Klausur SS 2011

20.07.2011

Name:	_____	Matr.Nr.:	_____
Vorname:	_____	Studiengang:	_____

Hinweise: (Bitte sorgfältig durchlesen!)

- Schreiben Sie auf **jedes Blatt** Ihren Namen und Ihre Matrikelnummer.
- Die Aufgaben können in der Regel auf den Aufgabenblättern beantwortet werden. Tragen Sie Ihre Lösungen in die dafür vorgesehenen Felder ein. Reicht der Platz nicht aus, **ist für jede Aufgabe ein neues Blatt zu verwenden**.
- Am Ende der Klausur ist das Deckblatt zusammen mit den Aufgabenblättern und evtl. zusätzlich verwendeten Blättern wieder abzugeben.
- Die Bearbeitungszeit beträgt **120 Minuten**.
- Es sind **keine Hilfsmittel** erlaubt.
- Die Klausur umfasst insgesamt **120** Punkte. Zum Bestehen genügen **60** Punkte.

Mit meiner Unterschrift bestätige ich, dass ich die Hinweise zur Kenntnis genommen habe.

_____
Unterschrift

Punktespiegel:

Aufgabe	1	2	3	4	5	6	7	$\sum$
Erreichbare Punkte	15	12	21	18	14	26	14	120
Erreichte Punkte								

Name: Matr.Nr.:

Aufgabe 1 (Allgemeine Grundlagen) **(6+3+6) = 15 Punkte**

a) Erläutern Sie knapp die Begriffe *Dienst*, *Protokoll* und *Dienstprimitiv*. Machen Sie in Ihrer Erläuterung auch klar, wie diese Begriffe in Zusammenhang stehen.

Dienst: Sammlung von Kommunikationsfunktionalitäten, die eine Kommunikation mit bestimmten Bedingung ermöglicht (Der Dienst definiert, dass "was" einer Kommunikationsschnittstelle)

Protokoll: Eine mögliche Implementierung eines Dienstes, welche die Funktionalität umsetzt. (Das Protokoll liest das "wie" einer Kommunikationsschnittstelle)

Primitive: Grundfunktionenen der Kommunikationsschnittstelle.

b) Erläutern Sie knapp, was man unter *vertikaler* und *horizontaler* Kommunikation versteht. Verwenden Sie für die Erläuterung ein *Beispiel aus dem Internet-Referenzmodell*.

Horizontal: Kommunikation zwischen zwei Instanzen der gleichen Schicht auf zwei Rechnern. (TCP sendet Signale an TCP Empfänger)

Vertikal: Kommunikation zwischen zwei benachbarten Schichten auf dem gleichen Rechner. (TCP Segment mit IP zur Versendung weitergeben)

Name: Matr.Nr.:

c) Sie verwenden eine Leitung, die auf der Bitübertragungsschicht eine Übertragungsrate von 1GBit/s bietet. Welche Ursachen können dazu führen, dass eine Anwendung, die auf dieser Leitung Daten überträgt, eine geringere Übertragungsrate misst? *Nennen Sie drei unterschiedliche Ursachen und erläutern Sie jeweils knapp, wieso sie zu einer geringeren Übertragungsrate führen.*

1) Protokolloverhead: Die Anwendung bekommt nicht die volle Datenrate für ihren Payload, ein Teil geht für Headerinformationen der ganzen Protokolle verloren.

2) Bitfehler: Neuübertragung verloren gegangener Rahmen.

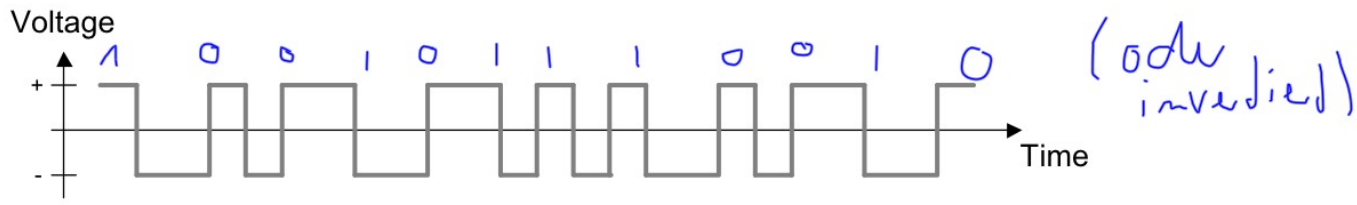
3) Kollisionen: Medienzugriff, falls CSMA/ CD eingesetzt wird, kann es zu Datenverlust/ Wartezeit kommen.

