

Name

Vorname

Studiengang (Hauptfach)

Fachrichtung (Nebenfach)

Matrikelnummer

Unterschrift der Kandidatin/des Kandidaten

Note

TECHNISCHE UNIVERSITÄT MÜNCHEN
Fakultät für Informatik

- Midterm
- Endterm
- Wiederholung

Prüfungsfach: Grundlagen Rechnernetze und Verteilte Systeme

Prüfer: Prof. Dr.-Ing. Georg Carle

Datum: 22.09.2014

Hörsaal: _____ **Reihe:** _____ **Platz:** _____

I II

1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Σ

--	--

Nur von der Aufsicht auszufüllen:

Hörsaal verlassen von ____ : ____ bis ____ : ____

Vorzeitig abgegeben um ____ : ____

Besondere Bemerkungen:





Wiederholungs-Klausur

Grundlagen Rechnernetze und Verteilte Systeme

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

Montag, 22.09.2014
11:30 – 13:00 Uhr

- Diese Klausur umfasst **19 Seiten** und insgesamt **6 Aufgaben** sowie ein zusätzlich ausgeteiltes Hilfsblatt mit Protokollheadern. Bitte kontrollieren Sie jetzt, dass Sie eine vollständige Angabe erhalten haben.
- Schreiben Sie bitte in die Kopfzeile **jeder Seite** Namen und Matrikelnummer.
- Schreiben Sie weder mit roter / grüner Farbe noch mit Bleistift.
- Die Gesamtzahl der Punkte beträgt 85.
- Als Hilfsmittel sind **ein beidseitig handschriftlich beschriebenes DIN-A4-Blatt** sowie **ein nicht-programmierbarer Taschenrechner** zugelassen. Bitte entfernen Sie alle anderen Unterlagen von Ihrem Tisch, schalten Sie Ihre Mobiltelefone aus und packen Sie diese weg.
- Mit * gekennzeichnete Aufgaben sind ohne Kenntnis der Ergebnisse vorhergehender Teilaufgaben lösbar.
- Halten Sie sich bei der Bearbeitung nicht zulange mit einer (Teil-)Aufgabe auf. Wenn Sie die Aufgabe nicht sofort lösen können, machen Sie lieber mit der nächsten Aufgabe weiter.
- **Es werden nur solche Ergebnisse gewertet, bei denen ein Lösungsweg erkennbar ist.** Textaufgaben sind **grundsätzlich zu begründen**, falls es in der jeweiligen Teilaufgabe nicht ausdrücklich anders vermerkt ist.

Aufgabe 1 Nochmal Fourierreihe (13 Punkte)

Gegeben sei das in Abbildung 1.1 dargestellte, periodische Signal, welches im Folgenden als Fourierreihe

$$s(t) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos(k\omega t) + b_k \sin(k\omega t))$$

dargestellt werden soll. Die Koeffizienten für alle ganzzahligen $k > 0$ lassen sich, wie aus der Vorlesung bekannt, wie folgt bestimmen:

$$a_k = \frac{2}{T} \int_{-T/2}^{T/2} s(t) \cos(k\omega t) dt, \quad b_k = \frac{2}{T} \int_{-T/2}^{T/2} s(t) \sin(k\omega t) dt.$$

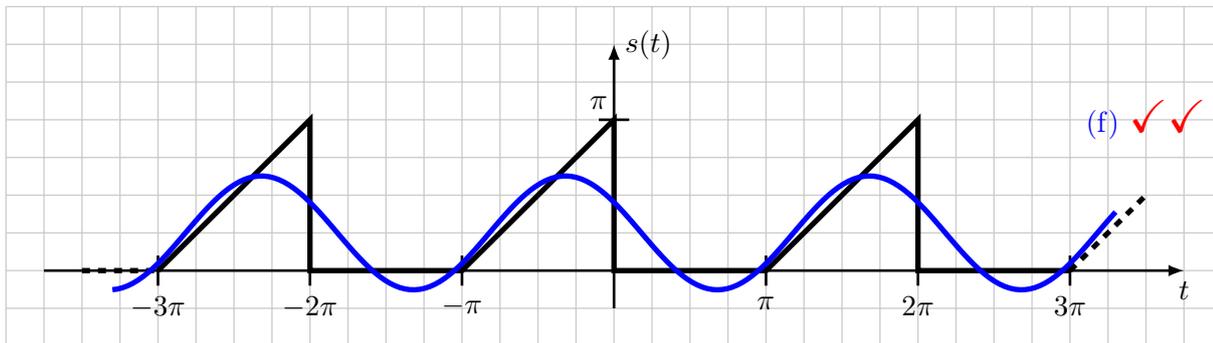


Abbildung 1.1: Periodischer Dreiecksimpuls $s(t)$

a)* Begründen Sie, weswegen dieser Grundimpuls nicht gleichstromfrei ist.



