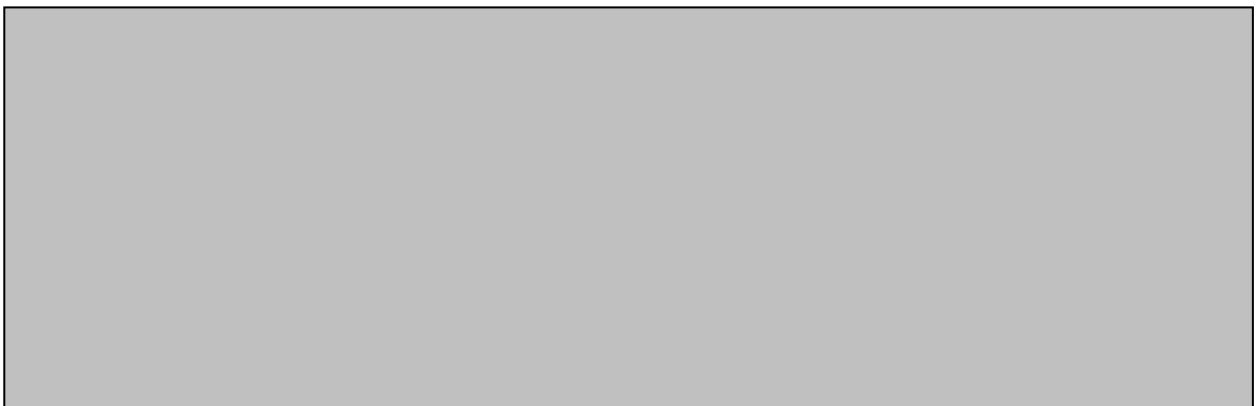


**Aufgabe 1****(20 Punkte)**

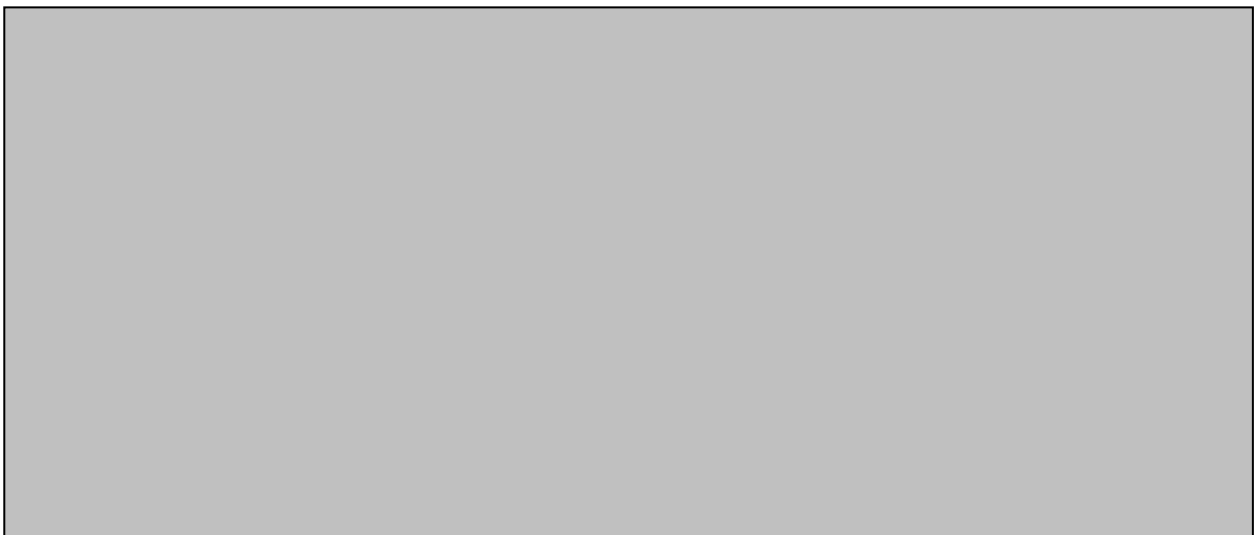
- 1.1 Geben Sie drei Klassifizierungsmerkmale aus dem Kurstext für den Begriff „Bedrohung“ an. (3 Punkte)



- 1.2 Was ist Steganographie? (1 Punkt)




- 1.3 Wozu benötigt man einen Repeater? Geben Sie genau an, welche Signale der Repeater weiterleitet. (2 Punkte)