4) Teilung der Datenrate: Andere Anwendungen nutzen die Leitung simultan.

Name: Matr.Nr.:

Aufgabe 2 (Signale) **(4+2+2+4) = 12 Punkte**

a) Welche *Bitfolge* erhält der Empfänger, wenn er folgendes Signal mit dem *Manchester-Code* decodiert?



Es sei nun eine Schrittgeschwindigkeit von `10.000 baud` gegeben. Welche *Datenrate* wird bei Verwendung des Manchester-Codes erreicht?

Hälfte der Schrittgeschwindigkeit: 5000 Bit/ s

b) Gegeben sei ein neuer Code mit dem Namen *9B/10B*. Welche *Effizienz* kann dieser Code wohl erreichen? Begründen Sie ihre Antwort.

90%, da 9Bit auf 10Bit kodiert werden.

c) Nennen Sie einen *Vorteil* und einen *Nachteil* des Manchester-Codes gegenüber dem NRZ-L-Code.

Vorteil: Taktrückgewinnung, Gleichstromfreiheit

Nachteil: Geringe Effizienz (50% der Kapazität nur genutzt)

Name: Matr.Nr.:

d) Gegeben sei ein Kanal mit einer Bandbreite von 3.000 Hz. Der Signal-Rauschabstand beträgt 30 dB. Mit Hilfe des Shannon-Theorems haben Sie bereits berechnet, dass die maximale Datenrate 30.000 Bit/s beträgt.
Nun entschließen Sie sich, den NRZ-L-Code einzuseten. *Berechnen Sie die maximale Datenrate mit Hilfe des Nyquist-Theorems*. Falls Sie dabei auf einen anderen Wert kommen als durch das Shannon-Theorem vorgegeben: *welcher der beiden Werte ist für Sie maßgebend und warum*?

Nyquist-Theorem: R = 2 * B * log2(n), (n = Signalstufen)
= 2 * 3000 * 1 = 6000 Bit/ s

Der kleinere Wert ist maßgebend (immer das Minimum), da beide Theoreme nur einen Teil der gesamten Einflüsse berücksichtigen. Hier Einflüsse berücksichtigen und den restriktiveren Wert verwenden.

Name: Matr.Nr.:

Aufgabe 3 (Sicherungsschicht) **(4+5+6+6) = 21 Punkte**

a) Schicht 2 des OSI-Referenzmodells ist in zwei Teilschichten aufgeteilt, die Logical Link Control (LLC) und die Medium Access Control (MAC). *Warum macht man diese Aufteilung und welche Aufgaben haben die beiden Teilschichten jeweils*?

MAC: Koordination des Mediumzugriff

LLC: Flusskontrolle, Fehlerbehandlung

MAC - hardwarenäheren Aufgaben (spezielle Netze/ Topologien)

LLC - hardwareunabhängigen Aufgaben (gemeinsam benötigte Funktionalität in allen Netzen)