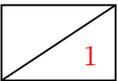
Der Impuls nimmt innerhalb einer Periode nur nicht-negative Werte an. Die positiven Anteile können sich daher nicht ausgleichen. ✓

b)* Bestimmen Sie die Periodendauer T und Kreisfrequenz ω des Signals.



$$T = 2\pi \checkmark, \quad \omega = 1 \checkmark$$

c)* Geben Sie einen analytischen Ausdruck für den Sendegrundimpuls an, also für $s(t)$ im Intervall $t \in [-\pi; \pi)$ an.



$$s(t) = \begin{cases} t + \pi & \text{für } -\pi \leq t < 0, \checkmark \\ 0 & \text{für } 0 \leq t < \pi. \checkmark \end{cases}$$

d)* Bestimmen Sie den Gleichanteil $\frac{a_0}{2}$.



$$\frac{a_0}{2} = \frac{\pi}{4} \checkmark \text{ (direkt aus Abbildung 1.1 oder mittels Integral bestimmbar)}$$

e)* Was lässt sich über a_k und b_k für $k > 0$ sagen? (Begründung!)



$s(t)$ ist weder punktsymmetrisch noch achsensymmetrisch zur Ordinate, weswegen beide Anteile nicht null sind. \checkmark

f) Bestimmen Sie die Kosinusanteile a_k für $k > 0$.

Hinweis: Je nach Lösungsweg ist einer der beiden folgenden Hinweise hilfreich:

$$\int t \cos(kt) dt = \frac{kt \sin(kt) + \cos(kt)}{k^2} + const$$

$$\int_a^b f'(t) \cdot g(t) dt = [f(t) \cdot g(t)]_a^b - \int_a^b f(t) \cdot g'(t) dt$$



$$\begin{aligned} a_k &= \frac{2}{T} \int_{-T/2}^{T/2} (\pi + t) \cos(k\omega t) dt \\ &= \int_{-\pi}^0 \cos(kt) dt + \frac{1}{\pi} \int_{-\pi}^0 t \cos(kt) dt \checkmark \\ &= \left[\frac{\sin(kt)}{k} \right]_{-\pi}^0 + \frac{1}{\pi} \left[\frac{kt \sin(kt) + \cos(kt)}{k^2} \right]_{-\pi}^0 \checkmark \\ &= \begin{cases} \frac{2}{k^2\pi} & \text{für } k = 1, 3, 5, \dots \checkmark \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

g) Bestimmen Sie die Sinusanteile b_k für $k > 0$.

Hinweis: Je nach Lösungsweg ist einer der beiden folgenden Hinweise hilfreich:

$$\int t \sin(kt) dt = \frac{\sin(kt) - kt \cos(kt)}{k^2} + const$$

$$\int_a^b f'(t) \cdot g(t) dt = [f(t) \cdot g(t)]_a^b - \int_a^b f(t) \cdot g'(t) dt$$



$$\begin{aligned}
 b_k &= \frac{2}{T} \int_{-T/2}^{T/2} (\pi + t) \sin(k\omega t) dt \\
 &= \int_{-\pi}^0 \sin(kt) dt + \frac{1}{\pi} \int_{-\pi}^0 t \sin(kt) dt \quad \checkmark \\
 &= \left[-\frac{\cos(kt)}{k} \right]_{-\pi}^0 + \frac{1}{\pi} \left[\frac{\sin(kt) - kt \cos(kt)}{k^2} \right]_{-\pi}^0 \quad \checkmark \\
 &= -\frac{1}{k} \quad \checkmark
 \end{aligned}$$

h) Skizzieren Sie das approximierte Signal $s'(t) = \frac{a_0}{2} + a_1 \cos(\omega t) + b_1 \sin(\omega t)$ in Abbildung 1.1.

Hinweis: Die Amplitude muss nicht exakt¹ stimmen. Wichtig ist, dass das Signal phasenrichtig eingezeichnet ist. Es kann hilfreich sein, zunächst die beiden Anteile getrennt einzuzichnen und anschließend deren Summe zu skizzieren.

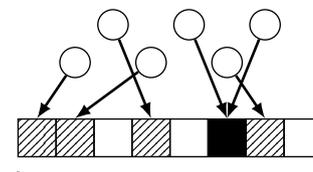


¹„Nicht exakt“ heißt, dass die Amplitude auf etwa ± 2 mm stimmen sollte. Außerdem sollten Sinus bzw. Kosinus als solche erkennbar sein.

Aufgabe 2 Framed Slotted ALOHA (15 Punkte)

Im Folgenden betrachten wir Framed Slotted ALOHA, eine Erweiterung zu Slotted Aloha, welches als Medienzugriffsverfahren bei RFID² zum Einsatz kommen kann. Wir gehen davon aus, dass eine Menge von n Stationen, im Folgenden Tags genannt, mit einem so genannten Reader kommunizieren. Wir betrachten in dieser Aufgabe lediglich einen Anwendungsfall, nämlich das Auffinden der verschiedenen Tags durch den Reader. Dies geschieht wie folgt:

- Der Reader sendet die Framelänge s an alle Tags in Reichweite. Die Framelänge ist dabei eine natürliche Zahl, welche die Anzahl der Slots angibt.
- Jeder Tag N_i , $1 \leq i \leq n$, wählt zufällig und gleichverteilt einen Slot S_j , $1 \leq j \leq s$, während dem der eigene Identifier an den Reader gesendet wird.
- Wenn mehrere Tags im selben Slot senden, kommt es zu einer Kollision. Diese wird vom Reader durch die Überprüfung der Prüfsumme erkannt.
- Ein Slot, in welchem eine Identifizierung gelingt, d.h. genau ein Tag sendet, wird als **Discovery Slot** bezeichnet.



