Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Eexam
Place student sticker here

Note:

- During the attendance check a sticker containing a unique code will be put on this exam.
- This code contains a unique number that associates this exam with your registration number.
- This number is printed both next to the code and to the signature field in the attendance check list.

Grundlagen Rechnernetze und Verteilte Systeme

Exam:	IN0010 / Hausaufgabe 11	**Date:**	Monday 15th June, 2020
Examiner:	Prof. Dr.-Ing. Georg Carle	**Time:**	14:00 – 23:59

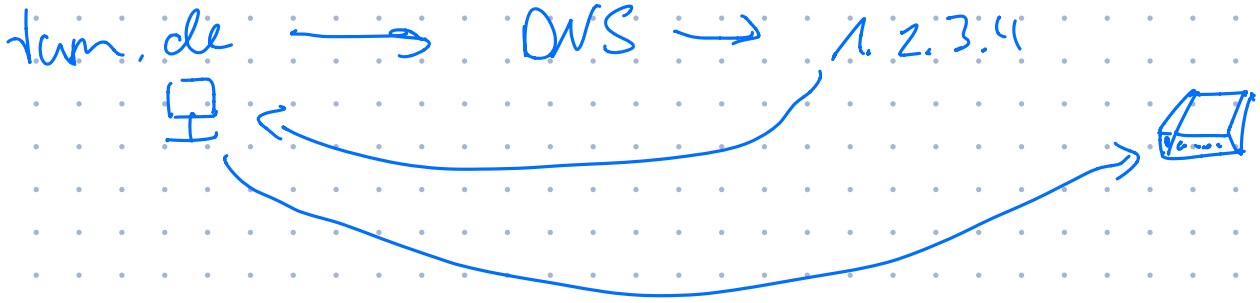
Working instructions

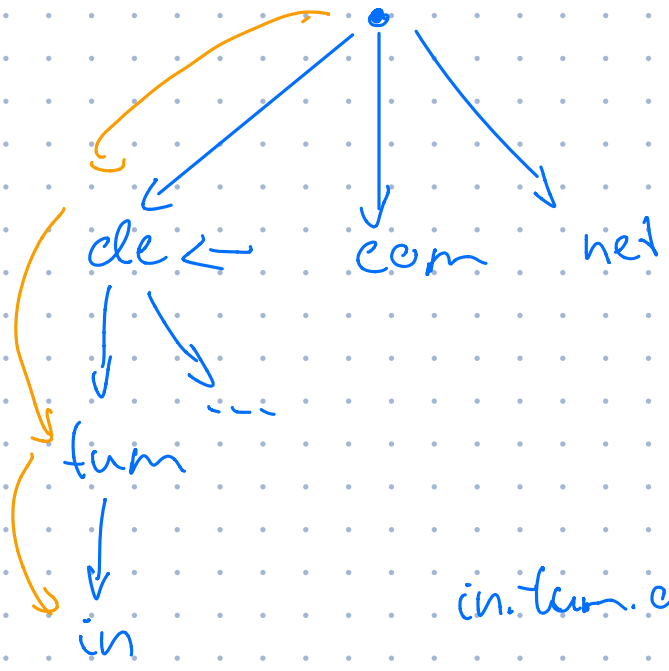
- Die erreichbare Gesamtpunktzahl beträgt 36 credits.
- Bitte geben Sie bis spätestens Montag, den **20. Juli um 23:59 CEST** über TUMexam ab.
  Bitte haben Sie Verständnis, wenn das Abgabesystem noch nicht reibungslos funktioniert. Wir arbeiten daran!
- Ihren **persönlichen** Link zur Abgabe finden Sie auf Moodle. Geben Sie diesen **nicht** weiter.
- Bitte haben Sie Verständnis, falls die Abgabeseite zeitweilig nicht erreichbar ist.

Bitte nehmen Sie die Hausaufgaben dennoch ernst:

- Neben der Einübung des Vorlesungsstoffs und der Klausurvorbereitung dienen die Hausaufgaben auch dazu, den Ablauf der Midterm zu erproben.
- Finden Sie einen für sich selbst praktikablen und effizienten Weg, die Hausaufgaben zu bearbeiten. Hinweise hierzu haben wir auf `https://grnvs.net.in.tum.de/homework_submission_details.pdf` für Sie zusammengestellt.