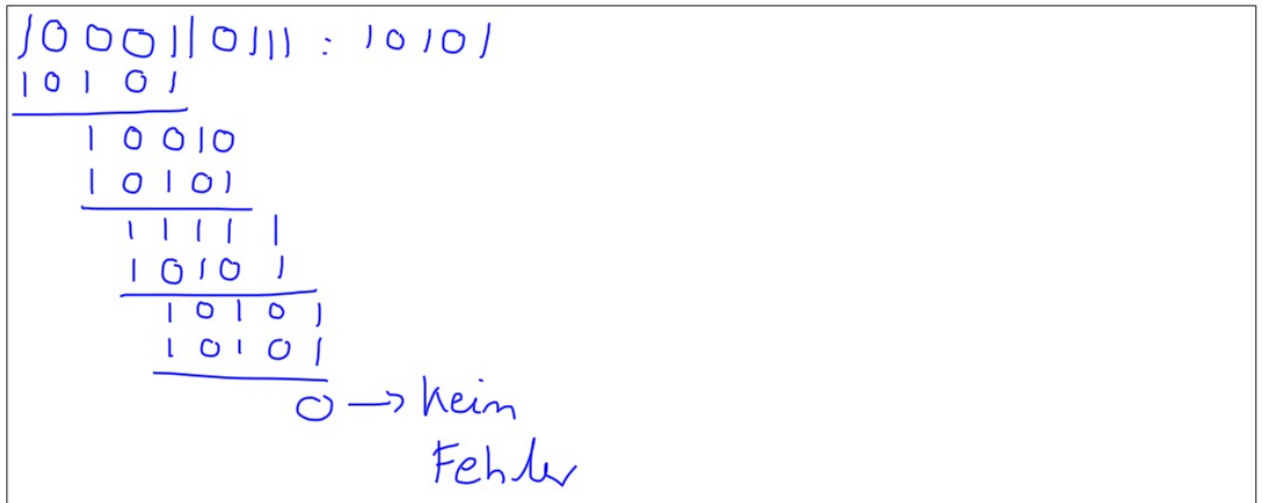
b) Sie verwenden *Cyclic Redundancy Checksum (CRC)* zur Erkennung von Übertragungsfehlern. Zwei Kommunikationspartner haben sich auf die Verwendung des Generatorpolynoms

$$G(x) = x^4 + x^2 + 1$$

geeinigt. Einer der beiden empfängt die folgende Bitsequenz:

1 0 0 0 1 1 0 1 1 1.

Ist ein Übertragungsfehler aufgetreten? Begünden Sie Ihre Antwort!



Name: Matr.Nr.:

c) Sie verwenden das Sliding-Window-Verfahren zusammen mit Go-Back-N zur Fehlerbehandlung. Es seien sowohl positive Quittungen (ACK) als auch negative Quittungen (NAK) möglich. *Beschreiben Sie beide Mechanismen knapp anhand der unten stehenden Fragen zum folgenden Beispiel*:

Gegeben seien ein Modulus $M = 11$ und eine Fenstergröße $W = 8$. Zum aktuellen Zeitpunkt seien die Rahmen mit den Sequenznummern 8, 9, 10, 0, 1 vom Sender gesendet worden, ohne dass eine Quittung eingegangen ist.

- Welche Rahmen dürfen in dieser Situation ohne jede Quittung gesendet werden?
- Wie ändert sich die Situation, falls ein Rahmen mit einer Quittungsnummer (ACK) 10 empfangen wird?
- Was passiert, wenn stattdessen ein NAK für die Sequenznummer 0 empfangen wird?

i) Sliding-Window erlaubt das Senden von bis zu W Rahmen ohne dass wir auf Quittungen warten müssen. (d.h. 2, 3, 4 können wir noch senden)

ii) Wenn eine Quittung eintrifft, kann das Fenster um die Zahl der quittierten Rahmen verschoben werden (d.h. 8, 9 bestätigt - es können zwei Rahmen mehr gesendet werden als bei i) also 5, 6)

iii) NACK 0 - bis 10 alles angekommen, ab 0 neu übertragen 0, 1, (2, 3, 4, 5, 6)

Name: Matr.Nr.:

d) Gegeben sei ein Netzwerk mit einer Bustopologie mit einer Ausdehnung von 50m, in dem CSMA/CD eingesetzt wird. Die Datenrate betrage 1 GBit/s, die Signalgeschwindigkeit im physikalischen Medium sei $2 \cdot 10^8 m/s$.

- Wieviel *Zeit* kann *maximal* vergehen, bis eine sendende Station eine *Kollision* erkennt?
- Welche *minimale Rahmenlänge* wäre für dieses LAN erforderlich?
- Sie wechseln nun zu einer Sterntopologie mit *Switch*, behalten aber Datenrate und Ausdehnung bei. *Ändert sich die erforderliche minimale Rahmenlänge? Begründen Sie Ihre Antwort!*

Neue Zeit: 2 * Laufzeit eines Signals über das Medium
Laufzeit t = 50m/2 * 10^8 = 2,5 * 10^-7 s
-> max. Zeit t(max) = 2 * t = 5 * 10^-7 s
min Rahmenlänge: 5 * 10^-7 * 16 Bit/ s = 500 Bit

