3.3.5 Das Binärsystem

Das Binär- bzw. Dualsystem ist ein Zahlensystem, welches zur Darstellung von Zahlen nur die Ziffern 0 und 1 verwendet. Jeder Computer nutzt dieses System, da dieser nur zwischen den Zuständen „an“ und „aus“ (zugeordnet den Werten 0 und 1) unterscheiden kann. Welcher der beiden Zustände gerade vorliegt, wird in einem *Bit* (=kleinste Informationseinheit, welche den Wert 0 oder 1 hat) gespeichert. Mit einem Bit lassen sich also 2 ($=2^1$) Zustände darstellen. Dementsprechend können mit zwei Bits 4 ($=2^2$) Zustände, mit drei Bits 6 (2^3) Zustände usw. verwirklicht werden.
Damit wir als Mensch mit dem Computer kommunizieren können, müssen die uns geläufigen Zeichen (Buchstaben, Zahlen usw.) in das Binärsystem „übersetzt“ werden. Beschränken wir uns hierbei auf das großgeschriebene Alphabet, so reicht schon ein 5-Bit-System ($2^5 = 32$ mögliche Zustände) aus, um alle Buchstaben ins Binärsystem zu übertragen. Eine mögliche Zuordnung ist in Tabelle 5 zu sehen.

Bitfolge	00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010
Zeichen	A	B	C	D	E	F	G	H	I	J	K
Bitfolge	01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101
Zeichen	L	M	N	O	P	Q	R	S	T	U	V
Bitfolge	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111	
Zeichen	W	X	Y	Z	Zur freien Verfügung						

Tabelle 5

Somit können ganze Wörter bzw. Sätze durch eine Folge von 0 und 1 dargestellt werden. Diese „Übersetzung“ ins Binärsystem reicht als sichere Verschlüsselung einer Nachricht natürlich nicht aus. Es wird ein Schlüssel - ebenfalls eine Folge aus 0 und 1 - benötigt. Die Zahlenfolge muss dabei mindestens so lang sein, wie die zu verschlüsselnde Nachricht in ihrer binären Darstellung. Die binäre Darstellung im untenstehenden Beispiel (siehe Tab. 6) besteht aus insgesamt 25 Ziffern. Dementsprechend muss der Schlüssel ebenfalls mindestens 25 Ziffern lang sein. Außerdem sollte der Schlüssel zufällig generiert sein und immer nur einmal verwendet werden (Merkmale eines sog. One-Time-Pad), um die Sicherheit der Verschlüsselung zu erhöhen.
Liegen nun Schlüssel und Nachricht in binärer Darstellung vor, erfolgt die eigentliche Verschlüsselung durch Addition der einander entsprechenden Elemente beider Zahlenfolgen. Das heißt, die erste Ziffer der Nachrichtenfolge wird zu der ersten Ziffer der Schlüsselfolge addiert und ergibt so die erste Ziffer in der Folge der codierten Nachricht. Ebenso wird für alle weiteren Elemente der Folgen verfahren.
Damit als verschlüsselte Nachricht wieder eine Folge von 0 und 1 entsteht, ist die Addition in diesem Falle wie folgt definiert:

Binäre Addition $\quad 1+0=1 \;\; ; \;\; 0+1=1 \;\; ; \;\; 0+0=0 \;\; ; \;\; 1+1=0$

Beispiel

Nachricht	H	A	L	L	O
binäre Darstellung	00111	00000	01011	01011	01110
Schlüssel	11110	11001	11110	11010	01010
verschlüsselte Nachricht	11001	11001	10101	10001	11100

Tabelle 6