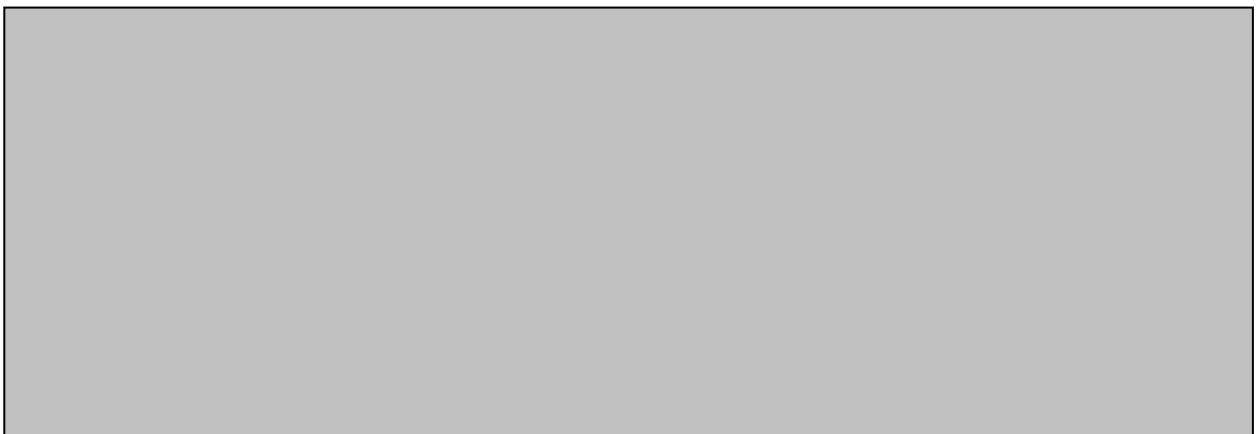


1.4 Geben Sie an, welche der folgenden Behauptungen wahr oder falsch sind. (2 Punkte)

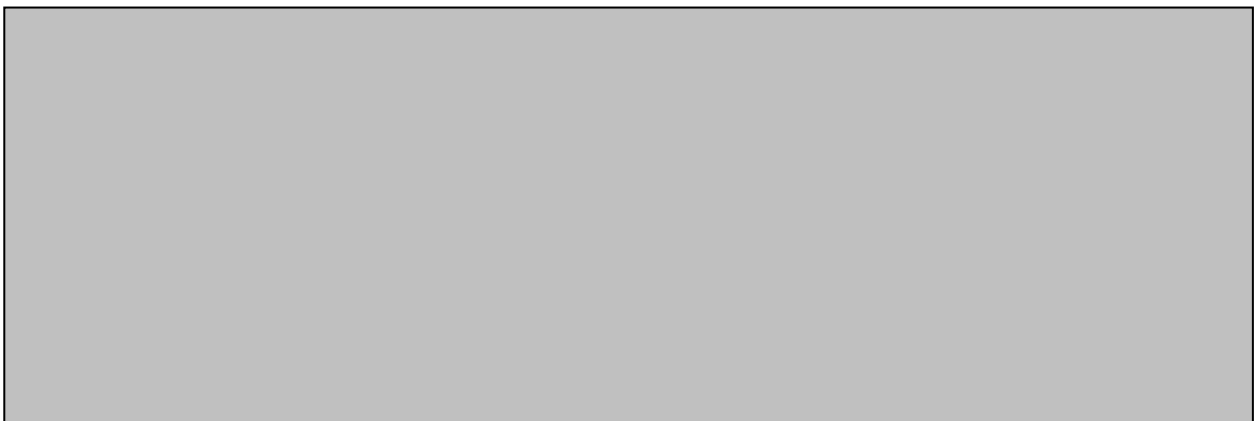
- a) Um zwei Netze unterschiedlicher Technologien (z.B. Ethernet und Token Ring) zu verbinden, benötigt man eine Bridge.
- b) TCP bedeutet: transmission control protocol.
- c) DNS bedeutet: domain name system.
- d) HTTP bedeutet: host transfer protocol.