Switch: keine Kollision, dadurch keine Einschränkung der Rahmenlänge

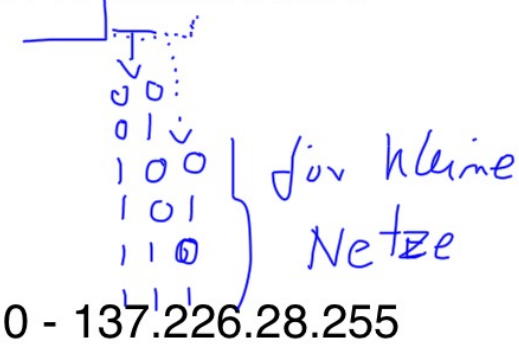
exam_ple

Name: Matr.Nr.:

Aufgabe 4 (Internet Protocol (IP)) **(6+2+2+4+4) = 18 Punkte**

a) Gegeben sei ein Netz mit dem IP-Adressbereich 137.226.28.0/22. Dieses möchten Sie unter kompletter Ausnutzung des zur Verfügung stehenden Adressraums in 6 Subnetze zerlegen, wobei zwei der Subnetze jeweils doppelt so groß sein sollen wie jedes der 4 anderen. *Geben Sie die Adressbereiche der Subnetze an.*

Kreise 4 Netze mit um 3 Bit erweiterte Subnetzmaske und
2 Netze mit um 2 Bit erweiterte Subnetzmaske.
2 Netze mit /25, 2 Netze mit /24
137.226.00011100.00000000



137.226.28.0 - 137.226.28.255
137.226.29.0 - 137.226.29.255
137.226.30.128 - 137.226.30.255
137.226.30.0 - 137.226.28.127
137.226.31.0 - 137.226.31.127
137.226.31.128 - 137.226.31.255

b) Woran kann ein Sender erkennen, dass die Ziel-IP-Adresse eines IP-Paketes sich *nicht in seinem eigenen Subnetz* befindet?

Verknüpfe Ziel-IP-Adresse mit im lokalen Netz verwendeter Subnetzmaske und vergleiche resultierendes Präfix mit im lokalen Netz verwendeten.

c) Ein Router habe ein IP-Paket erhalten, welches in sein eigenes Subnetz weitergeleitet werden muss. Was ist der *erste Schritt*, den der Router tätigen muss, um das Paket im Subnetz zuzustellen und *welches Protokoll* wird dazu verwendet?

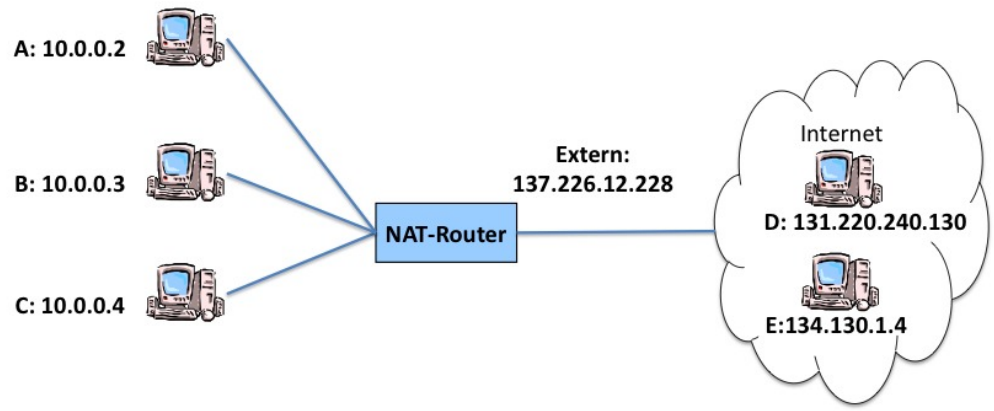
Adressauflösung (MAC Zieladresse unbekannt) ARP

d) Zwei wichtige Felder im IP-Header sind *Protocol* und *TTL*. *Wer prüft jeweils diese Felder und zu welchem Zweck*?

TTL: jede Zwischenstation, vermeide endlose Weiterleitung von Paketen

Protokoll: Nur der Empfänger an welches andere Protokollimplementierung muss Empfangenes Payload weitergeleitet werden

e) Gegeben ist das folgende kleine Firmennetzwerk mit den drei Rechnern A, B und C. Zur internen Kommunikation werden die angegebenen privaten IP-Adressen verwendet. Zugang zum Internet erfolgt mittels eines NAT-Routers, der nach außen hin die IP-Adresse 137.226.12.228 besitzt.



