Hochschule Bochum
Bochum University
of Applied Sciences

Fachbereich Wirtschaft
Prof. Blümel, Prof. Bockermann, Prof. Klingspor

Wirtschaftsinformatik 1

Übungsblatt 3

Aufgabe 1 (Zertifikate)

Rufen Sie in Ihrem Browser folgende Seiten auf und prüfen Sie, ob diese, Seiten vertrauenswürdig sind.

- `https://www.hochschule-bochum.de`
- `https://wiinftest.fbw.hs-bochum.de`t

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 Orginaltext wieder bestimmbar? Was ergibt sich daraus für die Wahl von Passwörtern?

Aufgabe 6 (Elektronische Signaturen)

Diese Datei ist elektronisch unterzeichnet. Können Sie nachprüfen, durch wen sie unterzeichnet wurde und ob die die Unterschrift vertrauenswürdig ist?

(Unter MacOs geht dies auf jeden Fall mit Adobe Acrobat. Ob und wie das auf anderen Computern funktioniert, können wir in der Übung klären).

Volker Klingspor

Digital unterschrieben von Volker Klingspor
Datum: 2024.04.24 10:46:58 +02'00'