

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Commerce & Mehrseitige Sicherheit

**Klausur zur Veranstaltung
„Mobile Commerce I“
Sommersemester 2005**

Punktezahl: 90
Mindestpunktezahl zum Bestehen: 45
Veranstalter: Prof. Dr. Kai Rannenberg
Zugelassene Hilfsmittel: Keine

Wir wünschen viel Erfolg!

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Commerce & Mehrseitige Sicherheit
www.m-lehrstuhl.de

Prof. Dr. Kai Rannenberg

Telefon +49 (0)69-798 25301
Telefax +49 (0)69-798 25306
E-Mail kai.rannenberg@m-lehrstuhl.de

Datum: 01.08.2005

Aufgabe 1: Technology Basics - Mobile Networks (10 Punkte)

- a) Erklären Sie den Begriff „Roaming“ in Bezug auf mobile Netzwerke und nennen Sie ein konkretes Beispiel für einen Roaming-Fall. (2 Punkte)

Lösung:

Roaming bedeutet die Änderung des Netzwerkzugriffs durch das Mobilgerät
(1 Punkt)

Konkretes Beispiel (1 Punkt):

- Wechsel von z.B. einer GSM- zu einer UMTS-Verbindung.
- Zellenwechsel (Handover)
- Wechsel zwischen Netzbetreibern
(Lecture 3, Slide 21)

- b) Nennen Sie eine (1) Schwachstelle des GSM-Sicherheitsmodells und deren mögliche Folgen. (3 Punkte)

Lösung:

Das Netz authentifiziert sich nicht selbst gegenüber dem Nutzer bzw. dessen Endgerät. Damit können dem Nutzer Geheimnisse entlockt werden, weil er glaubt, sie nur einem legitimen Netz anzuvertrauen, und letztendlich kann z.B. seine Kommunikation abgehört werden. (1 Punkt für Nennung und 2 Punkte für Folgen).
(Lecture 3, Slides 34,35)

- c) Nennen Sie jeweils einen (1) Vor- bzw. Nachteil von „General Packet Radio Service“ (GPRS) gegenüber der GSM-Standarddatenübertragung „Circuit Switched Data“ (CSD). (2 Punkte)

Lösung:

Vorteile (1 Punkt):

- „always on“
- höhere Übertragungsraten
- new billing methods (packet-oriented)

Nachteile (1 Punkt):

- hohe Aufrüstungskosten der GSM Infrastruktur
- neue Endgeräte erforderlich
- höhere Nutzungskosten
- neue Security-Konzepte aufgrund von Push-Diensten erforderlich

(Lecture 3, Slide 45)

- d) Nennen Sie zwei Vorteile der UMTS- gegenüber der GSM-Architektur. Bringt die UMTS Technologie in Bezug auf die sprachbasierte Kommunikation einen *wahrnehmbaren* Mehrwert für den Mobilfunkkunden? (3 Punkte)

Lösung:

Nennung (1 Punkt):

- Security
(UMTS Netz authentifiziert sich gegenüber dem Endgerät, größere Schlüssellänge)
- Performance
(Höhere Datenübertragungsraten)

(Lecture 3, Slides 52, 53)

Mehrwert (2 Punkte):

Nein, es gibt keinen wahrnehmbaren Mehrwert in Bezug auf die sprachbasierte Kommunikation, deshalb sind derzeit die UMTS Angebote auch hauptsächlich auf Datenübertragung ausgerichtet.

(Übung: Technology Basics)

Aufgabe 2: Technology Basics - Protocols (15 Punkte)

- a) Nennen Sie zwei für Mobile Commerce geeignete Datenübertragungskanäle und geben Sie dazu jeweils ein Beispiel für eine B2C (Business-to-Customer)-Anwendung an. (4 Punkte)

Lösung (pro Nennung 1 Punkt, maximal 2 Punkte):

- Wireless LAN
- IR
- Bluetooth
- DVB-T
- GSM

(Lecture 4, Slide 2)

Lösung (pro Nennung 1 Punkt, maximal 2 Punkte):

- Wireless LAN: z.B.: Hotspotbetreiberportale, Hotspotportal von Einkaufszentren oder Cafes
- GSM: Location Based Services: Routing
- DVB-T: Durch Rückkanal (ISDN in DVB-T-Boxen) Reaktionsmöglichkeit auf z.B. Produktwerbung.

