



## Distributed Systems

Schriftliche Prüfung

**8.2.2017**

<b>VORNAME</b>		<b>NACHNAME</b>	
<b>Matrikelnummer</b>		<b>Unterschrift</b>	

### Instruktionen:

**Tragen Sie Vorname, Nachname, Matrikelnummer und Unterschrift in die obigen Felder ein.**

**Sprechen Sie während der Prüfung nicht mit anderen Studenten. Wenn Sie mit anderen Studenten sprechen, wird ihre Prüfung mit 0 Punkten bewertet.**

**Wo sinnvoll, ist es erlaubt Annahmen zu treffen die nicht in den Aufgabenstellungen genannt sind. Schreiben Sie diese auf.**

**Es ist gestattet ein beidseitig beschriebenes A4-Cheatsheet sowie Wörterbücher/Vokabelzettel zur Prüfung mitzubringen. Taschenrechner und andere elektronische Hilfsmittel sind nicht gestattet.**

**Wenn möglich, schreiben Sie ihre Antworten direkt unter die Aufgabenstellungen. Viel Erfolg!**

**Viel Glück!**

# 1. Internet und Protokolle

Verteilte Systeme sind Hauptthema dieser Lehrveranstaltung.

- (i) Was bezeichnet der Begriff „Verteiltes System“? Beschreiben Sie kurz zwei wesentliche Merkmale von Verteilten Systemen. (5 Punkte)

- (ii) Was bezeichnet “Transparency“ in einem verteilten System? Geben Sie ein Beispiel. (5 Punkte)

Netzwerkprotokolle sind konzeptuell in einem Stack angeordnet. Dabei kommt es oft zu „Multiplexing“.

- (iii) Was bezeichnet „Multiplexing“ in Bezug auf Netzwerkprotokolle? Geben Sie ein Beispiel.

(5 Punkte)

Protokolle stellen sich gegenseitig Dienste und Schnittstellen zur Verfügung.

- (iv) Welchen Dienst stellt das HTTP-Protokoll zur Verfügung, und welchen Dienst des darunterliegenden Transportlayers nutzt es?

(5 Punkte)

## 2. Data Link Layer

Im Folgenden betrachten wir den (7,4)-Hamming-Code aus der Vorlesung, bei dem die Parity-Bits wie folgt berechnet werden:

$$p_1 = d_1 \oplus d_2 \oplus d_3,$$

$$p_2 = d_2 \oplus d_3 \oplus d_4,$$

$$p_3 = d_3 \oplus d_4 \oplus d_1.$$

- (i) Dekodieren Sie die folgenden Codewörter, und markieren Sie eventuelle Fehler in den Codewörtern.

1111100      0010111      1010110

(8 Punkte)

- (ii) Was passiert im (7,4)-Hamming Code, wenn mehr als ein Bit falsch übertragen wird?

(4 Punkte)

Zur Behandlung von Übertragungsfehlern gibt es fehlererkennende Codes und fehlerkorrigierende Codes.

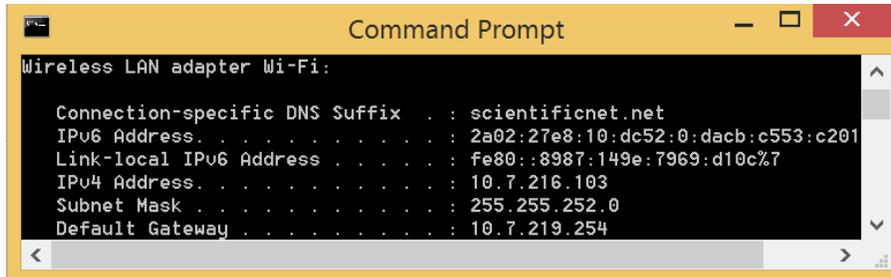
- (iii) Kreuzen Sie für die 4 folgenden Codes an, ob es fehlererkennende oder fehlerkorrigierende Codes sind.

	Erkennend	Korrigierend
CRC (Cyclic Redundancy Codes)	<input type="checkbox"/>	<input type="checkbox"/>
Hamming-Codes	<input type="checkbox"/>	<input type="checkbox"/>
Parity bits	<input type="checkbox"/>	<input type="checkbox"/>
IBANs	<input type="checkbox"/>	<input type="checkbox"/>

(4 Punkte)

### 3. Network Layer

Im folgenden ist ein Screenshot für die Ausführung von `ipconfig` aus dem Unibz-Netzwerk abgebildet.

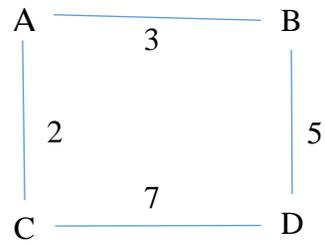


```
Command Prompt
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . . : scientificnet.net
IPv6 Address. . . . . : 2a02:27e8:10:dc52:0:dacb:c553:c201
Link-local IPv6 Address . . . . . : fe80::8987:149e:7969:d10c%7
IPv4 Address. . . . . : 10.7.216.103
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 10.7.219.254
```

(i) Wieviele IPv4-Adressen gibt es im Unibz-Netzwerk? (4 Punkte)

(ii) Was ist die höchste IP-Adresse im Unibz-Netzwerk? Was ist die niedrigste? (6 Punkte)

Routingtabellen werden im Network-Layer für das Routing von Paketen verwendet. Betrachten wir das Netzwerk im folgenden Beispiel, welches aus 4 Routern, A, B, C und D, besteht.



(iii) Zeichnen Sie die Routingtabelle für Router A.

(5 Punkte)

## 4. DNS

DNS ist ein Protokoll zur Namensauflösung im WWW.

(i) Was ist ein DNS Root Server?

(4 Punkte)

(ii) Wieso reicht es, dass es weltweit 13 DNS Root Server gibt?

(4 Punkte)

- (iii) Beschreiben Sie detailliert, was auf Ebene des DNS-Protokolls passiert, wenn man im Browser die URL [www.cs.uq.edu.au](http://www.cs.uq.edu.au) eingibt, die man nie zuvor besucht hat.

(12 Punkte)

## 5. Sicherheit

RSA ist ein wichtiges asymmetrisches Kryptosystem.

- (i) Wie können RSA-Schlüsselpaare verwendet werden, um Nachrichten geheim zu übertragen?  
(3 Punkte)

- (ii) Wie können RSA-Schlüsselpaare verwendet werden, um die Identität eines Absenders zu verifizieren?  
(4 Punkte)

(iii) Warum sind Certificate Authorities essentiell für asymmetrische Verschlüsselung im Internet?

(4 Punkte)

(iv) Was sind Certificate-Chains? Beschreiben Sie anhand eines Beispiels.

(4 Punkte)