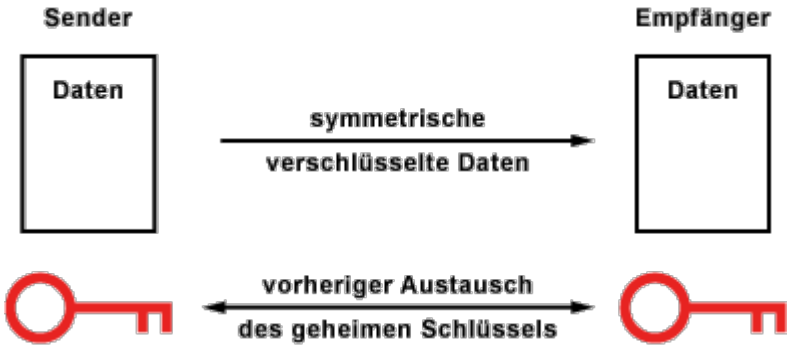
Symmetrische Kryptografie/Verschlüsselung

Die Verschlüsselungsverfahren, die mit einem geheimen Schlüssel arbeiten, der zum Ver- und Entschlüsseln dient, nennt man symmetrische Verfahren oder Secret-Key-Verfahren. Üblich sind auch die Bezeichnungen Secret-Key-Kryptografie und Secret-Key-Verschlüsselung. Fast alle symmetrischen Verfahren sind auf ressourcenschonende Umgebungen optimiert. Sie zeichnen sich durch geringe Hardwareanforderungen, geringen Energieverbrauch und einfache Implementierung in Hardware aus.

Prinzip



Die Verschlüsselungsverfahren der symmetrischen Kryptografie arbeiten **mit einem einzigen Schlüssel**, der bei der Ver- und Entschlüsselung vorhanden sein muss. Diese **Verfahren sind schnell** und bei entsprechend **langen Schlüsseln bieten sie auch eine hohe Sicherheit**.

Der **Knackpunkt liegt in der Schlüsselübergabe** zwischen den Kommunikationspartnern. Vor der sicheren Datenübertragung mit Verschlüsselung müssen sich die Kommunikationspartner auf den Schlüssel einigen und austauschen. Wenn der Schlüssel den selben Kommunikationspfad nimmt, wie die anschließend verschlüsselten Daten, dann besteht die Gefahr, dass ein Angreifer in Besitz des Schlüssels gelangt, wenn er die Kommunikation abhört. Wenn der Angreifer den Schlüssel hat, dann kann er nicht nur die Daten entschlüsseln, sondern auch selber Daten verschlüsseln, ohne das es die Kommunikationspartner bemerken. Knackpunkt ist der unsichere Schlüsselaustausch und die Authentifizierung der Kommunikationspartner.

Sicher ist die Schlüsselübergabe nur dann, wenn sich zwei Personen persönlich treffen und den Schlüssel austauschen oder der Schlüssel einen anderen Weg nimmt (Seitenkanal), wie es die Daten tun. Ein Möglichkeit wäre der postalische Weg (Brief, Einschreiben mit Rückschein). Allerdings nicht per E-Mail (Postkarten-Effekt). Zur Unsicherheit trägt außerdem bei, wenn einer der Kommunikationspartner den Schlüssel nur ungenügend sicher aufbewahrt.

Der sichere Schlüsselaustausch ist eines der vielen Probleme der Kryptografie. Mit der asymmetrischen Kryptografie versucht man dieses Problem zu lösen. Weil die asymmetrische Kryptografie weit komplexere Verfahren umfasst, kombinieren die übliche kryptografischen Protokolle sowohl symmetrische als auch asymmetrische Verfahren.

Vorteile

- Gleicher Schlüssel zum Verschlüsseln und Entschlüsseln
- Je zwei Teilnehmer benötigen einen Schlüssel
- Beide müssen den Schlüssel stets geheim halten
- Anzahl der Schlüssel wächst quadratisch mit der Teilnehmerzahl

Nachteile

- Sichere Verteilung des Schlüssels (Telefon, schriftlich,…)
- Nicht geeignet für Digitale Signatur

Symmetrische Verschlüsselungsverfahren

Jede symmetrische Verschlüsselung basiert auf einem bestimmten Algorithmus. Bei einem Verschlüsselungsalgorithmus bzw. Chiffre wird in den Klartext eine Geheiminformation, den Schlüssel, eingebracht und so der Geheimtext gebildet. Der Schlüssel kann ein Passwort, eine geheime Nummer oder auch nur eine zufällige Bitfolge sein.

Monoalphabetische Substitutionschiffren

Die einfachste Art der Verschlüsselung erreicht man, in dem man jeden Buchstaben ein festes Symbol zuordnen. Diese Verfahren sind monoalphabetisch. Sie sind bei genügend Verschlüsselungsmaterial leicht durch eine Häufigkeitsanalyse zu brechen. In jeder Schriftsprache kommen bestimmte Buchstaben häufiger vor. Man kann also mit einfachen statistischen Mitteln eine Kryptoanalyse machen. Mit Computer-Unterstützung geht es automatisch und noch schneller.