- b) Erläutern Sie den Begriff „Wireless LAN“ (WLAN) und nennen Sie zwei Komponenten, die für den Betrieb eines WLANs benötigt werden. (3 Punkte)

Lösung (pro Nennung 0,5 Punkt, maximal 2 Punkte):

- Es handelt sich um eine Funkübertragung
- WLAN ist zellenbasiert
- WLAN bietet eine geographische Erweiterung zu einem kabelgebundenen Netzwerk
- Eine WLAN Zelle versorgt ein bestimmtes Gebiet (local area), indem ein Teilnehmer sich frei bewegen kann.

(Lecture 4, Slide 3)

Lösung (pro Nennung 0,5 Punkt, maximal 1 Punkt):

- WLAN-Karte (USB, PCMCIA, PCI,)
- Access Point (WLAN-Router, Hotspot, ...)

(Lecture 4, Slide 4)

- c) Welche Problematik ergibt sich bei der Verwendung von WLAN in Bezug auf Roaming? Nennen Sie drei Punkte. (1,5 Punkte)

Lösung (pro Nennung 0,5 Punkt, maximal 1,5 Punkte):

- Es existiert noch kein Standard für Roaming zwischen Access Points
- Verbindungsabbrüche beim Wechseln der Zelle sind derzeit die Regel
- Es existiert keine einheitliches übergreifendes Abrechnungssystem

(Lecture 4, Slide 6-8)

- d) Überlegen Sie sich eine mögliche Roaming-Lösung für WLAN. Gehen Sie dabei von einer Infrastruktur mit zwei Access Points und einem WLAN-Teilnehmer aus. (5 Punkte)

Lösung (maximal 5 Punkte):

- Der WLAN-Teilnehmer merkt sich den aktuellen Access Point (MAC-Adresse)
 - Bei Abnahme des Empfangssignals, werden andere Access Points in der Umgebung ausgemacht.
 - Der Wechsel zu einem empfangsstärkeren Access Point wird vollzogen
 - Pakete, die an beim alten Access Point in der Zwischenzeit auflaufen, sind vorzuhalten.
 - Nach der Anmeldung an den neuen Access Point wird dem Access Point mitgeteilt, mit welchem Access Point der WLAN-Teilnehmer zuvor verbunden war.
 - Der alte Access Point wird kontaktiert.
 - Ein Redirect vom alten zum neuen Access Point wird gesetzt und vorgehaltene Nachrichten werden weitergeleitet.
- (angelehnt an Lecture 4, Slide 9)

- e) Nennen Sie drei Beschreibungssprachen für die Darstellung mobiler Inhalte. (1,5 Punkte)

Lösung (pro Nennung 0,5 Punkt, maximal 1,5 Punkte):

- WML (für WAP)
 - cHTML (für IMODE)
 - HTML (für WWW)
- (Lecture 4, Slide 57-60)

Aufgabe 3: Economic Basics - Market Structure, Value Building & Revenue Models (15 Punkte)

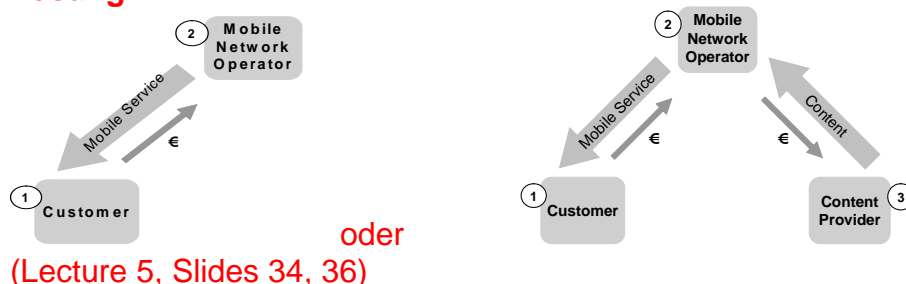
- a) Nennen und beschreiben Sie drei Arten von Akteuren im M-Commerce Markt. (3 Punkte)

Lösung (pro Nennung 1 Punkt):

- Mobilfunkbetreiber
 - Infrastrukturanbieter
 - Endgerätehersteller
- (Lecture 5, Slide 8)

- b) Skizzieren Sie ein klassisches Geschäftsmodell für einen mobilen Dienst (Akteure, Geld- und Leistungsströme). (3 Punkte)

Lösung:



