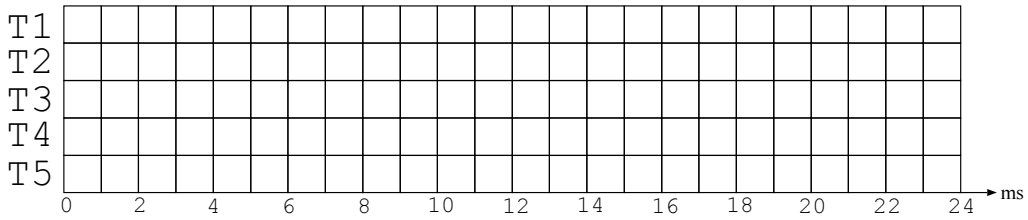
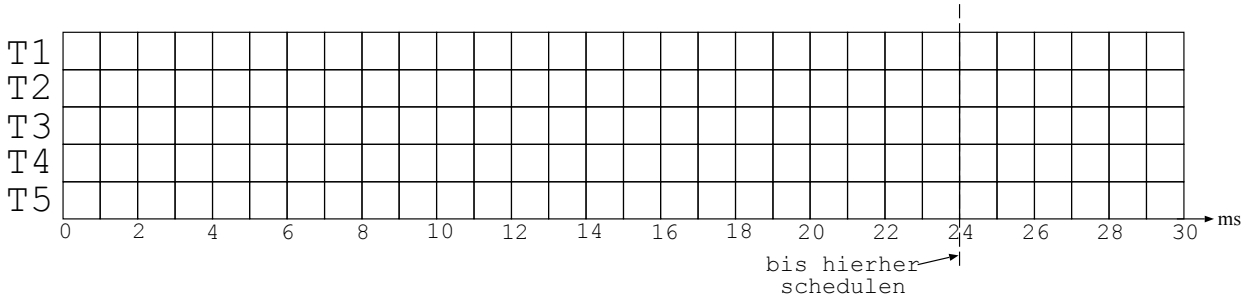
Ersatz a)



Ersatz b)



4 Security (20)

a) (10)

Was versteht man unter einem *aktiven* Security Threat?

Welche *aktiven* Security Threats gibt es?

Was versteht man unter einem *passiven* Security Threat?

Welche *passiven* Security Threats gibt es?

b) (4)

Was versteht man unter *Audit Records*?

Wozu dienen *Audit Records*?

c) (6)

Wann nennt man einen Verschlüsselungsalgorithmus *symmetrisch*?

Wann nennt man einen Verschlüsselungsalgorithmus *asymmetrisch*?

Welchen Vorteil hat die symmetrische gegenüber der asymmetrischen Verschlüsselung?

Welchen Vorteil hat die asymmetrische gegenüber der symmetrischen Verschlüsselung?

4 Security (20)

a) (3)

Welche drei Sicherheitsanforderungen gibt es?

b) (3)

Welche Sicherheitsanforderungen sind in den folgenden Beispielen verletzt? (bitte kurze **Begründung** angeben!)

- Ein Druckprogramm erlaubt fälschlicherweise den Ausdruck einer Datei mit geheimen Daten.
- Ein Benutzer ändert unerlaubterweise das Passwort eines autorisierten Benutzers.

c) (1)

Ein frustrierter Programmierer, der sich aufgrund seiner bevorstehenden Kündigung an seiner Firma rächen will, fügt in das Buchhaltungsprogramm eine Routine ein, die einen Tag nach seiner Kündigung alle Daten löscht. Geben Sie den englischen Fachbegriff für diese Routine an!

d) (1)

Ein unautorisierter Benützer kann alle Files in einem Computersystem lesen. Wie bezeichnet man diesen *threat* und gegen welche Sicherheitsanforderung verstößt er?

e) (4)

Erklären Sie die *Grundzüge* des Public-Key Verschlüsselungsverfahren, sowie die *Vor-* und *Nachteile* gegenüber konventionellen Verschlüsselungsverfahren.

