Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2021
(LV 4121 und 4241)

3. Aufgabenblatt

Ziel dieser Übung ist es, die grundsätzlichen Aspekte der Informationssicherheit herauszustellen. Ferner werden erste Überlegungen hinsichtlich der Sicherheit von kryptographischen Algorithmen und Verschlüsselungsverfahren angestellt. Des weiteren streift diese Übung kurz die Themenbereiche digitale Signatur sowie die häufigsten Formen des Computermissbrauchs.

Aufgabe 3.1

a) Was versteht man unter "Sicherheit eines IT-Systems"?

b) Nennen und erläutern Sie fünf grundsätzliche Aspekte der Informationssicherheit.

c) Welches sind die häufigsten Formen des Missbrauchs informationstechnischer Systeme?

d) Wie schätzen Sie die prozentuale Verteilung der verschiedenen Missbrauchsformen bzgl. statistisch erfasster Schadensereignisse ein?

e) Informieren Sie sich über die häufigsten Missbrauchsdelikte und stellen Sie das Resultat graphisch dar.

Aufgabe 3.2

a) Welche Mindestanforderungen werden grundsätzlich an einen Verschlüsselungs-algorithmus gestellt?

b) Durch welchen Parameter sollte die Sicherheit eines Verschlüsselungsalgorith-mus in der Praxis bestimmt sein?

c) Unter welchen Voraussetzungen gilt ein Kryptoalgorithmus im allgemeinen als sicher? Wann ist er uneingeschränkt sicher?

d) Was besagt das Prinzip von A. Kerckhoffs?

e) Welcher Unterschied besteht zwischen symmetrischen und asymmetrischen Ver-fahren im Hinblick auf die Schlüsselmannigfaltigkeit?

Aufgabe 3.3

a) Welche Komponenten (Algorithmen, Schlüssel etc.) benötigen Sie, um eine digitale Signatur zu erstellen?

b) Schildern Sie schematisch den Vorgang einer Signaturerstellung.

c) Unter welchen Bedingungen endet die Signaturprüfung mit einem positiven Prüfergebnis?

d) Recherchieren Sie im Internet, was man unter einer *qualifizierten* digitalen Signatur versteht.

Aufgabe 3.4

a) Wie funktioniert ein hybrides Verschlüsselungsverfahren?

b) Welchen Schlüssel benutzt man für die Entschlüsselung einer Nachricht bei einer asymmetrischen Verschlüsselung?

Aufgabe 3.5

a) Zeichnen Sie das Prinzip der Berechnung eines Message Authentication Codes (MAC).

b) Welches Verfahren erhält man, wenn man bei der Berechnung eines Message Authentication Code (MAC) den symmetrischen Verschlüsselungsalgorithmus gegen einen asymmetrischen Verschlüsselungsalgorithmus vertauscht?