Distributed Systems

RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Klausur
"Sichere Verteilte Systeme"
SS 2010

Name, Vorname: «NACHNAME», «VORNAME»

Matrikelnummer: «MATNR»

Zur Beachtung:

- Die Klausur besteht aus 6 Aufgaben und 18 Seiten.
- Bitte legen Sie Ihren Personalausweis/Reisepass und Studentenausweis auf den Tisch, damit wir die Überprüfung ohne Störung während der Klausur durchführen können.
- Es dürfen keine weiteren Hilfsmittel verwendet werden.
- Schreiben Sie Ihre Lösungen – soweit möglich – nur in die entsprechenden Stellen der Aufgabenblätter.
- Fassen Sie Ihre Antworten kurz und präzise.
- Die Klausur dauert 120 Minuten und es gibt insgesamt 120 Punkte.
- Bewahren Sie ihre Klausurnummer auf. Nur unter dieser werden die Ergebnisse veröffentlicht.

Ich bestätige, dass ich die Klausur selbstständig bearbeitet habe.

_____

(Unterschrift)

Punkte:

Aufgabe	1 (16 P)	2 (17 P)	3 (12 P)	4 (34 P)	5 (11 P)	6 (30 P)	**Σ (120P)**	**Note**
Punkte								
Kürzel								

Aufgabe 1: Allgemeine Grundlagen (7 + 3 + 4 + 2 = 16 Punkte)

a) *Skizzieren* Sie die beiden in der Vorlesung vorgestellten Protokollreferenzmodelle und benennen Sie die einzelnen Schichten. Angenommen all die Protokollfunktionalität sei in einer einzigen Schicht implementiert. Ergeben sich damit irgendwelche Vorteile gegenüber den Schichtenmodellen? Wenn ja, welche?

ISO/OSI (7 Schichten), Skizze siehe Folien, hier nur eben der Reihe nach die Namen aufgelistet:

Anwendungsschicht, Darstellungsschicht, Sitzungsschicht, Transportschicht, Vermittlungsschicht, Sicherungsschicht, Bitübertragungsschicht.

Internet-Referenzmodell. Skizze (wie oben):

Anwendungsschicht, Transportschicht, Vermittlungsschicht, Host-to-Network (Netzzugangs-) Schicht.

Vorteil bei Implementierung aller Funktionalität in einer einzigen Schicht: Effizienz aufgrund optimierter Abläufe, da keine Modularität mehr da ist und keine Schnittstellen mehr berücksichtigt werden müssen.

b) Nennen Sie *drei typische Gemeinsamkeiten* der Sicherungs- und Transportschicht am Beispiel von Ethernet und TCP. *Erläutern* Sie diese mit jeweils einem Satz.

1. Strukturierung des Datenstroms: Ethernet teilt die zu übertragenden Daten in Rahmen ein, TCP in Segmente.
2. Flusskontrolle zur Vermeidung der Überlast des Empfängers – Sliding-Window bei beiden Protokollen.
3. Fehlererkennung: in beiden Fällen durch Prüfsumme (CRC bei Ethernet, Einerkomplement bei TCP)

c) *Formulieren* Sie das Abtasttheorem von Shannon und Rabe. Geben Sie ein in der Vorlesung vorgestelltes Beispiel aus der Praxis, wo das Theorem in der Bitübertragungsschicht seine Anwendung findet.

Theorem: Die Abtastfrequenz f_A muss mindestens doppelt so hoch sein wie die höchste im abzutastenden Signal vorkommende Frequenz f_S.

Beispiel aus der Praxis: PCM Modulation → Abtastfrequenz ist gleich 8.000 Hz um die Grenzfrequenz 3.400 Hz richtig abzutasten und zu kodieren.

d) Welche der beiden folgenden IPv4-Subnetzmasken ist gültig und welche ungültig? Warum?

