

Kryptologie

1. Grundlagen der Kryptologie

Manchmal möchte man Informationen nur mit bestimmten Personen teilen. Beispielsweise soll nur ein Mitschüler den Text auf einem Zettelchen verstehen, nicht aber der Lehrer, der das Zettelchen vielleicht abfängt. Seit langem gibt es daher die Idee, eine Nachricht so zu verschlüsseln, dass nur der intendierte Empfänger sie entziffern kann.

Dieses Gebiet der Informatik nennt sich **Kryptologie** und beinhaltet die Teilgebiete **Kryptographie** und **Kryptoanalyse**.

Gerade in der digitalen Welt spielt dieses Verfahren eine zentrale Rolle: Sensible Daten wie Passwörter müssen geschützt übertragen werden, damit Unbefugte keinen Zugriff darauf erhalten. Dabei beschränkt sich die Verschlüsselung nicht nur auf geschriebene Texte, sondern kann ebenso auf digitale Audiodateien, Videos oder den Programmcode von Software angewendet werden.

Wir fangen mit den wichtigsten Grundbegriffen an, welche wir am Beispiel im untenstehenden Bild erläutern werden.

Begriffe mit Alice und Bob

Alice möchte Bob einen Text geheim übermitteln, damit ihn keine Drittperson verstehen kann.

- Die ursprüngliche, verständliche Nachricht wird **Klartext** genannt. Im Beispiel ist das «Hallo Bob».
- Nun wandelt Alice den Text in eine unverständliche Nachricht um. Diese Veränderung nennt man **Verschlüsselung**. So wird der Text «Hallo Bob» zu «Kdoor Ere». Der **Schlüssel** ist die geheime Information, mit der die Nachricht mit einem gewählten Verfahren unverständlich gemacht wird.
- Die verschlüsselte Form der Nachricht, in diesem Fall «Kdoor Ere» nennt man **Geheimtext**.
- Bei der **Entschlüsselung** wird der Geheimtext mithilfe des passenden Schlüssels wieder in den Klartext zurückverwandelt. So kann Bob die Nachricht verstehen, während eine Drittperson ohne den Schlüssel nur den unverständlichen Geheimtext sieht.



In der Kryptologie werden wir mehrmals dem Begriff **Schlüsselraum** begegnen. Der Schlüsselraum bezeichnet die Menge aller möglichen Schlüssel, die bei einem Verschlüsselungsverfahren verwendet werden können.

Kleiner Rückblick...

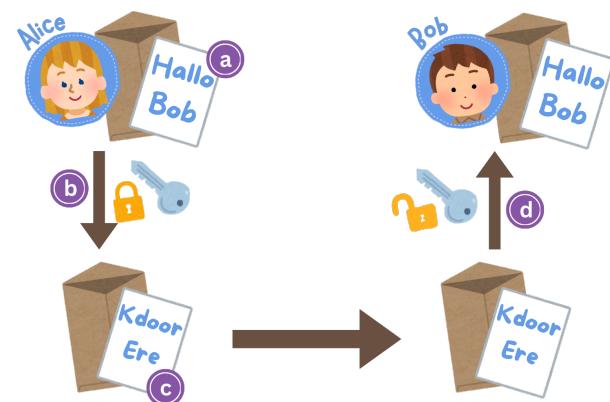
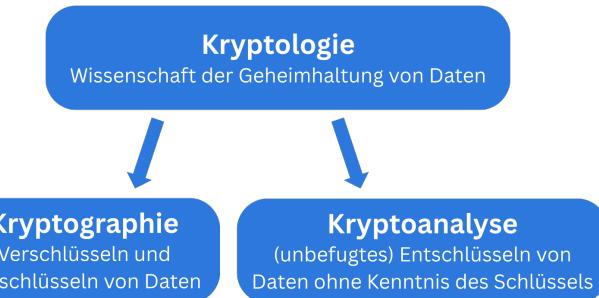
Im ersten Jahr des Gymnasiums haben Sie den Begriff Codierung kennengelernt. Die Begriffe Codierung und Verschlüsselung werden im manchmal gleich verwendet, bezeichnen in der Informatik jedoch unterschiedliche Konzepte.

Codierung

Bei der Codierung werden Daten nach festen, allgemein bekannten Regeln umgewandelt. Das Ziel ist, Daten **einheitlich, platzsparend oder maschinenlesbar** zu machen (z.B. ASCII, UTF-8).

Verschlüsselung

Bei einer Verschlüsselung wird eine Nachricht gezielt unlesbar gemacht, sodass sie nur mit einem geheimen Schlüssel wieder verständlich wird. Das Ziel ist der **Schutz der Information vor Unbefugten**.



Wichtig

Damit eine Kommunikation wie die zwischen Alice und Bob funktionieren kann, müssen beiden denselben Schlüssel (die gleiche Information) haben!

2. Historische Verschlüsselungen

Verschlüsselung ist keine Erfindung der digitalen Welt. Bereits in der Antike bestand das Bedürfnis, Informationen geheim zu übermitteln, etwa im Militär, in der Politik oder im Handel. Aus diesem Bedarf heraus entstanden die ersten Verschlüsselungssysteme. Viele moderne Verschlüsselungsmethoden beruhen auf ähnlichen Prinzipien, sind jedoch deutlich weiterentwickelt.

