünglichen Nachricht um  $n$  Stellen verschoben werden. Zur Entschlüsselung muss diese Verschiebung umgekehrt werden, d.h. formal die Umkehrfunktion angewendet werden.

Die Schrittweite der Verschiebung kann frei gewählt werden. Für Sie kann jede natürliche Zahl von 1 bis 25 gewählt werden.

- b) LSZQUPHSBQIJF,  $n = 1$ , Cäsar-Verschlüsselung
- c) Bearbeitung individuell.
- d) Die Ver- und Entschlüsselung von Information mittels der Cäsar-Verschlüsselung ist mit wenig Aufwand verbunden und lässt sich unkompliziert umsetzen. Allerdings können auch relativ einfach alle möglichen Verschiebungen (bei einem einzelnen Parameter) erstellt werden und so die Informationen entziffert werden – sofern das Verfahren bekannt ist.  
Grundsätzlich sollten Ver- und Entschlüsselungsprozesse mit überschaubarem Aufwand umsetzbar sein. Gleichzeitig sollten sie aber auch nicht für Dritte zu entziffern sein – selbst wenn das Verfahren bekannt ist.

DIDAKTIK DER MATHEMATIK

Universität Würzburg

DIDAKTIK DER MATHEMATIK

Universität Würzburg