universität wien

PR Netzwerktechnologien
Sommersemester 2012

Aufgabenblatt 6

Abgabetermin: Dienstag, 26.06.2012, 23.59 Uhr

Abgabe als PDF im CEWebS

Aufgabe 6.1: *CSMA/CD*

1 Punkte

1. Wie lange wartet ein Netzwerkadapter, der CSMA/CD verwendet, nach einer Kollision, bevor er erneut versucht zu senden? Wie hängen Datenrate, minimale Framegröße und maximale räumliche Ausdehnung des Netzwerks zusammen?
2. In einem 100Mbps-Ethernet seien alle Knoten über einen Hub verbunden. Wie groß darf die maximale Distanz zwischen Knoten sein, um eine Effizienz von 50% zu erreichen? Kann ein Knoten erkennen, ob gleichzeitig mit ihm auch ein anderer Teilnehmer sendet? Wie groß sind im Vergleich hierzu die maximalen Distanzen in IEEE 802.3u definiert?

Aufgabe 6.2:

1 Punkte

1. Welches SNR erfordert eine $BER \leq 10^{-4}$ bei QAM256? Stellt Ihr Ergebnis einen Mindest- oder einen Höchstwert dar?

Aufgabe 6.3: *Netzwerksicherheit*

3 Punkte

1. Bietet ein Hash einen besseren Integritätscheck als eine Prüfsumme? Kann aus einer Prüfsumme bzw. einem Hash die ursprüngliche Nachricht rekonstruiert werden?
2. Was versteht man unter *Man-in-the-Middle Attack*? Kann dies auftreten, wenn symmetrische Verschlüsselung benutzt wird? Erklären Sie einen *Side Channel Attack* anhand eines Beispiels.
3. Verwenden Sie RSA mit den Parametern $p = 5$ und $q = 11$ um ein Wort Ihrer Wahl zu verschlüsseln und danach wieder zu rekonstruieren.
4. Die (wenig sichere) *monoalphabetische Substitutionsmethode* soll dreimal hintereinander auf einen Klartext angewendet werden, um – ähnlich wie 3DES im Vergleich zu DES – sicherere Verschlüsselung zu bieten. Diskutieren Sie die Eigenschaften dieses Verfahrens! Wie viele Schlüssel gibt es insgesamt? Wie viele sind sinnvoll?

Gesamt: 5 Punkte