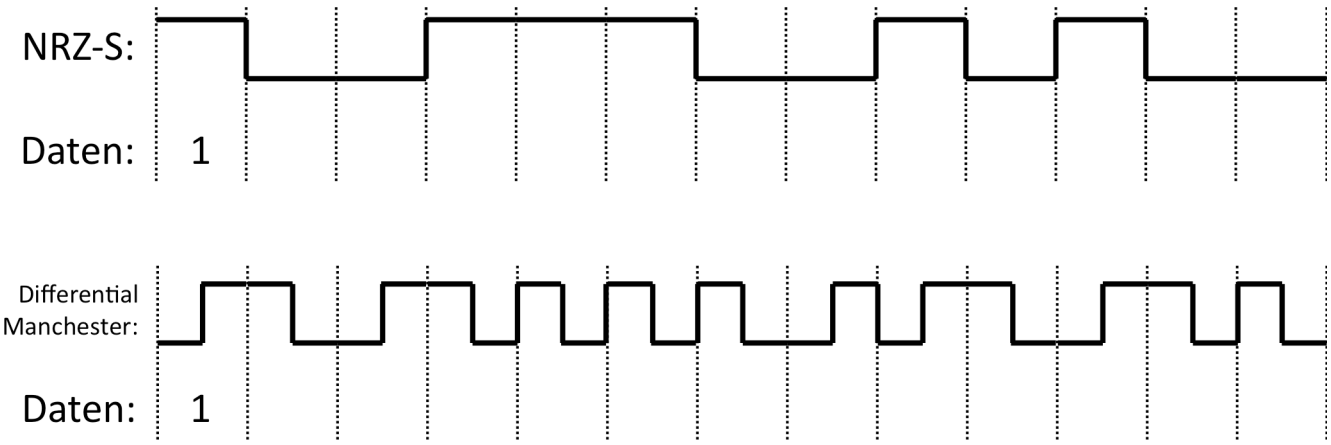
- 255.255.96.0
- 255.255.128.0

255.255.96.0 ist ungültig weil damit eine Lücke (96 = 0110 000) in dem Präfix entsteht. Nach einer 0 darf keine 1 mehr folgen, da keine (für den menschlichen Administrator einfach ersichtliche) richtige Unterscheidung zwischen dem Netz und Hostteil gemacht werden kann.

255.255.128.0 ist eine gültige Subnetzmaske, weil sie ein gültiges Präfix angibt, nämlich 128 = 1000 0000 → /17.

Aufgabe 2: Bitübertragungsschicht
(4 + 2 + 3 + 8 + 4 = 21 Punkte)

a) Im Folgenden erhalten Sie zwei physikalische Signale. Das erste ist in Non-Return-to-Zero-Space (NRZ-S), das zweite in Differential Manchester codiert. Decodieren Sie die Signale in Bitfolgen.



NRZ-S: 1:010110100001, DiffMan: 1:111000101110

b) Angenommen, bei der Übertragung dieser beiden Signale liegt die Anzahl der Pegelwechsel bei jeweils 25000 Wechseln pro Sekunde. Wie hoch ist jeweils die Datenübertragungsrate in Bit/s?

NRZ-S: Codeeffizienz 100% => 25 000 Bit/s

Differential Manchester Codeeffizienz 50% => 12 500 Bits/s

c) Wie hoch ist die Datenrate eines Kanals mit einer Bandbreite von 50KHz und 256 verschiedenen Signalstufen?

Nyquist: 2 * B * ld (n)

256 Signalstufen: ld 256 = 8, also 8 Bits pro Schritt

2 * 50 000 * 8 = 800 000 = 800 kBit/s

d) Angenommen, der unter c) angegebene Kanal bietet einen Signal-Rausch-Abstand von 20dB. Kann dies zu Problemen führen? Begründen Sie ihre Antwort! Wie viele Bits pro Schritt sind unter diesen Umständen maximal codierbar?

dB = 10 * lg(S/N) => S/N = 10 ^ (dB/10)

S/N = 10 ^ (20/10) = 100

Shannon-Theorem: B * ld(S/N + 1)

Vergleich mit Shannon: max Bit/s = 50 000 * ld (101) < 50 000 * ld (128) = 350 000

Shannon < 800 kBit/s => Kanal kann keine 8 verschiedenen Pegel übertragen.

Wie viele wären übertragbar? Suche Anzahl von Pegeln, bei denen wir unter Shannon-Limit bleiben:

7 bits: Nyquist sagt: 2 * 7 * 50 000 = 700 000.

Aber Shannon war < 350 000 (Abschätzung oben)

Ebenso 6 bit, 5 bit, 4 bit.

3 Bits: Nyquist sagt: 2 * 3 * 50 000 = 300 000

Könnte passen. Schätze Shannon in andere Richtung ab:

50 000 * ld (101) > 50 000 * ld(64) = 50 000 * 6 = 300 000

Ok, passt!

Also Lösung: 3 Signalstufen.

e) Wieso wurde bei der Spezifikation der „schnelleren“ Ethernet-Variante (FastEthernet, damit 100 Mbit/s statt 10 Mbit/s) die maximale Segmentlänge auf 100m reduziert? *Begründen* Sie ihre Antwort.

