LU06a - Verschlüsselung: Einführung

In der Vergangenheit war eine Verschlüsselung nur solange sicher, wie das Verfahren und der Schlüssel geheim blieben. Sobald ein Angreifer das Verfahren (z.B. Caesar, Vigenère, ...) kannte, war es durch Ausprobieren möglich, die Verschlüsselung zu knacken. Durch die Einführung leistungsfähiger Computer wurde das Ausprobieren von vielen Schlüsseln zu einer Sache von Sekundenbruchteilen.

Moderne Verfahren

Die Algorithmen moderner Verschlüsselungsverfahren sind jedem bekannt. Die Sicherheit hängt von 4 Faktoren ab.

Authentizität

Kann nur der Absender diese Nachricht gesendet haben?

Integrität

Kann der Empfänger sicher sein, dass die Nachricht unverändert bei ihm ankommt?

Verifizierbarkeit

Kann der Absender einer Nachricht mit Sicherheit identifiziert werden?

Beweisbarkeit

Kann der Empfänger beweisen, dass die Nachricht vom Absender stammt.

Symmetrische Verschlüsselung

Bei diesen Verfahren verwendet der Absender und Empfänger den gleichen Schlüssel. Jeder der den Schlüssel kennt, kann die Nachrichten verschlüsseln und entschlüsseln. In der Praxis muss ich für jede Kommunikation einen eigenen Schlüssel haben.

Asymmetrische Verschlüsselung

Bei diesen Verfahren kommen zwei Schlüssel zum Einsatz:

- Private Key: Diesen Schlüssel kennt nur der Besitzer des Schlüssels.
    - Mit seinem private Key entschlüsselt der Empfänger eine Nachricht.
    - Mit seinem private Key signiert der Absender eine Nachricht.
- Public Key: Diesen Schlüssel darf jeder kennen.
    - Mit dem public Key des Empfängers wird die Nachrichte verschlüsselt.
    - Mit dem public Key des Absenders wird eine Signatur überprüft.

---

m114-A0G