Grundzüge:

Vorteile:

Nachteile:

f) (3)

Was für potenzielle Schwachstellen(mind. 3) weißt das Passwort *password* auf?

g) (3)

Welche Regeln(mind. 3) sollten bei der Wahl eines "sicheren" Passwortes angewandt werden?

3 Security (20)

a) (4)

Was versteht man unter dem Schlagwort *Least Priviledge*?

Geben Sie dazu ein Beispiel an:

b) (6)

Nennen Sie bitte drei Arten von Security Threats und geben Sie jeweils ein Beispiel dazu an:

c) (10)

Ist es möglich mit einem symmetrischen Verschlüsselungsalgorithmus eine fälschungssichere elektronische Unterschrift zu realisieren?

◯ Ja ◯ Nein

Wenn ja, geben Sie bitte an wie so ein Algorithmus funktioniert. Im Fall, dass Sie die vorherige Frage mit nein beantwortet haben, begründen Sie bitte, warum das nicht möglich ist.

Welchen Vorteil hat die symmetrische gegenüber der asymmetrischen Verschlüsselung?

4 Security (20)

a) (3)

Was beschreibt das Modell von Bell und LaPadula?

b) (4)

Im Modell von Bell und LaPadula gibt es die *Simple Security Property* und die $\star$*-Property*. Beschreiben Sie für jeden der beiden Begriffe was er besagt und was das damit verbundene Konzept bewirken soll.

c) (5)

Beschreiben Sie die Funktionsweise von *Public Key Verschlüsselungsverfahren*. Erklären Sie insbesonders, welche Schüssel man bei diesem Verfahren benötigt, wer welche Schlüssel kennen darf und wie die Schlüssel von den Sendern und Empfängern von Daten verwendet werden.

d) (8)

Geben Sie die Schritte an, die zum Senden und beim Empfangen einer mit einem Public Key Verfahren verschlüsselten und signierten Nachricht notwendig sind. Welche Schlüssel braucht man dabei?

3 Security (20)

a) (2)

Geben Sie mit Begründung an, ob aktive oder passive *Secutity Threats* schwierieger zu erkennen sind.

b) (3)

Was bedeutet das Prinzip *Least Priviledge*?

Nennen Sie ein Beispiel, wo dies verletzt wäre:

c) (6)

Beschreiben Sie das Prinzip des Public-Key Verschlüsselungsverfahrens, sowie die Vor- und Nachteile gegenüber symmetrischen Verschlüsselungsverfahren.

Prinzip:

Vorteile:

Nachteile:

d) (6)

Nennen Sie drei Methoden eines Hackers zum Herausfinden von Passwörtern:

Nennen Sie drei potentielle Schwachstellen des Passwortes "*passwort*":

e) (3)

Was beschreibt das Modell von Bell und LaPadula?

3 Security (25)

3.1 Begriffe (10)

Was versteht man unter *Confidentiality (Secrecy)*, *Integrity* und *Availability*. Erklären Sie die drei Begriffe und geben Sie jeweils ein Beispiel einer Security Attacke an, welche die Eigenschaft verletzt.

- Confidentiality:

- Integrity:

- Availability:

Arten der Bedrohung (Types of Threats)

Füllen Sie folgende Tabelle derart aus, dass Sie jede angegebene Art der Bedrohung einem der Begriffe *Confidentiality (Secrecy)*, *Integrity* und *Availability* zuordnen (Fehlende Antworten werden negativ, falsche Antworten werden doppelt negativ gewertet!):

Art der Bedrohung	**bedroht**
Interruption	
Interception	
Modification	
Fabrication	

3.2 Bedrohungen (8)

Erläutern Sie die folgenden Bedrohungen: *Logic Bomb*, *Trojan Horse*, *Virus* und *Worm*.

- Logic Bomb:

- Trojan Horse:

- Virus:

- Worm:

3.3 Verständnisfragen (7)

Beurteilen Sie die folgenden Aussagen! Fehlende Antworten werden negativ, falsche Antworten werden doppelt negativ gewertet!

◯ Ja ◯ Nein *Network security* umfasst Maßnahmen zum Schutz der Daten während der Übertragung.