- c) Ein Content-Provider bietet Börsennachrichten für mobile Endgeräte an. Auf seiner mobilen Website wird das Werbebanner der XY-Bank angezeigt. Für jeden Aufruf der XY Bank-Website über dieses Werbebanner erhält der Content-Provider 0,01 Cent von der XY Bank.
Nennen Sie den Typ des Erlösmodells des *Content-Providers*, welches diesem Angebot zugrunde liegt. Nennen Sie einen weiteren Erlösmodelltyp! (4 Punkte)

Lösung:

Transaktionsbasierte (1,5 Punkte) / indirekte Erlöse (1,5 Punkte)

Weiteres Erlösmodell:

Transaktionsunabhängige / indirekte Erlöse (1 Punkt)

(Lecture 6, Slides 7-11)

- d) Erklären Sie den Begriff „Preisdifferenzierung“ und nennen Sie eine Voraussetzung für diese. Ist die von Ihnen genannte Voraussetzung im M-Commerce Markt erfüllt? (3 Punkte)

Lösung:

- Angebot eines Produktes zu unterschiedlichen Preisen für unterschiedlichen Kundensegmente. (1 Punkt)

Voraussetzung: z.B. Arbitragefreiheit (1 Punkt)

Arbitragefreiheit ist im M-Commerce Markt aufgrund der vorhandenen Personalisierungsmöglichkeiten gegeben (1 Punkt)

(Lecture 6, Slides 18,19)

- e) Ein Mobilfunkkunde erzeugt im Durchschnitt 6 MB Datenverkehr pro Monat. Er steht nach Ablauf seines Vertrages vor der Entscheidung für folgende neue Tarifoptionen:
- 20 € Grundgebühr + 1 € für jedes angefangene MB (Tarif 1)
 - 5 € pro 1 MB Datenvolumen (Tarif 2)

Für welche Tarifoption wird er sich als homo oeconomicus entscheiden? Begründen Sie Ihre Antwort. (2 Punkte).

Lösung:

(1) $20 + 6 = 26$

(2) $5 * 6 = 30$

Er entscheidet sich für Tarifoption (1)

(Übung: Economic Basics)

Aufgabe 4: Economic Basics - E-Commerce vs. M-Commerce (10 Punkte)

- a) Nennen und beschreiben Sie zwei Charakteristika durch die sich die mobile Ökonomie von der Ökonomie des stationären Internets abgrenzen lässt. (3 Punkte)

Lösung:

- Ortsunabhängigkeit

- Always on

- Personal Sphere

- Context Sensitivity

(jeweils pro Nennung 0,5 Punkte und für die Erklärung jeweils 1 Punkt)

(Lecture 7, Slide 11)

- b) Die Darstellung von Inhalten auf einem mobilen Endgerät gestaltet sich derzeit sehr aufwendig. Nennen Sie zwei Gründe dafür und beschreiben Sie die Konsequenz für

die Anbieter und Konsumenten mobiler Inhalte. (4 Punkte).

Lösung:

- Unterschiedliche Darstellungsfähigkeiten und Transfergeschwindigkeiten der mobilen Endgeräte (2 Punkte)
 - Großer Aufwand und somit steigende Kosten für mobile Inhalte (2 Punkte)
- (Lecture 7, Slide 27)

- c) Im Bereich des stationären Internet ist der Aufwand für die Darstellung von Inhalten wesentlich geringer. Begründen Sie diese Tatsache mit Bezug auf die Anzahl verfügbarer Browser und deren Marktanteil. (3 Punkte).

Lösung:

Es gibt eine Vielzahl von Browsern, aber der Microsoft Internet Explorer dominiert den Markt. Websites werden vornehmlich auf diesen Browser hin optimiert.

(Lecture 7, Slide 25)

Aufgabe 5: Mobile Devices (5 Punkte)

- a) Nennen Sie drei Hauptunterscheidungsmerkmale mobiler Endgeräte. (3 Punkte)

Lösung (pro Nennung 1 Punkt, maximal 3 Punkte):

- Größe
 - Akkulaufzeit
 - Display
 - Prozessor
 - Speicher
 - Eingabegeräte
 - Betriebssystem
- (Lecture 8, overall)

- b) Beschreiben Sie den Memory-Effekt eines Akkumulators. (2 Punkte)

Lösung (pro Nennung 0,5 Punkt, maximal 2 Punkte):

