LU06b - Verschlüsselung

Siehe http://de.wikipedia.org/wiki/Verschl%C3%BCsselung und https://www.cryptool.org/de/cryptool-online

Einführung

Die Verschlüsselung von Daten (Kryptologie) will verhindern, dass fremde Personen die Daten lesen können. Bereits in der Antike wurden verschiedene Verfahren zur Verschlüsselung entwickelt. Heute werden Daten für die Übermittlung (z.B. eMail) und zur Aufbewahrung verschlüsselt.

Im Gegenzug versucht ein Angreifer, die geheimen Daten zu entschlüsseln (Kryptoanalyse).

Begriffe

Kryptologie

Kryptologie ist die Wissenschaft der Informationssicherheit. Sie lässt sich in die beiden Teile **Kryptographie** und **Kryptoanalyse** unterteilen.

Kryptographie

Kryptographie befasst sich mit der Verschlüsselung von Daten. Dabei werden Verfahren entwickelt um Daten sicher und effizient zu verschlüsseln.

Kryptoanalyse

Die Kryptoanalyse versucht die verschlüsselten Daten zu entschlüsseln. Die Methoden der Kryptoanalyse werden eingesetzt um kryptographische Verfahren zu analysieren.

- Entweder um ein Verschlüsselungsverfahren zu brechen (zu umgehen). Dadurch wird es möglich, die Daten zu entschlüsseln.
- Oder um die Sicherheit eines Verfahrens zu prüfen bzw. zu messen. Damit lassen sich Aussagen über die Sicherheit einer Verschlüsselung machen.

Brute force

Der Angreifer versucht mit „roher Gewalt“ den Schlüssel zu knacken. Dazu wird er einfach solange unterschiedliche Schlüssel ausprobieren, bis einer passt.

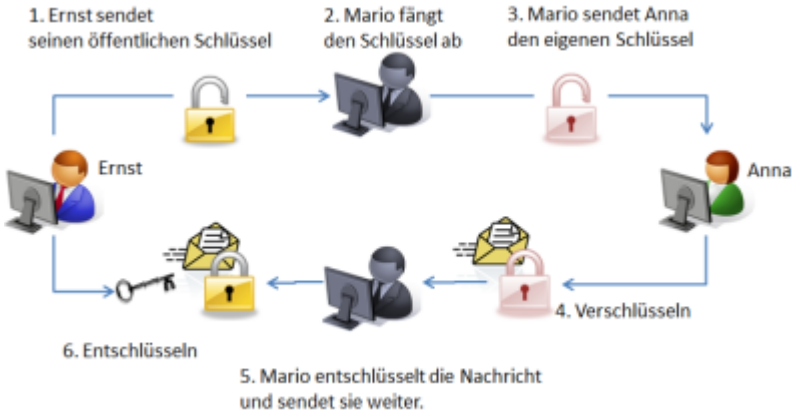
Mittels brute force lässt sich theoretisch jede bekannte Verschlüsselung knacken. Allerdings steigt der

Zeit- und Kostenaufwand bei einem starken Schlüssel sehr schnell an. Was nützt es, eine Datei zu knacken, deren Inhalt völlig veraltet ist.

Zum Beispiel: 200 Jahre nach meinem Tod darf jemand gerne meinen Schlüssel knacken.

Man-in-the-middle

Der „Mann in der Mitte“ versucht gar nicht erst, einen Schlüssel zu knacken. Stattdessen fängt er den Schlüssel ab und ersetzt ihn durch seinen eigenen. Damit verschlüssle ich meine Daten unwissentlich mit dem Schlüssel des Angreifers.



In der Grafik gibt Mario (man in the middle) seinen eigenen Schlüssel an Anna (Absenderin). Nun kann Mario die Nachricht entschlüsseln und lesen. Verschlüsselt Mario die Nachricht anschliessend mit dem öffentlichen Schlüssel von Ernst (Empfänger), so bleibt sein Eingreifen völlig unerkannt.

Steganographie

Bei der Steganographie geht es darum, die Übermittlung der Daten zu verstecken. Ein Angreifer soll nicht erfahren, dass überhaupt eine Nachricht verschickt wurde. Dazu tarnt man oft die eigentliche Nachricht als Teil einer anderen Datei.

Zum Beispiel wird die Nachricht in den Farbinformationen eines Bildes versteckt. Niemand wird bemerken, dass der Blauanteil des Himmels an einigen Stellen 1/256tel mehr oder weniger ist.