◯ Ja ◯ Nein Bei symmetrischen Crypto-Systemen werden zum Ver- und Entschlüsseln dieselben Keys verwendet.

◯ Ja ◯ Nein *Threshold detection* ist ein statistisches Verfahren zur Intrusion Detection.

◯ Ja ◯ Nein Das *Least Privilege* Prinzip besagt, dass jeder Benutzer alle Rechte per default hat.

◯ Ja ◯ Nein Bei *Masquerading* wird der Inhalt einer Message verändert.

◯ Ja ◯ Nein Eine *Trapdoor* ist ein geheimer Einstiegspunkt, der zur Umgehung der Zugriffskontrolle dient.

◯ Ja ◯ Nein Eine *denial-of-service* Attacke ist eine passive Attacke.

4 Security (25)

Security Threats (6)

Beschreiben Sie die Security Threats? Geben Sie jeweils ein Beispiel an.

Data Oriented Access Control (3)

Beschreiben Sie die *Data Oriented Access Control*? Welche Elemente hat das Modell?

Design for Security (4)

Was bedeutet das Prinzip *Open Design*? Erklären Sie anhand eines Beispiels die Vorteile des Open Design Prinzips.

Verschlüsselung (5)

Beschreiben Sie das Prinzip des Public-Key Verschlüsselungsverfahrens, sowie die Vor- und Nachteile gegenüber symmetrischen Verschlüsselungsverfahren.

Program Related Threats (2)

Beschreiben Sie 4 Program Related Threats.

Reference Monitor (1)

Was ist ein Reference Monitor?

Intrusion Detection (4)

Was ist *Intrusion Detection*, und wozu wird es verwendet?

Beschreiben Sie 3 *Intrusion Detection* Methoden, und geben Sie jeweils ein Beispiel an.

3 Security (25)

Security Threats (6)

Beschreiben Sie die 3 grundsätzliche Arten von Security Threats? Geben Sie jeweils ein Beispiel an.

Verschlüsselung (4)

Beschreiben Sie das Prinzip des Public-Key Verschlüsselungsverfahrens, sowie die Vor- und Nachteile gegenüber symmetrischen Verschlüsselungsverfahren.

Prinzip:

Vorteile:

Nachteile:

Reference Monitor (2)

Was ist ein Reference Monitor?

Intrusion Detection (5)

Was ist *Intrusion Detection*, und wozu wird es verwendet?

Beschreiben Sie 3 *Intrusion Detection* Methoden, und geben Sie jeweils ein Beispiel an.

Authentification (2)

Was ist Authentification und wie wird das gemacht?

Verständnisfragen (6)

Beurteilen Sie die folgenden Aussagen! Fehlende Antworten werden nicht gewertet, falsche Antworten werden negativ gewertet!

◯ Ja ◯ Nein *Network security* umfasst Maßnahmen zum Schutz der Daten während der Übertragung.

◯ Ja ◯ Nein Bei Asymmetrischen Crypto-Systemen werden zum Ver- und Entschlüsseln dieselben Keys verwendet.

◯ Ja ◯ Nein *Threshold detection* ist ein statistisches Verfahren zur Intrusion Detection.

◯ Ja ◯ Nein Das *Least Privilege* Prinzip besagt, dass jeder Benutzer keine Rechte per default hat.

◯ Ja ◯ Nein Bei *Masquerading* wird der Inhalt einer Message verändert.

◯ Ja ◯ Nein Eine *denial-of-service* Attacke ist eine aktive Attacke.

4 Security (20)

4.1 Begriffe (8)

Was versteht man unter *Confidentiality (Secrecy)*, *Integrity* und *Availability*? Erklären Sie die drei Begriffe.

- Confidentiality:

- Integrity:

- Availability:

Arten der Bedrohung (Types of Threats)

Füllen Sie folgende Tabelle derart aus, dass Sie jede angegebene Art der Bedrohung einem der Begriffe *Confidentiality (Secrecy)*, *Integrity* und *Availability* zuordnen (Fehlende Antworten werden negativ, falsche Antworten werden doppelt negativ gewertet!):

Art der Bedrohung	**bedroht**
Interruption	
Interception	
Modification	
Fabrication	

4.2 Bedrohungen durch Programme oder Programmfragmente (8)

Erläutern Sie die folgenden Bedrohungen: *Logic Bomb*, *Trojan Horse*, *Virus* und *Worm*.

