Fachbereich Wirtschaft
Prof. Bockermann, Prof. Grote, Prof. Klingspor

Wirtschaftsinformatik 1

Übungsblatt 3a (Verschlüsselung und sichere Verbindungen)

Aufgabe 1 (Caesar-Chiffre)

- Verschlüsseln Sie das Wort GEHEIM mit dem Schlüssel 7.
- Entschlüsseln Sie ZPJOLY (Schlüssel 7).
- In einem langen deutschen Geheimtext ist "r" der mit Abstand häufigste Buchstabe. Welcher Schlüssel liegt nahe — und warum funktioniert dieser Angriff, ganz ohne alle Schlüssel durchzuprobieren?

Aufgabe 2 (Der Bauplan der sicheren Verbindung) Die Vorlesung hat drei Schritte zu einer sicheren Verbindung entwickelt: (1) die Daten verschlüsseln, (2) den Schlüssel austauschen, (3) der Gegenseite vertrauen. Ordnen Sie jedem Schritt die passende Technik zu (Zertifikat/Signatur, symmetrische Verschlüsselung, asymmetrische Verschlüsselung) und begründen Sie jede Zuordnung in einem Satz.

Aufgabe 3 (Hybrides Verfahren)

- Warum verschlüsselt der Browser nicht einfach die gesamte Kommunikation asymmetrisch?
- Was genau wird beim HTTPS-Aufbau asymmetrisch verschlüsselt?
- Warum darf der private Schlüssel den Server niemals verlassen?

Aufgabe 4 (Zertifikate — Praxis, Chrome) *Bitte im Chrome-Browser (steht auch in der Prüfung zur Verfügung; auf Pool-Rechner ausweichen, falls nicht installiert).*

- Rufen Sie `https://www.hochschule-bochum.de` auf und öffnen Sie das Zertifikat (Schloss-Symbol → Zertifikat). Notieren Sie: Wer ist der Aussteller? Bis wann ist es gültig? Wie sieht die Zertifikatskette aus?
- Rufen Sie die Testseiten `https://expired.badssl.com` und `https://wrong.host.badssl.com` auf. Was meldet der Browser jeweils — und welcher Bestandteil des Zertifikats ist das Problem?

Aufgabe 5 (HTTPS als Geschäftsfaktor) Ein kleiner Online-Shop läuft noch ohne gültiges HTTPS-Zertifikat.

- Was zeigt der Browser den Besuchern an — und warum ist das gerade für einen Shop ein Problem?
- Nennen Sie zwei Gründe, warum sich HTTPS *betriebswirtschaftlich* auszahlt (über die reine Technik hinaus).
- Der Inhaber scheut die Kosten. Was entgegnen Sie ihm?

Aufgabe 6 (Hash-Funktionen — Praxis)

- Berechnen Sie online (Suche: "SHA-256 online") den Hashwert Ihres Vornamens. Ändern Sie dann einen einzigen Buchstaben. Was beobachten Sie?
- Warum speichern Web-Shops Passwort-Hashes statt der Passwörter selbst?
- Warum ist "password" trotzdem unsicher, obwohl nur der Hash gespeichert wird?

Aufgabe 7 (Passwörter und 2FA) Welches Passwort ist nach aktueller BSI-Empfehlung stärker: `T7$x!q` oder `pferd-wolke-blau-tasse`? Begründen Sie mit dem Grundsatz "Länge vor Komplexität".

Drei Login-Verfahren: (A) nur Passwort, (B) Passwort + SMS-Code, (C) Passwort + Code aus einer Authenticator-App (TOTP).

- Welche Faktoren (Wissen/Besitz/Biometrie) stecken in jedem Verfahren?
- Bringen Sie die drei Verfahren in eine Rangfolge nach Sicherheit und begründen Sie — insbesondere: Was ist die bekannte Schwachstelle der SMS-Variante?