



openHPI – Sicherheit im Internet Einführung in die Verschlüsselungstechnik

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Kryptographie – die Wissenschaft von der Verschlüsselung (1/3)

- Probates Mittel, um Nachrichten vor unberechtigten Lesern zu schützen, ist diese durch „**Verschlüsselung**“ unlesbar zu machen
- Bei einer Verschlüsselung wird eine Nachricht mit Hilfe eines Verschlüsselungsverfahrens in eine unleserliche Zeichenfolge verwandelt („verschlüsselt“ bzw. „kodiert“), die nur ein berechtigter Empfänger wieder in die ursprüngliche Nachricht zurückverwandeln („entschlüsseln“ bzw. „dekodieren“) kann
- Verschlüsselungs- und Entschlüsselungsverfahren sind Parameter-gesteuert, der Parameter heißt „**Schlüssel**“
- Empfänger kann verschlüsselte Nachricht („Schlüsseltext“ oder „Chiffre“) nur dann entschlüsseln, wenn er im Besitz des zum Verschlüsselungsschlüssel passenden Entschlüsselungsschlüssels ist ...

Kryptographie ist die Wissenschaft von der **Verschlüsselung**, heute allgemeiner oft auch verstanden als die Wissenschaft der **Informationssicherheit**

- Die Güte von Verschlüsselungsverfahren hängt davon ab, inwieweit es möglich ist, unbefugt – also ohne passenden Entschlüsselungsschlüssel – Nachrichten zu entschlüsseln
 - schwache bzw.
 - starke Kryptographie

Kryptoanalyse ist Teilgebiet der Kryptographie, in dem die Güte von Entschlüsselungstechniken und mögliche Angriffe gegen die Verschlüsselung untersucht werden

Um unbefugt in den Besitz der Information zu erlangen, muss ein Angreifer

- die verschlüsselte Nachricht abfangen und dann
- (mehr oder weniger) aufwändig entschlüsseln

Immer möglich und nicht zu verhindern sind

Brute-Force-Angriffe:

- Angreifer versucht, Schlüsseltext zu entschlüsseln, indem er systematisch alle prinzipiell möglichen Schlüssel durchprobiert ...
- Die Schwierigkeit, Verschlüsselungsverfahren „zu knacken“, hängt also wesentlich von der Länge des Schlüssels ab, denn mit jedem zusätzlichen Schlüsselzeichen multipliziert sich die Zahl der prinzipiell möglichen Schlüssel ...

Verschlüsselungstechniken helfen, verschiedene Sicherheitsziele zu erreichen

Vertraulichkeit:

- Nur Berechtigte erhalten Zugang zu einer Information

Integrität:

- Manipulationsschutz für Nachrichten

Authentizität:

- Sicherstellung der Urheberschaft einer Nachricht

Verbindlichkeit:

- Urheber einer Nachricht, darf Urheberschaft nicht abstreiten können

Methoden zur Verschlüsselung

Methoden der klassischen Kryptographie:

■ **Transposition:**

- Umsortieren der Buchstaben in einem Wort / Satz / Text

■ **Substitution:**

- Ersetzen einzelner Buchstaben durch andere Zeichen / Buchstaben

Methoden der modernen Kryptographie:

- Anwendung der Verfahren auf Bit-Ebene (erhöht Kombinationsmöglichkeiten)
- Symmetrische oder 1-Schlüsselverfahren („Secret Key“)
- Asymmetrische oder 2-Schlüsselverfahren („Public Key“)