Left room from _____ to _____ / Early submission at _____





in.tum.de.

in.tum

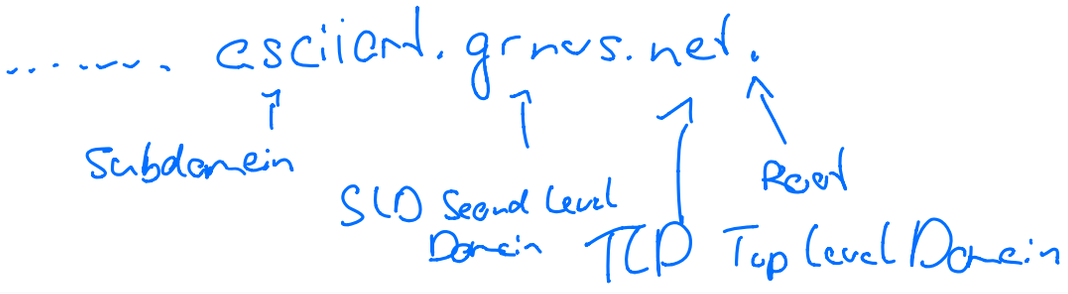
Problem 1 Domain Name System (DNS) (14 credits)

Hinweis: Angelehnt an Endterm 2015
Zentrale Aufgabe des Domain Name Systems (DNS) ist es, menschenlesbare Namen auf IP-Adressen abzubilden, die dann für die Wegwahl auf der Netzwerkschicht verwendet werden können. Bei dem Namen `asciiart.grnvs.net.` handelt es sich um einen sog. *Fully Qualified Domain Name (FQDN)*.

0 1 a)* Was ist der Unterschied zwischen einem vollqualifizierten Domain Name (FQDN) und einem nicht-(voll)qualifizierten?

Ein FQDN ist immer relativ zur globale root. (Endet mit einem .)
Ein nicht-fully qualified domain name ist relativ zu einer anderen Domain. (Endet nicht mit einem Punkt)

0 1 2 b)* Benennen Sie die einzelnen Bestandteile des FQDNs, sofern es dafür gängige Bezeichnungen gibt.



In Abbildung 1.1 sind ein PC sowie eine Reihe von Servern dargestellt. Wir nehmen an, dass PC1 den Router als Resolver nutzt. Der Router wiederrum nutzt einen Resolver von Google unter der IP-Adresse 8.8.8.8 zur Namensauflösung. Ferner nehmen wir an, dass der Google-Resolver gerade neu gestartet wurde (also insbesondere keine Resource Records gecached hat) und rekursive Namensauflösung anbietet.
Die autoritativen Nameserver für die jeweiligen Zonen sind in Tabelle 1.1 gegeben.

Zone	autoritativer Nameserver
.	`d.root-servers.net.`
`com.`, `net.`	`a.gtld-servers.net.`
`google.com.`	`ns1.google.com.`
`grnvs.net.`	`bifrost.grnvs.net.`

Table 1.1: Zonen mit zugehörigen autoritativen Nameservern

0 1 2 c)* Erläutern Sie den Unterschied zwischen einem *Resolver* und einem *Nameserver*.

Nameserver: Server der autoritativ für eine Zone (Domains) ist

Resolver: Ein Server der Namensauflösung anbietet, Resolver erhebt iterativer Namensauflösung und gibt das Ergebnis der Namensauflösung an den Anfragenden zurück.

d)* Welche Funktion erfüllen `d.root-servers.net` und `a.gtld-servers.net`?

0
1

a-root-servers.net: Autoritativ für die Root Zone.

a.gtld-servers.net: Autoritativ für com. und net.

e)* Erklären Sie den Unterschied zwischen iterativer und rekursiver Namensauflösung.