- Wird der Akku eines Mobiltelefons nicht gänzlich entladen bevor er erneut aufgeladen wird, so verliert er dadurch dauerhaft einen Teil seiner Leistungsfähigkeit.
 - Dieser Effekt ist stark abhängig von der Akku-Art
- (Zusatz zur Info: Nickel-Cadmium-Zellen sind davon sehr stark betroffen, die z.Zt. gebräuchliche Nickel-Metallhydrid-Technologie weniger stark und die neueren Lithium-Ionen-Akkus (angeblich) gar nicht mehr)
- Der Akku sollte zumindest ab und an komplett entladen und neu aufgeladen werden
- (Lecture 8, slide 16)

Aufgabe 6: Smartcards & Infrastructures (15 Punkte)

- a) Erläutern Sie den Begriff „SIM-Karte“ durch Nennung von vier smartcard-spezifischen Eigenschaften. (3 Punkte)

Lösung (pro Nennung 0,75 Punkt, maximal 3 Punkte):

- SIM-Cards sind Smartcards
 - Sie dienen als Sicherheitsmedium
 - Sie besitzen eine IMSI (International Mobile Subscriber Identity)
 - Sie besitzen einen Key (Ki) zugeteilt vom Netzbetreiber.
 - Eine Smartcard ist ein kleiner Computer
 - Sie besitzt Speicher, ein Betriebssystem, Software
 - einen Prozessor, ein I/O-Interface und Access Controls
 - Die Auslegung als kleiner Computer mit eigener Hardware und wohldefinierter Schnittstelle bietet einen besonderen Schutz gegen Manipulation
- (Lecture 9, Slide 3-6)

- b) Die folgende Abbildung stellt den Authentifizierungsprozess in einem WLAN dar. Wie nennt man dieses Verfahren? Existiert ein Äquivalent im Mobilfunkbereich und welche Aufgabe könnte ein solches Verfahren dort erfüllen? (3 Punkte)

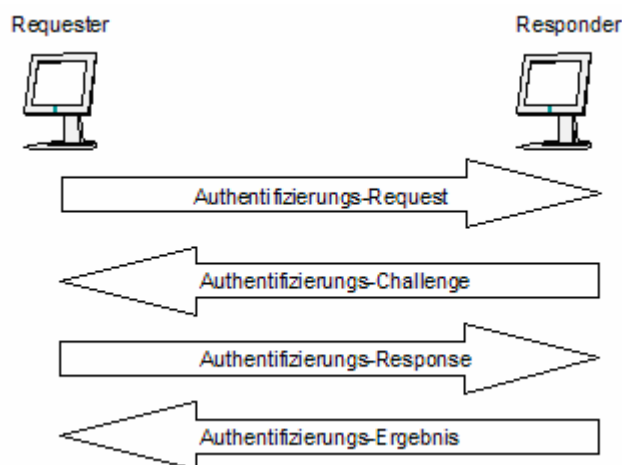


Abbildung 1: WLAN-Authentifizierungsprozess

Lösung (pro Nennung 1 Punkt, maximal 3 Punkte):

- Das Verfahren heißt: Challenge-Response-Verfahren.
- Ja, es gibt ein Äquivalent im Mobilfunkbereich.
- Im Mobilfunkbereich wird das Challenge-Response-Verfahren für die Authentifizierung der Subscriber im GSM-Netzwerk verwendet.

- c) Nennen Sie den Hauptvorteil des, in Abbildung 1 dargestellten, Authentifizierungsprozesses. (1 Punkte)

Lösung (pro Nennung 1 Punkt, maximal 1 Punkte):

- Der geheime Schlüssel wird zu keinem Zeitpunkt in einem ungeschützten Bereich übertragen.

- d) Erläutern Sie die Hauptmerkmale des Authentifizierungsprozesses, der in Abbildung 1 dargestellt ist. (4 Punkte)

Lösung (pro Nennung 1 Punkt, maximal 4 Punkte):

- Zwei oder mehrere beteiligte Parteien teilen sich ein gemeinsames Geheimnis.
- Teilnehmer B erzeugt eine Klartextnachricht und übermittelt diese an Teilnehmer A
- Teilnehmer A verschlüsselt die Nachricht und sendet diese an Teilnehmer B
- Teilnehmer B überprüft das Ergebnis seiner Verschlüsselung der Klartextnachricht mit dem Ergebnis der Verschlüsselung der Klartextnachricht von Teilnehmer A
- Falls Übereinstimmung dann Authentifizierung erfolgreich.

