Aufgaben zu Kapitel 1: Einführung

Aufgabe 1.1 (Kryptosysteme)

a) Aus welchen Bestandteilen besteht ein Kryptosystem?

b) Welche Beziehung muss zwischen Ver- und Entschlüsselungsfunktion bestehen?

c) Welche der folgenden drei Eigenschaften muss jede Verschlüsselungsfunktion besitzen?

- surjektiv (rechtstotal)
- injektiv (linkseindeutig)
- bijektiv (surjektiv und injektiv)

Aufgabe 1.2 (Symmetrische und asymmetrische Verschlüsselung) Erläutern Sie den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Gehen Sie dabei auf folgende Aspekte ein:

- Zusammenhang zwischen Ver- und Entschlüsselungsschlüssel
- Geheimnisbesitz
- Fähigkeit zum Ver- und Entschlüsseln

Aufgabe 1.3 (Schutzziele) In früheren Jahrhunderten wurden wichtige Briefe durch heißes Siegelwachs verschlossen, in das dann ein Siegel gedrückt wurde. Welche Schutzziele wurden durch dieses Verfahren erreicht? Für welche Schutzziele eignet sich das Verfahren nicht? Begründen Sie Ihre Antwort.

Aufgabe 1.4 (Kerckhoffs'sches Prinzip)

a) Was sagt das Kerckhoffs'sche Prinzip aus?

b) Ein Kommilitone argumentiert, dass ein Verschlüsselungsverfahren, bei dem sowohl der Schlüssel als auch das Verfahren geheimgehalten wird, sicherer sein muss als ein Verfahren, bei dem nur der Schlüssel geheimgehalten wird. Was können Sie ihm entgegnen?

Aufgabe 1.5 (Plaintext Angriffsszenarien) Erläutern Sie den Unterschied zwischen einem Known-Plaintext-Angriff und einem Chosen-Plaintext-Angriff. Welche Angriffsart ist aus Sicht des Angreifers vielversprechender? Erläutern Sie Ihre Antwort.