Frame mit s Slots

○ RFID-Tag (Anzahl n)

□ Freier Slot

▨ Discovery Slot

■ Slot mit Kollisionen

Abbildung 2.1: Funktionsweise Framed Slotted Aloha

a)* Um welche Art von Multiplexing-Verfahren handelt es sich hierbei?

Time Devision Multiplexing (TDM) ✓

b)* Bestimmen Sie allgemein die Wahrscheinlichkeit p , dass ein Tag N_i im Slot S_j sendet.

$$p = \frac{1}{s} \checkmark$$

Sei X_j die Zufallsvariable, welche die Anzahl gleichzeitig sendender Tags während des Slots S_j angibt. Diese ist abhängig von der Anzahl der Slots s im Frame und der Anzahl der Tags n . $\Pr_{s,n}[X_j = k]$ beschreibt also die Wahrscheinlichkeit, dass bei gegebenem s und n genau k Tags im Slot S_j senden.

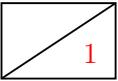
c) Bestimmen Sie allgemein die Wahrscheinlichkeit dafür, dass es sich bei Slot S_j um einen Discovery Slot handelt.

$$\Pr_{s,n}[X_j = 1] \checkmark = np \cdot (1 - p)^{n-1} \checkmark$$

²Dabei handelt es sich um ein Verfahren zur kabellosen Identifikation von Objekten, z.B. elektronische Etiketten in der Warenwirtschaft.

Gehen Sie nun von $n = 10$ Tags und einer Framelänge von $s = 20$ Slots aus.

d) Berechnen Sie nun die Wahrscheinlichkeit aus Teilaufgabe c) als Zahlenwert.



$$\begin{aligned}\Pr_{20,10}[X = 1] &= 10 \cdot \frac{1}{20} \cdot \left(1 - \frac{1}{20}\right)^9 \checkmark \\ &= 0,315 \checkmark\end{aligned}$$

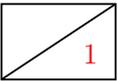
e)* Bestimmen Sie für den allgemeinen Fall die maximale Anzahl $m(s, n)$ der in einem Frame identifizierbaren Tags in Abhängigkeit von der Framelänge s und der Anzahl der Tags n .

Hinweis: Fallunterscheidung.



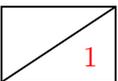
$$m(n, s) = \begin{cases} s - 1, & \text{wenn } n > s \checkmark \checkmark \\ n, & \text{wenn } n \leq s \end{cases}$$

f)* Begründen Sie, welches Problem auftritt, wenn $n \ll s$ gilt, d.h. die Anzahl der Tags erheblich kleiner ist als die Anzahl der Slots.



Das Übertragungsmedium wird nicht effektiv genutzt \checkmark , da viele Slots unbenutzt bleiben. \checkmark

g)* Begründen Sie, welches Problem auftritt, wenn $n \gg s$ gilt, d.h. die Anzahl der Tags erheblich größer ist als die Anzahl der Slots.



Kollisionswahrscheinlichkeit ist sehr hoch \checkmark , dadurch Kanal nicht effektiv genutzt \checkmark .
Alternativ: Es können nicht alle Tags in einen Frame identifiziert werden, da das Schubfachprinzip gilt.

Gehen Sie nun von einer Datenrate von $r = 2400 \frac{\text{bit}}{\text{s}}$ für die Tags aus. Die Größe eines gesendeten Identifiers mit Prüfsumme betrage $l = 12 \text{ B}$.



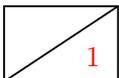
h)* Bestimmen Sie die Dauer t_{slot} eines Slots.

$$t_{\text{slot}} = t_s = \frac{l}{r} = \frac{12 \text{ B}}{2400 \frac{\text{bit}}{\text{s}}} \checkmark = 0,04 \text{ s} \checkmark$$



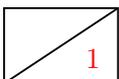
i) Geben Sie allgemein die Wahrscheinlichkeit dafür an, dass im Slot S_j **kein** Tag sendet.

$$\Pr_{s,n}[X_j = 0] \checkmark = \left(1 - \frac{1}{s}\right)^n \checkmark$$



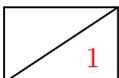
j) Bestimmen Sie die erwartete Zeit t_{idle} in Sekunden innerhalb eines Frames, während der kein Tag sendet.

$$t_{\text{idle}} = \sum_{j=1}^s \Pr_{s,n}[X_j = 0] \cdot t_{\text{slot}} \checkmark = s \cdot \Pr_{s,n}[X_1 = 0] \cdot t_{\text{slot}} = \left(1 - \frac{1}{20}\right)^{10} \cdot 20 \cdot 0,04 \text{ s} = 0,479 \text{ s} \checkmark$$



k) Bestimmen Sie die Zähldichte (diskrete Wahrscheinlichkeitsdichte) $\Pr_{s,n}[X_j = k]$.

$$\Pr_{s,n}[X_j = k] = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k} \checkmark$$



l) Welche Verteilung liegt X_j zu Grunde?