[Achtung: Ethernet-Varianten kamen dieses Jahr in der Vorlesung nicht dran] Zur Kollisionserkennung muss das Signal so lange anliegen, dass das erste Bit das gesamte Kabel hin sowie (im Worst case) das erste kollidierende Bit das Kabel zurück durchlaufen hat (1x Round-Trip-Time), bevor die Übertragung des letzten Bits abgeschlossen ist. Da die Datenrate um Faktor 10 erhöht wurde, aber die gleiche Codierung beibehalten wurde, wäre die minimale Rahmenlänge auch um das Zehnfache gestiegen. Um aber weiterhin Abwärtskompatibel mit dem „alten“ Ethernet zu bleiben (minimale Rahmenlänge 64 Byte), wurde die Segmentlänge verkürzt.

Aufgabe 3: Sicherungsschicht

(3 + 4 + 2 + 3 = 12 Punkte)

a) Wodurch unterscheiden sich gerade und ungerade Parität? Zeigen Sie dies durch die Berechnung der beiden Paritäten für die Bitfolge 1001.

Gerade Parität: Wähle Parität so, dass Anzahl aller Einsen gerade ist.

Ungerade Parität: Wähle Parität so, dass Anzahl aller Einsen ungerade ist.

Gerade Parität also: 1001:0

Ungerade Parität also: 1001:1

b) Ein Verfahren zur Sicherung der Übertragung ist die Kreuzparität. Führen Sie das Kreuzparitätsverfahren für die unten angegebenen Daten aus. Dabei soll die Querparität gerade und die Blockparität ungerade sein. Das mit X gekennzeichnete Feld müssen Sie nicht ausfüllen.

	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Parität
Bit 0	0	0	0	1	1	1
Bit 1	1	1	1	0	0	0
Bit 2	1	0	0	0	1	1
Bit 3	1	0	1	0	0	1
Bit 4	1	1	0	1	0	0
Bit 5	0	0	1	0	0	0
Bit 6	1	0	0	1	0	1
Parität	1	0	1	1	0	X

c) Welchen Vorteil bietet das Kreuzparitätsverfahren gegenüber einfacher Parität? Welchen Nachteil?

Mehr Fehler können erkant werden, einige können auch korrigiert werden (so z.B. alle Einzelfehler)

Nachteil ist der hohe Overhead zur Übertragung aller nötigen Paritäten.

d) Forward Error Correction erlaubt die Wiederherstellung von inkorrekt empfangenen oder verlorenen Paketen. Nutzen Sie ein aus der Vorlesung bekanntes Verfahren, bei dem zusätzlich zu den Nutzdaten ein weiteres Paket mit Wiederherstellungsinformationen übertragen wird. Drei Pakete sind gegeben:

a. P1: `10011101`
b. P2: `01010110`
c. P3: `11100110`

Mit welchem Verfahren wird P4 berechnet? Geben Sie P4 an.

[Achtung: dieses Verfahren war dieses Jahr nicht in der Vorlesung enthalten. Statt dessen wurde der Hamming-Code als FEC-Verfahren eingeführt.]

