Übungsblatt 11

Aufgabe 1

a)
Symmetrische sowie asymmetrische Verschlüsselungsverfahren haben jeweils ihre Vorteile und Nachteile, weswegen diese für verschiedene Situation besser passen als das jeweilige Gegenstück.
Symmetrische Verschlüsselungsverfahren ist allgemein schneller als asymmetrisch da hier nur ein Schlüssel verwendet werden muss. Problem dabei ist dass falls mehrere Leute z.B. untereinander Nachrichten mit symmetrischen Schlüsseln austauschen wollen, dann brauchen diese $\frac{n(n-1)}{2}$ Schlüssel, was bei 5 Leuten schon 10 Schlüssel bedeutet. Außerdem ist das austauschen der Schlüssel schwer.
Der wichtigste Vorteil von asymmetrischen Verschlüsselung ist die hohe Sicherheit, basierend auf einem sehr schweren mathematischem Problem. Das Problem dabei ist dass, wenn man genug Rechnerleistung hat, die verschlüsselte Nachricht in z.B. 10 Jahren wenn die generelle Rechnerleistung deutlich höher ist knacken kann. Da man die verschlüsselte Nachricht abfangen kann und diese zwischenspeichern kann. Da dieses Verfahren rechenintensiv ist ist diese auch deutlich langsamer als die symmetrische Verschlüsselung.

b)
Z.B. beim https, wird mit dem asymmetrischem Verfahren die Schlüssel ausgetauscht, weil das sehr sicher ist. und die Kommunikation zwischen den Partnern findet dann mit dem ausgetauschtem symmetrischem Schlüssel statt, da man mit diesem weniger rechenintensiv kommunizieren kann.

Aufgabe 2