Streng geheim

Am 08. Februar 1587 wurde Maria Stuart, Königin von Schottland, in England hingerichtet. Schlecht verschlüsselte Nachrichten kosteten sie das Leben.

Nach vielen Kämpfen, Intrigen, Verrat und Mordanschlägen wurde Maria Stuart zunächst in ihrer schottischen Heimat verhaftet und eingesperrt. Es gelang ihr die Flucht nach England zu ihrer Cousine Elisabeth I.. Doch sie war nicht willkommen und Elisabeth I. hielt ihre Cousine an verschiedenen Orten gefangen, da sie Maria als Konkurrentin auf den englischen Thron ansah. 19 Jahre verbrachte Maria Stuart in Gefangenschaft.

Durch die sogenannte Babington-Verschwörung einiger Adliger im Jahre 1586 sollte die protestantische Königin Elisabeth I. ermordet werden, um die Katholikin Maria Stuart auf den Thron von England zu heben. Maria korrespondierte mit den Verschwörern über verschlüsselte Briefe. Dem Sicherheitsminister von Elisabeth gelang es, die verschlüsselten Briefe abzufangen und zu entschlüsseln.

Mit den entzifferten Texten konnte der Ankläger beweisen, dass Maria Stuart von dem Komplott wusste und diesen Mord auch billigte. Daraufhin unterschrieb Königin Elisabeth I. das Todesurteil.

Verschlüsselungen

Etwas Geheimes besitzt immer eine große Faszination und weckt Neugierde. Bereits Kinder lieben es, geheime Botschaften untereinander auszutauschen, ohne dass andere ihre Texte lesen können. Sie verwenden unsichtbare Tinte aus Essig oder Zitronensaft oder sie manipulieren das Alphabet, indem sie Buchstaben vertauschen. Der Empfänger muss dann wissen, wie er die geheime unsichtbare Schrift wieder lesbar machen kann.

Sender und Empfänger müssen in jedem Fall gleiche Codierungen verwenden, denn nur dann kann die Botschaft am Ende auch gelesen werden.

Aber nicht nur Kinder wollen geheime Botschaften verfassen und versenden. Regierungen, Kriegsparteien, Kriminelle oder aufständische Gruppen wollen Nachrichten versenden, die nur für Insider lesbar sind. Der Sender verschlüsselt die Botschaft auf geheimnisvolle Weise und der Empfänger besitzt die Lösung zur Entschlüsselung der Botschaft.

Im Laufe der Jahrhunderte hat man Codierungssysteme entwickelt, die immer komplexer und sicherer wurden. Auf der anderen Seite versuchte man, Decodierungssysteme zu entwickeln, die die verschlüsselten Texte wieder lesbar machten. Es war und ist ein ständiger Kampf zwischen Codierung und Decodierung.

Geschichte der Verschlüsselung

Der Versuch, Botschaften für andere unleserlich zu machen, ist wohl so alt wie die Geschichte der Nachrichtenübermittlung überhaupt.

Eine sehr frühe Variante von Verschlüsselung verwendeten die Spartaner im alten Griechenland. Mit

Skytale | Bild: Spionagemuseum Berlin

Hilfe der Skytale, einem Holzstab von einem definierten Durchmesser, konnten Nachrichten unlesbar gemacht werden. Ein Band aus Leder oder Pergament wird in Streifen um den Stab gewickelt. Längs des Stabes wird der Text geschrieben. Wickelt man das Band ab, so sieht man nur eine sinnlose Aufeinanderfolge von Buchstaben. Erst wenn das Band beim Empfänger auf einen Stab mit gleichem Durchmesser gewickelt wird, entsteht wieder ein lesbarer Text.

