

## **Gruppenarbeit - Kryptografische Verfahren:**

### **2-3 Schüler, PPT, Handout, Vortrag (15-30Min)**

Termin: 9BW, Mo

#### **1. Symmetrische Verschlüsselung**

- Was ist symmetrische Kryptographie und wie funktioniert sie?
- Was ist ein Schlüssel und wie wird er in der symmetrischen Kryptographie verwendet?
- Was ist eine Blockchiffre und wie unterscheidet sie sich von einer Stromchiffre?
- Was sind die gängigsten symmetrischen Verschlüsselungsalgorithmen und wie unterscheiden sie sich?
- Was ist der Unterschied zwischen einem Verschlüsselungs- und einem Entschlüsselungsalgorithmus?
- Wie wird der Schlüssel in der symmetrischen Kryptographie verteilt?
- Was ist die Rolle von Initialisierungsvektoren (IVs) in der symmetrischen Kryptographie?
- Wie wird die Stärke der Verschlüsselung in der symmetrischen Kryptographie gemessen?
- Wie sicher ist symmetrische Kryptographie und welche Bedrohungen gibt es?
- Wie kann die Sicherheit von symmetrischer Kryptographie verbessert werden?
- Was sind die Vor- und Nachteile von symmetrischer Kryptographie?
- Wie wird symmetrische Kryptographie in der heutigen

# Welt eingesetzt?

## 1. Asymmetrische Verschlüsselung

- Was ist asymmetrische Kryptographie und wie funktioniert sie?
- Was ist der Unterschied zwischen symmetrischer und asymmetrischer Kryptographie?
- Was ist ein Public Key und was ist ein Private Key?
- Was sind die gängigsten asymmetrischen Verschlüsselungsalgorithmen und wie unterscheiden sie sich?
- Wie wird der Public Key verteilt und wie wird die Vertraulichkeit der Kommunikation gewährleistet?
- Wie wird die Integrität der Daten in der asymmetrischen Kryptographie sichergestellt?
- ~~Was ist digitale Signatur und wie funktioniert sie?~~
- Was ist eine Public-Key-Infrastruktur (PKI) und wie wird sie verwendet?
- Wie sicher ist asymmetrische Kryptographie und welche Bedrohungen gibt es?
- Wie kann die Sicherheit von asymmetrischer Kryptographie verbessert werden?
- Was sind die Vor- und Nachteile von asymmetrischer Kryptographie?
- Wie wird asymmetrische Kryptographie in der heutigen Welt eingesetzt?

## 1. Hashwertverfahren

- Was ist eine Hash-Funktion und wofür wird sie verwendet?
- Was sind die Eigenschaften einer guten Hash-Funktion?
- Was ist der Unterschied zwischen einer kryptographischen

## Hash-Funktion und einer nicht-kryptographischen Hash-Funktion?

- Wie wird die Stärke einer Hash-Funktion gemessen?
- Was sind die gängigsten Hash-Funktionen und wie unterscheiden sie sich?
- Wie wird eine Hash-Funktion in der Praxis verwendet?
- Was ist eine digitale Signatur und wie wird sie mit einer Hash-Funktion erstellt?
- Wie kann eine Hash-Funktion verwendet werden, um die Integrität von Daten zu überprüfen?
- Was sind die Herausforderungen bei der Entwicklung von Hash-Funktionen?
- Wie sicher sind Hash-Funktionen und welche Bedrohungen gibt es?
- Wie können Hash-Funktionen verwendet werden, um Passwörter zu speichern?
- Was sind die Vor- und Nachteile von Hash-Funktionen?
- Wie werden Hash-Funktionen in der heutigen Welt eingesetzt?

### 1. Digitale Signatur

- Was ist eine digitale Signatur und wofür wird sie verwendet?
- Wie funktioniert eine digitale Signatur?
- Was sind die Bestandteile einer digitalen Signatur?
- Was ist der Unterschied zwischen einer digitalen Signatur und einer elektronischen Signatur?
- Wie wird die Integrität der Daten in einer digitalen Signatur sichergestellt?
- Wie wird die Authentizität des Absenders in einer digitalen Signatur gewährleistet?
- Was ist eine Public-Key-Infrastruktur (PKI) und wie wird

sie für digitale Signaturen verwendet?

- Was sind die gängigsten digitalen Signaturalgorithmen und wie unterscheiden sie sich?
- Wie wird die Sicherheit einer digitalen Signatur gemessen?
- Was sind die Herausforderungen bei der Verwendung von digitalen Signaturen?
- Wie sicher sind digitale Signaturen und welche Bedrohungen gibt es?
- Was sind die Vor- und Nachteile von digitalen Signaturen?
- Wie werden digitale Signaturen in der heutigen Welt eingesetzt?

## **1. Zertifikat**

- Was ist ein digitales Zertifikat und wofür wird es verwendet?
- Wie funktioniert ein digitales Zertifikat?
- Was sind die Bestandteile eines digitalen Zertifikats?
- Was ist eine Zertifizierungsstelle (CA) und wie wird sie für digitale Zertifikate verwendet?
- Wie wird die Integrität und Authentizität von digitalen Zertifikaten gewährleistet?
- Was ist der Unterschied zwischen einem selbst signierten Zertifikat und einem von einer Zertifizierungsstelle ausgestellten Zertifikat?
- Wie werden digitale Zertifikate in der Praxis verwendet?
- Was sind die Herausforderungen bei der Verwendung von digitalen Zertifikaten?
- Wie sicher sind digitale Zertifikate und welche Bedrohungen gibt es?
- Was sind die Vor- und Nachteile von digitalen Zertifikaten?
- Wie werden digitale Zertifikate in der heutigen Welt eingesetzt?

- Was sind die Alternativen zu digitalen Zertifikaten?