Binomialverteilung (Schlussfolgerung aus k) \checkmark

Aufgabe 3 Hexfun (21 Punkte)

Gegeben sei der Hexdump aus Abbildung 3.1, welcher einen 86 B langen Rahmen (Ethernet ohne FCS) darstellt. Die linke Spalte gibt den Offset (hexadezimal) in Vielfachen von Bytes an. Die beiden nachfolgenden Spalten repräsentieren die Daten (hexadezimal) in Blöcken zu je 8 Byte in Network-Byte-Order.

```

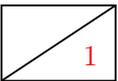
0x0000:  08 60 6e 45 dc e6 00 1c   14 01 4e 18 86 dd 60 00
0x0010:  00 00 00 20 06 40 2a 01   04 f8 0d 16 19 43 00 00
0x0020:  00 00 00 00 00 02 2a 02   02 e0 03 fe 10 01 77 77
0x0030:  77 2e 00 02 00 85 ce 44   00 50 9b 94 59 c9 2f e7
0x0040:  5d 10 50 10 65 00 85 88   00 00 47 45 54 20 2f 68
0x0050:  65 78 0d 0a 0d 0a

```

Abbildung 3.1: Hexdump eines Ethernet-Rahmens (inkl. L2-Header) in Network-Byte-Order.

Im Folgenden werden wir diese Nachricht schrittweise untersuchen. **Nutzen Sie zur Lösung die auf dem Beiblatt abgebildeten Protokoll-Header und Zusatzinformationen.**

a)* Was ist der Unterschied zwischen „Host-Byte-Order“ und „Network-Byte-Order“?



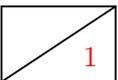
Host-Byte-Order ist die native Byte-Order eines Hosts, also Little- oder Big-Endian (bestimmt durch die CPU-Architektur). ✓ Network-Byte-Order ist stets Big-Endian. ✓

b)* Begründen Sie, weswegen überhaupt zwischen Host-Byte-Order und Network-Byte-Order zu unterscheiden ist.



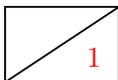
Da unklar ist, welche Byte-Order ein Host verwendet, ✓
muss die Network-Byte-Order festgelegt sein. ✓
— oder —
Schicht 1 spezifiziert im Netzwerkbereich typischerweise die Übertragung von 8-bit-Wörtern (“Oktetten”).
✓
Wie größere Wörter auf Oktette aufgeteilt werden muss daher zusätzlich spezifiziert werden. ✓

c) Das Datum 0x12 habe die Byte-Order Little-Endian. Geben Sie das Datum in Big-Endian an.



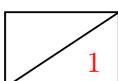
0x12 (da nur 1 B langes Datum) ✓

Für die nachfolgenden Teilaufgaben ist es sicher hilfreich, wenn Sie sich Anfang und Ende der jeweiligen Header in Abbildung 3.1 markieren. **Bitte beachten Sie, dass die nachfolgenden Teilaufgaben nur dann bewertet werden, wenn ersichtlich ist, wie Sie auf die Antwort gekommen sind** (z. B. Angabe der Werte der betreffenden Header-Felder).



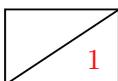
d)* Geben Sie für das erste und letzte Byte des Ethernet-Headers den Offset in Bytes vom Beginn des Rahmens an.

0x0000 – 0x000D (14 B langer Ethernet-Header) ✓



e) Welches Protokoll wird auf Schicht 3 verwendet?

Type-Feld (Ethertype) im Ethernet-Header: 0x86dd (Big-Endian) = IPv6 ✓
Falsch: Version-Feld im IP-Header, da zunächst unklar, ob überhaupt IP verwendet wird.



f) Geben Sie Funktion und Wert der L3-Header-Felder an, welche auf dem Transportweg von Routern verändert werden müssen.

Hop-Limit, Funktion: endlose Weiterleitung in Loops zu verhindern ✓, hier: 0x40 = 64 Hops ✓



g) Welche Länge hat die L3-SDU?

Payload-Length-Feld im IPv6-Header: 0x0020 = 32 B ✓



h) Markieren Sie die Absender- und Empfänger-Adresse im L3-Header. (Zeichnen Sie es direkt in Abbildung 3.1 ein und machen Sie kenntlich, welche der Adressen zum Absender und welche zum Empfänger gehört.)

i) Woran ist zu erkennen, dass TCP als L4-Protokoll verwendet wird?



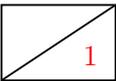
Next-Header-Feld im IPv6-Header: 0x06 = TCP ✓

Abbildung 3.2 zeigt die Schicht-4-PDU (TCP) des in Abbildung 3.1 abgebildeten Rahmens. Diese soll im Folgenden weiter untersucht werden. **Auch für die folgenden Teilaufgaben ist jeweils eine Begründung anzugeben.**

```
0x0000:  ce 44 00 50 9b 94 59 c9    2f e7 5d 10 50 10 65 00
0x0010:  85 88 00 00 47 45 54 20    2f 68 65 78 0d 0a 0d 0a
```

Abbildung 3.2: Hexdump der TCP-Payload (inkl. L4-Header) in Network-Byte-Order.

j)* Geben Sie den Quellport der Nachricht in Dezimaldarstellung an.



0xce44 (BigEndian) = 52804 ✓

k)* Geben Sie den Zielport der Nachricht in Dezimaldarstellung an.



0x0050 (BigEndian) = 80 ✓

l) Für welches Protokoll auf der Anwendungsschicht ist die Nachricht offenbar bestimmt?