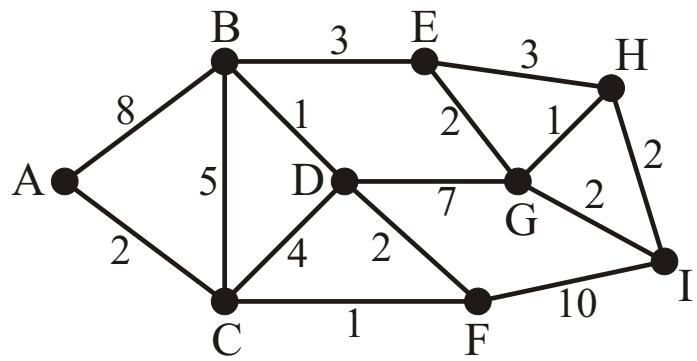
Die Abbildungstabelle des NAT-Routers sei zunächst leer. Rechner A sendet nun an D mit Absender-Port 134 und Ziel-Port 80. *Welche Aktion führt der NAT-Router durch und welche Einträge legt er dabei in seiner Abbildungstabelle an*? Kurz darauf sende Rechner E an 137.226.12.228:4936. *Welche Aktion führt der NAT-Router nun durch?*

Aktion: Eintrag in Abbildungstabelle anlegen und ersetzen von IP-Adresse 10.0.0.2 durch 137.226.12.228
10.0.0.2:134 137.226.12.128:134 131.220240130:80
ii) verwerfe Paket, da kein passender Eintrag in Abbildungstabelle

Name: Matr.Nr.:

Lösung 1 (Routing) **(8+4+2) = 14 Punkte**

Gegeben sei das folgende Netzwerk. Die Kanten sind mit der Entfernung der anliegenden Knoten beschriftet.



a) Berechnen Sie mit Hilfe des *Dijkstra-Algorithmus* den kürzesten Pfad von A nach I. Ergänzen Sie hierfür die folgende Tabelle, indem Sie spaltenweise die einzelnen Schritte des Algorithmus' dokumentieren. Verwenden Sie Einträge der Form (n,X), die den Knotenbeschriftungen des jeweiligen Schritts entsprechen. Dabei ist $n \in \mathbb{N}$ die Länge des bisher kürzesten Weges zum betrachteten Knoten und $X \in \{A, \ldots, I\}$ der unmittelbare Vorgängerknoten auf diesem Weg. Wird ein Knoten als permanent markiert, soll dies durch eine zusätzliche Umrahmung der Markierung notiert werden (siehe Knoten A im Schritt 0). Alle noch nicht erreichbaren Knoten werden mit ∞ beschriftet. Um Schreibarbeit zu sparen, brauchen die Markierungen von bereits als permanent markierten Knoten nicht mehr in jeder Spalte wiederholt werden (vgl. Zeile A).

	0	1	2	3	4	5	6	7	8
A	**(0,-)**	-	-	-	-	-	-	-	-
B	∞	**(8,A)**	**(7,C)**	**(7,C)**	**(6,D)**	-	-	-	-
C	∞	**(2,A)**	-	-	-	-	-	-	-
D	∞	∞	**(6,C)**	**(5,F)**	-	-	-	-	-
E	∞	∞	∞	∞	∞	**(9,B)**	-	-	-
F	∞	∞	**(3,C)**	-	-	-	-	-	-
G	∞	∞	∞	∞	**(12,D)**	**(12,D)**	**(11,E)**	-	-
H	∞	∞	∞	∞	∞	∞	**(12,E)**	**(12,EG)**	-
I	∞	∞	∞	**(13,F)**	**(13,F)**	**(13,F)**	**(13,F)**	**(13,FG)**	**(13,FG)**

Kürzester Pfad: ACFI

b) Die im vorherigen Teil berechneten Informationen reichen aus, damit A seine komplette Routing-Tabelle für das gegebene Netz erstellen kann. Der Eintrag zum Erreichen von Router C ist bereits vorgegeben. *Füllen Sie die Routing-Tabelle entsprechend Ihrer Ergebnisse aus dem vorherigen Teil aus*.

