

Kryptographie

Die Kryptographie

Ganz allgemein beschäftigt sich die Kryptographie (aus dem griechischen „kryptós“ für „versteckt“ und „gráphein“ für „schreiben“) mit der Verschlüsselung von Nachrichten. Schon in der Antike wurden Verschlüsselungsverfahren verwendet, damit nicht jeder eine Nachricht lesen konnte. Allen Verfahren gemein ist, dass ein sogenannter „Klartext“ mithilfe einer bestimmten Vorschrift (dem Schlüssel) in einen Geheimtext umgewandelt wird, der dann vom Empfänger einer Nachricht mit entweder demselben Schlüssel (dann spricht man von symmetrischer Verschlüsselung) oder einem anderen Schlüssel (asymmetrische Verschlüsselung) wieder in den Klartext überführt werden kann.

Die Cäsar-Verschlüsselung

Bei der Cäsar-Verschlüsselung, die schon von Julius Cäsar vor über 2000 Jahren verwendet wurde, wird jeder Buchstabe des Klartextes um eine feste Anzahl von Buchstaben im Alphabet (diese Anzahl ist der Schlüssel) verschoben, wobei man bei dieser Verschiebung hinter dem Buchstaben Z wieder bei A beginnt. Jedem Buchstaben wird also ein anderer Buchstabe zugeordnet. Dies kann man am einfachsten anhand zweier Kreisscheiben, auf denen das Alphabet aufgetragen ist und die gegeneinander verdreht werden können, verdeutlichen. Als Schlüssel reicht die Kenntnis eines Buchstabens (z. B. der Buchstabe, der im Geheimtext dem A entspricht). Kennt der Empfänger diesen Buchstaben, kann er den Geheimtext wieder in den Klartext überführen.

Das Vigenère-Verfahren

Die Cäsar-Verschlüsselung lässt sich leicht „brechen“, da man lediglich 26 Möglichkeiten (die Buchstaben des Alphabets) testen muss. Etwas allgemeiner ist das Vigenère-Verfahren (benannt nach Blaise Vigenère) aus dem 16. Jahrhundert, bei dem nicht ein einzelner Buchstabe sondern ein ganzes Wort oder gar Text als Schlüssel verwendet wird: Ist das Wort PHYSIK das Codewort, so verwendet man für den ersten Buchstaben des Klartexts den Buchstaben P in der Cäsar-Verschlüsselung, für den zweiten Buchstaben den Buchstaben H, für den dritten den Buchstaben Y, und so weiter. Nach dem sechsten Buchstaben, der mit K verschlüsselt wird, beginnt man wieder mit dem ersten Buchstaben des Codeworts P. Je länger das Codewort ist, umso besser ist der Schlüssel. Mit modernen Computern lässt sich dieses Verfahren aber ebenfalls schnell knacken, sofern die Texte lang genug sind (oder der Schlüssel häufiger verwendet wird).



Cäsar:
KRYPTOGRAPHIE
→TAHYCXPAJYQRN

Vigenère:
GEHEIMNIS
+PHYSIKPHY

VLFWQWCPQ

Das One-Time-Pad

Das One-Time-Pad ist ein Protokoll (d. h. eine Abfolge von genauen Vorschriften) zur Ver- und Entschlüsselung eines Klar- und Geheimtexts, das das Vigenère-Verfahren verallgemeinert: Der Schlüssel sollte genauso lang sein wie der Klartext, er sollte aus zufällig gewählten Buchstaben bestehen und nur einmal verwendet werden. Da man jeden beliebigen Klartext (z. B. mithilfe einer ASCII-Tabelle) in eine Folge von 0 und 1 umwandeln kann, besteht der Schlüssel in einem One-Time-Pad oftmals aus einer zufälligen Folge von 0 und 1, die genauso lang wie der Klartext sein muss, nur einmal verwendet wird und nur dem Sender und Empfänger bekannt ist. Statt einer Verschiebung von Buchstaben kann man hier die „Addition modulo 2“ verwenden, bei der $0+0=0=1+1$ und $0+1=1=1+0$ als Regel verwendet wird (was für nur zwei Zeichen mit der Cäsar-Verschlüsselung übereinstimmt). Dieses Verfahren ist vollkommen sicher. Der kritische Punkt ist somit nur noch der sichere Austausch des Schlüssels zwischen Sender und Empfänger; die Forschung dazu ist ein Teilgebiet der Quantenkryptographie.

Grille-Verschlüsselung (Verfahren mit Schablonen)

Es gibt viele andere Verschlüsselungsverfahren. Bekannt sind beispielsweise die sogenannten „Grille-Verschlüsselungen“, bei denen eine Schablone zur Verschlüsselung verwendet wird.

Das Cardan-Gitter verwendet eine Schablone, in deren Ausstufungen der Klartext geschrieben wird, welcher dann ohne die Schablone durch einen beliebigen harmlosen Text ergänzt wird. Ohne die Schablone ist der Klartext nicht zu erkennen.

Lieber Besucher,
wir hoffen, Dir gefällt unsere interaktive Ausstellung „Quanten auf Reisen“ zu Themen und Anwendungen der Quantenphysik. Gerne besuchen wir euch auch vor Ort (Schulen und Unternehmen in der Region um Freiburg i. Br.) und bieten Fortbildungen und Workshops an.
Viele Grüße
Q-Bus-Team

