



1. Übung zur Vorlesung

Public-Key-Infrastrukturen

SS 2006

Aufgabe 1: Bücherkauf im Internet

Ein Buchhändler bietet seine Bücher über das Internet zum Verkauf an. Hierzu veröffentlicht er die Liste der bei ihm angebotenen Bücher auf Webseiten. Die Webseiten werden bei seinem Internet-Provider gehostet. Die Buchliste beinhaltet unter anderem Titel, Verlag und den Preis der Bücher. Ein Kunde kann nun beim Kauf die gewünschten Bücher auswählen, zur Bestellung vormerken und die von ihm gewünschte Zahlungsart angeben. Daraufhin bekommt er vom Händler voraussichtliche Lieferzeit, Preis und Versandmodalitäten genannt. Er kann nun die Bestellung zusammen mit den Daten für die Abwicklung der Zahlung absenden, deren Erhalt wiederum vom Händler quittiert wird.

- a) Welche Sicherheitsziele spielen in welchem Schritt eine Rolle?
- b) Wo bestehen Parallelen zu dem in der Vorlesung gezeigten Szenario "Zintl-Umbau"?
- c) Worin unterscheiden sich ggf. die Sicherheitsziele und weshalb?

Aufgabe 2: Vorstandswahlen

Im folgenden will der Verein *InterNett* einen neuen Vorstandsvorsitzenden wählen. Da die Mitglieder des Vereins über die ganze Welt verstreut sind und der Verein sich zudem mit der sicheren Kommunikation im Internet beschäftigt, sollen die Wahlen online abgewickelt werden, was auch mit der Vereinssatzung vereinbar ist. Diese sieht bei der Wahl eines Vorstandsmitglieds folgendes vor:

- Jedes reguläre Vereinsmitglied darf wählen und hat genau eine Stimme.
- Die Personenwahl muss geheim erfolgen.
- Es müssen wenigstens 10 Stimmberechtigte an der Wahl teilnehmen.
- Es muss aus dem Wahlprotokoll hervorgehen, wer an der Wahl teilnimmt und wie die Wahl ausgeht.

Zur Vereinfachung können Sie annehmen, dass die Liste der Kandidaten schon feststeht.

Welche Sicherheitsziele sind hier wichtig?

Bemerkung: Es soll in dieser Aufgabe kein vollständiges Protokoll für elektronische Wahlen "erfunden" werden. Dennoch ist es sinnvoll, sich die groben Schritte zu überlegen, in denen so eine Wahl erfolgen kann.

Aufgabe 3: Cryptool

Cryptool ist ein Freeware-Programm, mit dessen Hilfe Sie kryptographische Verfahren anwenden und analysieren können.

Sie finden es auf der Seite <http://www.cryptool.de>. Dieses Programm bietet Ihnen die Möglichkeit einige der verwendeten Basisverfahren am Beispiel nachzuvollziehen. So können sie verschiedene symmetrische, asymmetrische und hybride Verschlüsselungsverfahren testen, usw. Interessant ist auch die Möglichkeit, ein RSA-Modul zu faktorisieren, d.h. das Verfahren zu brechen. Das funktioniert natürlich nur, wenn n klein genug ist.