1.5 Wie viele mögliche IP(v4)-Adressen gibt es? Geben Sie Ihre Lösung als Zweierpotenz an. (1 Punkt)



1.6 Geben Sie drei der im Kurstext beschriebenen Virentypen an. (3 Punkte)



1.7 Was ist der Hauptunterschied zwischen Viren und Würmern?

(2 Punkte)



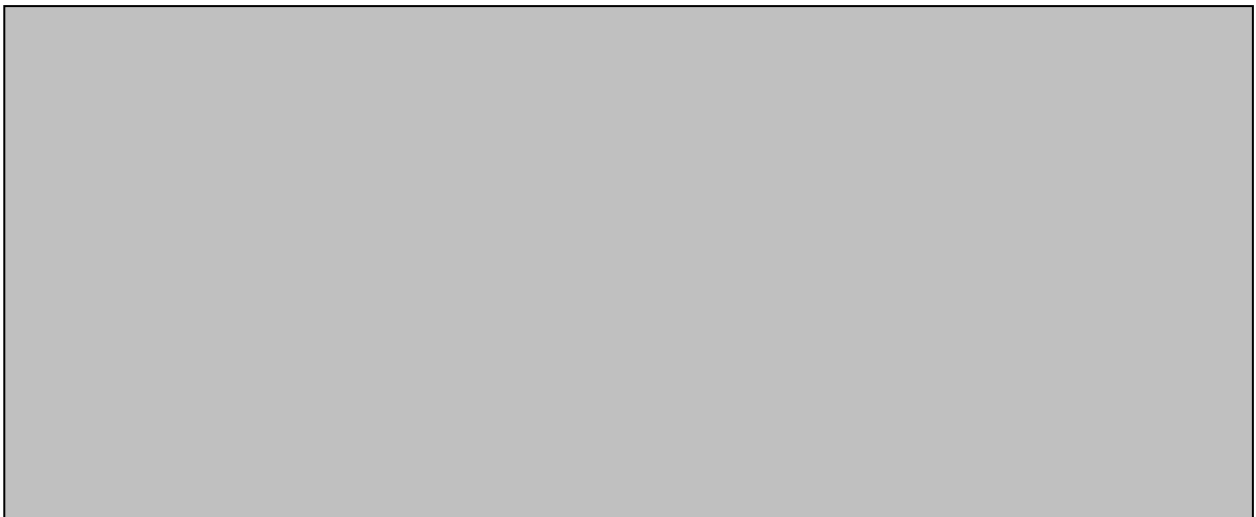
1.8 Was ist ein Trojanisches Pferd?

(1 Punkt)



1.9 Wie viele Kombinationen müssen Sie im schlimmsten Fall bei einer Brute-Force-Attacke auf das in `/etc/passwd` eingetragene Passwort eines Ihnen bekannten Benutzers ausprobieren, wenn Sie wissen, dass das Passwort  $n$  Zeichen lang ist, dass jedes Zeichen ein Groß- oder Kleinbuchstabe (ohne Umlaute) oder eine Ziffer von 0 bis 4 sein kann, und dass das Salt  $m$  Bit umfasst? Geben Sie die Anzahl als Formel an.

(5 Punkte)



**Aufgabe 2****(32 Punkte)**

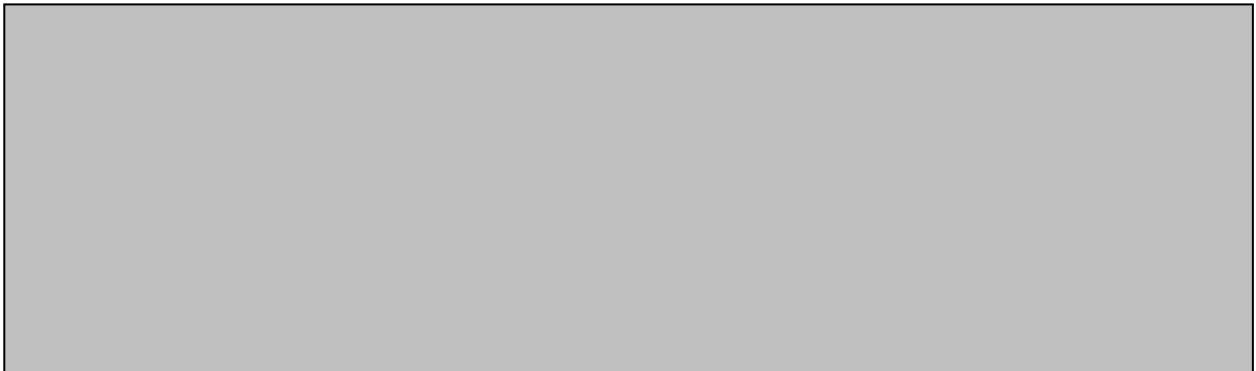
2.1 Wie funktioniert ein hybrides Verschlüsselungsverfahren?

