1. Aufgabe

Es scheint praktisch unmöglich zu sein, aus der Analyse von Coca Cola auf das Rezept zu schliessen. Andererseits ist es offensichtlich auch nicht möglich, mit einem anderen Rezept ein zu Coca Cola identisches Getränk zu produzieren.

a) Nennen Sie einen kryptologischen Begriff, der vergleichbare Eigenschaften aufweist.

2. Aufgabe

Ordnen Sie den folgenden Tätigkeiten und Objekten die Begriffe „Vertraulichkeit", „Authentikation" und „Integrität" zu.

- Rose im Knopfloch
- Brief in Umschlag stecken und zukleben
- Fingerabdruck
- Briefsiegel
- Unterschrift

3. Aufgabe

Erklären Sie das Prinzip der asymmetrischen Verschlüsselungsverfahren anhand von Briefen welche in mit Namensschildern versehene Briefkästen gesteckt werden.

4. Aufgabe

Bitte übersetzen!

Ensuring Data Integrity with Hash Codes

A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values are used with digital signatures because hash values represent a large amount of data as a much smaller numeric value. You can efficiently sign a hash value instead of signing the larger value. Hash values are also useful for verifying the integrity of data sent through insecure channels. The hash value of received data can be compared to the hash value of data as it was sent to determine whether the data was altered. This section describes how to generate hash codes using the classes in the System.Security.Cryptography namespace.

5. Aufgabe

Zum Abspeichern von Passworten wird gelegentlich das folgende Verfahren vorgeschlagen: Jedem Passwort wird ein zufällig gewählter Wert (salt) angehängt und die daraus resultierende Zeichenkette wird anschliessend in einer Einweg-Funktion verrechnet. In der Passwortdatei werden das Ergebnis der Einweg-Funktion und der zufällig gewählte Wert abgelegt.

a) Wie wird beim Einloggen die Gültigkeit des eingegebenen Passwortes überprüft?

b) Ergeben sich durch das beschriebene Verfahren Vorteile, obwohl der zufällig gewählte Wert im Klartext abgespeichert und deshalb einem Angreifer bekannt ist? Falls ja, welche?