1190

Testklausur: Einführung in die EDV WS 2009/10

Immatrikulationsnr. _____

Name, Vorname _____

Hinweise:

- Halten Sie die Klausurblätter geschlossen, bis durch die Aufsichtspersonen der Beginn angezeigt wird
- Achten Sie bitte darauf, dass auf Ihren Blättern links oben immer die gleiche Zahl steht. Falls nicht, melden Sie sich bitte bei einer Aufsichtsperson
- lesen Sie die einzelnen Aufgaben sorgfältig durch
- kreuzen Sie dann die richtige (nur *eine*!) Antwortalternative an
- Betrugsversuche haben sofortigen Ausschluss von der Klausur und Nichtbestehen zur Folge
- Legen Sie Personalausweis und Studiausweis gut sichtbar auf Ihren Tisch

Fragenblock
In den Übungen wurden die Grundlagen der Erstellung von Webseiten mittels HTML als auch die Dokumentenerstellung mit LaTeX vermittelt. Folgender Fragenblock bezieht sich auf diesen Teil der Übungen:

Frage 1
Bei welchem der folgenden Zeichenfolgen handelt es sich *nicht* um ein HTML-Tag?
- a ☐ li
- b ☐ re
- c ☐ head
- d ☐ name

Frage 2
Betrachten Sie folgendes LaTeX Fragment:

```
\begin{itemize}
\item Folgende Punkte:
\begin{enumerate}
\item Unterpunkt 1
X
Y
```

Was sollte anstatt den Platzhaltern X und Y stehen?
- a ☐
  ```
  X=\end{abstract} Y=\end{document}
  ```
- b ☐
  ```
  X=\end{enumerate} Y=\end{itemize}
  ```
- c ☐
  ```
  X=\end{document} Y=\end{abstract}
  ```
- d ☐
  ```
  X=\end{itemize} Y=\end{enumerate}
  ```

Fragenblock
Ein großes Thema in der Vorlesung war "Verschlüsselung". Dabei wurde sowohl auf mögliche Einsatzzwecke von Verschlüsselung eingegangen, als auch konkrete Verschlüsselungsverfahren erläutert.

Frage 3
Wie sollte ein OTP erzeugt werden?
- a ☐ zufällig
- b ☐ die 01-Sequenz sollte der Binärdarstellung von π entsprechen
- c ☐ völlig egal
- d ☐ auf jeden Fall muss in jedem Präfix die Anzahl der 1en die Anzahl der 0en übersteigen

Frage 4

Ihr Freund hat einen RSA-Schlüssel K1 auf seine Webseite gestellt und einen passenden RSA-Schlüssel K2 an einem sicheren Ort verwahrt.

Wie ist der Ablauf, wenn Sie Ihrem Freund eine Nachricht M schicken wollen, sodass kein Dritter den Inhalt mitlesen kann?

- *a* ☐ Nachricht M wird mit K2 verschlüsselt; die verschlüsselte Nachricht an Ihren Freund geschickt, der die verschlüsselte Nachricht mit K2 wieder entschlüsselt (K1 ist nur ein Reserveschlüssel)
- *b* ☐ Nachricht M wird mit K1 verschlüsselt; die verschlüsselte Nachricht an Ihren Freund geschickt, der die verschlüsselte Nachricht mit K1 wieder entschlüsselt (K2 ist nur ein Reserveschlüssel)
- *c* ☐ Nachricht M wird mit K1 verschlüsselt; die verschlüsselte Nachricht an Ihren Freund geschickt, der die verschlüsselte Nachricht mit K2 entschlüsselt
- *d* ☐ Nachricht M wird mit K2 verschlüsselt; die verschlüsselte Nachricht an Ihren Freund geschickt, der die verschlüsselte Nachricht mit K1 entschlüsselt

Frage 5

Bei welchem der folgenden Verfahren handelt es sich um *kein* Verschlüsselungsverfahren

- *a* ☐ OneTimePad
- *b* ☐ RSA-Code
- *c* ☐ AES
- *d* ☐ Hamming-Code

Frage 6

Ihr Freund hat einen RSA-Schlüssel K1 auf seine Webseite gestellt und einen passenden RSA-Schlüssel K2 an einem sicheren Ort verwahrt.