(2 Punkte)

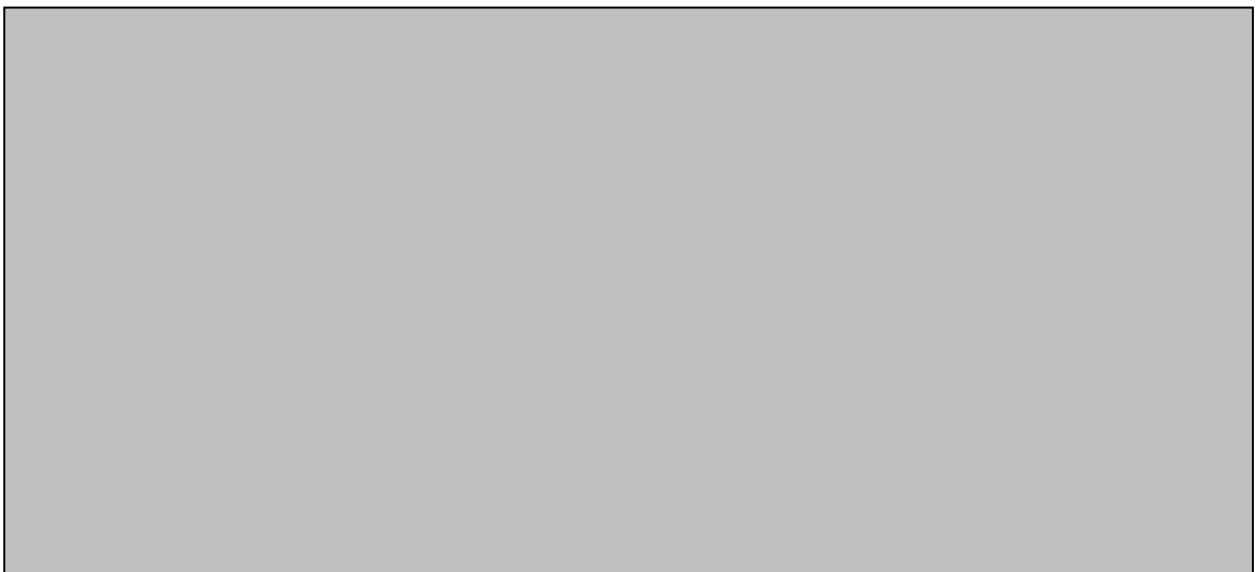


2.2 Wenn Sie eine VoIP-Verbindung verschlüsseln wollen, welchen Verschlüsselungsmodus würden Sie wählen? Warum?

(2 Punkte)

2.3 Verschlüsseln Sie den Text „ANFANG“ mit der Chiffre  $(x + 4) \bmod 26$ , wenn die Buchstaben A bis Z mit 0 bis 25 codiert sind.

(3 Punkte)



2.4 Was ist das Kennzeichen einer polyalphabetischen Chiffre?

(2 Punkte)



2.5 Gegeben sei der Schlüssel „ABCD“. Verschlüsseln Sie den Text „ANFANGAN“ mit der Vigenère-Chiffre. Die Buchstaben A bis Z sollen mit 1 bis 26 codiert sein. (2 Punkte)



2.6 Schildern Sie eine Runde des Feistel-Verfahrens in pseudo-algorithmischer Notation (Zuweisung „ $\leftarrow$ “, logische Operationen ( $\lll$  [linkszirkuläres Shiften], AND, NOT, OR, XOR, z.B.:  $a \text{ AND } b$ ,  $a \lll b$ ), Funktionen “ $F(x,y,\dots)$ “, eine arithmetische Funktion „+“ ). Als Eingaben haben Sie  $L_0$ ,  $R_0$ , sowie  $S_0$ . Ausgaben sind  $L_1$  und  $R_1$ . (3 Punkte)