- Logic Bomb:

- Trojan Horse:

- Virus:

- Worm:

4.3 Security by Obscurity vs. Open Design (4)

Beschreiben Sie den Unterschied zwischen *Security by Obscurity* und *Open Design*. Geben Sie die Vor- und Nachteile an.

3 Security (25)

3.1 Nennen und erklären Sie die Threats of Security. Geben Sie jeweils ein konkretes Beispiel an! (5)

3.2 Erklären Sie die Funktionsweise von Kerberos! (5)

3.3 Wie funktioniert Public Key Encryption? (5)

3.4 Beschreiben Sie das UNIX Passwort Scheme! (4)

3.5 Erläutern Sie zwei Ansätze zum Angriff auf ein konventionelles Encryption Scheme! (6)

3 Security (20)

3.1 Begriffe (8)

Was versteht man unter *Confidentiality (Secrecy)*, *Integrity* und *Availability*? Erklären Sie die drei Begriffe.

- Confidentiality:

- Integrity:

- Availability:

Arten der Bedrohung (Types of Threats)

Füllen Sie folgende Tabelle derart aus, dass Sie jede angegebene Art der Bedrohung einem der Begriffe *Confidentiality (Secrecy)*, *Integrity* und *Availability* zuordnen (Fehlende Antworten werden negativ, falsche Antworten werden doppelt negativ gewertet!):

Art der Bedrohung	**bedroht**
Interruption	
Interception	
Modification	
Fabrication	

3.2 Design Principles for Security (8)

Nennen Sie mindestens 4 Design Prinzipien für Security und beschreiben Sie diese kurz:

3.3 Maßnahmen gegen Passwortattacken (4)

Nennen Sie mindestens 4 Maßnahmen gegen Passwortattacken:

2 Security (20)

2.1 Security by Obscurity vs. Open Design (4)

Beschreiben Sie den Unterschied zwischen *Security by Obscurity* und *Open Design*. Geben Sie die Vor- und Nachteile an.

2.2 Verständnisfragen (4)

Beurteilen Sie die folgenden Aussagen! Fehlende Antworten werden negativ, falsche Antworten werden doppelt negativ gewertet!

◯ Ja ◯ Nein *Threshold detection* ist ein statistisches Verfahren zur Intrusion Detection.

◯ Ja ◯ Nein Das *Least Privilege* Prinzip besagt, dass jeder Benutzer alle Rechte per default hat.

◯ Ja ◯ Nein Bei *Masquerading* wird der Inhalt einer Message verändert.

◯ Ja ◯ Nein Eine *denial-of-service* Attacke ist eine passive Attacke.

2.3 Begriffe (8)

Was versteht man unter *Confidentiality (Secrecy)*, *Integrity* und *Availability*? Erklären Sie die drei Begriffe.

- Confidentiality:

- Integrity:

- Availability:

2.4 Wie funktioniert Public Key Encryption? (4)

2 Security (21)

2.1 Begriffe (6)

Was versteht man unter *Confidentiality (Secrecy)*, *Integrity* und *Availability*? Erklären Sie die drei Begriffe.

- Confidentiality:

- Integrity:

- Availability:

