LU05a - Kryptographie Basics

Lernziele

1. Die Begriffe Kodierung und Verschlüsselung erklären und unterscheiden können.
2. Wichtige kryptographische Begriffe nennen und in eigenen Worten erklären können.
3. Die „Maxime von Kerhoff“ erläutern und Bezug auf die Gegenwart nehmen können.
4. die drei Verschlüsselungsarten/-varianten erläutern können.

1. Von der Codierung zur Verschlüsselung

1.1 Codierung

Sie haben gelernt, wie alltägliche Informationen wie Buchstaben, Zahlen, Pixel oder Töne digitalisiert werden. Beispielsweise wird einem Buchstaben ein Dezimal-Zahlenwert zugewiesen, welcher dann ins duale Zahlensystem überführt, und so auf einen Datenträger mit Nullen und Einsen gespeichert werden kann. Übersetzungen von einer Sprache in eine andere Sprache funktionieren nach dem gleichen Prinzip: das Deutschen Wort *ja* wird beispielsweise das Französische Wort *Oui* übersetzt.

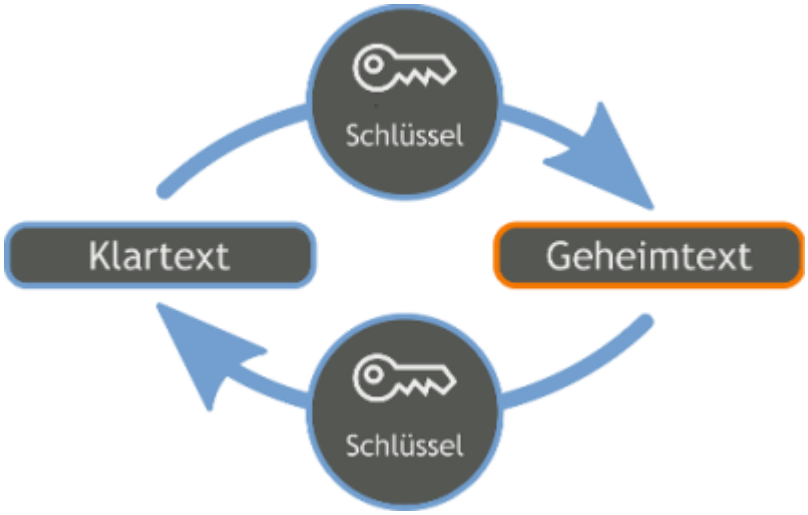
Bei Sprachen-Übersetzungen wird ein Wörterbuch verwendet. Um Zahlen vom dezimalen ins duale/binäre Zahlensystem überführen zu können, benötigen wir eine Rechenvorschrift. Dieses *Kochrezept* der Konversion (Zeichen aller Art) ist offen zugänglich und daher für alle nachvollziehbar. **Das Verfahren ist also allen grundsätzlich bekannt**.

LSB	MSB							
Binär	000	001	010	011	100	101	110	111
	Steuerzeichen				Großbuchstaben		Kleinbuchstaben	
0000	NUL	DLE	SP	0	@	P		p
0001	SOH	DC1	!	1	A	Q	a	q
0010	ATX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EOT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	`	7	G	W	h	w
1000	BS	CAN	(	8	H	X	g	x
1001	HAT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	^	n	~
1111	SI	US	/	?	O		o	DEL

Freiwillig: Studyflix-Video ASCII-Code

1.2 Verschlüsselung

Gemäss Definition heisst Kryptographie übersetzt Verschlüsselung bedeutet nichts anderes als, dass diese Rechenvorschrift nicht-autorisierten gegenüber geheim gehalten wird. D.h. eine Nachricht wird mit einem **geheimen «Regelwerk** in eine andere Darstellung gebracht, sodass die Nachricht in verschlüsselter Form nicht lesbar ist. Sie kann erst wieder mit einer passenden **Gegen-Regelwerk** entschlüsselt werden.



1.3 Kryptologie

Die Kryptologie hingegen beschäftigt sich mit Fragen der Geheimhaltung von Nachrichten. Sie ist unterteilt in zwei sich *befeindende* Teilgebiete:

- Die **Kryptograhie** versucht eine kryptologische Sicherheit zu erlangen, welche nicht geknackt werden kann wie der Geheimhaltung der Geheimnachricht (Angriff)
- Die **Kryptoanalyse** beschäftigt sich wissenschaftlich damit, kryptographische Verfahren zu knacken, also mit der Offenlegung einer Geheimnachricht (Verteidigung)