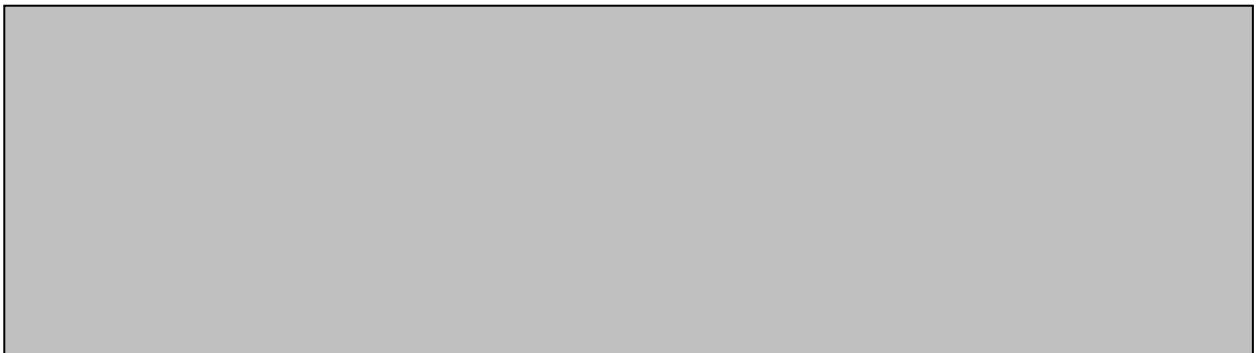
2.7 Wie funktioniert der electronic code book-Mode?

(1 Punkt)



2.8 Wie funktioniert cipher block chaining?

(1 Punkt)



2.9 Welchen Schlüssel benutzt man für die Entschlüsselung einer Nachricht bei einer asymmetrischen Verschlüsselung? (1 Punkt)



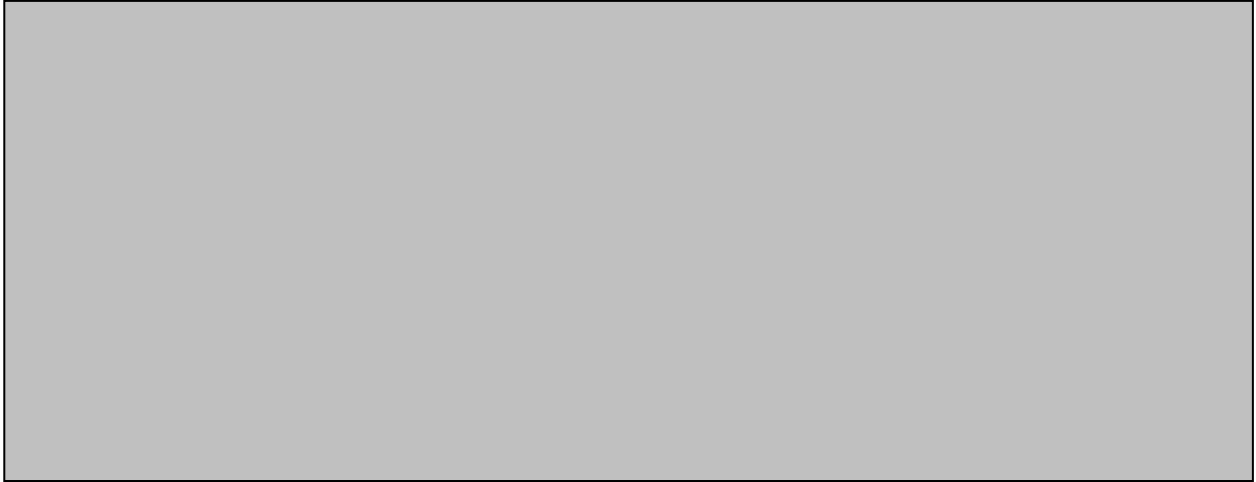
2.10 Auf welchem schwierigen mathematischen Problem beruht die Sicherheit der El-Gamal-Verschlüsselung? (1 Punkt)



2.11 Schildern Sie das Verfahren von Diffie-Hellmann zur Übermittlung eines geheimen Schlüssels. (5 Punkte)



2.12 Was ist eine Kollision bei Hash-Werten und wieso gibt es überhaupt Kollisionen?  
(2 Punkte)



2.13 Gegeben sei eine Hash-Funktion, die 1 000 000 unterschiedliche Hash-Werte erzeugen kann, z.B. Zahlen aus dem Intervall von 0 bis 999 999.