Ziel	Next Hop	Kosten
B	**C**	**6**
C	**C**	**2**
D	**C**	**5**
E	**C**	**9**
F	**C**	**3**
G	**C**	**11**
H	**C**	**12**
I	**C**	**13**

c) Die beiden prominenten Kategorien für Routing-Verfahren sind *Distance Vector* und *Link State*. Was ist der *Hauptunterschied* dieser beiden Kategorien?

Distance Vector gibt globale Informationen lokal weiter, Link State gibt lokale Informationen global weiter.

Name: Matr.Nr.:

Aufgabe 6 (TCP) **(8+4+6+8) = 26 Punkte**

a) Da IP verbindungslos arbeitet, können keine Garantien bezüglich der korrekten Datenübertragung gegeben werden. Deshalb wird auf Transportebene oft das TCP-Protokoll eingesetzt. *Beschreiben Sie detailliert, wie TCP jeweils auf die folgenden Fehlersituationen reagiert*:

- Zwei Pakete erreichen den Empfänger in falscher Reihenfolge.
- Eine Quittung trifft erheblich verspätet beim Sender ein.

i) Bis 1 alles korrekt empfangen, dann trifft direkt Segment 3 ein, wird zwischengespeichert, bei Eintreffen von Segment 2 werden direkt beide Segmente zusammen bestätigt. (oder go-back-N)

ii) Sender hat Timeout, senden Paket erneut, der Empfänger erkennt es zwar als Duplikat und verwirft es, schickt aber trotzdem die Quittung nochmal.

b) Angenommen, die Round-Trip-Time auf TCP-Ebene betrage 10s und die TCP-Fenstergröße der kommunizierenden Prozesse sei durch 25000 Byte limitiert. *Berechnen Sie die maximale Übertragungsrate*, die in dieser Situation erreicht werden kann.

Siehe nächste Seite

Lösung 2 (TCP) **(8+4+6+8) = 26 Punkte**

a) Da IP verbindungslos arbeitet, können keine Garantien bezüglich der korrekten Datenübertragung gegeben werden. Deshalb wird auf Transportebene oft das TCP-Protokoll eingesetzt. *Beschreiben Sie detailliert, wie TCP jeweils auf die folgenden Fehlersituationen reagiert*:

- Zwei Pakete erreichen den Empfänger in falscher Reihenfolge.
- Eine Quittung trifft erheblich verspätet beim Sender ein.

Siehe Videoaufzeichnung.

