

Wirtschaftsinformatik 1

Übungsblatt 3

Aufgabe 1 (Zertifikate)

Für diese Aufgabe verwenden Sie bitte den Chrome-Browser, da Ihnen dieser auch bei der Prüfung zur Verfügung steht. Falls Sie ein Tablett benutzen, oder Chrome nicht installiert haben, verwenden Sie bitte einen Pool-Rechner.

Rufen Sie in einem Chrome-Browser folgende Seiten auf und prüfen Sie, ob diese, Seiten vertrauenswürdig sind.

- <https://www.hochschule-bochum.de>
- <https://wiinfest.fbw.hs-bochum.de>

Schauen Sie sich die Eigenschaften der Zertifikate genau an, und überlegen Sie, warum das erste Zertifikat gültig ist, obwohl es für eine andere URL ausgestellt wurde, und warum das Zertifikat der zweiten Seite nicht vertrauenswürdig ist.

Aufgabe 2 (Symmetrische Verschlüsselung)

Warum muss bei symmetrischer Verschlüsselung der Schlüssel geheim gehalten werden?

Was kann passieren, wenn der Schlüssel bekannt wird?

Aufgabe 3 (Asymmetrische Verschlüsselung)

Wenn bei asymmetrischer Verschlüsselung ein Text mit dem privaten Schlüssel verschlüsselt wird, wer kann den Text entschlüsseln (bzw. was braucht man für die Entschlüsselung)?

Wer kann einen Text entschlüsseln, der mit dem öffentlichen Schlüssel verschlüsselt wurde?

Aufgabe 4 (RansomWare)

Wie funktioniert RansomWare? Schauen Sie mal bei Wikipedia nach oder googeln Sie.

Wann und wie können verschlüsselte Dateien wieder entschlüsselt werden?

Aufgabe 5 (Hashfunktionen)

Nennen Sie (kryptographischen) Hashfunktionen! (Wikipedia kann da gut helfen :-))

Berechnen Sie mit Hilfe des Internets den Hashwert für "password" und ein weiteres beliebiges selbst ausgedachtes Wort.

Können Sie mit Hilfe des Internets für die beiden Hashwerte wieder das Originalwort bestimmen?

Wieso ist bei manchen Hashwerten der Originaltext wieder bestimmbar? Was ergibt sich daraus für die Wahl von Passwörtern?