Kapitel 1: Einführung in die Kryptologie

In diesem Kapitel wirst du dich mit den Grundlagen der Kryptologie vertraut machen und einen Einblick in dem Teilgebiet der Informatik gewinnen können. Dieses Wissen in Kapitel 1 benötigst du für die zwei weiteren Kapiteln, da diese die Fachbegriffe voraussetzen. Bitte lese dir deshalb den Informationstext sorgfältig durch. Viel Spaß bei der Bearbeitung! 😊

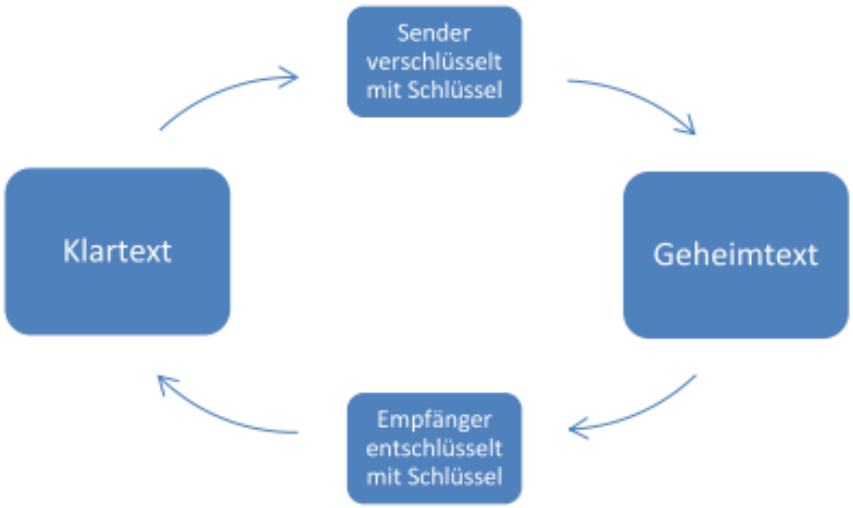
Lektion 1: Grundlagen

Die Kryptologie wird laut Duden definiert als ein „Teilgebiet der Informatik, das sich mit der Lehre von der Entwicklung und der Bewertung von Verfahren zur Verschlüsselung von Daten im Rahmen des Datenschutzes befasst.“[1] Das Wort „kryptós“ stammt aus dem Griechischen und bedeutet „geheim“ bzw. „verborgen“. Die Kryptologie beinhaltet sowohl die **Kryptographie**, welche die Wissenschaft der Verschlüsselung von Informationen ist, als auch die **Kryptoanalyse**, welche die Wissenschaft der Entschlüsselung ohne Kenntnis des Schlüssels ist. Einen weiteren unabhängigen und häufig mit der Kryptographie kombinierten Bereich bildet die **Steganographie**. Die Steganographie bezeichnet die Wissenschaft des Versteckens von Informationen. Dabei wird die Existenz der Botschaft verheimlicht. Das Wort stammt ebenfalls aus dem Griechischen und bedeutet „verdecktes Schreiben“.

Somit kann man im Allgemeinen sagen, dass die Kryptologie sich mit der Sicherheit von Informationen beschäftigt. Ein Klassisches Beispiel ist das Verschlüsseln von Nachrichten von einem Sender zu einem Empfänger, so dass ein unbefugter Dritter eine abgefangene Nachricht nicht entschlüsseln kann.

Der ursprüngliche Text vom Sender wird als **Klartext** bezeichnet, der verschlüsselte Text dann als **Geheimtext**. Ein Klartext ist also die Information, die der Empfänger erhalten soll. Ein Geheimtext ist ein verschlüsselter Klartext, das heißt für Andere nicht mehr lesbar. Den Vorgang der Verschlüsselung bezeichnet man auch als **Chiffrierung**, den der Entschlüsselung als **Dechiffrierung**.

[1] https://www.duden.de/rechtschreibung/Kryptologie [Abgerufen am 28.08.2020]



Die geheime Information, die zur Verschlüsselung und Entschlüsselung dient, nennt man **Schlüssel**. Wird zum Chiffrieren und Dechiffrieren der gleiche Schlüssel benutzt, so spricht man von einem **symmetrischem Verfahren**. Dem gegenüber gibt es Verfahren, bei denen zwei oder mehr Schlüssel verwendet werden, das heißt der Chiffrierschlüssel ist ein anderer als der Dechiffrierschlüssel. Diese Verfahren sind **asymmetrisch.**