Welchen Namen hat der Schlüssel K1 ?

- *a* ☐ Privater Schlüssel
- *b* ☐ Geheimer Schlüssel
- *c* ☐ Superschlüssel
- *d* ☐ Öffentlicher Schlüssel

Frage 7

Ihr Freund hat einen RSA-Schlüssel K1 auf seine Webseite gestellt und einen passenden RSA-Schlüssel K2 an einem sicheren Ort verwahrt.
Ihr Freund möchte Ihnen eine Nachricht M schicken, von der Sie sichergehen können, dass Sie von ihm kommt (es sei zunächst unwichtig, ob jemand die Nachricht mitlesen kann oder nicht). Wie ist der Ablauf, um das zu erreichen?

- *a*☐ Nachricht M wird mit K2 verschlüsselt; die verschlüsselte Nachricht samt der Originalnachricht an Sie geschickt; Sie entschlüsseln die verschlüsselte Nachricht mit K1, falls der Inhalt mit der unverschlüsselten Nachricht übereinstimmt, kam Sie von Ihrem Freund
- *b*☐ Nachricht M wird mit Schlüssel K1 verschlüsselt und zusammen mit der unverschlüsselten Nachricht an Sie verschickt; Sie entschlüsseln mit K1 und K2 die Nachricht und können feststellen, ob Sie von Ihrem Freund stammt
- *c*☐ Nachricht M wird mit K1 verschlüsselt; die verschlüsselte Nachricht samt der Originalnachricht an Sie geschickt; Sie entschlüsseln die verschlüsselte Nachricht mit K2, falls der Inhalt mit der unverschlüsselten Nachricht übereinstimmt, kam Sie von Ihrem Freund
- *d*☐ Nachricht M wird mit Schlüssel K2 verschlüsselt und zusammen mit der unverschlüsselten Nachricht an Sie verschickt; Sie entschlüsseln mit K1 und K2 die Nachricht und können feststellen, ob Sie von Ihrem Freund stammt

Frage 8

Sie haben mit Ihrem Freund folgendes OTP ausgetauscht:
0101011000110111010101110101000101 01
und möchten folgende Nachricht verschlüsseln:
0100101010101101010101010011011000
Welche verschlüsselte Nachricht verschicken Sie an Ihren Freund?

- *a*☐ 000111000001101000000010111111010
- *b*☐ 000111001001101000000010011111010
- *c*☐ 010101110010101001100110010101010
- *d*☐ 01001101000000010011

Fragenblock

Folgende Fragen beziehen sich auf den Übungsabschnitt über Tabellenkalkulationen.

Frage 9

Betrachten Sie folgende beiden Einträge in zwei (verschiedenen) Zellen Ihrer Tabellenkalkulation:

- =B1*B2
- =B1*B2

Worin besteht der Unterschied?

- *a*☐ Die zweite Zeile greift auf Daten außerhalb des aktuellen Sheets zu.
- *b*☐ In der ersten Zelle werden B1 und B2 relativ referenziert, in der zweiten Zelle werden B1 und B2 absolut referenziert
- *c*☐ Beide Zelleneinträge sind völlig äquivalent
- *d*☐ In der ersten Zelle werden B1 und B2 absolut referenziert, in der zweiten Zelle werden B1 und B2 relativ referenziert

Fragenblock
In der Vorlesung wurden sowohl Sinn und Zweck von Kompressionsverfahren behandelt, als auch auf einige konkrete Kompressionsverfahren im Detail eingegangen. Die folgenden Fragen beziehen sich auf diesen Vorlesungsabschnitt:

Frage 10
Nehmen wir an, Sie verschicken viele Dokumente per EMail, in denen Buchstaben mit folgenden Häufigkeiten auftreten:

- A: 20%
- B: 50%
- C: 25%
- D: 5%

Um Bandbreite bei der Übertragung der Texte zu sparen, erstellt Ihnen Ihr Praktikant 4 Codes. Welcher dieser Codes könnte ein Shannon-Fano-Code sein, wie er in der Vorlesung behandelt wurde?

a☐ A:101 B:1 C:11 D:100
b☐ A:1 B:2 C:3 D:4
c☐ A:110 B:0 C:10 D:111
d☐ A:101 B:100 C:01 D:00

Frage 11
Welche zwei grundlegend verschiedenen Arten von Kompression wurden in der Vorlesung angesprochen

a☐ legale und illegale Kompression
b☐ sichere und unsichere Kompression
c☐ effiziente und nichteffiziente Kompression
d☐ verlustfreie und verlustbehaftete Kompression

Frage 12
Welche drei der folgenden Dateiformate gehören einer Klasse von Kompressionsverfahren an?

(1) MP3
(2) ZIP
(3) MPEG2
(4) Ogg Vorbis
(5) PNG
(6) Bz2

a☐ 1,5,6
b☐ 2,3,4
c☐ 2,5,6
d☐ 1,3,5

Fragenblock
Fehlerkorrekturcodes waren ein weiteres, recht ausführlich behandeltes Thema in der Vorlesung. Folgende Fragen beziehen sich auf den entsprechenden Block in der Vorlesung.

Frage 13
Sie haben Ihren Praktikanten beauftragt, Ihre Daten durch Speicherung eines "Parity Bits" stärker gegen ungewollte Verfälschungen zu schützen. Was ist das richtige Parity Bit für folgende binär kodierte Nachrict:
010110010101
- a ☐ 0
- b ☐ 6
- c ☐ 1
- d ☐ 5

Frage 14
Was ist die Hamming-Distanz folgender beider Codewörter?
0110110101100
1001100111001
- a ☐ 9
- b ☐ 8
- c ☐ 7
- d ☐ 6

Frage 15
Das Wort
0101
wurde kodiert zu
000111000111
Um welchen Code handelt es sich höchstwahrscheinlich?
- a ☐ Repetition-Code
- b ☐ Hufmann-Code
- c ☐ Hamming-Code
- d ☐ Shannon-Fano-Code

Fragenblock
Grundlagen zum Aufbau von Soft- und Hardware war das erste in der Vorlesung behandelte Theme. Folgende Fragen beziehen Sich auf diesen Themenkomplex.

Frage 16
Die Tatsache, dass das Betriebssystem einem Prozess die Kontrolle über die CPU/den Speicher/... entziehen kann nennt sich
- a ☐ Nash Multitasking
- b ☐ anarchistic Multitasking
- c ☐ präemptives Multitasking
- d ☐ kooperatives Multitasking

Frage 17
Welche dieser Aussagen ist nicht korrekt?
- *a* ☐ Jedes Multitasking-Betriebssystem ist auch ein Multiuser-Betriebssystem
- *b* ☐ Sowohl MacOS als auch Linux sind Multitasking Betriebssysteme.
- *c* ☐ Sowohl MacOS als auch Linux sind Multiuser Betriebssysteme.
- *d* ☐ Jedes Multiuser-Betriebssystem ist auch ein Multitasking-Betriebssystem

Frage 18
Was ist größenordnungsmäßig die Anzahl der Zeichen, die eine typische moderne Festplatte speichern kann?
- *a* ☐ 500 Billionen Zeichen
- *b* ☐ 500 Milliarden Zeichen
- *c* ☐ 500 Millionen Zeichen
- *d* ☐ 500 Trillionen Zeichen

Frage 19
Was ist die Größenordnung der Taktfrequenz moderner Prozessoren in Desktop-PCs?
- *a* ☐ 3 Milliarden
- *b* ☐ 3 Billionen
- *c* ☐ 3 Billiarden
- *d* ☐ 3 Millionen

Fragenblock
Folgende Fragen beziehen sich auf den Übungsabschnitt über elektronische Bildverarbeitung.

