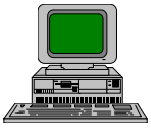

Computerunterstützte Verschlüsselung

Bei der Entschlüsselung der Enigma im Bletchley Park wurden erstmals "Computer" als Hilfsmittel eingesetzt. Die "Bomben", wie sie genannt wurden, waren zwar noch nicht Compter im heutigen Sinn sondern eher mechanische Rechenmaschinen. Sie waren aber das erste (elektrotechnische) Instrument, das den Kryptoanalytikern beim Durchprobieren der Tausenden von Möglichkeiten half. Im konkreten Fall der Enigmaentschlüsselung ging es darum viele verschiedene Walzeneinstellungen durchzutesten.

In der Folge wurden Computer nicht nur in der Gesellschaft immer wichtiger, sondern natürlich auch in der Kryptoanalyse. Werden Botschaften mit dem Computer verschlüsselt, so geht das im Prinzip genau gleich wie die mechanische Verschlüsselung z.B. mit der Enigma oder wie die manuelle Verschlüsselung. Drei Unterschiede lassen sich aber aufzeigen:

1. Eine mechanische Chiffriermaschine ist durch ihre bautechnischen Möglichkeiten beschränkt. So lassen sich beispielsweise in der Enigma nicht beliebig viele Walzen einbauen. Der Computer dagegen stellt eine hypothetische Chiffriermaschine von immenser Komplexität dar. Er kann so programmiert werden, dass die Bewegungen von hunderten von Walzen simuliert werden. Es ist sogar möglich das Programm so zu gestalten, dass einzelne Walzen sich nach einer gewissen Anzahl von Buchstaben automatisch ein- oder ausschalten.
2. Die Geschwindigkeit der computergestützten Verschlüsselung ist um Faktoren schneller als die mechanische. So kann beispielsweise eine lange Nachricht mit einem Enigma-Simulationsprogramm auf dem Computer innert Bruchteilen von Sekunden verschlüsselt werden.
3. Der wichtigste Unterschied zwischen mechanischer und computergestützter Verschlüsselung liegt darin, dass der Computer nicht Buchstaben sondern Zahlen, genauer Folgen von 0 und 1 (sog. Binärfolge) verschlüsselt. Es ist deshalb notwendig, die Buchstaben in Zahlenfolgen zu codieren.

A	1000001
B	1000010
C	1000011
D	1000100
E	1000101
F	1000110
G	1000111
H	1001000
I	1001001
J	1001010
K	1001011
L	1001100
M	1001101
N	1001110
O	1001111
P	1010000
Q	1010001
R	1010010
S	1010011
T	1010100
U	1010101
V	1010110
W	1010111
X	1011000
Y	1011001
Z	1011010

Zur Umwandlung von Buchstaben in 01-Folgen existieren verschiedene Standards. Der am häufigsten verwendete Code ist der ASCII-Code (american standard code for information interchange). Die nebenstehende Tabelle zeigt die entsprechende Zuordnung. Es handelt sich dabei nur um den Ausschnitt des Codes, der zur Codierung der Grossbuchstaben gebraucht wird. Der vollständige Code enthält ausserdem auch die Kleinbuchstaben, Zahlen, Satz- und Sonderzeichen.

Buchstaben: `OBWALDEN`

ASCII: `1001111 1000010 1010111 1000001 1001100 1000100 1000101 1001110`

Um nun die eigentliche Verschlüsselung durchzuführen müssen der Sender und der Empfänger ein Schlüsselwort abmachen (Schlüsseltauschproblem!). In unserem Beispiel nehmen wir `COMPUTER` als Schlüsselwort. Auch das Schlüsselwort wird mit dem ASCII-Code codiert und unter den (binären) Klartext geschrieben. Die Lücken zwischen den Buchstaben dient nur zur besseren Lesbarkeit.

```
OBWALDEN:   1001111 1000010 1010111 1000001 1001100 1000100 1000101 1001110
COMPUTER:   1000011 1001111 1001101 1010000 1010101 1010100 1000101 1010010
Geheimtext: 0001100 0001101 0011010 0010001 1011001 0010000 0000000 0011100
```

Der Geheimtext entsteht durch Vergleichen der jeweils darüberstehenden Ziffern des Klartextes und des Schlüssels. Unterscheiden sich die Ziffern nicht, so wird eine 0 geschrieben. Unterscheiden sie sich, so schreibt man eine 1.

Diese Art des Vergleichens kann auch als Addition aufgefasst werden, wobei kein Stellenübertrag stattfindet. Sie empfiehlt sich deshalb, weil elektrische Schaltungen, die eine solche (binäre) Addition durchführen einfach zu realisieren sind.

Der erhaltene Geheimtext wird nun zum Computer des Empfängers gesendet und dort entschlüsselt. Neben dem Problem, dass der Sender und der Empfänger den Schlüssel vorgängig miteinander abmachen müssen existiert zusätzlich das Problem der Datenübertragung. Alle Leitungen zum Übertragen von Daten haben eine gewisse Fehlerwahrscheinlichkeit. Es kann also vorkommen, dass eine gesendete 1 als 0 beim Empfänger eintrifft oder umgekehrt. Die Informatik hat Lösungen für dieses Problem geschaffen. Es existieren sogenannte fehlererkennende und sogar fehlerkorrigierende Codes. Da sie nur indirekt mit der Datenverschlüsselung zu tun haben, werden wir in der Folge nicht tiefer darauf eingehen.

Man beachte, dass mit der computerunterstützten Verschlüsselung die Problematik des Schlüsseltausches von wesentlich grösserer Bedeutung ist als zu Zeiten Caesars oder Vigenères. Bereits mit der Enigma im zweiten Weltkrieg nahm die Wichtigkeit des Problems zu, mussten doch U-Boot die längere Zeit unterwegs waren vorgängig mit den Tagesschlüsseln für die ganze Reise ausgerüstet sein. Einem U-Boot auf hoher See ein neues Codebuch zukommen zu lassen ist logistisch nicht ganz einfach.

Sitzen nun Sender und Empfänger über die ganze Welt verteilt, wie es heute bei der globalen Vernetzung der Fall ist, so ist es schlicht und einfach unmöglich, dass Sender und Empfänger den Schlüssel persönlich miteinander austauchen. Über ihre Datenleitung können sie es auch nicht tun, dann wenn ein Spion in der Datenleitung ausgerechnet den Schlüssel herauspicken könnte, dann wäre die ganze folgende Verschlüsslung überflüssig.

Für Interessierte sei hier noch auf den DES (data encrypting standrad) hingewiesen. Es handelt sich hierbei um einen in den 70er Jahren von IBM entwickelten Standard, der immer noch angewendet wird. DES ist eine symmetrische Verschlüsselung und basiert auf der oben geschilderten Vorgehensweise, welche aber mehrfach angewendet wird. (vgl. weiterführende Links)

Weiterführende Links (19.11.06)

http://www.ib.hu-berlin.de/~mh/gedv/ascii.htm

http://www-lehre.informatik.uni-osnabrueck.de/~rspier/referat/internet/DES-Algorithmus.html

http://members.chello.at/s.peer/

http://de.wikipedia.org/wiki/Data_Encryption_Standard