- e) Nennen Sie zwei von fünf Backend-Infrastrukturen, die für einen mobilen Dienst benötigt werden und dazu jeweils zwei konkrete Technologiekomponenten. (4 Punkte)

Lösung (pro Nennung 1 Punkt, maximal 2 Punkte):

- Content
 - Content-management ("Server")
 - Application server
 - Communication (internet and/or mobile radio)
 - Terminal for display, interaction, processing
- (Lecture 9, Slide 38-48)

Lösung (pro Nennung 0,5 Punkt, maximal 2 Punkt):

- 2 aus (SGML, XML, HTML, WML, cHTML, PDF, Postscript, RTF, LaTeX, JPEG, GIF)
 - oder 2 aus (CSS, PHP, SQL, CGI)
 - oder 2 aus (Java Beans, Servlets, IIS, Apache, Tomcat, SAP, Tivoli, SIP/MBS, Web-sphere, WebObjects)
 - oder 2 aus (TCP/IP, X.500, GSM, GPRS, HSCSD, SMS-C, UUCP, SMTP, HTTP, SSL, WTLS, WAP, POP3, IMAP4, SOAP, EDI / EDIFACT)
 - oder 2 aus (Browser, Operating System, I/O, SIM)
- (Lecture 9, Slide 38-48)

Aufgabe 7: Applications - Location Based Services (10 Punkte)

- a) Erklären Sie den Begriff „Location Based Services“ (LBS). (1 Punkt)

Lösung:

Positionsinformationen als Basis für Anwendungen aller Art im mobilen Kontext
(Lecture 11, Slide 3)

- b) Nennen Sie zwei typische Anwendungsgebiete von LBS und beschreiben Sie zu jedem dieser Anwendungskluster einen möglichen Dienst. Gehen Sie dabei auch auf unterschiedliche Dienstausrüstungen ein und schildern Sie die Problematik, die derzeit am Markt vorherrscht. (4 Punkte)

Lösung:

- Security, Billing/Payment, Tracking, Information (Lecture 11, Slide 26)
 - Dienstausrüstung: Push/Pull
 - Dienstbeschreibungen
 - Problematik: Zu hohe Kosten bei der Lokalisierung
- (Pro Nennung max. 2 Punkte)

- c) Das Global Positioning System (GPS) stellt eine seit Jahren etablierte Lokalisierungstechnologie dar. Geben Sie an wie viele Parameter für die Positionsbestimmung notwendig sind und beschreiben sie warum „Assisted GPS“ in mobilen Endgeräten eine Verbesserung bedeuten kann. (2 Punkte)

Lösung:

- 4 Parameter (3 Laufzeitmesswerte und die Zeit) (1 Punkt)

„Assisted GPS“: (1 Punkt)

- Schnelleres Fixing.

- Batteriesparend (wurde in der Vorlesung erwähnt).

(Lecture 11, Slide 13 und 21)

- d) Kann die Cell-Of-Origin (COO) Lokalisierungstechnologie für Routing-Anwendungen verwendet werden? Nennen Sie zwei Gründe entweder dafür oder dagegen. (2 Punkte)

Lösung:

Nein, kann man nicht: Ortung zu teuer (1 Punkt) und zu ungenau (1 Punkt)

(Lecture 11, Slide 12)

- e) Nennen Sie mindestens eine weitere mögliche Lokalisierungstechnologie außer GPS und COO. (1 Punkt)

Lösung:

WLAN, Bluetooth, Infrarot, OTD, RFID

(Lecture 11, Slide 38)

Aufgabe 8: Security (10 Punkte)

- a) Nennen Sie vier Sicherheitsrisiken, die im Internet existieren. (2 Punkte)

Lösung (pro Nennung 0,5 Punkt, maximal 2 Punkte):

- Denial-of-Service Attacken

- Phishing-Aktionen

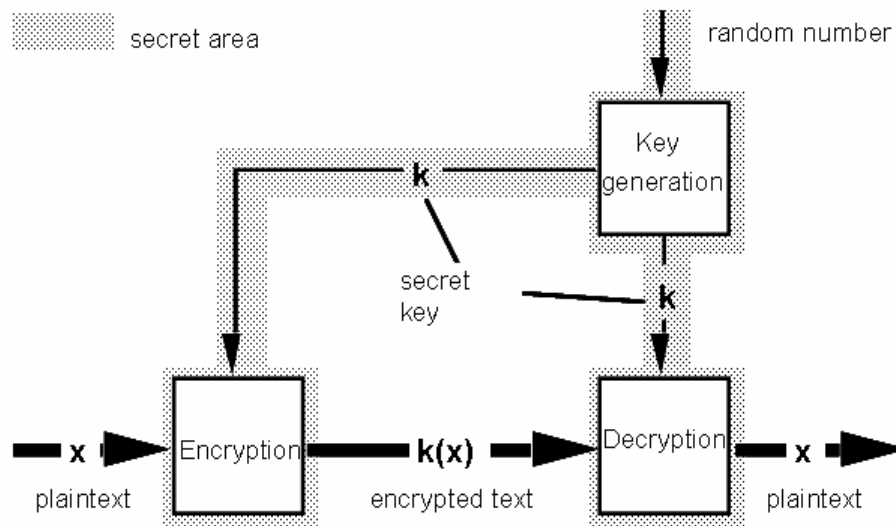
- Loggen von Tastatureingaben (Datendiebstahl)