Verschlüsselungsverfahren

Substituationsverfahren

Beim Substituationsverfahren werden die Buchstaben durch andere Buchstaben oder Symbole ersetzt. Im einfachsten Fall werden einfach Buchstaben des Alphabeths vertauscht:

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Jeder Buchstabe wird mit dem anderen Buchstaben in der gleichen Spalte vertauscht. **D** ⇒ **W** oder **R** ⇒ **I**

Transpositionsverfahren

Beim Transpositionsverfahren wird die Reihenfolge der Buchstaben verändert. Damit der Empfänger die Nachricht rekonstruieren kann, muss diese Umstellung der Reihenfolge nach vorher definierten Regeln erfolgen.

Klartext

Die unverschlüsselte Nachricht ist der Klartext. Der Klartext kann von Menschen gelesen und verstanden werden.

Chiffretext

Die verschlüsselte Nachricht wird als Chiffretext bezeichnet. Der Chiffretext muss zunächst entschlüsselt werden, damit die Nachricht wieder Sinn macht.

Verschlüsselungsverfahren

Das Verfahren beschreibt, wie der Klartext in den Chiffretext umgewandelt wird. Moderne Verfahren beschreiben sehr komplexe Berechnungen für die Umwandlung.

Schlüssel

Die meisten Verschlüsselungsverfahren verwenden einen Schlüssel. Der Schlüssel ist ein wichtiger Teil der Berechnungen und beeinflusst das Resultat. Obwohl verschiedene Personen das gleiche, standardisierte Verfahren verwenden, entstehen durch den Schlüssel völlig unterschiedliche Chiffre.

Private Key

Der persönliche Schlüssel erlaubt bei einem Public Key-Verfahren das Entschlüsseln des Chiffretext. Dieser Schlüssel darf niemals weitergegeben werden. In der Regel ist der Schlüssel zusätzlich mit einem Passwort-Text geschützt.

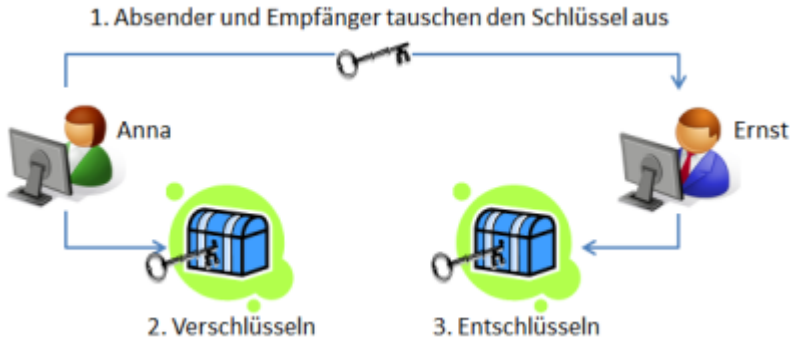
Public Key

Beim Public Key-Verfahren wird dieser Schlüssel zum Verschlüsseln benutzt. Diesen Schlüssel können Sie öffentlich machen und mit jeder interessierten Person teilen.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel zum verschlüsseln und entschlüsseln eingesetzt. Daher müssen Sender und Empfänger zunächst den Schlüssel auf einem sicheren Weg austauschen.

Sinnbild



Anna und Ernst verpacken Ihre Nachricht in eine Truhe mit einem Schloss. Beide verfügen über einen Schlüssel um das Schloss zu öffnen bzw. zu schliessen.

Asymmetrische Verschlüsselung

Bei diesen Verfahren verfügt der Empfänger über zwei unterschiedliche Schlüssel:

- Privater Schlüssel zum Entschlüsseln der Nachricht.
- Öffentlicher Schlüssel zum Verschlüsseln der Nachricht.

Der Sender benötigt den öffentlichen Schlüssel des Empfängers. Mit dem öffentlichen Schlüssel kann der Sender die Nachricht verschlüsseln. Zum Entschlüsseln wird der private Schlüssel, den hoffentlich nur der Empfänger kennt, benötigt.

Sinnbild

Ernst (der Empfänger) hat sich ein Vorhängeschloss mit Schlüssel gekauft. Er übergibt an Anna (die Absenderin) sein Vorhängeschloss. Nun kann Anna die Nachricht mit dem Vorhängeschloss sichern. Nur mit dem Schlüssel kann das Vorhängeschloss wieder geöffnet werden.

Beispiele für Symetrische Verschlüsselungsverfahren

Im Kapitel LU05c - Verschlüsselungsverfahren finden Sie eine Auswahl an Beispielen für verschiedene Verschlüsselungsverfahren.

---

m114-A0G