Aus dem alten Rom stammt der sogenannte Caesar-Code. Dabei werden zwei Alphabete verwendet, das Klartextalphabet und das Geheimalphabet. Das Geheimalphabet ist lediglich um einige Stellen nach rechts verschoben.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Da die Verschiebung des zweiten Alphabets beliebig ist, können auf diese Weise viele verschiedene Verschlüsselungen vorgenommen werden. Der Empfänger muss nur wissen, um wieviel Stellen das Geheimalphabet verschoben wurde. Das Wort „Frieden“ verschlüsselt lautet in diesem Beispiel:

I	U	L	H	G	H	Q

Diese Art der Verschlüsselung ist durch einfaches Ausprobieren jedoch relativ schnell zu knacken.

Es gab in der Folgezeit immer wieder Versuche, die Verschlüsselungen besser und damit sicherer zu machen. Wie das tragische Beispiel von Maria Stuart zeigt, waren die Verschlüsselungen mehr oder weniger erfolgreich.

Technische Geräte zur Verschlüsselung

Zur weiteren Verbesserung von Verschlüsselungen wurden vielfältige technische Apparate entwickelt. Ein Höhepunkt dieser Entwicklungen war die Konstruktion der sogenannten ENIGMA.

1923 entwickelte der deutsche Ingenieur Arthur Scherbius die erste ENIGMA. Diese Rotor-Chiffriermaschine wurde im Zweiten Weltkrieg von den Nationalsozialisten verwendet, um geheime Befehle zu übermitteln. Die Marine verwendete in ihren U-Booten eine Weiterentwicklung der ENIGMA.

Diese Maschine arbeitete so hochkomplex, dass sie in dieser Zeit als nahezu nicht entschlüsselbar galt. Der Text wird wie auf einer Schreibmaschine eingetippt. Ein Mechanismus aus verschiedenen Walzen verschlüsselt dann die Botschaft.

Enigma | Bild: Spionagemuseum Berlin

Einem Team unter dem Engländer Alan Turing gelang es 1940, nach Vorarbeiten von polnischen Fachleuten, die ENIGMA zu knacken. Dieser Meisterleistung ist es wohl zu verdanken, dass der Zweite Weltkrieg um einige Zeit verkürzt werden konnte.

Verschlüsselung heute

In der heutigen digitalen Welt läuft nahezu nichts ohne Verschlüsselungen. Die Nutzung des Internets verändert die Art der Kommunikation und damit auch die Notwendigkeit, Informationen immer besser zu verschlüsseln, damit diese sicher von einem Absender zu einem vielleicht weit entfernten Empfänger gelangen können.

Bezahlen mit Bank- oder Kreditkarten oder die Abwicklung von Geschäften über das Internet sind nur einigermaßen sicher, wenn entsprechende Verschlüsselungen vorgenommen werden. Codierung ist also nicht nur ein Problem für Spezialisten, es betrifft heute alle Bereiche des gesellschaftlichen Lebens.

Cyberangriffe von Hackern können unübersehbaren Schaden anrichten. Daten können auf dem angegriffenen Rechner verschlüsselt und erst gegen eine Lösegeldzahlung wieder freigegeben werden. Oder es werden zu Spionagezwecken Daten abgegriffen. Hacker besorgen die Daten und andere Spezialisten entschlüsseln dann die geheimen Daten.

Die heute übliche sogenannte „End-to-End“-Verschlüsselung ist ein weitgehender Garant dafür, dass Informationen sicher zwischen einem Sender und einem Empfänger ausgetauscht werden können.

Da die Codierungsmethoden immer besser werden, kommt schnell die Frage auf, inwieweit der Staat durch die Strafverfolgungsbehörden den Datenverkehr und die Kommunikation der Bürger überwachen darf. Hier stehen sich verschiedene Meinungen gegenüber. Das Recht auf Privatsphäre einerseits und die Sicherheit der Bürger andererseits müssen hier sehr sorgfältig gegeneinander abgewogen werden.

Sicher ist aber, dass es die totale Sicherheit nicht gibt, vielleicht nie geben kann.

Günter Ganz