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.

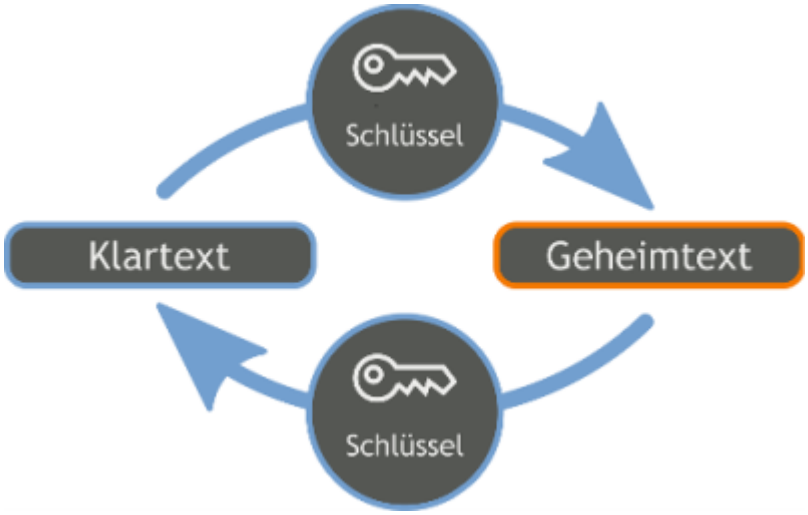
Bei Sprachen-Übersetzungen wird ein Wörterbuch verwendet. Um Zahlen vom dezimalen ins duale/binäre Zahlensystem überführen zu können, benötigen wir eine Rechenvorschrift. Dieses *Kochrezept* der Konversion (Zeichen aller Art) ist offen zugänglich und daher für alle nachvollziehbar. **Das Verfahren ist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

2. Begriffe

Die nachfolgenden Begriffe werden in der Krypto-Szene verwendet, wobei Sie zum Teil eine etwas andere Bedeutungen als in der normalen Sprache haben können:

- **Plaintext**: Auch *Klartext* oder *dechiffrierter Text* genannt. Sie ist die Informationen, die geheim transportiert werden sollen. Ist der Ursprungstext für die Verschlüsselung bzw. das Ergebnis der Entschlüsselung.
- **Ciphertext**: Auch *chiffrierter Text* oder „verschlüsselte Text“ genannt. Enthält die verschlüsselten Informationen, also das Ergebnis der Verschlüsselung.
- **Schlüssel** bzw. **Key**: Bezeichnet das Element, das zur Ver- und Entschlüsselung verwendet wird.
- **Code**: Wörter oder Sätze des Klartextes werden durch andere Wörter oder Buchstabenfolgen, unter Verwendung eines Codebuches, ersetzt.
- **Konfusion**: Der Zusammenhang zwischen Plaintext und Ciphertext wird verwischt.
- **Diffusion**: Die Information des Plaintext wird über weite Teile des Ciphertextes verteilt.

- **Umkehrbarkeit**: Die Verschlüsselung muss unter Verwendung des beim Verschlüsseln angewandten Schlüssels wieder umkehrbar sein.

3. Kryptographie

Durch die Verbreitung des Internets erlangten kryptografische Verfahren, welche früher vor allem im militärischen Bereich eingesetzt wurden, auch eine grosse Bedeutung für Private. Ein Überbleibsel an frühere *kalter Krieg*-Zeiten ist, dass bis vor wenigen Jahren in den USA kryptographische Verfahren unter das Kriegsmaterialgesetz fielen und nicht exportiert werden durften.

3.1 Ziele

Kryptografische Verfahren werden eingesetzt, um zwei Ziele zu erreichen:

1. **Vertraulichkeit**: Es soll nicht beteiligten-Personen verunmöglicht werden, eine geheime Nachricht zu lesen.
2. **Authentizität**: Es soll nicht beteiligten-Personen verunmöglicht werden, eine Nachricht zu verfälschen, ohne dass dies bemerkt wird.

3.2 Die drei Dimensionen der IT-Sicherheit = CIA-Triad

Mögliche Angreifer eines IT-Systems haben es grundsätzlich auf mindestens eine der nachfolgenden Dimensionen der IT-Sicherheit abgesehen.