- a) Weiterhin sei eine Nachricht  $N$  mit Hash-Wert  $H(N)$  gegeben. Wie viele Nachrichten müssen Sie erzeugen, um mit einer Wahrscheinlichkeit größer als  $\frac{1}{2}$  eine Nachricht mit demselben Hash-Wert  $H(N)$  zu erhalten? (2 Punkte)
- b) Wie viele zufällige verschiedene Nachrichten müssen Sie erzeugen, damit mit einer Wahrscheinlichkeit größer als  $\frac{1}{2}$  mindestens zwei (beliebige) dieser Nachrichten denselben Hash-Wert haben? (3 Punkte)





2.14 Was ist der prinzipielle Unterschied in der Berechnung zwischen Message Authentication Codes (MACs) und Digitalen Signaturen? (1 Punkt)



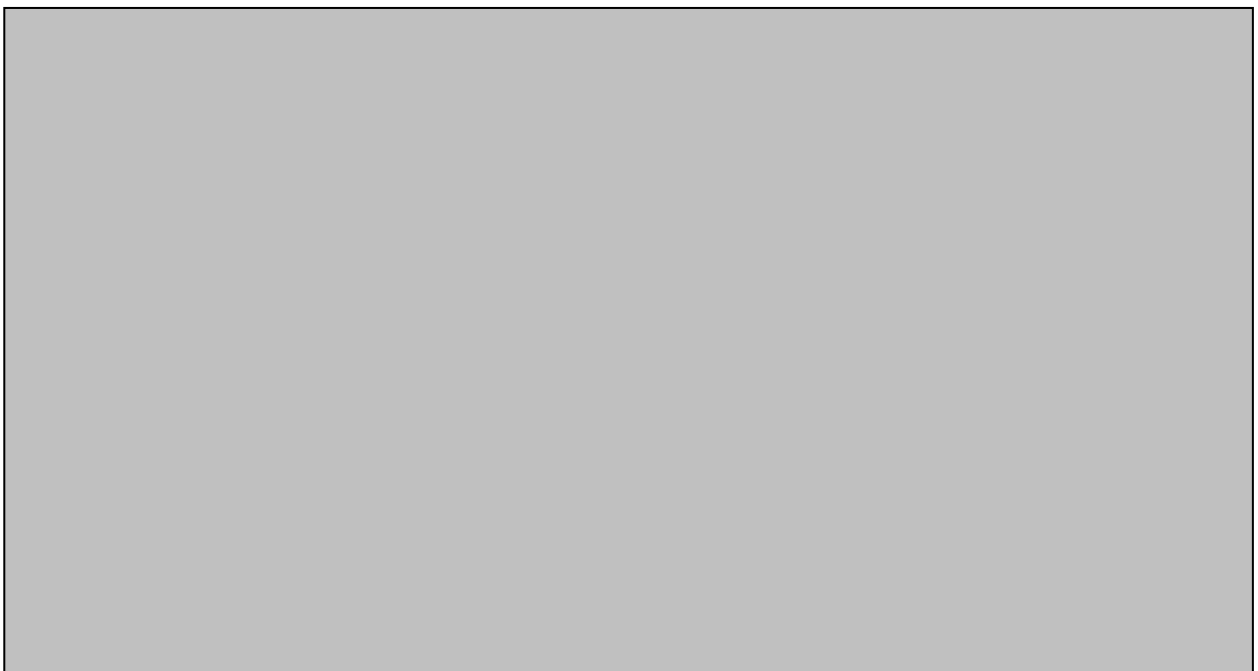
2.15 Was macht eine Bridge-CA? (1 Punkt)