Frage 20
In welcher Größenordnung liegt die Pixelanzahl einer aktuellen Digital-Spiegelreflexkamera?
- *a* ☐ 8 Tausend Pixel
- *b* ☐ 8 Millionen Pixel
- *c* ☐ 8 Billionen Pixel
- *d* ☐ 8 Milliarden Pixel

Frage 21
Warum muss manchmal ein Weißabgleich durchgeführt werden?
- *a* ☐ Weil der Sensor durch zu viele Weißanteile Schaden nehmen kann
- *b* ☐ Weil der Fokus des Objektives mit der Motivstruktur abgeglichen werden muss.
- *c* ☐ Weil es sonst zu Überstrahlungen und Rauschen kommt.
- *d* ☐ Weil je nach Lichtquelle der Farbeindruck eines Bildes variiert

Frage 22
In welcher Größenordnung liegt die Anzahl an Farben, die in einem Pixel einer aktuellen Digital-Spiegelreflexkamera unterschieden werden kann?
- *a* ☐ 16 Tausend
- *b* ☐ 16 Milliarden
- *c* ☐ 16 Billionen
- *d* ☐ 16 Millionen

Frage 23
In den Übungen haben wir mittels GIMP eine Animation erstellt. Welche Funktionalität von Gimp war dabei entscheidend?

- a ☐ Flächen
- b ☐ Ebenen
- c ☐ Das Reparaturwerkzeug
- d ☐ Der Kanalmixer

Fragenblock
Ein weiteres Thema war das "Internet" und "Anonymität im Internet". Folgende Fragen beziehen sich auf diesen Themenblock.

Frage 24
Der Google PageRank ist ein integraler Bestandteil der Google Websuche, der den Rang (d.h. die Position in der Ergebnisliste) eines Suchergebnisses stark beeinflußt). Welche Maßnahme führt am Ehesten dazu, eine Webseite zum Thema "Kaninchenfutter" hoch in den Suchergebnissen zu platzieren?

- a ☐ Den Begriff "Kaninchenfutter" in allen möglichen Abkürzungen (Kaninchenf., Kan.futter, ...) auf der Webseite aufführen
- b ☐ Durch eine ansprechende Qualität der Seite viele andere Internetbenutzer dazu zu bringen, Ihre Seite zu verlinken.
- c ☐ Den Suchbegriff "Kaninchenfutter" mit besonders großer Schrift auf der Webseite darstellen
- d ☐ Den Suchbegriff "Kaninchenfutter" möglichst oft auf der Webseite erwähnen

Frage 25
Welche Maßnahme ist am ehesten geeignet, Ihre Identität beim Besuch von Webseiten zu verschleiern?

- a ☐ Immer die neuesten Betriebssystemupdates eingespielt haben.
- b ☐ Alle Webseiten nie direkt ansurfen, sondern immer erst nach einer Google-Suche
- c ☐ Benutzung eines/mehrerer Anonymisierer-Proxies
- d ☐ Den neuesten Virenscanner installiert haben.

Frage 26
Sie rufen die Webseite www.google.de auf. In welcher Reihenfolge treten dabei folgende Abläufe auf:

(1) Transfer des HTML-Codes von der Webseite

(2) Anfrage an den DNS-Server nach der IP-Adresse von www.google.de

(3) Verschicken einer Anfrage an die entsprechende IP-Adresse mit Bitte um den HTML-Code

(4) Transfer der IP-Adresse vom DNS-Server

- a ☐ (2), (4), (3), (1)
- b ☐ (1), (4), (3), (2)
- c ☐ (1), (2), (3), (4)
- d ☐ (4), (2), (3), (1)

Frage 27
Was ist die Größenordnung der Anzahl der Benutzer des Internets weltweit?
- *a* ☐ 1 Million
- *b* ☐ 1 Billion
- *c* ☐ 1 Milliarde
- *d* ☐ 100000

Fragenblock
Das Art und Weise wie Nachrichten im Internet weitergeleitet werden, wurde in der Vorlesung behandelt; der folgende Frageblock bezieht sich auf diesen Vorlesungsteil.

