Gedächnisprotokoll IT-Sicherheit mündlich

1. Symmetrische Kryptografie
    a. One-Time-Pad VL 02 S. 15 - 17
        i. Funktion
        ii. Zeichnen
        iii. Sicherheit (XOR) Entschlüsselung / Passwort knacken möglich?
        iv. Probleme?
            1. Wirkliche Zufälligkeit
            2. Key Exchange (Schlüssel-Austausch)
        v. Voraussetzungen:
            1. Random Number (Zufallszahl)
            2. Key gleiche Länge wie Message
            3. Key wird nur einmal verwendet (und dann verworfen)

2. Diffie-Hellmann VL 03 S. 22 - 25
    a. Funktion
       Secure Key Exchange
    b. Formel
    c. Anwenden / Berechnen mit Zahlen
    d. Knackbar? Mit Man-In-The-Middle-Angriff (MITM) abfangbar?
    e. Sicherheit von Diffie-Hellmann
    f. Attacken gegen Diffie-Hellmann

3. Asymmetrische Kryptografie
    a. Wie verhindert man MITM-Angriffe?
    b. Digitale Signatur VL04 S. 14 - 19
        i. Funktion
        ii. Zeichnen
        iii. Zertifizierungsstellen (CA) haben eigenen Key
             Verifizieren mit Ihrem Key den public Key des Absenders (z.B. Bob)

4. Authentifizierung
    a. Challenge Response Verfahren VL05 S. 21 - 22
        i. Zeichnen
        ii. Funktion
    b. Passwort Speicherung (Password Storage)
        i. Wie sollten Passwörter gespeichert werden
           Bevorzugt als Hash nicht im Klartext
    c. Salted Passwords
        i. Wie funktioniert das?
           Passwörter werden meinem einem Random String ergänzt
           Das Knacken eines Passworts führt damit nicht zum Hacken eines anderen identischen, da der Random String (Salt) sich unterscheidet

5. Websecurity
    a. SQL-Injection VL07 S. 6 - 10
        i. Formel Beispiel mit direkten „‘x OR 1 = !“
        SELECT * FROM users WHERE name = 'steve'
        AND password = 'x' or '1'='1

        ii. Warum funktioniert eine SQL-Injektion immer? = TRUE
        iii. Wie kann man eine SQL-Injektion verhindern?
            1. Prepared Statements verwenden
            2. Code und Daten trennen
        iv. Code und Daten unterschiedlich markieren
            1. „OR“ gehört zu Daten!