- Viren / Trojaner / Spyware (Lecture 12-14, Slide 3-8)

- b) Erklären Sie anhand einer Abbildung wahlweise die Funktionsweise der symmetrischen **oder** asymmetrischen Verschlüsselung und nennen Sie jeweils eine Beispielimplementierung für Ihr gewähltes Verfahren. (6 Punkte)

Lösung:

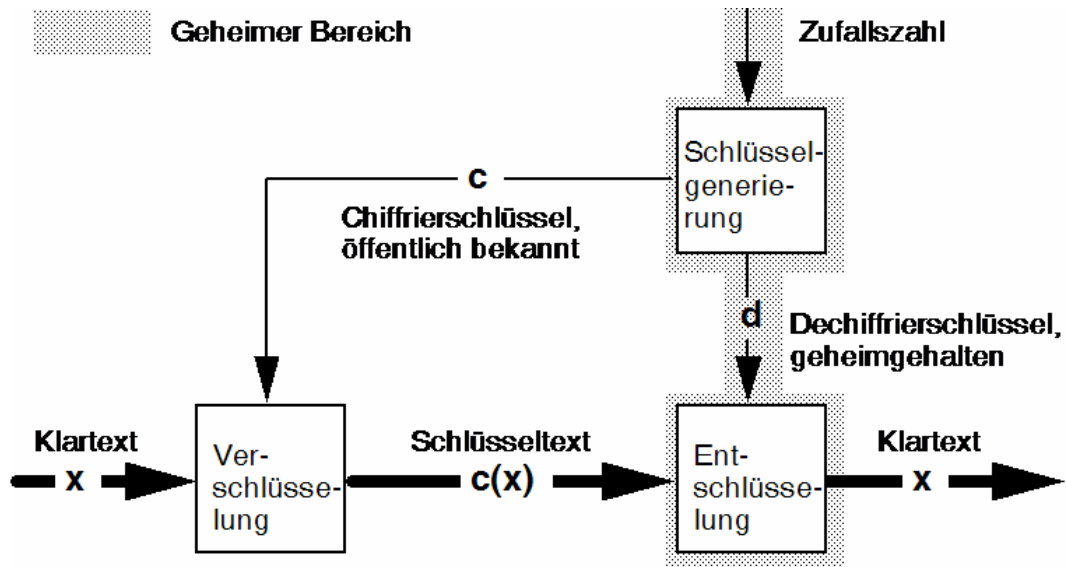
Symmetrische Verschlüsselung



Lösung (pro Nennung 1 Punkt, maximal 6 Punkte):

- Entschlüsselungskomponente
 - Verschlüsselungskomponente
 - Schlüsselerzeugungskomponente
 - Ein gemeinsamer geheimer Schlüssel
 - Verbindungen untereinander
 - Beispiel: AES, DES
- (Lecture 12-14, Slide 52)

Asymmetrische Verschlüsselung



Lösung (pro Nennung 1 Punkt, maximal 6 Punkte):

- Entschlüsselungskomponente
- Verschlüsselungskomponente
- Schlüsselerzeugungskomponente
- Es existieren zwei Schlüssel. Ein geheimer und ein öffentlicher Schlüssel
- Verbindungen untereinander
- Beispiel: RSA, Diffie-Hellman
(Lecture 12-14, Slide 64)

c) Wo sehen Sie den Hauptkritikpunkt einer symmetrischen Verschlüsselung? (2 Punkte)

Lösung (pro Nennung 0,5 Punkt, maximal 2 Punkte):

- Bei der Durchführung des Schlüsselaustausches (1 Punkt)
- Der Schlüssel muss von allen Parteien geheim gehalten werden (0,5 Punkte)
- Die Schlüsselverwaltung von mehreren Parteien ist komplex (0,5 Punkte)
(Lecture 11, angelehnt an Slide 54)