Datensicherheit, Übung 5

Henry Haustein

Aufgabe 1

(a) Verschlüsselung und Kodierung

(b) Zuerst verschlüsseln, dann kodieren

Aufgabe 2

Die Sicherheit eines Verfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen, sondern nur von der Geheimhaltung des Schlüssels. Schlüssel sind leichter geheimzuhalten als das Verfahren, weil das Verfahren ja auch dem Kommunikationspartner bekannt sein muss.

Aufgabe 3

(a) Für jede Kommunikation einen Schlüssel: $\frac{20 \cdot 19}{2} = 190$

(b) Jeder braucht 2 Schlüssel: $2 \cdot 20 = 40$

Aufgabe 4

(a) alle Verschlüsselungssysteme hintereinander schalten

(b) Parallele Verwendung von allen Verschlüsselungssystemen $\Rightarrow$ mehr Prüfsummen

Aufgabe 5

Folgende Möglichkeiten gibt es:

(1) Zuerst verschlüsseln, dann die MAC berechnen

(2) MAC und Verschlüsselung parallel aus der Nachricht berechnen

(3) MAC berechnen, dann MAC + Klartext verschlüsseln

	(1)	**(2)**	**(3)**
Integrität Klartext	✓	✓	✓
Integrität Schlüsseltext	✓		
Parallelität Verschlüsselung		✓	
Parallelität Entschlüsselung	✓		

Aufgabe 6

(a) Vertraulichkeit: nicht gegeben, weil Signatur keine Verschlüsselung ist, Zurechenbarkeit: hängt vom Vertrauen in die Instanz ab, Integrität: gegeben

(b) Vertraulichkeit: nicht gegeben, weil Signatur keine Verschlüsselung ist, Zurechenbarkeit: gegeben, Integrität: gegeben

Aufgabe 7

(a) asymmetrisches Authentifikationssystem: Wichtig ist, von wem die Nachricht kommt, der Inhalt ist nicht ganz so wichtig, Verschlüsselung wäre trotzdem schön.

(b) symmetrisches Authentifikationssystem: es muss schnell gehen, noch besser wäre allerdings Verfahren zur Prüfung der Integrität der Daten zu nutzen wie z.B. CRC.

(c) asymmetrisches Konzelations- und Authentifikationssystem: ähnlich wie (a), allerdings sind Preisinformationen deutlich schützenswerter als Vor- und Nachteile einer Wohnung.