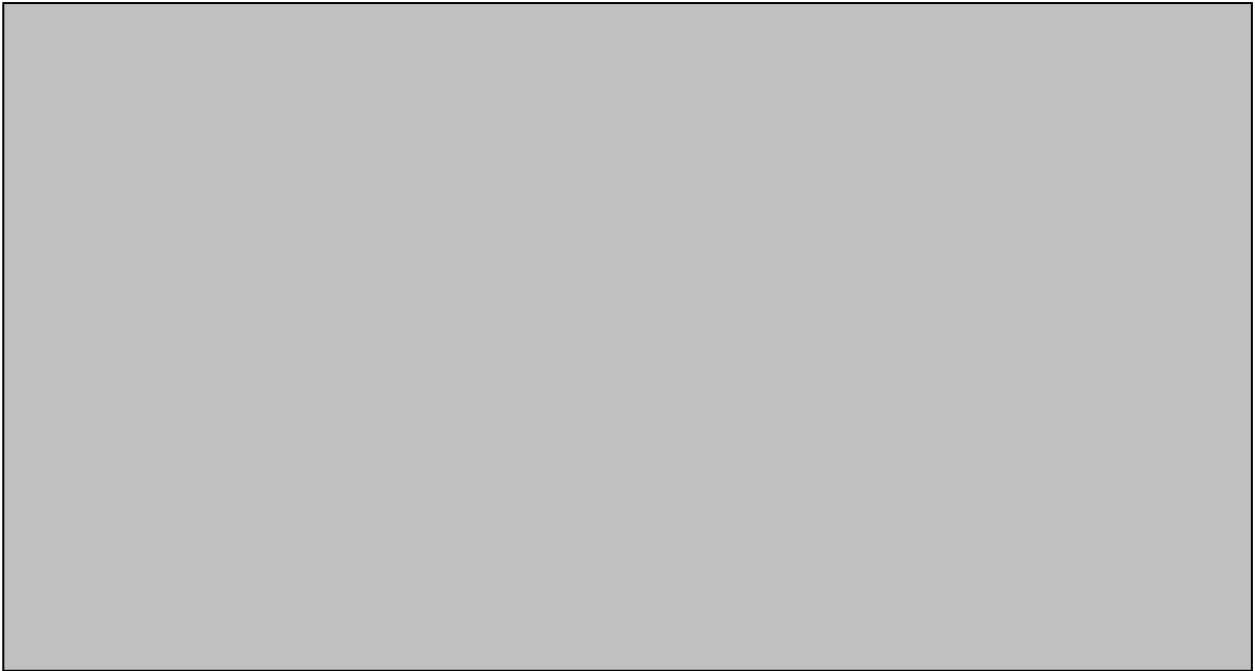
### Aufgabe 3

**(10 Punkte)**

3.1 Wie funktioniert die RSA-Authentisierung bei SSH-Verbindungen (Client / Server) bei der erstmaligen Verbindung des Client mit dem Server? (6 Punkte)



3.2 Schildern Sie die Grundidee der User Account Control (ab Windows Vista). (4 Punkte)



#### **Aufgabe 4**

**(14 Punkte)**

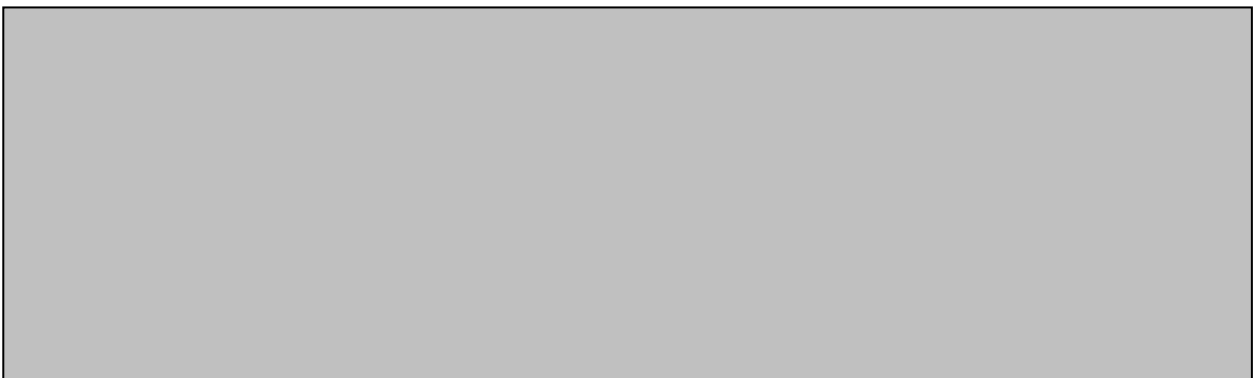
4.1 Wozu dient caching beim Proxy?