1. **Verfügbarkeit**: Ein Computersystem muss dann verfügbar sein, wenn es gebraucht wird. Angriffe zielen darauf diese Verfügbarkeit zu reduzieren oder zu zerstören.
2. **Vertraulichkeit**: Informationen sollten nicht an unberechtigte Personen weitergeben werden. Angreifer möchte genau an solche Informationen (beispielsweise Passwörter, Gesundheitsdate, etc.) herankommen, um den Informationseigentümern Schaden zuzufügen.
3. **Integrität**: Informationen sollen beispielsweise zwischen Sender und Empfänger nicht verändert werden. Vor allen nicht dann, wenn der Sender nichts davon weiss. Das Ziel eines Angriffes ist die Vertrauens- und/oder Glaubwürdigkeit des Senders zu reduzieren oder zu zerstören.

3.3 Prinzipien

Bis in die 1990er Jahre wurde noch oft versucht, Geheimhaltung dadurch zu erreichen, in dem der Verschlüsselungsalgorithmus verheimlicht wurde. 1995/6 wurde dann der bis dahin als sicher geltende40 Bit-SSL-Verschlüsselung des Netscape Navigator vom CCC (Chaos Computer Club) geknackt. Dies wurde erreicht, indem der zugrunde liegenden Zufallszahlen-Generator nachgebaut werden konnte. Das Super-Sichere-Verfahren war also offengelegt.

Spannend, dass führende Kryptologen dies schon einige Zeit vor 1990 gewusst haben:

Shannon's Maxime [US Kryptologe 1916 – 2001]:
«Der Feind kennt das System (Verfahren).»

Kerckhoff's Maxime [Niederländischer Kryptologe 1835 – 1903]:
«Die Sicherheit eines kryptographischen Verfahrens beruht alleine auf dem Schlüssel, der zum Dechiffrieren benötigt wird.»

Alle aktuell in der Praxis eingesetzten Verschlüsselungsverfahren sind gut und ausführlich beschrieben. Dadurch sind sie auch um Grössenordnungen besser getestet als proprietäre Mechanismen. Das Verschlüsselungsverfahren ist daher sehr bekannt und kein Garant für die Geheimhaltung von Nachrichten.

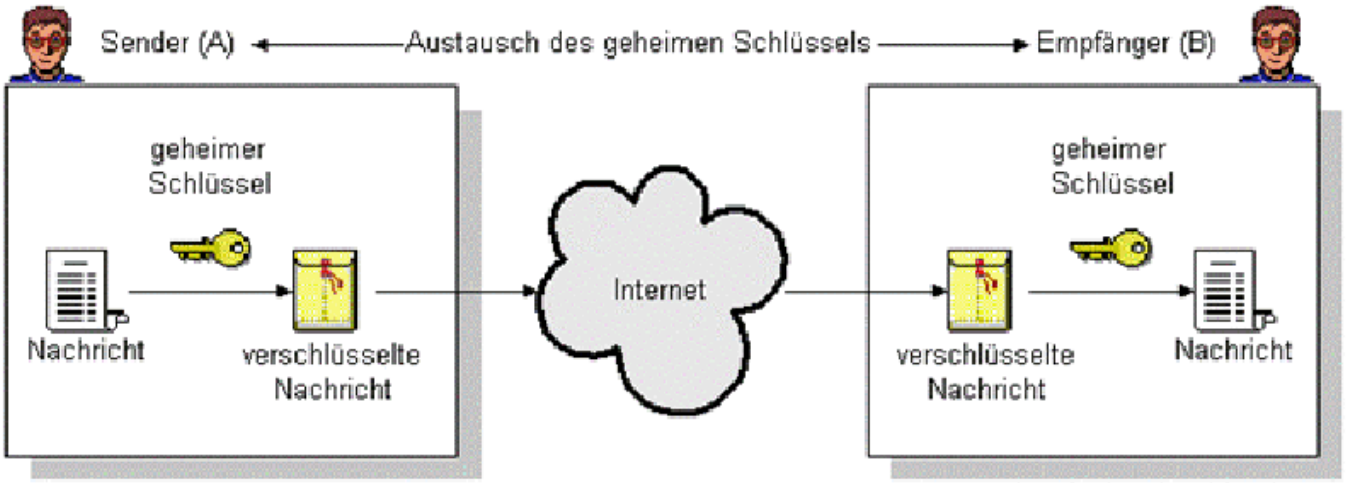
Merke: Wenn also gemäss Shannon das Verschlüsselungsverfahren bekannt ist und gemäss Kerckhoffs Maxime der Schlüssel der einzige Garant für die Sicherheit ist, dann ist es umso wichtiger, dass dieser selbst strikt geheim bleibt. D.h. je länger und komplizierter der Schlüssel, desto sicher ist die Nachricht.