TCP 80 (well-known Port) = HTTP ✓



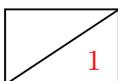
m)* Geben Sie zwei Gründe an, weswegen Sie auf Basis der Ihnen bekannten Informationen nicht bestimmen können, wie viele Byte bis zum jetzigen Zeitpunkt über diese TCP-Verbindung bereits ausgetauscht wurden.

- Die initialen Sequenznummern, die beim Verbindungsaufbau ausgetauscht wurden, sind nicht bekannt. ✓ Es fehlt also der Bezugspunkt, auf den sich Sequenz- und Bestätigungsnummern beziehen.
- Es wäre möglich, dass die Sequenznummern bereits einen Wrap-Around hatten, also mehr als 4 GiB Daten ausgetauscht wurden. ✓



n)* Wie groß ist die TCP-Payload für die Anwendungsschicht?

TCP-Header hat keine Optionen (Offset-Feld ist 5), d.h. 32 B - 20 B des TCP-Headers ✓ ergibt 12 B Payload. ✓



o)* Können nach diesem Segment innerhalb der laufenden TCP-Verbindung weiterhin Daten in dieselbe Richtung übertragen werden?

Ja, da das FIN-Flag im TCP-Header nicht gesetzt ist. ✓



p)* Können nach diesem Segment innerhalb der laufenden TCP-Verbindung noch Daten in die Gegenrichtung übertragen werden?

Unbekannt ✓, da die Gegenseite die TCP-Verbindung mittels eines vorherigen FINs bereits geschlossen haben könnte. ✓

Aufgabe 4 Domain Name System (15 Punkte)

15

Es sei zunächst die in Abbildung 4.1 dargestellte DNS-Struktur gegeben.

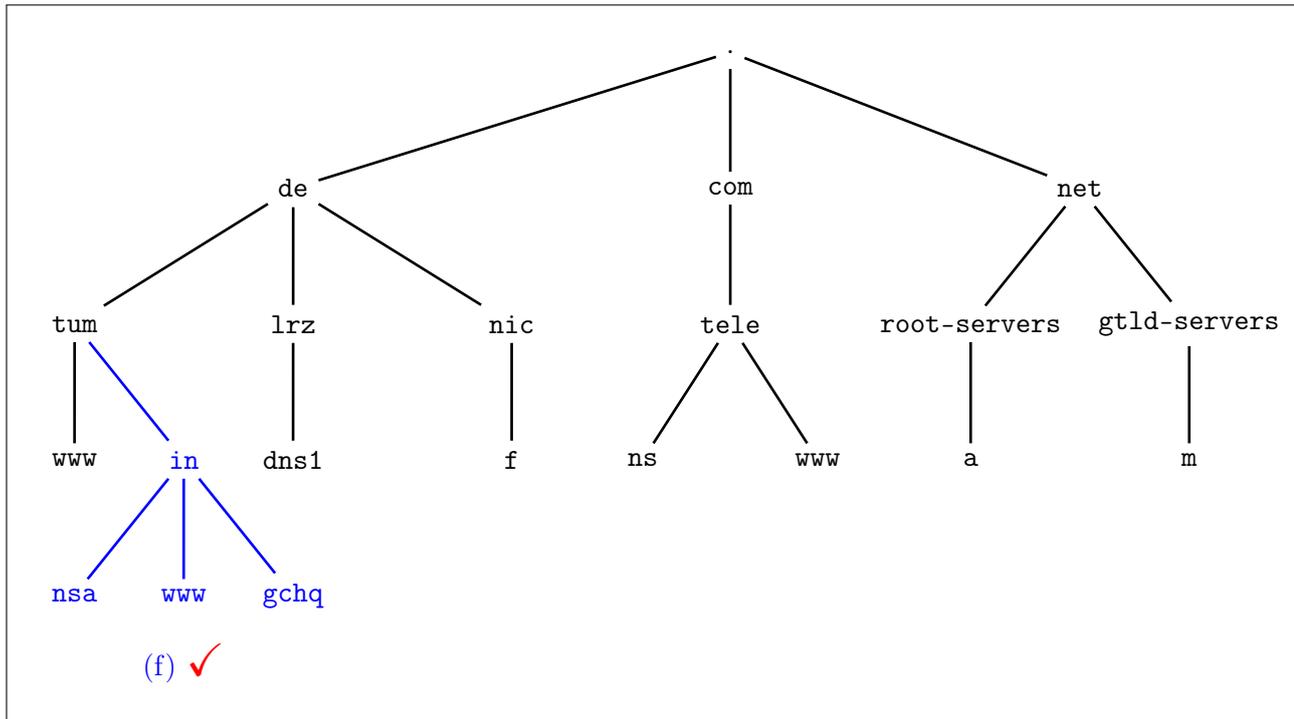


Abbildung 4.1: DNS-Struktur

a)* Erläutern Sie kurz, wozu DNS verwendet wird.