Auf dieser Seite finden Sie zwei konkrete Beispiele von historisch bekannten Verschlüsselungsverfahren, die grossen Einfluss in der Geschichte hatten. Und auf den nächsten Seiten werden dann einfachere, für uns Anfänger verständlichere Verfahren vorgestellt, die die Entwicklung der Kryptographie massgeblich geprägt haben.

Zimmermann-Telegramm (1. Weltkrieg)

Im Januar 1917 verschickte der deutsche Aussenminister Arthur Zimmermann eine geheime Nachricht an Mexiko, das sogenannte Zimmermann-Telegramm. Darin schlug Deutschland ein Bündnis gegen die USA vor, falls diese ihre Neutralität im ersten Weltkrieg aufgeben würden. Mexiko sollte im Gegensatz dafür an die USA verlorene Gebiete zurückhalten. Die Nachricht war verschlüsselt, wurde jedoch vom britischen Geheimdienst abgefangen und entschlüsselt.

Die Briten kannten schon frühere deutsche Codes, weil ein Diplomat sein Codebuch verlor. Dieses Zufallswissen half, das Telegramm schneller zu entschlüsseln.

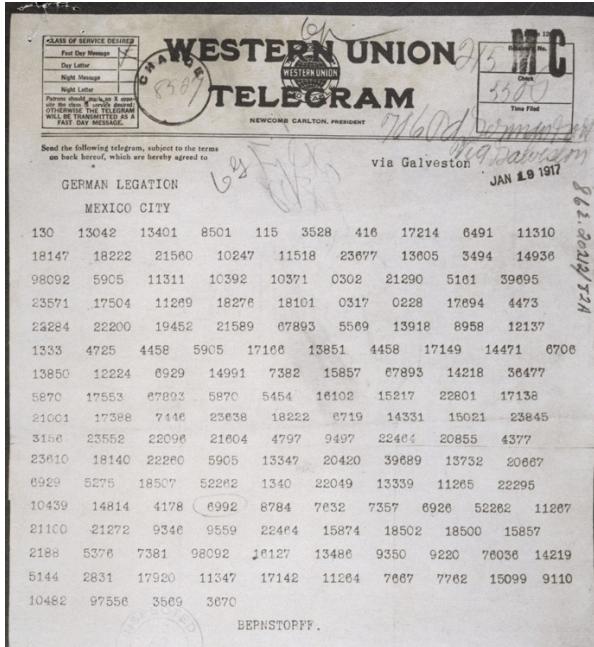


Abbildung 1: Das Telegramm bestand nur aus Zahlenreihen.

Daraufhin empfahlen die Briten der USA ihre Neutralitätspolitik zu überdenken, was entscheidend dazu beitrug, die US-amerikanische Öffentlichkeit für den Kriegseintritt einzustimmen.

Enigma-Verschlüsselung (2. Weltkrieg)

Im Zweiten Weltkrieg verschlüsselte Deutschland seine militärischen Funksprüche mit der Maschine Enigma. Sie arbeitete mit rotierenden Walzen und erzeugte sehr komplexe Codes, die als sicher galten. Die deutsche Führung nutzte sie für wichtige militärische Befehle.



Abbildung 2: Die Enigma-Maschine war so klein, damit man sie praktisch unterwegs eingesetzt werden konnte.

Doch im britischen Codezentrum Bletchley Park gelang es Kryptologen, die Verschlüsselung systematisch zu brechen. Eine wichtige Rolle spielte dabei der Mathematiker Alan Turing. Darum nennt man die grossen Maschinen, die dazu gebaut wurden, die Enigma-Verschlüsselung zu knacken, auch «Turing-Bomben».

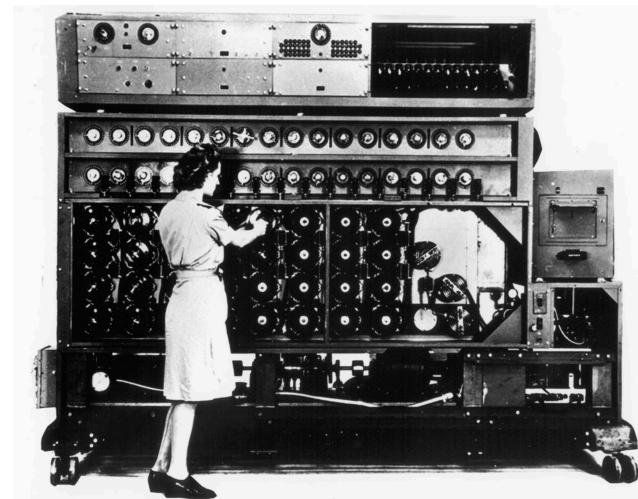


Abbildung 3: Über 200 solcher Turing-Bomben wurden eingesetzt, um die Enigma-Codes zu knacken.

Da viele Nachrichten der deutschen Armee immer mit den gleichen Worten starteten («Heil Hitler»), half dieses vorhersehbare Muster den Briten, die Verschlüsselungen zu knacken.

Durch die Entschlüsselung erhielten die Alliierten entscheidende Informationen über die deutschen militärischen Pläne. Historiker gehen davon aus, dass dies den Krieg deutlich verkürzte.

Lösungen