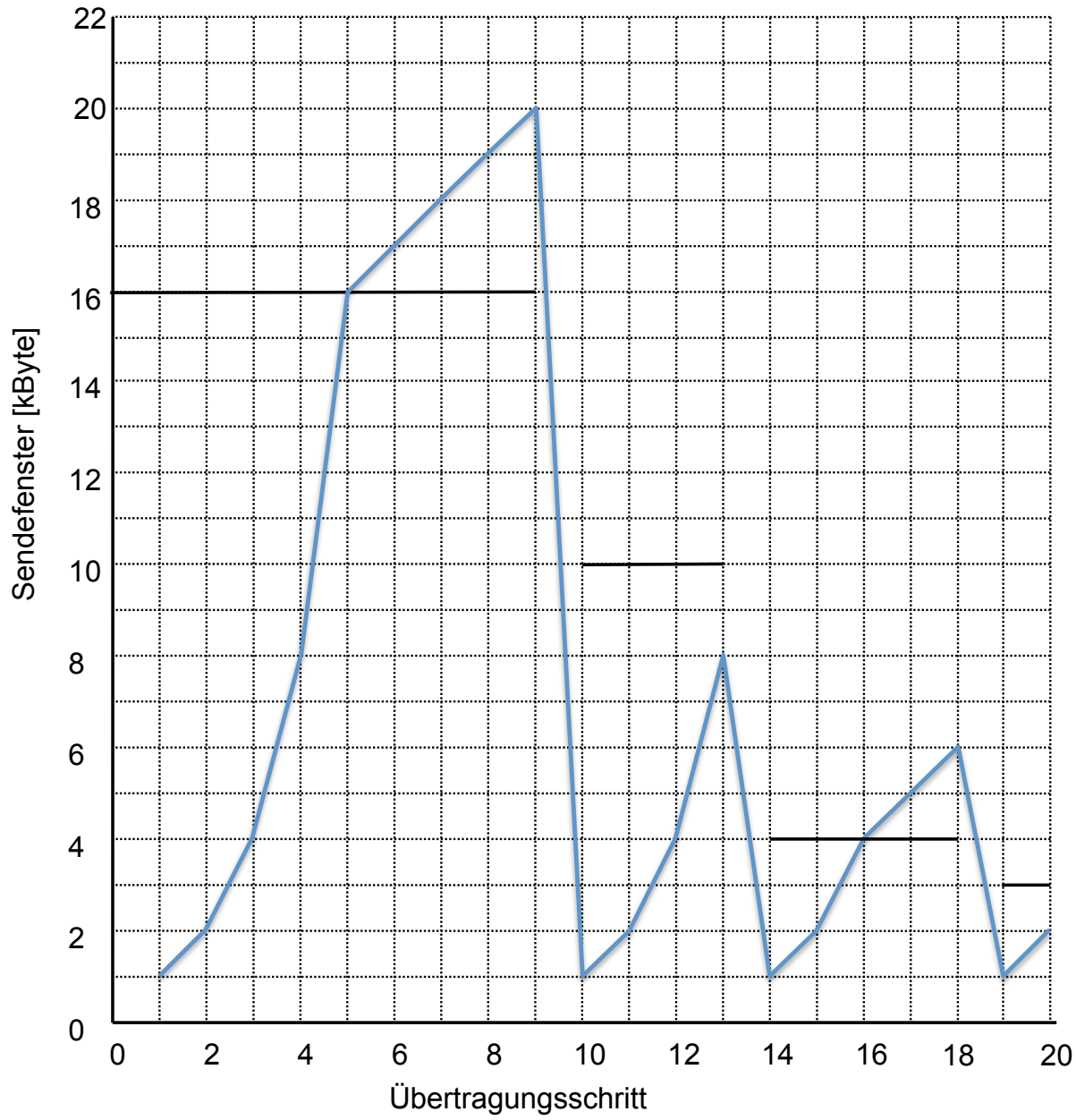
b) Angenommen, die Round-Trip-Time auf TCP-Ebene betrage 10s und die TCP-Fenstergröße der kommunizierenden Prozesse sei durch 25000 Byte limitiert. *Berechnen Sie die maximale Übertragungsrate*, die in dieser Situation erreicht werden kann.

Sliding Window sagt: sende 25.000 Byte, dann warte auf Quittungen. Erst bei Erhalt von Quittungen darf das Fenster dementsprechend weitergeschoben werden. Quittungen können erst nach der RTT kommen, also erst nach 10 Sekunden. Also kann man in 10 Sekunden 25.000 Byte schicken, somit 2.500 Byte in 1 s. Umrechnen in Bit macht: 20.000 Bit/s = 20 kBit/s.

c) Bei einem Datenaustausch zwischen zwei Kommunikationspartnern kann es neben einer Überlastung des Empfängers auch zu einer Überlastung des Netzwerks kommen. Die für diese Aufgabe betrachtete TCP-Verbindung nutzt den *Slow-Start-Algorithmus* mit einem Schwellwert (Slow Start Threshold, `ssthresh`) zur *Congestion Avoidance* von anfangs 16 kByte. Die MSS sei 1 kByte, die Window Size des Empfängers 32 kByte.

Es soll dargestellt werden, wie sich die Datenrate in diesem Szenario ändert. Dazu ist unten ein Diagramm angegeben, in welchem für die Übertragungsschritte 1 bis 20 die jeweils erreichte Übertragungsrate (ausgedrückt über die Größe des Sendefensters) dargestellt werden soll. Als ein Übertragungsschritt werde hier die Versendung der möglichen Datenmenge samt Empfang der Quittungen bezeichnet; wurden alle Quittungen des aktuellen Übertragungsschrittes erhalten, soll im nächsten Übertragungsschritt wieder die nun mögliche Datenmenge versendet werden. Beim 9., 13. und 18. Übertragungsschritt finde ein Timeout statt, der vom Sender als Netzüberlastung interpretiert wird.