1

Mapping zwischen FQDNs und IP-Adressen. ✓

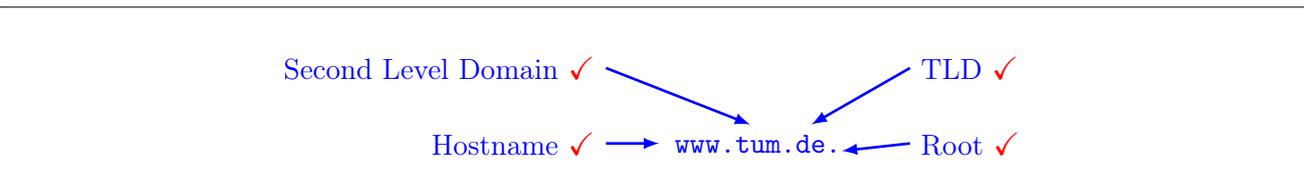
b)* Ordnen Sie DNS einer Schicht im ISO/OSI-Modell zu. (keine Begründung notwendig)

1

Schicht 7. ✓

c)* Markieren und benennen Sie für den FQDN `www.tum.de`. alle Namensbestandteile.

2



Es sei nun zusätzlich die Zonendatei für `in.tum.de.` aus Abbildung 4.2 gegeben. Für diese Zone ist ein DNS-Server namens `nsa.in.tum.de.` autoritativ.

```

$ORIGIN in.tum.de.
$TTL 1H

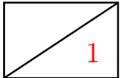
@ IN SOA nsa.in.tum.de. admin.in.tum.de. (...)

in.tum.de.      IN  NS   nsa.in.tum.de.
in.tum.de.      IN  MX   10 gchq.in.tum.de.

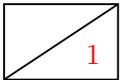
nsa.in.tum.de.  IN  A    131.159.0.1
www.in.tum.de. IN  A    168.144.144.106
gchq.in.tum.de. IN  A    131.159.0.76

```

Abbildung 4.2: DNS Zonendatei auf `nsa.in.tum.de`

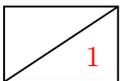


d)* Markieren Sie in Abbildung 4.2 die Zeilen, welche die Adress-Records für Hosts enthalten.

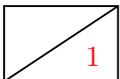


e)* Welche Funktion hat der MX-Record?

Verweist auf den FQDN eines Mailservers für die Domäne `in.tum.de..` ✓

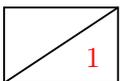


f) Ergänzen Sie Abbildung 4.1 basierend auf den Informationen aus der Zonendatei in Abbildung 4.2.



g)* Welche Möglichkeiten ergeben sich, wenn mehrere FQDNs auf dieselbe IP-Adresse verweisen?

Beispielsweise mehrere Webseiten auf demselben Server bzw. unter derselben IP-Adresse. ✓



h)* Welche Vorteile kann es haben, wenn einem FQDN mehrere IP-Adressen zugeordnet sind?

Loadbalancing ✓ (alternativ: IP-Dual-Stack, d.h. gleichzeitige Erreichbarkeit über IPv4 und IPv6)

Wir betrachten nun die in Abbildung 4.3 dargestellte Netzwerktopologie. Der Client nutzt den Router als Zugangspunkt zum Internet sowie als rekursiven DNS-Server (sogenannter Resolver). Der Router seinerseits nutzt `ns.tele.com.` als Resolver zur rekursiven Namensauflösung. Dessen IP-Adresse sei dem Router bekannt. Alle anderen DNS-Server nutzen iterative Namensauflösung, wobei nur `ns.tele.com.` Rekursion erlaubt. Die für die jeweiligen Zonen autoritativen Namensserver sind in Tabelle 4.1 aufgelistet.

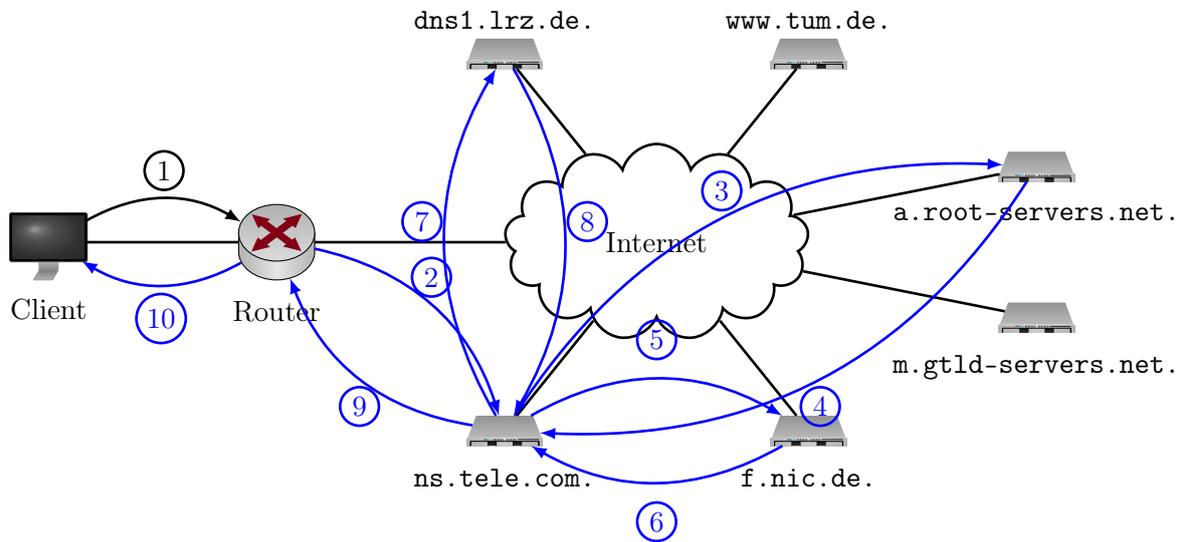


Abbildung 4.3: Netztopologie

Zone	autoritativer DNS-Server
.	a.root-servers.net.
com., net.	m.gtld-servers.net.
de.	f.nic.de.
tum.de., lrz.de.	dns1.lrz.de.
tele.com.	ns.tele.com.

