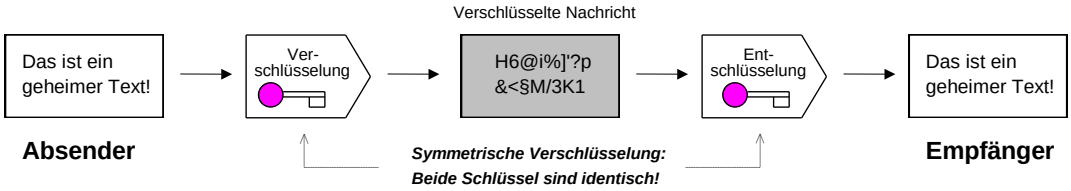
1. Verschlüsselungsverfahren

Definition Verschlüsselung

Unter Verschlüsselung versteht man Verfahren und Algorithmen, die Daten (Klartext) mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form (Geheimtext) umwandeln. Diesen Vorgang bezeichnet man als Verschlüsseln. Gleichzeitig wird dafür gesorgt, dass nur mit dem Wissen eines Schlüssels die geheimen Daten wieder entschlüsselt werden können. Anstatt von Verschlüsselung spricht man auch von Chiffrierung, was das gleiche meint. Ein Verschlüsselungsverfahren besteht somit aus einem Algorithmus zum Verschlüsseln und Entschlüsseln, sowie Verfahren zum Schlüsselaustausch.
Grundsätzlich wird zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden. Die Klassifikation erfolgt anhand der Schlüsselhandhabung.

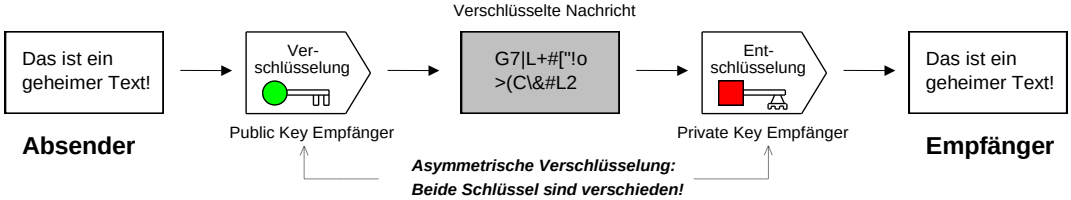
Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung kommt ein und derselbe Schlüssel sowohl zur Chiffrierung als auch zur Dechiffrierung verschlüsselter Daten zum Einsatz. Möchten zwei kommunizierende Parteien verschlüsselte Daten austauschen, muss ein Weg gefunden werden, auch den gemeinsamen Schlüssel geheim zu übermitteln. Beispiele: AES, DES usw.



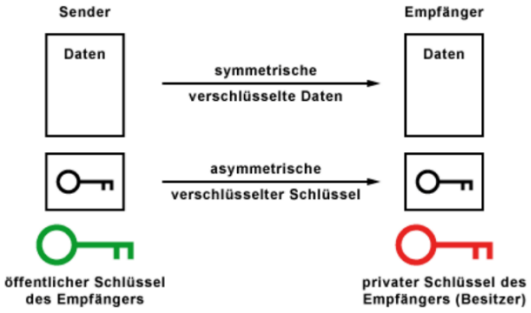
Asymmetrische Verschlüsselung

Kennzeichen der asymmetrischen Verschlüsselung ist, dass zur Verschlüsselung ein völlig anderer Schlüssel als zur Entschlüsselung benutzt wird. Man unterscheidet hier zwischen dem „öffentlichen Schlüssel“, der zum Verschlüsseln benutzt wird, und dem „privaten Schlüssel“ zum Entschlüsseln des Geheimtextes. Man spricht von einem Public-Key-Verfahren. Der private Schlüssel bleibt dabei geheim. Beispiele: RSA, PGP usw.



Hybrid-Verschlüsselung

Die Hybrid-Verschlüsselung verwendet beide Verschlüsselungsverfahren. Sie setzt ein asymmetrisches Verfahren für den Schlüsselaustausch ein und verschlüsselt die Datenübertragung mit einem symmetrischen Verfahren. Ziel dieser Kombination ist es, die Schwächen des einen Systems durch die Stärken des anderen zu kompensieren. Sie werden daher häufig in einem kryptografischen Protokoll (SSL/TLS, SSH usw.) eingesetzt werden.



Arbeitsauftrag 1:

Beantworten Sie folgende Fragen!

Beschreiben Sie den Unterschied von symmetrischer und asymmetrischer Verschlüsselung!

Symmetrisch: gleicher Schlüssel zur verschlüsselung und entschlüsselung

Asymmetrisch: verschiede Schlüssel zum entschlüsseln und verschlüsseln

Nennen Sie Vor- und Nachteile der symmetrischen Verschlüsselung!

Vorteil: Schneller

Nachteil: Jede Kommunikation braucht ein paar an Schlüsseln

Nennen Sie Vor- und Nachteile der asymmetrischen Verschlüsselung!

Vorteil: Private Schlüssel müssen nicht übertragen werden -> Sicherer

Nachteil: Deutlich mehr Aufwand für Verschlüsselung und Entschlüsselung

Beschreiben Sie den wesentlichen Vorteil hybrider Verschlüsselungsverfahren!

Vorteil: Schnelligkeit der symmetrischen und Sicherheit der asymmetrischen Verschlüsselung

2. Ausgewählte praktische Verschlüsselungsverfahren

Cäsar-Verschlüsselung

Der römische Staatsmann und Feldherr Gaius Julius Caesar (100 - 44 v. Chr.) verwendete manchmal in seinen Briefen, wenn er Informationen geheim halten wollte, die folgende Verschlüsselungsmethode, die heute auch Caesar-Verschlüsselung genannt wird. Es handelt sich um eine spezielle Substitution, bei der also die Buchstaben des Klartextes einzeln durch die Buchstaben des Geheimtextes ersetzt werden. Bei der Caesar-Verschlüsselung wird jeder Buchstabe der Nachricht um eine bestimmte Zahl im Alphabet weitergeschoben. Diese Zahl ist der geheime Schlüssel.

Beispiel:

Das Wort „CAESAR“ soll mit dem Schlüssel „3links“ in einen verschlüsselten Geheimtext umgewandelt werden. Dadurch verschiebt sich das Alphabet um 3 Stellen nach links:

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
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

Dadurch wird aus dem Wort „CAESAR“ der verschlüsselte Geheimtext „FDHVDU“!

Arbeitsauftrag 2:

Verschlüsseln Sie mithilfe der Caesar-Verschlüsselung Ihren eigenen Namen!

Verwenden Sie dazu den geheimen Schlüssel „3links“!

PDULXV URVVJRWWHUHU

Dechiffrieren (entschlüsseln) Sie folgenden Geheimtext: „VBPPHWULVFKHV YHUIDKUHQ“

Der geheime Schlüssel ist „3links“.

Symmetrisches Verfahren

Beschreiben Sie, um welche Art von Verschlüsselungsverfahren es sich bei der Cäsar-Verschlüsselung handelt!

Symmetrisch

Beschreiben Sie, ob die Caesar-Verschlüsselung eine geeignete technische Maßnahme ist!

Nein, viel zu einfach zu entschlüsseln