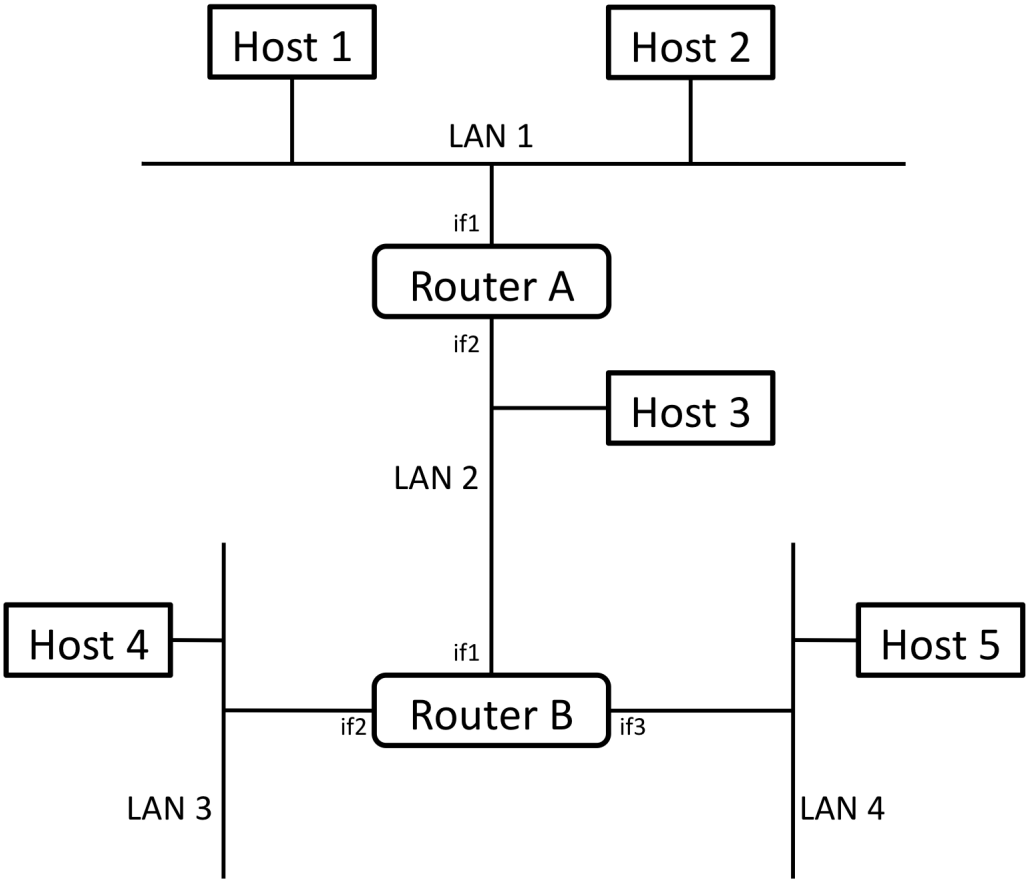
Alle Pakete werden bitweise mit XOR verknüpft, das Ergebnis ist P4.

Daher: P4 = 00101101

Aufgabe 4: Netzwerkschicht

(10 + 4 + 6 + 3 + 10 + 1 = 34 Punkte)

Gegeben sei das in der folgenden Grafik dargestellte Netz. Dabei sind in jedem Subnetz (LAN1-LAN4) exemplarisch ein oder zwei Hosts dargestellt.



Für Aufgabenteil d) benötigen Sie die MAC-Adressen der einzelnen Interfaces:

Host 1	01:02:03:04:05:11
Host 2	01:02:03:04:05:12
Host 3	01:02:03:04:05:13
Host 4	01:02:03:04:05:14
Host 5	01:02:03:04:05:15
Router A, if1	01:02:03:04:05:A1
Router A, i2	01:02:03:04:05:A2
Router B, if1	01:02:03:04:05:B1
Router B, if2	01:02:03:04:05:B2
Router B, if3	01:02:03:04:05:B3

a) Sie haben zur Konfiguration dieses Netzes den Adressbereich 134.130.56.0/21 erhalten. LAN 1 enthält ca. viermal so viele Rechner wie (jeweils) LAN 2, 3 und 4. Konfigurieren Sie die Subnetze entsprechend. Geben Sie eine kurze Begründung für ihre Aufteilung.

	Adresse (Netz-ID)	Maske
LAN 1	134.130.56.0	/22
LAN 2	134.130.60.0	/24
LAN 3	134.130.61.0	/24
LAN 4	134.130.62.0	/24

(Beispiel für einen Eintrag: Adresse „213.133.49.0“, Maske „/16“ oder „255.255.0.0“)

Unterteile gegebenen Adressblock in Achtel. LAN 1 erhält 4 Achtel, LAN2, 3 und 4 jeweils ein Achtel. Das letzte Achtel liegt bracht.

Unterteilung in 8 Teile: 3 Bit nötig, daher haben kleine LANs die Maske /24. Das große LAN hat durch die vierfache Größe die Maske /22

b) Teilen Sie jedem Interface eine gültige IPv4-Adresse zu.

Host 1	134.130.56.2
Host 2	134.130.56.3
Host 3	134.130.60.3
Host 4	134.130.61.2
Host 5	134.130.62.2
Router A, if1	134.130.56.1
Router A, if2	134.130.60.1
Router B, if1	134.130.60.2
Router B, if2	134.130.61.1
Router B, if3	134.130.62.1

c) Zum Internetworking ist es erforderlich, dass die Router wissen, wie sie Pakete weiterzuleiten haben. Geben Sie die Routingtabellen für beide Router an. Kennzeichnen Sie direkte Verbindungen mit einem Stern (*).