Tabelle 4.1: Zonen und autoritative DNS-Server

i)* Erläutern Sie den Unterschied zwischen rekursiver und iterativer Namensauflösung.



Bei rekursiver Auflösung wird nur eine Anfrage an konfigurierten DNS-Server gestellt, welcher die finale Antwort zurückliefert. ✓
 Bei iterativer Auflösung wird stattdessen der FQDN beginnend bei der Root-Zone aufgelöst, indem die für die jeweiligen Zonen autoritativen Namensserver angefragt werden. ✓

Nehmen Sie für die folgenden Teilaufgaben an, dass alle DNS-Caches zunächst leer sind.



j) Der Client möchte nun auf `www.tum.de.` zugreifen. Zeichnen Sie in Abbildung 4.3 unter Verwendung von Tabelle 4.1 alle notwendigen DNS-Nachrichten mittels Pfeilen ein und nummerieren Sie diese der Reihenfolge nach. Die erste Nachricht ist als Hilfestellung bereits gegeben.

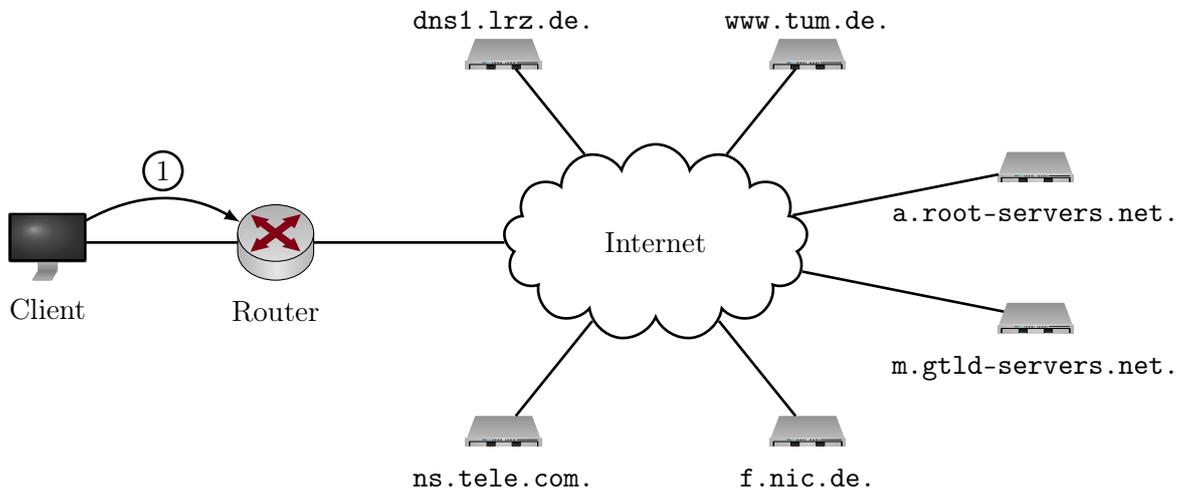
Hinweis: Bei Bedarf finden Sie am Ende dieser Aufgabe einen weiteren Vordruck von Abbildung 4.3. Bitte streichen Sie ungültige Lösungen deutlich.



k) Im unmittelbaren Anschluss möchte der Client nun `www.in.tum.de.` auflösen. Erläutern Sie kurz, inwiefern sich diese Auflösung von der in Teilaufgabe j) unterscheidet.

Infolge der in den Caches befindlichen Informationen `ns.tele.com.` direkt bei `dns1.lrz.de.` anfragen.
 ✓ Im Anschluss findet wieder eine iterative Anfrage bei `nsa.in.tum.de.` statt. ✓

Zusätzlicher Vordruck für Teilaufgabe j):

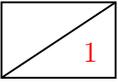


Aufgabe 5 Verschlüsselung (12 Punkte)

In dieser Aufgabe betrachten wir eine binäre Blockchiffre mit Blockgröße $n = 4$ bit. Die Verschlüsselung wird durch eine Permutation der Bits realisiert.



a)* Berechnen Sie die Anzahl der möglichen Schlüssel.



$$n! = 24 \checkmark$$

Verwenden Sie nun die konkrete Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Als Initialisierungsvektor wird $IV = 1010$ verwendet.

b)* Verschlüsseln Sie den Klartext $m = 1001\ 0011\ 1011\ 0111$ mit Hilfe des ECB-Modes.



$$m_1 = 1001 \rightarrow c_1 = 0011 \checkmark$$

$$m_2 = 0011 \rightarrow c_2 = 0110 \checkmark$$

$$m_3 = 1011 \rightarrow c_3 = 0111 \checkmark$$

$$m_4 = 0111 \rightarrow c_4 = 1110 \checkmark$$

c)* Bestimmen Sie die Klartextnachricht m für den Chiffretext $c = 1000\ 1110\ 1100$ unter der Annahme, dass der CBC-Mode für die Verschlüsselung verwendet wurde.



$$m_1 = c_0 \oplus E^{-1}(c_1) = 1010 \oplus 0100 = 1110 \checkmark$$

$$m_2 = c_1 \oplus E^{-1}(c_2) = 1000 \oplus 0111 = 1111 \checkmark$$

$$m_3 = c_2 \oplus E^{-1}(c_3) = 1110 \oplus 0110 = 1000 \checkmark$$

d)* Nennen Sie zwei Schwächen des ECB-Modes.