Frage 28
Welcher der folgenden Begriffe beschreibt *keine* Netzwerktopologie wie er in der Vorlesung aufgeführt wurde?
- *a* ☐ Meshtopologie
- *b* ☐ Baumtopologie
- *c* ☐ Lokaltopologie
- *d* ☐ Sterntopologie

Frage 29
Betrachten wir zwei parallele Straßen zwischen Stadt A und Stadt B. Auf der oberen Straße braucht man immer – unabhängig von der Verkehrslage – 2 Stunden, um von A nach B zu kommen. Auf der unteren Straße hängt die Zeit von der Anzahl der anderen Autos, die dort entlang fahren, ab und zwar beträgt die Dauer (x/1000) Stunden. 2000 Autos fahren jeden Morgen (zur gleichen Zeit) von A nach B; wenn sich jeder gemäß den Prinzipien des selfish-routing für eine Straße entscheidet, was ist dann die durchschnittliche Reisezeit?
- *a* ☐ 1 1/2 Stunden
- *b* ☐ 2 Stunden
- *c* ☐ 1 Stunde
- *d* ☐ 2 1/2 Stunden

Frage 30
Betrachten wir zwei parallele Straßen zwischen Stadt A und Stadt B. Auf der oberen Straße braucht man immer – unabhängig von der Verkehrslage – 2 Stunden, um von A nach B zu kommen. Auf der unteren Straße hängt die Zeit von der Anzahl der anderen Autos, die dort entlang fahren, ab und zwar beträgt die Dauer (x/1000) Stunden. 2000 Autos fahren jeden Morgen (zur gleichen Zeit) von A nach B; wenn diktatorisch festgelegt werden kann, wer wo langfährt, was ist dann die bestmögliche durchschnittliche Reisezeit?
- *a* ☐ 1 Stunde
- *b* ☐ 2 1/2 Stunden
- *c* ☐ 1 1/2 Stunden
- *d* ☐ 2 Stunden

Frage 31

Wie nennt man den Effekt, dass durch Hinzufügung einer Handlugsalternative (z.B. Bau einer zusätzlichen Straße) sich die Equilibriumslösung unter der Selfish-Routing Annahme verschlechtert?

- a ☐ Nash Paradox
- b ☐ Braess' Paradox
- c ☐ Beautiful Mind Paradox
- d ☐ Anarchy Paradox

Frage 32

Betrachten wir zwei parallele Straßen zwischen Stadt A und Stadt B. Auf der oberen Straße braucht man immer – unabhängig von der Verkehrslage – 2 Stunden, um von A nach B zu kommen. Auf der unteren Straße hängt die Zeit von der Anzahl der anderen Autos, die dort entlang fahren, ab und zwar beträgt die Dauer (x/1000) Stunden. 2000 Autos fahren jeden Morgen (zur gleichen Zeit) von A nach B; was ist der "Price of Anarchy", d.h. das Verhältnis der Nash-Equilibriumslösung zur global optimalen Lösung in diesem Fall?

- a ☐ 4/3
- b ☐ 3/2
- c ☐ 2 Stunden
- d ☐ 2

Frage 33

Wir hatten in der Vorlesung zwei grundlegend verschiedene Routing-Methoden kennen gelernt, welche beiden sind das?

- a ☐ sicheres und unsicheres Routing
- b ☐ zentrales und dezentrales Routing
- c ☐ zentrales und ineffizientes Routing
- d ☐ effizientes und ineffizientes Routing