## Wie funktioniert ein geheimer Austausch von Nachrichten?

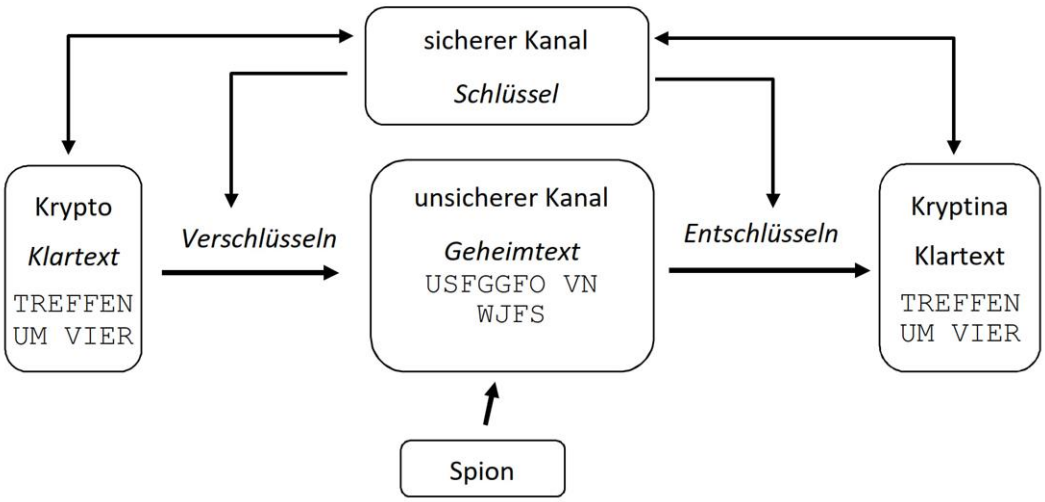


Abb.: Schema eines symmetrischen Verschlüsselungsverfahrens

Krypto hat folgende Nachricht, die er an Krptina verschicken möchte: TREFFEN UM VIER.

Diese Nachricht nennen wir in der Kryptologie den Klartext. Mit einem Schlüssel möchte Krypto den Klartext verschlüsseln. Sagen wir mal, er nimmt folgenden Schlüssel: Ersetze jeden Buchstaben durch den nachfolgenden im Alphabet.

Wendet Krypto diesen Schlüssel an, erhält er: USFGGFO VN WJFS VIS.

Diesen Buchstabensalat nennen wir den Geheimtext. Der Geheimtext kann nun über einen unsicheren Kanal verschickt werden, z.B. ist eine Postkarte ein unsicherer Kanal, denn jeder Spion kann diese auch lesen. Ist die Nachricht verschlüsselt, geht das nicht mehr so einfach. Kryptina bekommt nun den Geheimtext, mit dem kann sie auf den ersten Blick nichts anfangen, aber sie hat ja auch den Schlüssel. Mit dem ist sie nun in der Lage, den Geheimtext zu entschlüsseln und bekommt den Klartext: TREFFEN UM VIER wieder.

**Aber Achtung:** Das Ganze geht nur, wenn Krypto und Kryptina vorher einen gemeinsamen Schlüssel über einen sicheren Kanal vereinbart haben, z.B. wenn sie sich vorher im Geheimen getroffen haben und den Schlüssel austauschen.

Verschlüsselungsverfahren, die auf diese Weise funktionieren sind z.B. die Cäsar-Verschlüsselung, die Freimaurer-Verschlüsselung und die Vigenère-Verschlüsselung.