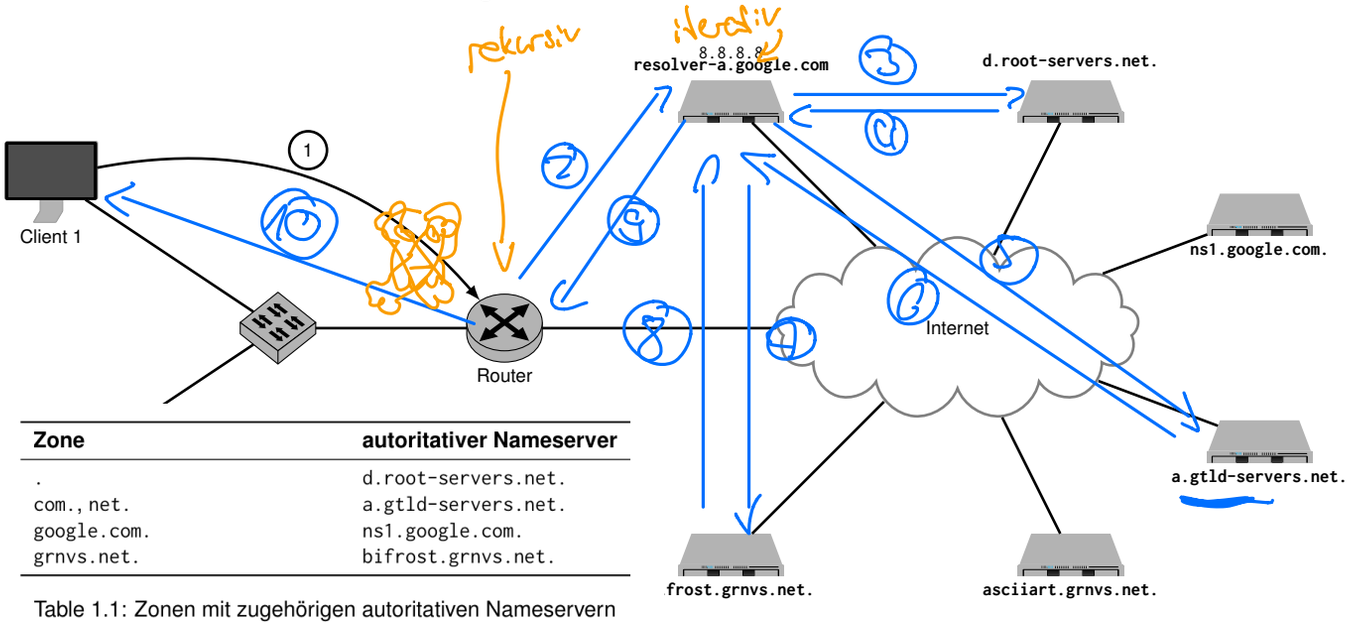
0
1
2

iterativ: Ein Server fragt nacheinander die autoritativen Nameserver von der Root hoch an um eine Domain aufzulösen.

rekursiv: DNS-Anfrage wird an einen Resolver weiter geleitet, Resolver betreibt iterative Namensauflösung und gibt die resultierende IP an den Auftraggeber zurück.

f) Zeichnen Sie in Abbildung 1.1 alle DNS-Nachrichten (Requests / Responses) ein, die ausgetauscht werden, sobald PC1 auf `asciiart.grnvs.net` zugreift. Nummerieren Sie die Nachrichten gemäß der Reihenfolge, in der sie zwischen den einzelnen Knoten ausgetauscht werden.

0
1
2
3
4
5



Zone	autoritativer Nameserver
.	d.root-servers.net.
com., net.	a.gtld-servers.net.
google.com.	ns1.google.com.
grnvs.net.	bifrost.grnvs.net.

Table 1.1: Zonen mit zugehörigen autoritativen Nameservern

Figure 1.1: Vorlage zu Aufgabe 1f)

g)* Wie wird im DNS sichergestellt, dass kein bösartiger Nameserver Anfragen für andere Domänen beantwortet? (Wir gehen davon aus, dass keine Man-in-the-Middle-Angriffe möglich sind.)

0
1

Es wird sichergestellt, dass keine bösartigen Nameserver angefragt werden, in dem an Nameserver stets nur andere Nameserver gistet, denen er vertraut.

Der Resolver muss daher nur dem Root-Nameserver vertrauen.

Die Erweiterung DNSSEC führt diese Kommunikation zwischen verschlüsselt aus.

Problem 2 **Kompression: Huffman-Kodierung (12 credits)**

Gegeben sei das Alphabet $\mathcal{A} = \{a, b, c, d\}$ und die Nachricht

$$m = \text{aabcbdacababbbbcbddbbbaababdbdbb} \in \mathcal{A}^{32}.$$

0 1 2 a)* Bestimmen Sie die Auftrittswahrscheinlichkeiten $p_i \in \mathcal{A}$ der einzelnen Zeichen in m.