	Ziel	Interface	Gateway
Router A	134.130.56.0/22	if1	*
	134.130.60.0/24	if2	*
	134.130.61.0/24	if2	134.130.60.2
	134.130.62.0/24	if2	134.130.60.2
Router B	134.130.56.0/22	if1	134.130.60.1
	134.130.60.0/24	if1	*
	134.130.61.0/24	if2	*
	134.130.62.0/24	if2	*

d) Host 2 hat eine HTTP-Verbindung zu Host 5 aufgebaut und verschickt ein Paket mit HTTP-Daten. Welchen Weg nimmt das Paket? Geben Sie für jedes Teilstück der Strecke die Ziel-MAC-Adresse und Ziel-IP-Adresse an. (Hinweis: sollten Sie Aufgabenteil b) nicht lösen können, so tragen Sie in die dortige Tabelle beliebige IP-Adressen ein, und nutzen diese hier.)

Host2 => LAN 1 => Router A: MAC 01:02:03:04:05:A1, IP 134.130.62.2

Router A => LAN 2 => Router B: MAC 01:02:03:04:05:B1, IP 134.130.62.2

Router B => LAN 4 => Host 5: MAC 01:02:03:04:05:15, IP 134.130.62.2

e) Nehmen Sie an, das in Teilaufgabe d) versendete IP-Paket habe eine Payload von 1200 Byte. Die MTU für LAN1 und LAN 2 betrage 1400 Byte, für LAN 3 und LAN4 576 Byte. Führen Sie die notwendige Fragmentierung durch. Geben Sie für jedes Fragment die folgenden Werte an:

- Größe der Payload in Bytes
- Wert des MF-Flags
- Wert im Fragment-Offset-Feld

Gehen Sie dabei von einem Standard-IPv4-Paket ohne Headeroptionen aus.

Wir haben 1200 Byte zu übertragen. Die MTU beträgt 576 Bytes [HTTP läuft über TCP, TCP verwendet die kleinere MSS, orientiert an der kleineren MTU]. Da jedes Fragment einen IP-Header braucht, können nur 556 Bytes Payload pro Fragment übertragen werden.

Das Fragment-Offset-Feld gibt das Offset in 8-Byte-Blöcken an, aber 556 ist nicht durch 8 teilbar. Deshalb können nur 552 Byte Payload pro Fragment übertragen werden.

Die Lösung lautet also:

Fragment 1: 552 Byte Payload, MF=1, Fragment Offset = 0

Fragment 2: 552 Byte Payload, MF=1, Fragment Offset = 69 (69 * 8 = 552)

Fragment 3: 96 Byte Payload, MF=0, Fragment Offset = 138

f) Was geschieht mit dem Paket, wenn Host 2 das DF-Flag auf 1 gesetzt hat?

Router B verwirft das Paket

(und sendet Teile des Pakets mit einem ICMP-Paket zurück: Destination unreachable. War aber nicht explizit gefragt.)

Aufgabe 5: Transport- und Anwendungsschicht

(2 + 2 + 3 + 4 = 11 Punkte)

a) Woran und auf welcher Schicht erkennt ein Endsystem, für welche Anwendung ein bestimmtes Paket bestimmt ist?

Erkennung auf Transportschicht, anhand von Ports.

b) Bei der Verwendung von negativen Bestätigungen (NAK) signalisiert der Empfänger dem Sender, wenn er ein Paket nicht oder nicht korrekt erhalten hat. Wie erkennt dies der Sender, falls keine NAKs verwendet werden?

Timeouts (reichen alleine schon)

(Dup-ACKs)

c) Ein großer Vorteil von TCP gegenüber UDP ist die gesicherte Datenübertragung. Deshalb wird UDP hauptsächlich in Bereichen eingesetzt, in denen es nicht auf 100%ige Übertragungssicherheit ankommt, wie zum Beispiel Multimediastreaming. Daneben kommt UDP aber auch noch anderen wichtigen Anwendungsschichtprotokollen aus anderen Gründen zum Einsatz. Nennen Sie ein solches Protokoll, und erläutern Sie, worin in dem Fall der Vorteil besteht.

Beispiel DNS: kleine Anfrage, kleine Antwort. UDP spart den in diesem Fall erheblich ins Gewicht fallenden Overhead von Verbindungsauf- und –abbau.