Zeichnen Sie für die Übertragungsschritte 1 bis 20 jeweils die Größe des Sendefensters sowie den Threshold in das Diagramm ein.



d) TCP arbeitet bidirektional. Welche TCP-Headerfelder werden für die *Rolle als Empfänger* in der Datenaustauschphase verwendet? *Geben Sie vier Felder an und begründen Sie, warum/wofür der Empfänger sie verwendet.*

Jede Menge, der Empfänger verwendet fast alle Felder, z.B.:

- Sequenznummer eingehender Pakete muß geprüft werden, um festzustellen, ob dies das nächste erwartete Segment ist und eine Quittung geschickt werden kann.
- Entsprechend wird die Quittungsnummer beim Versenden von Quittungen benötigt.
- ... und damit zusammen das ACK-Flag, damit die andere Seite die Quittungsnummer betrachtet.
- Das WIN-Feld wird in Quittungen benötigt: wir teilen dem Sender mit jeder Quittung mit, wie viel Buffer noch zur Verfügung steht.

Lösung 3 (Sicherheit) **(6+3+5) = 14 Punkte**

a) *Berechnen Sie einen geheimen Schlüssel unter Verwendung des Diffie-Hellman-Algorithmus'*. Nutzen Sie $p = 11$ und $g = 3$. Verwenden Sie als Geheimzahlen der Kommunikationspartner kleine Zahlenwerte.

1.) Alice wählt $a = 3$ und berechnet $A = g^a \bmod p = 3^3 \bmod 11 = 5$.

2.) Alice sendet g, p und A an Bob (oder nur A, falls der Rest vorher schon bekannt war).

3.) Bob wählt $b = 2$, berechnet $B = g^b \bmod p = 3^2 \bmod 11 = 9$ und noch dazu den Schlüssel $K = A^b \bmod p = 5^2 \bmod 11 = \mathbf{3}$. Außerdem sendet Bob seinen Wert B an Alice.

4.) Nun kann Alice auch den Schlüssel berechnen: $K = B^a \bmod p = 9^3 \bmod 11 = \mathbf{3}$.

b) Sie verwenden *RSA* als asymmetrisches Verschlüsselungsverfahren und haben $p = 7$ and $q = 3$ gegeben. *Ist* $< 3, 21 >$ *ein gültiger geheimer Schlüssel?* Begründen Sie Ihre Antwort.

Berechne zunächst $\phi(n)$ mittels $n = p * q = 21$: $\phi(n) = (p-1) * (q-1) = 12$.
Wähle e relativ prim zu 12 sowie als multiplikativ Inverses zu $d = 3\ mod\ 12$. D.h.: existiert ein e mit $e * 3 mod 12 = 1$? Da 3 Faktor von 12 ist, gibt es keins. Man kann die Lösung auch schon abkürzen, indem man direkt sagt, dass die 3 bereits teilerfremd zu 12 sein müsste.
Wer das nicht weiß, muss alle Werte auf der Suche nach einem Inversen durchtesten (was nicht lange dauert, da es nicht viele sind) und findest nix. Oder man führt overkillmäßig den erweiterten euklidischen Algorithmus durch, aber der ist hier völlig überflüssig.

c) Die Firma SecureSys bietet ihre Sicherheitssoftware S auf ihrer Webseite zum Download an. Der Webserver hat ein Zertifikat mit einem öffentlichen Schlüssel; der zugehörige private Schlüssel ist sicher hinterlegt. Der Systemadministrator schlägt folgende Authentifizierungsmethode für den vertrauenswürdigen Download der Software vor: Zusammen mit Software S wird der folgende Wert im Download zur Verfügung gestellt: $H(S||KU_W)$.

Es gilt die folgende Syntax:

- S: Software
- KR_W: privater Schlüssel des SecureSys-Webservers
- KU_W: öffentlicher Schlüssel des SecureSys-Webservers
- $H(M)$: kryptographischer Hash von M
- $||$: Konkatenation zweier Bitfolgen

Ist die vorgeschlagene Methode geeignet, um den Download zu authentifizieren? Wenn ja, warum? Und wenn nein, was sollte stattdessen getan werden?

Die Methode ist nicht geeignet, denn jeder der die Hashfunktion und den öffentlichen Schlüssel kennt, kann die Authentifizierungsinformationen fälschen. Der Hashwert sollte mit dem privaten Schlüssel verschlüsselt werden! Wobei da schon der Hashwert über S reicht.