Zeichen	p_i
a	$8/32 = 1/4$
b	$16/32 = 1/2$
c	$3/32 \approx 0{,}09$
d	$5/32 \approx 0{,}16$

0 1 2 b) Bestimmen Sie den Informationsgehalt $I(p_i)$ der einzelnen Zeichen aus $\mathcal{A}$.

$I(p_a) = -\log_2\left(\frac{1}{4}\right) = 2$ bit

$I(p_b) = -\log_2\left(\frac{1}{2}\right) = 1$ bit

$I(p_c) \approx 3{,}4$ bit

$I(p_d) \approx 2{,}7$ bit

$I(p_i) = -\log_2(p_i)$

0 1 2 c) Die Nachricht m stamme aus einer Nachrichtenquelle X. Bestimmen Sie auf Basis der bisherigen Ergebnisse die Quellenentropie $H(X)$.

$$H(X) = \sum_{x \in X} p_x \, I(p_x)$$

$$= \frac{1}{4} \cdot 2\,\text{bit} + \frac{1}{2} \cdot 1\,\text{bit} + \frac{3}{32} \cdot 3{,}4\,\text{bit} + \frac{5}{32} \cdot 2{,}7\,\text{bit}$$

$$\approx 1{,}738\,\text{bit}$$

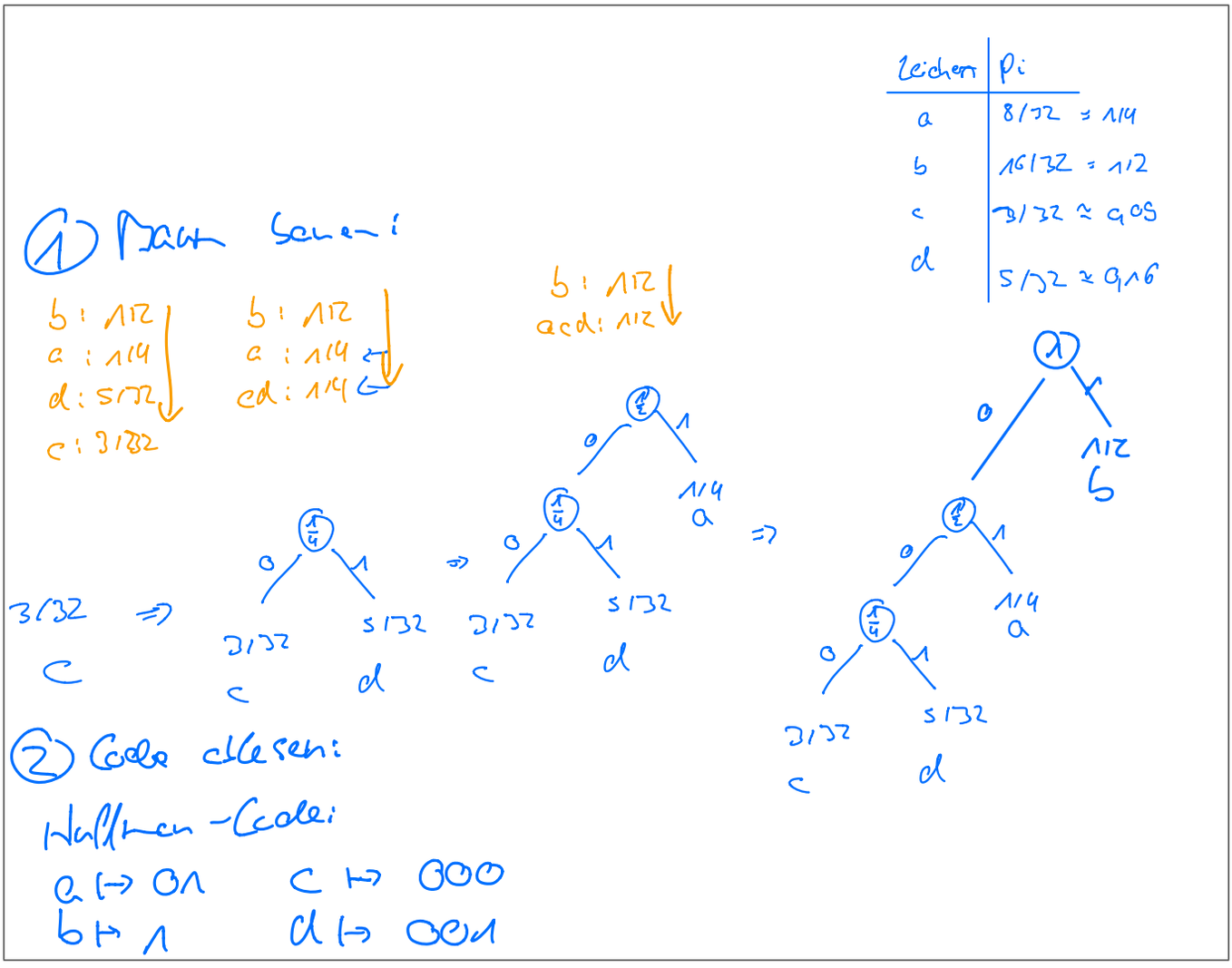
Jedes Zeichen lässt sich somit mit durchschnittlich 1,738 bit codieren.

Naive Codierung: 2 bit pro Zeichen!

d) Bestimmen Sie nun einen binären Huffman-Code C für diese Nachrichtenquelle.

0 1 2 3

Zeichen	p_i
a	8/32 = 1/4
b	16/32 = 1/2
c	3/32 ≈ 0,09
d	5/32 ≈ 0,16



e) Bestimmen Sie die durchschnittliche Codewortlänge von C.

0 1 2

$$\overline{L_C} = \sum_{i \in A} p_i \cdot l(i)$$

$$= \frac{1}{4} \cdot 2 \text{ bit} + \frac{1}{2} \cdot 1 \text{ bit} + \frac{3}{32} \cdot 3 \text{ bit} + \frac{5}{32} \cdot 3 \text{ bit} = 1{,}75 \text{ bit}$$

f) Vergleichen Sie die durchschnittliche Codewortlänge von C mit der Codewortlänge eines uniformen[1] Binärcodes.

0 1

Der uniforme Binärcode verwendet 2 bit pro Zeichen
Der Huffman Code durchschnittlich 1,75 bit pro Zeichen

⇒ Verbesserung um 12,5 %

[1] Ein Code heißt *uniform*, wenn alle Codewörter dieselbe Länge aufweisen.

Problem 3 SMTP (Hausaufgabe) (10 credits)

Für daheim: Mailversand von der Kommandozeile
Sie haben in der Vorlesung gelernt, dass mithilfe des Programms `telnet` bzw. mit dem s_client von OpenSSL Verbindungen zu Webservern aufgebaut werden können.
Ihre Aufgabe ist nun, sich mithilfe des s_client mit dem SMTP-Servers Ihres Mailproviders zu verbinden und sich selbst eine e-Mail zu schicken. Die notwendigen Schritte können Sie sich aus dem RFC 5321 erschließen. Alternativ ist es auch möglich entsprechende Tutorials zu konsultieren. Der initiale Befehl könnte folgendermaßen aussehen: `openssl s_client -crlf -connect <smtp.server.org>:465`
Sollten Sie CRAM-MD5 verwenden wollen, könnte Ihnen die folgende Bash-Funktion zur Berechnung der Response auf eine vom Server gegebene Challenge helfen:

```
cram() {
  challenge=$1
  username=$2
  challenge=$(echo -n $challenge|base64 -d)
  echo "Challenge is: $challenge"
  read -sp "Password for $username: " password
  echo ""
  hash=$(echo -n "$challenge" |openssl md5 -hmac "$password" -hex|cut -d" " -f 2 )
  response=$(echo -n "$username $hash" |base64)
  echo "Response for server is: "
  echo $response
}
```

Rufen sie Sie dann folgendermaßen auf:
`cram <CHALLENGE> <USERNAME>`

0 1 2 3 4

a)* Pasten Sie den Output.

b) Ermitteln Sie, welche Authentifizierungsmethoden der von Ihnen gewählte SMTP-Server anbietet und erläutern Sie den Unterschied zwischen den Methoden.

0 1 2 3 4

c) Warum ist überhaupt eine Authentifizierung notwendig? Welche Probleme werden dadurch behoben oder zumindest verringert?

0 1 2

Additional space for solutions–clearly mark the (sub)problem your answers are related to and strike out invalid solutions.