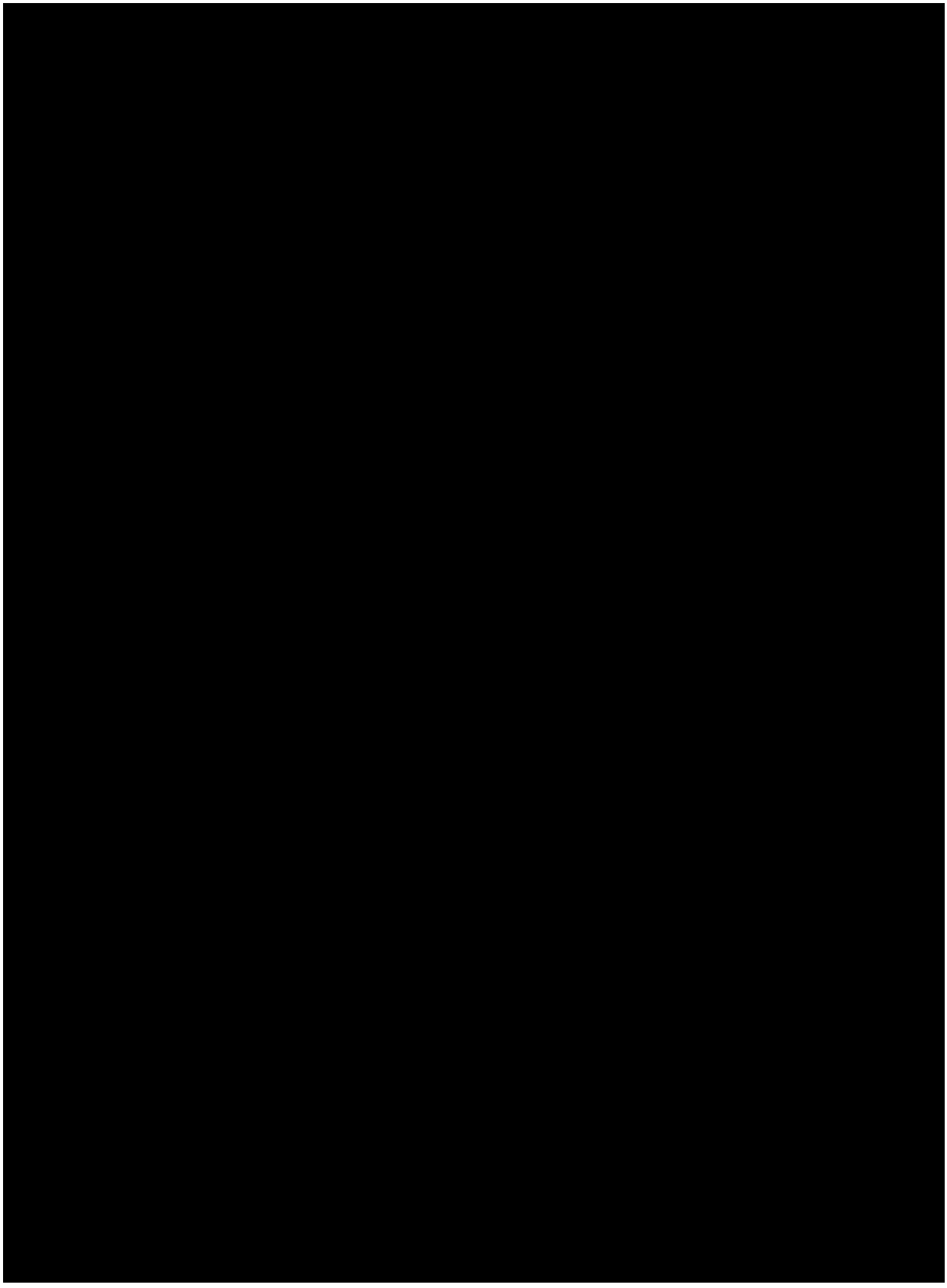
2.2 Security Threats (4)

Füllen Sie folgende Tabelle derart aus, dass Sie jede angegebene Art der Bedrohung einem der Begriffe *Confidentiality (Secrecy)*, *Integrity* und *Availability* zuordnen:

Art der Bedrohung	**bedroht**
Interruption	
Interception	
Modification	
Fabrication	

2.3 Design Principles for Securiy (7)

Nennen Sie *sieben* Designprinzipien für Security!



2.4 Bedrohungen durch Malware (4)

Erläutern Sie die folgenden Bedrohungen: *Logic Bomb*, *Trojan Horse*, *Virus* und *Worm*.

- Logic Bomb:

- Trojan Horse:

- Virus:

- Worm: