ZT IT-KOLUMNE

Kryptografie – Teil I

Selbstverständlich verschicken wir im Zeitalter der Informationstechnik Informationen mittels Internet von A nach B. Dabei werden die Rufe nach mehr Sicherheit und Geheimhaltung der Informationsübertragung immer lauter. Die Kryptografie spielt hier eine große Rolle und soll deshalb in einer Artikelserie genauer beleuchtet werden.

Was bedeutet der Begriff Kryptografie?

„Kryptografie" stammt aus dem Griechischen und besteht aus den Worten „kryptós" (verborgen) und „gráphein" (schreiben). Zu Beginn galt sie ausschließlich als die Wissenschaft der Informationsverschlüsselung, entwickelte sich dann jedoch weiter und beinhaltet heute hauptsächlich alle Bereiche der Informationssicherheit. Dazu gehören die Konzeption, Definition und Konstruktion von Informationssystemen, die geschützt sind gegen äußere Eingriffe und das Lesen durch unbefugte Personen. Die Kryptografie ist neben der Kryptoanalyse (auch: Kryptanalyse) ein Bestandteil der Kryptologie.

Die Kryptoanalyse beschäftigt sich nicht mit der Verschlüsselung, sondern mit der unbefugten Entschlüsselung von bereits verschlüsselten Daten. Da die Kryptografie aber ohne Kryptoanalyse wenig Sinn macht, wird zwischen Kryptologie und Kryptografie in den meisten Fällen nicht unterschieden. In der Artikelserie bleibe ich deshalb auch bei dem Begriff Kryptografie. Prinzipiell ist die Kryptografie eine Teildisziplin der Informatik, die auch IT-Sicherheit bzw. Computersicherheit genannt wird. Sie umfasst einen sehr großen Bereich.

Die Geschichte der Kryptografie

Die Kryptografie hat bereits eine lange Geschichte, jedoch konnte sie sich erst im 20. Jahrhundert zu einer streng mathematischen Wissenschaftsdisziplin entwickeln, und erst durch das Internet mit seinen vielfältigen Kommunikationsdiensten konnte die Kryptografie auch zur Anwendung gelangen.

Schon in vorchristlicher Zeit (ca. 1.500 Jahre v. Chr.) verwendeten die Mesopotamier mit Keilschrift beschriebene Tontafeln, um Botschaften zu verschleiern bzw. zu verschlüsseln. Durch Verändern der Keilschrift konnten ganz individuelle Geheimschriften erzeugt werden. Die Keilschrift war also eine der ersten primitiven Verschlüsselungstechniken, die der Mensch erfunden hat. Spartaner verwendeten für geheime militärische Botschaften im 5. Jh. v. Chr. ein Verschlüsselungsgerät namens Skytale (Abb. 1). Die Skytale war ein mit Pergament oder einem Lederband umwickelter Stab, auf den eine geheime Botschaft geschrieben wurde. Wickelt man das Pergament vom Stab wieder ab, ist der Text erst wieder lesbar, wenn man ihn um einen Stab gleichen Durchmessers wickelt. Damit war die Skytale auch das erste Verschlüsselungsgerät mit einem variablen „Schlüssel". Der Empfänger der geheimen Botschaft konnte nur mit einem Stab mit demselben Durchmesser den Text lesen. Der geheime Schlüssel bei der Skytale ist somit der Durchmesser des Stabes.

Ein weiteres sehr bekanntes kryptografisches Beispiel in der Antike ist die sogenannte Cäsar-Chiffre. Mit diesem Chiffrierverfahren kommunizierte Kaiser Julius Cäsar mit seinen Generälen. Für die Verschlüsselung von Texten wurden einfach die Buchstaben systematisch vertauscht. Die Cäsar-Chiffre gehört zu den symmetrischen Verschlüsselungsverfahren, das auf einer monografischen und monoalphabetischen Substitution basiert. Bei der Verschlüsselung wird jeder Buchstabe des Klartextes auf einen Geheimtextbuchstaben abgebildet. Die Anzahl der verschobenen Zeichen bildet den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt.

Beispiel für eine Verschiebung um drei Zeichen:

- Klar: 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
- Geheim: 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

Aus dem Klartext „caesar" wird somit der Geheimtext „FDHVDU". Für die Entschlüsselung werden die Buchstaben des Alphabets um dieselbe Anzahl Zeichen wieder nach links verschoben.

Merke: Der sogenannte Geheimtext (auch Chiffrat, Chiffre, Chiffretext, Ciphertext, Kryptogramm, Kryptotext oder Schlüsseltext) ist der Text in der Kryptografie, der so stark verändert wurde, dass er für jeden Dritten, der nicht eingeweiht ist, ein Rätsel darstellt. Es existieren zahlreiche kryptografische Verfahren und Schlüssel, mithilfe derer der Inhalt so codiert werden kann.

In der Renaissance, in der die Mathematik und Naturwissenschaften wieder auflebten, entwickelte der italienische Mathematiker, Philosoph und Komponist Leon Alberti ein interessantes Verschlüsselungsgerät, das als Vorläufer der elektromechanischen Verschlüsselungsmaschinen gilt. Die Chiffrierscheibe bestand aus zueinander verschiebbaren Ringen, auf denen Buchstaben standen. Am äußeren Rand der Scheiben waren jeweils unterschiedliche Alphabete oder Symbole angegeben. Durch Verdrehen der Scheiben gegeneinander verschoben sich diese Alphabete, was dann zur Verschlüsselung verwendet wurde.