Anderes Beispiel: Jegliches Protokoll, dass Multi- oder Broadcast verwendet, weil dies nicht mit TCP verwirklicht werden kann.

d) In der Vorlesung wurden zwei Protokolle behandelt, mit denen ein Host im Netz die Zuweisung einer IP-Adresse erbitten kann. Nennen Sie die beiden Protokolle. Welches ist das umfassendere? Nennen Sie eine zusätzliche Information, die Sie im umfassenderen Protokoll zusätzlich zur zugewiesenen IP-Adresse erhalten.

RARP und DHCP

DHCP gibt noch zusätzliche Informationen wie Subnetzmaske, Gateway

Aufgabe 6: Sicherheit (6 + 4 + 10 + 10 = 30 Punkte)

a) *Beschreiben* Sie kurz die Sicherheitsfunktionen von *Authentication Header* (*AH*) in IPSec. *Skizzieren* Sie, wie AH in das normale IP-Protokoll integriert wird.

Sicherheitsfunktionen von AH:

Datenintegrität, d.h. die versendeten Daten wurden auf dem Weg zum Ziel nicht modifiziert.

Authentifizierung des Senders: Das empfangenen Pakete können sicher dem Sender zugeordnet werden.

Integration in das IP-Protokoll

| IP Header | AH Header | IP Payload |

b) Was versteht man unter dem Begriff *Spoofing*? Welche Internet-Protokolle sind davon betroffen? Nennen und erläutern Sie 4 Beispiele.

Spoofing = Vortäuschen einer falschen Identität, da in Internet- Protokollen keine Authentifizierung vorgenommen wird).

- ARP-Spoofing (= Hinterlegen falscher Adressauflösungen in ARP-Caches)
- IP-Spoofing (= Senden unter falscher IP-Adresse)
- ICMP-Spoofing (= z.B. Senden eines Redirect-Befehls unter falscher Adresse)
- Mail-Spoofing (= Senden unter falscher E-Mail-Adresse

c) Das Needham-Schroeder Protokoll enthielt in seiner frühen Version die folgende Sicherheitslücke: Nachdem Herausfinden des Schlüssels von Alice zum KDC konnte der Angreifer vom KDC einen geheimen Schlüssel (ein Ticket) für Bob anfordern. Wenn Alice ihren Schlüssel nach dem Angriff änderte, blieb das Ticket für Bob trotzdem gültig. *Beschreiben* Sie wie es zu dieser Schwachstelle gekommen ist und *skizzieren* Sie wie diese in einer weiteren Version des Protokolls geschlossen wurde.

Die Schwachstelle resultiert sich daraus, dass Bob beim Beginn der Kommunikation mit Alice nicht überprüft, ob das Ticket noch aktuell ist. Damit ist es dem Angreifer möglich, alte Tickets wiedereinzuspielen :

Alice → KDC (Anfrage des Tickets zum Bob)

KDC → Alice: $K_A\{N_1$, "Bob", K_{AB}, ticket to Bob$\}$ mit ticket = $K_B\{K_{AB}$, „Alice"$\}$

Alice → Bob: ticket, $K_{AB}\{N_2\}$

...

Zum Schließen der Sicherheitslücke wurde das zusätzliche Nonce N_B eingeführt, das Bob beweist, dass der Schlüssel K_{AB} noch aktuell ist.

Alice →Bob: I want to talk with you

Bob → Alice: $K_B\{N_B\}$

Alice → KDC: N_1, Alice wants Bob, $K_B\{N_B\}$

KDC → Alice: $K_A\{N_1$, "Bob", K_{AB}, ticket to Bob$\}$ mit ticket = $K_B\{K_{AB}$, "Alice", $N_B\}$

Alice → Bob: ticket, $K_{AB}\{N_2\}$ (← hier kann Bob im Ticket überprüfen, ob K_{AB} noch aktuell ist)

d) Ein bekanntes asymmetrisches Verfahren ist *RSA*. Sie belauschen eine per RSA gesicherte Kommunikation und erhalten den verschlüsselten Text c. Der öffentliche Schlüssel, der zur Verschlüsselung verwendet wurde, ist <e = 29, n = 221>. *Ermitteln Sie den privaten Schlüssel d mit dem erweiterten euklidischen Algorithmus*. *Erläutern* Sie durch Angabe des Rechenwegs, wie die verschlüsselte Nachricht damit entschlüsselt werden kann.

n = 221 => p = 13, q = 17, phi(n) = 192

d * 29 = 1 mod 192

i	q_i	r_i	v_i
-2		192	0
-1		29	1
0	6	18	-6
1	1	11	7
2	1	7	-13
3	1	4	20
4	1	3	-33
5	1	1	53

d = 53

c^d mod n = m