(1 Punkt)



4.2 Warum anonymisiert ein Proxy, wenn http-requests von innen nach außen über den Proxy gehen?

(1 Punkt)



4.3 Was ist der Unterschied zwischen Screened Subnet und DMZ?

(1 Punkt)



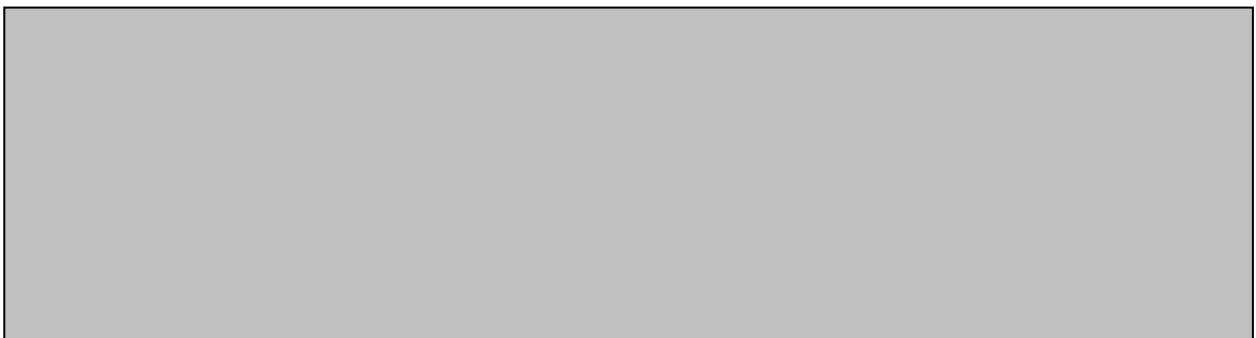
4.4 Was ist der Unterschied in Bezug auf die Hardware zwischen single- und dual homed application level gateways? (ALG)?

(1 Punkt)



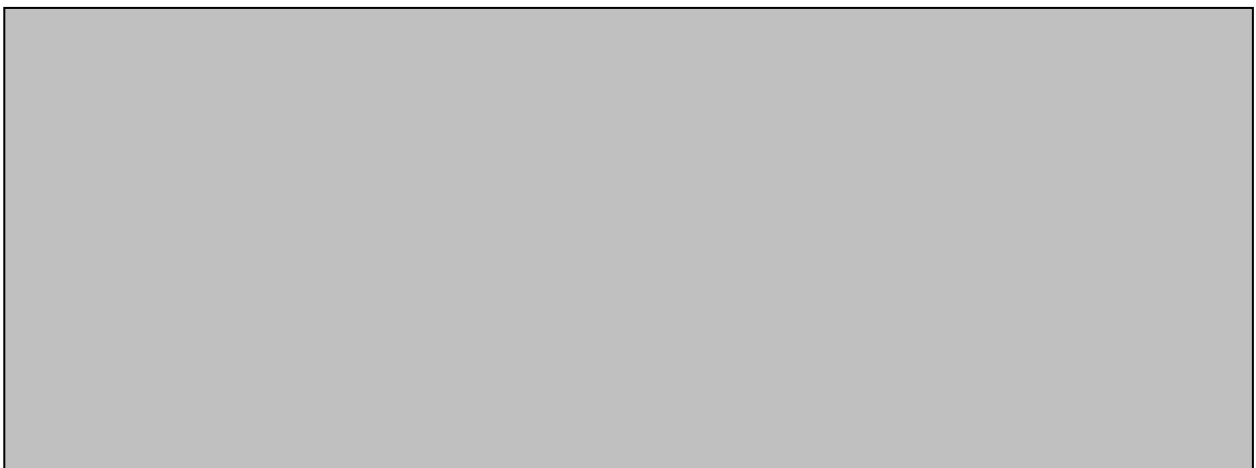
4.5 Was sind mangle Regeln bei iptables?

(1 Punkt)



4.6 Was bedeutet die Abkürzung ITIL und wie hängt ITIL mit IT-Sicherheit zusammen?

(3 Punkte)



4.7 Ordnen Sie die folgenden Risiken in die angegebene probability impact Matrix ein:

- 1) Ein Hacker manipuliert die Homepage derart, dass dort dumme Witze und Links zu zwielichtigen Web-Servern installiert werden.
- 2) Der Administrator-Zugang zum Web-Server ist eine telnet-Verbindung über das Internet.
- 3) Durch Probleme in der internen Ablauforganisation werden die HTML-Seiten auf dem Server nicht rechtzeitig aktualisiert, sondern mit einer Stunde Verzögerung. (6 Punkte)

Auswirkung	Hoher Schaden			
	Niedriger Schaden			
		Niedrig		Hoch
		Eintrittswahrscheinlichkeit		