- 8.1.2.1.1) Cäsar-Chiffre

Polyalphabetische Substitutionschiffren

Wesentlich schwieriger sind polyalphabetische Geheimtexte. Hier kann ein Buchstabe mehreren Symbole entsprechen. Statistische Verfahren funktionieren hier nicht mehr so einfach.

- 8.1.2.1.2) Vigenere-Chiffre
- 8.1.2.1.3) One Time Pad (Vernam-Chiffre)

Permutationschiffren

Eine Umordnung, eine Permutation einer gegebenen Zeichenfolge, nennt man Permutations- oder Transpositionschiffre. Dies trifft in diesem Fall auf die Skytale zu. Permutationschiffren werden auch als Transposition bezeichnet. Die Skytale ist ein Spezialfall der Transposition. Denkbar wäre nämlich eine Permutationschiffre, die zur Erstellung des Geheimtextes erst den ersten, dann den 47-ten, danach den 32-ten Buchstaben nimmt, usw. Bei der Skytale wird jedoch, wie oben als Matrix betrachtet, die Nachricht zeilenweise aufgetragen und chiffriert liegt diese spaltenweise vor. Die

Skytale ist also letztendlich eine einfache Matrixtransposition.

Bei einer Permutations-Chiffre werden somit die Buchstaben den Klartext nicht ersetzt sondern durcheinander gewürfelt. Fast man zB immer 5 Buchstaben des Klartextes zusammen und lässt sich durch die Permutations-Chiffre mit dem Schlüssel (4,1,2,5,3), dann erhält man zB folgenden Chiffretext:

```
IE SBGE TZIW EARNT LVU ENNUTS: EHOLEC, ZDI UE EENB DGRIENS; NWS ANI
EFAEANNG.

ES GIBT ZWEI ARTEN VON LEUTEN: SOLCEH DIE ZU ENDE BRINGEN, WAS SIE ANFANGEN.
```

Die Art der Verschlüsselung lässt sich durch Probieren – abhängig von der Schlüssellänge – mehr oder weniger schnell knacken. Auch die Häufigkeitsanalyse liefert wieder Rückschlüsse über die verwendete Sprache etc.

- 8.1.2.1.4) Skytale

Operationen

Alle gängigen symmetrische Verfahren arbeiten ausschließlich mit Bit-weisen Operationen. Hier werden Schlüssel, Klartext und Geheimtext in Form von Bitfolgen verarbeitet. In dem die Funktionen nahezu beliebig miteinander kombiniert werden, lassen sich neu symmetrische Verfahren in nahezu beliebiger Zahl entwickeln und mit bekannten Angriffen auf Schwächen testen. In der Regel kombinieren symmetrische Verschlüsselungsalgorithmen Substitutionschiffren und Permutationschiffren miteinander und wiederholen den Vorgang mehrmals (Runden), wobei eine härtere Verschlüsselung entsteht. Typische Bestandteile von symmetrischen Verschlüsselungsalgorithmen sind:

- Exklusiv-oder-Verknüpfung
- Permutation: Reihenfolge einer Bit-Folge wird verändert.
- Substitution: Eine Bit-Folge wird durch eine andere ersetzt.

Erfahrungsgemäß sind für eine wirkungsvolle Verschlüsselung keine aufwendigen Funktionen notwendig. Insbesondere beim Hardware-nahen Programmieren oder der Implementierung in Hardware ist das von Vorteil, weil sich so eine hohe Geschwindigkeit erreichen lässt. Beim praktischen Einsatz von Verschlüsselungsalgorithmen stellt sich auch immer die Frage, wie groß die Rechenleistung für die Verschlüsselung ist. Generell gilt, je schneller ein Verschlüsselungsverfahren arbeitet, desto niedriger sind die Hardwarekosten.

Moderne(re) Verschlüsselungsverfahren

Bei den symmetrischen Verschlüsselungsverfahren gilt der AES als Maß der Dinge. Es gibt aber auch weitere…

- 8.1.2.1.5) DES
- 8.1.2.1.6) AES
- 3DES - Triple DES

- IDEA - International Data Encryption Algorithm
- RC4 (Rivest-Cipher 4)
- Blowfish (von Bruce Schneier)
- RC5, RC5a, RC6 (Rivest-Cipher 5 bzw. 5a bzw. 6)
- A5 (GSM)
- Serpent
- Twofish (von Bruce Schneier)
- MARS
- SAFER/SAFER+
- CAST (Carlisle Adams und Stafford Tavares)
- MAGENTA
- MISTY1
- Camellia
- Ascon

Quellen

- Elektronik Kompendium
- Kryptografie.de
- Cryptool
- Wikipedia