Walther-Rathenau-Gewerbeschule Freiburg	**Wiederholung und Zusammenfassung** Digitale Signatur, Zertifikate Public Key Infrastruktur Tunnel	Fach: ITS 30. März 202 Name: Klasse: alle Punkte: /

Netzwerksicherheit

Das Internet wurde in den 1980er Jahren hauptsächlich an amerikanischen Universitäten und Einrichtungen entwickelt. Es gab nur sehr wenige Rechner und damit war die Anzahl der Teilnehmer in den Netzen sehr klein und jeder kannte jeden persönlich und alle haben sich **vertraut**. Die damals entwickelten Protokolle hatten daher keinerlei Verschlüsselungs- und Authentifizierungsvorkehrungen.
Inzwischen ist das Internet kommerzialisiert und es soll im Jahr 2020 etwa 50 Mrd (!) internetfähiger Geräte geben. Damit ist eine Verschlüsselung und Authentifizierung zwingend geworden.
Hier folgen ein paar Fragen, die dieses Thema wiederholen.

Public Key Verfahren

Beschreiben Sie das Public-Key-Verfahren.
Dabei sollen folgende Begriffe geklärt werden:
PublicKey, PrivateKey, RSA, Hauptmodul, Verschlüsselungsexponent, Entschlüsselungsexponent

Hash-Algorithmen

Was macht ein Hash-Algorithmus? Formulieren Sie einen einfachen Hash-Algorithmus, der beliebig lange Texte auf die Zahlen 0-999 abbildet. Ist der Hash-Algorithmus umkehrbar, d.h. kann man aus dem Hash-Wert wieder die Original-Daten zurückrechnen? Wenn nein, warum nicht?

Digitale Signatur

Beschreiben Sie, wie mit dem Public-Key-Verfahren Daten (Dokumente, Dateien, einfache Textstrings) *digital signiert* werden können.
Man bildet aus der Datei einen Hashwert und verschlüsselt diesen mit dem eigenen, **privaten** Schlüssel. D.h. **jeder** der den zughörigen PublicKey hat kann das wieder entschlüsseln. Parallel dazu wird die Datei richtig sicher verschlüsselt übertragen. Der Empfänger vergleicht dann die Hash-Werte der empfangenen Datei und der digitalen Signatur.

Zertifikate

Was ist ein digitales Zertifikat? Was enthält es im Detail?

Zertifikate erstellen

Beschreiben Sie, welche Schrittte notwendig sind, um ein offizielles (nicht selbstsigniertes) Zertifikat zu erhalten.

Tunnel im Internet

Beschreiben Sie wie getunnelter Datenverkehr im Internet funktioniert. Was kann man sich unter der tun-Schnittstelle auf einem Rechner mit *openvpn* vorstellen?