4. Varianten der Kryptographie/Verschlüsselung

Grundsätzlich gibt es 2 Varianten der Verschlüsselung: die **symmetrische** und **asymmetrische Verschlüsselung**. Die hybride Verschlüsselung ist eine Kombination der beiden Verfahren.

4.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung handelt es sich um die älteste Methode Informationen zu verschlüsseln. Dabei wird zum Ver- und Entschlüsseln derselbe Schlüssel verwendet.

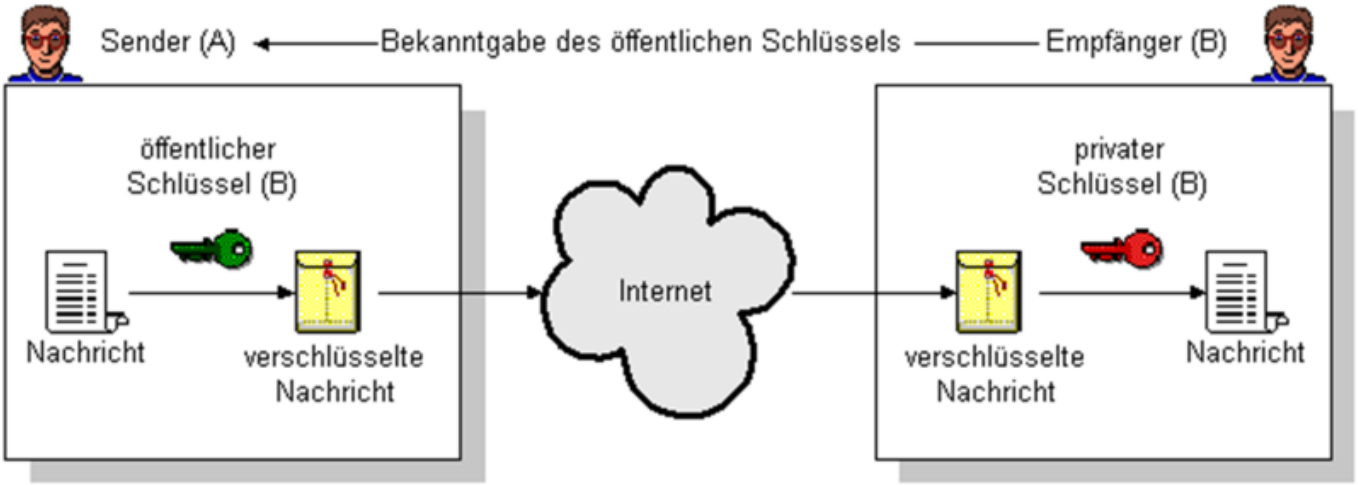


Der Nachteil dieses Verfahrens ist, dass der Schlüssel geheim gehalten werden bzw. auf einem sicheren Weg dem Kommunikationspartner zugestellt werden muss. Ein weiteres Problem stellt die Anzahl der Schlüssel dar, da praktisch für jeden Kommunikationspartner ein eigener Schlüssel angelegt werden muss.

Studyflix: Die symmetrische Verschlüsselung

4.2 Die Asymmetrische Verschlüsselung

1978 bewiesen die Mathematiker Rivest, Shamir und Adleman am MIT mit dem nach ihnen benannten RSA-Algorithmus, dass es möglich ist, bei der Verschlüsselung mit zwei unterschiedlichen Schlüsseln zu arbeiten. Bei dieser asymmetrischen Verschlüsselung (Public Key Verschlüsselung) genannt, wird ein Schlüsselpaar erstellt. D. h. zwei Schlüssel, die eine gemeinsame mathematische Basis (z. B. Primzahl mit 200 Dezimalstellen) haben. Einer dieser Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet. Keiner der Schlüssel kann, trotz mathematischer Basis, aus dem anderen hergeleitet werden. Der Schlüssel, der zur Verschlüsselung verwendet wird, kann daher beliebig verbreitet und sogar in eigenen Verzeichnissen (Schlüsselserver) hinterlegt werden. Man spricht daher auch vom öffentlichen Schlüssel (public key). Der zur Entschlüsselung verwendete private Schlüssel (private key) bleibt hingegen in der Obhut des Empfängers.



Studyflix: Die asymmetrische Verschlüsselung