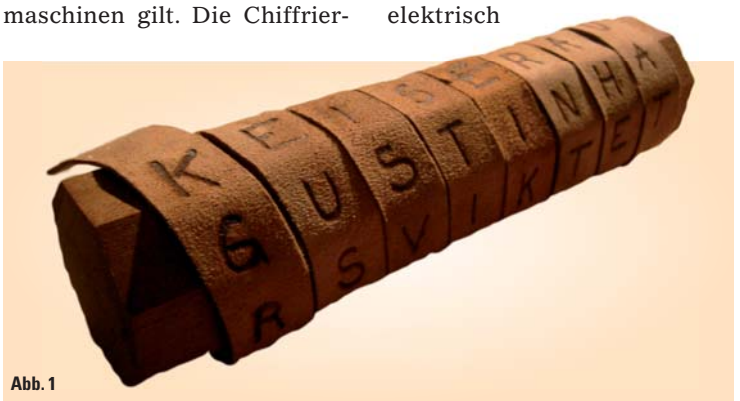

Abb. 1

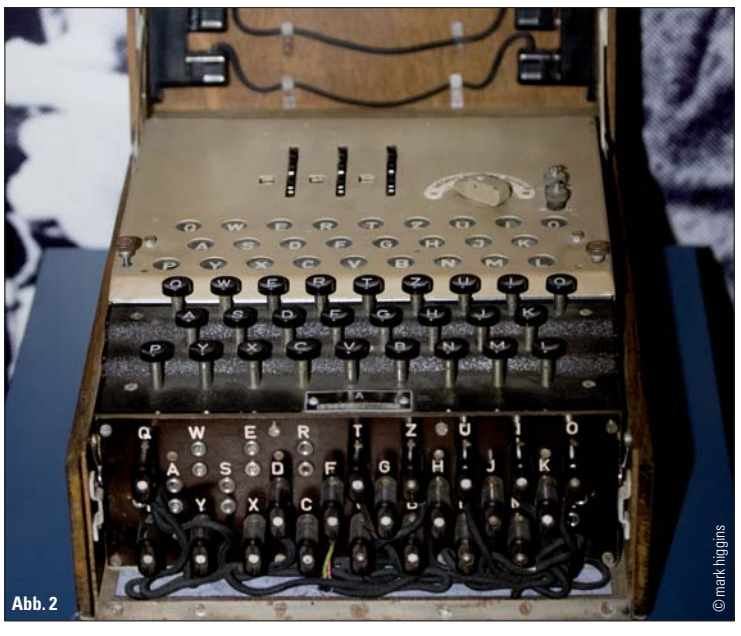

Abb. 2

Im Zweiten Weltkrieg kam dann der große Boom der Informationsverschlüsselung. Die berühmteste aller Chiffriermaschinen war wohl die legendäre Enigma (Abb. 2), mit der die deutsche Armee im U-Boot-Krieg Funksprüche verschlüsselte. Die Enigma sah fast wie eine Schreibmaschine aus. Sie hatte auch ungefähr die Größe einer Schreibmaschine und wog 20 bis 30 Kilo. Technisch gesehen gehört die Enigma zu den Rotormaschinen. Die Rotoren sind elektrisch isolierte Scheiben, die an jeder Seite eine bestimmte Anzahl von Schleifkontakten haben. Jeder Kontakt auf der einen Seite der Scheibe war mit einem Kontakt auf der anderen Seite der Scheibe verbunden.

Als Erfinder der Enigma gilt der promovierte deutsche Ingenieur Arthur Scherbius (1878–1929), dessen erstes Patent hierzu vom 23. Februar 1918. Zur Fertigung der Maschine wurde am 9. Juli 1923 die Chiffriermaschinen-Aktiengesellschaft in Berlin gegründet. Die Enigma wurde zunächst nur als ziviles Chiffriergerät gebaut und kommerziell auf Messen zum Kauf angeboten, wie auf dem internationalen Postkongress des Weltpostvereins 1923 in Bern und 1924 in Stockholm. Das weckte natürlich sofort auch das Interesse des deutschen Militärs, das eine Wiederholung der kryptografischen Katastrophe im Ersten Weltkrieg auf jeden Fall vermeiden wollte und daher diese neue Art der maschinellen Verschlüsselung als sicherste Lösung erkannte. Schätzungsweise sind im Zweiten Weltkrieg mehr als 30.000 Maschinen hergestellt worden (einige Schätzungen reichen bis 200.000 Stück). Bis zum Kriegsende 1945 und noch darüber hinaus kamen viele verschiedene Modelle und Varianten der Enigma zum Einsatz. Die meistverwendete Maschine war die Enigma I.

Erst durch die Erbeutung eines Enigma-Geräts bzw. nach dem Knacken ihrer Verschlüsselungsverfahren wurde die kriegsentscheidende Vorherrschaft der West-Alliierten im Nordatlantik möglich. In den 70er-Jahren des vorigen Jahrhunderts wurde die Kryptografie dann zu einer wissenschaftlichen akademischen Disziplin, die viele Mathematiker und Informatiker in den Bann zog. Mit der Erfindung des Computers wurde dann ein wahrer Boom in der Findung von immer raffinierteren Verschlüsselungs- bzw. Entschlüsselungsmethoden ausgelöst. Mit der immer stärkeren Verbreitung von Mobilfunktelefonie und des weiter rasant wachsenden Internetmarktes ist die Verschlüsselung heute nicht mehr wegzudenken und zu einer Basistechnologie des Informationszeitalters geworden. Mit der Entwicklung von Quantencomputern wird ein neues Zeitalter auch der Kryptologie erwartet.

Ausblick

Im nächsten Teil der Kryptografie-Serie geht es dann verstärkt in die kryptografischen Verfahren. Es wird spannend, bleiben Sie also dran. ZT

Infos zum Autor

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung
& Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft