**Lernzettel 5: Grundlagen der Kryptographie**

**1. Grundlagen der Kryptographie**

* **Kryptographie:** Wissenschaft der Verschlüsselung von Nachrichten, um Informationen vor unautorisiertem Zugriff zu schützen.
* **Kryptoanalyse:** Techniken zur Entschlüsselung von Nachrichten ohne Kenntnis des verwendeten Schlüssels.
* **Kryptologie:** Kombination aus Kryptographie und Kryptoanalyse.
* **Steganographie:** Verbirgt die Existenz einer Nachricht, nicht nur deren Inhalt.

**Lernbrücke:** Während die Kryptographie den Inhalt schützt, kann die Steganographie auch die Existenz der Kommunikation selbst verbergen.

**2. Integritätsprüfung und Authentifizierung**

* **Message Authentication Code (MAC):** Stellt die Integrität und Authentizität von Nachrichten sicher, indem ein geheimer Schlüssel mit einem Hashwert kombiniert wird.
* **Hash-based Message Authentication Code (HMAC):** Eine sicherere Variante von MACs, die durch eine doppelte Hash-Funktion (innen und außen) höhere Sicherheit bietet.
* **CBC-MAC:** Verwendet Blockchiffren wie DES oder AES, wobei der letzte verschlüsselte Block als MAC-Wert verwendet wird.

**Lernbrücke:** MACs und HMACs sind entscheidend, um sicherzustellen, dass Nachrichten nicht manipuliert wurden und tatsächlich vom angegebenen Absender stammen.

**3. Passwortverwaltung und -überprüfung**

* **Einwegfunktionen (OWF) und MACs:** Systeme speichern nicht das Passwort selbst, sondern einen Hashwert davon, um die Sicherheit zu erhöhen.
* **Wörterbuchangriffe:** Angriffe, bei denen vorher berechnete Hashwerte aus einem Wörterbuch mit den gespeicherten Hashwerten verglichen werden.
* **Salting:** Fügt einen zufälligen Wert (Salt) zum Passwort hinzu, um Wörterbuchangriffe zu erschweren.

**Lernbrücke:** Durch den Einsatz von Salting und starken Hash-Algorithmen wird die Sicherheit von Passwortsystemen erheblich gesteigert.

**4. Digitale Signaturen**

* **Ziel:** Nachweis der Urheberschaft eines Dokuments durch asymmetrische Verschlüsselung.
* **RSA-Signatur:** Basiert auf der Hashfunktion der Nachricht und der Verschlüsselung des Hashwerts mit einem privaten Schlüssel.
* **Angriffsschutz:** Durch das Signieren des Hashwerts (statt der Nachricht selbst) wird die Sicherheit erhöht und Angriffe erschwert.

**Lernbrücke:** Digitale Signaturen bieten nicht nur Authentizität, sondern auch Integrität, da jede Veränderung der Nachricht nach der Signierung sofort erkannt wird.

**5. Verschlüsselungsverfahren**

* **Symmetrische Chiffren:** Verwenden denselben Schlüssel für Verschlüsselung und Entschlüsselung (z.B. DES, AES).
* **Asymmetrische Chiffren:** Nutzen unterschiedliche Schlüssel für Verschlüsselung (öffentlich) und Entschlüsselung (privat), z.B. RSA.
* **Hybride Systeme:** Kombinieren symmetrische und asymmetrische Chiffren, um die Vorteile beider zu nutzen (z.B. symmetrische Chiffren für die Nachricht und asymmetrische für den Schlüsselaustausch).

**Lernbrücke:** Hybride Verschlüsselungssysteme bieten die Sicherheit asymmetrischer Verfahren mit der Geschwindigkeit symmetrischer Chiffren, was sie ideal für viele Anwendungen macht.