Aufgaben zu Kapitel 1: Einführung

Aufgabe 1.1 (Kryptosysteme)

a) Bestandteile: P Menge der Klartexte, C Menge der Geheimtexte, K Menge der Schlüssel, e Verschlüsselungsfunktion $e : P \times K \to C$, d Entschlüsselungsfunktion $d : C \times K \to P$.

b) Beziehung zwischen e und d: Für alle $k \in K$ gibt es ein $k' \in K$ mit $d(e(x,k),k') = x$ für alle $x \in P$.

c) Für festes $k \in K$ muß die Verschlüsselungsfunktion $e(\,\cdot\,,k) : P \to C, x \mapsto e(x,k)$ zum Schlüssel k injektiv sein.

Aufgabe 1.2 (Symmetrische und asymmetrische Verschlüsselung)

	Symmetrisch	**Asymmetrisch**
Zusammenhang zwischen Ver- und Entschlüsselungsschlüsselung	Schlüssel zum Entschlüsseln leicht ermittelbar aus Schlüssel zum Verschlüsseln	Schlüssel zum Entschlüsseln nicht in angemessener Zeit aus Schlüssel zum Verschlüsseln ermittelbar
Geheimnisbesitz	Sender und Empfänger müssen ein gemeinsames Geheimnis (den Schlüssel) besitzen.	Sender und Empfänger müssen kein Geheimnis austauschen.
Fähigkeit zum Ver- und Entschlüsseln	Wer verschlüsseln kann, kann auch entschlüsseln.	Wer verschlüsseln kann, kann nicht entschlüsseln.

Aufgabe 1.3 (Schutzziele) Erreichte Schutzziele:

- Integrität: Die Nachricht kann nicht verändert werden, ohne das Siegel zu zerbrechen.
- Authentizität: Jeder Absender hatte ein eigenes, schwer fälschbares Siegel.
- Nicht-Abstreitbarkeit des Versands: Niemand außer dem Sender besitzt sein Siegel.

Ungeeignet für:

- Vertraulichkeit: Ein abgefangener Brief kann gelesen werden (durch den Bruch des Siegels ist das aber erkennbar).
- Nicht-Abstreitbarkeit des Empfangs: Für den Sender nicht erkennbar, ob der Brief den Empfänger erreicht hat.
- Anonymität: Identität des Senders durch das Siegel erkennbar.

Aufgabe 1.4 (Kerckhoffs'sches Prinzip)

a) Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels abhängen, nicht von der Geheimhaltung des Verschlüsselungsverfahrens.

b) Mögliche Einwände:

- Schwachstellen von geheimgehaltenen Verfahren werden nur schwer entdeckt, da sehr wenige Leute das Verfahren auf Schwächen prüfen können.
- Die Erfahrung zeigt, dass sehr viele geheime Verschlüsselungsverfahren tatsächlich Schwachstellen enthielten, die erst von den Angreifern entdeckt wurden.
- Bei nicht-öffentlichen Verfahren kann schwer ausgeschlossen werden, dass sie keine Hintertüren enthalten.
- Verfahren lassen sich praktisch nur sehr schwer Geheimhalten (Reverse-Engineering, Wissen der Implementierer).

Aufgabe 1.5 (Plaintext Angriffsszenarien)

Known-Plaintext-Angriff:
Der Angreifer kennt einen oder mehrere Geheimtexte und zugehörige Klartexte.

Chosen-Plaintext-Angriff: Der Angreifer kann beliebige, frei wählbare Klartexte chiffrieren lassen.

Chosen-Plaintext-Angriffe bieten für Angreifer mehr Ansatzpunkte, da er den Klartext gezielt variieren und die dadurch entstehenden Veränderungen am Geheimtext analysieren kann.