Hochschule für Technik und Wirtschaft
Studiengang Kommunikationsinformatik
Studiengang Praktische Informatik
Prof. Dr.–Ing. Damian Weber

Kryptographie – Übung 5

Aufgabe 1 (Authentifizierung)

Implementieren Sie ein Challenge–Response–Protokoll zwischen einem Netzwerkclient und einem Netzwerkserver. Der Client muß sich gegenüber dem Server authentifizieren, um eine Antwort des Servers zu erhalten. Als Antwort Ihres Servers können Sie die Ausgabe einer Datei wählen.

Wenn beispielsweise die Datei `index.html` hieße, wäre authentifiziertes Surfen möglich; der Server wüßte, welche Clients ihn wirklich kontaktieren.

Benutzen Sie RSA–Verschlüsselung *(nonces!)*, um die Challenge–Response zu realisieren.