- Gleiche Klartextblöcke werden bei gleichem Schlüssel gleich verschlüsselt ✓
- Eine Änderung der Reihenfolge der Chiffretextblöcke wird nicht erkannt. ✓

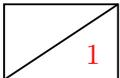
Eine Methode zum Brechen einer Verschlüsselung ist der sogenannte Brute-Force-Angriff. Dabei werden einfach alle möglichen Schlüssel auf einen Geheimentext angewendet und das Ergebnis mit einem bekannten Klartext verglichen, bis der korrekte Schlüssel ermittelt wurde.

Nehmen Sie an, dass ein 56 bit langer Schlüssel bei einer Blockgröße von jetzt $n' = 64$ bit verwendet wurde. Ihnen liegt zu einem Chiffretext der entsprechende Klartext vor. Ferner sind Sie in der Lage, pro Sekunde 100 GB zu ver- bzw. entschlüsseln.



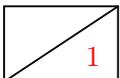
e)* Berechnen Sie die Anzahl der Schlüssel, die auf diese Weise pro Sekunde getestet werden können.

$$r_k = \frac{100 \frac{\text{GB}}{\text{s}}}{64 \text{ bit}} = 1.25 \cdot 10^{10} \frac{\text{Schlüssel}}{\text{s}} \quad \checkmark$$



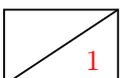
f) Berechnen Sie die mittlere Zeit, bis der richtige Schlüssel gefunden ist.

$$\bar{t} = \frac{1}{2} \frac{2^{56}}{r_k} \approx 33 \text{ d} \quad \checkmark$$



g) Welche Schlussfolgerung bezüglich der langfristigen Sicherheit der so verschlüsselten Daten können Sie aus der obigen Rechnung ziehen?

Aufgrund des kurzen Schlüssels unsicher. ✓



h)* Welche Kriterien muss eine Zahl erfüllen, sodass es sich um eine Primzahl handelt?

Primzahlen sind natürliche Zahlen mit genau zwei Teilern, nämlich sich selbst und 1. ✓

Aufgabe 6 Kurzaufgaben (9 Punkte)

Die folgenden Kurzaufgaben sind **jeweils unabhängig voneinander**. Stichpunktartige Antworten sind ausreichend!



a)* Ein Router fragmentiert ein eingehendes IPv4-Paket der Größe 1280 B aufgrund einer Folge-MTU von 660 B. Geben Sie in der nachfolgende Tabelle entsprechend die Werte der IPv4-Header-Felder an. Gehen Sie von minimalen IPv4-Headern aus.



Paket/Fragment	Total Length ✓	DF ✓	MF ✓	Fragment Offset ✓
eingehendes Paket	1280	0	0	0
ausgehendes Fragment 1	660	0	1	0
ausgehendes Fragment 2	640	0	0	80

b)* Beschreiben Sie, was man unter einer Collision Domain versteht.



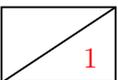
Den Teilbereich eines Netzwerks, innerhalb dessen bei gleichzeitigem Senden ✓ zweiter Knoten eine Kollision auftritt. ✓

c)* Beschreiben Sie, was man unter einer Broadcast Domain versteht.



Den gesamten Bereich eines Netzwerks, welcher durch einen Broadcast auf Layer 2 erreichbar ist ✓ (also alles bis zum nächsten Router).

d)* Was ist der wesentliche Unterschied zwischen Switching und Routing?



Beim Switching werden Weiterleitungsentscheidungen auf Basis von Layer-2-Adressen getroffen ✓, beim Routing auf Basis von Layer-3-Adressen (logischen Adressen mit Struktur). ✓

e)* Was versteht man unter einem „Burstfehler“?



Das Kippen mehrerer Bits ✓ in Folge. ✓

f)* Nennen Sie je eine Gemeinsamkeit und einen Unterschied zwischen Bus und Hub.



Hub ist ein Sternverteiler ✓, bildet intern aber einen Bus. ✓

—oder—

Unterschied: ein Hub kann Signale verstärken. ✓

Gemeinsamkeit: beide bilden Kollisionsdomänen. ✓

g)* Geben Sie die Datenrate $r = 1 \frac{\text{Gbit}}{\text{s}}$ in der Einheit $\frac{\text{MiB}}{\text{s}}$ an.



$$r' = \frac{r \cdot 10^9}{2^{20} \cdot 8} \checkmark = 119,21 \frac{\text{MiB}}{\text{s}} \checkmark$$

h)* Eine IPv4-Adresse ist 4 B lang. Wie lang ist eine IPv6-Adresse?



16 B ✓ (s. Beiblatt)

