Mündliche Abiturprüfung

Fach Informatik – Grundkurs

Prüfender Fachlehrer (Autor der Aufgabe): Max Herzler

Vorbereitungszeit: 20 min, Prüfungszeit 30 min

Informationssicherheit und Verschlüsselungsverfahren

1. Einordnung der Aufgabe in den Lehrplan, Taxonomie:

Lernbereich 4: Informationssicherheit	**10 Ustd.**
Kennen von Anforderungen an die Informationssicherheit - Vertraulichkeit - Integrität - Authentizität - Verfügbarkeit	Datensicherheit, Datensicherung, Datenschutz
Kennen der Grundprinzipien kryptographischer Verfahren zur Gewährleistung der Vertraulichkeit von Informationen - symmetrisch - asymmetrisch - hybrid	Schlüsselpaar, Einweg- und Falltürfunktion ➔ LB 3
Übertragen der Kenntnisse zu asymmetrischen Verschlüsselungsverfahren auf Verfahren zur Gewährleistung der Integrität und Authentizität von Informationen	digitale Signaturen ➔ LB 3
Kennen einer Maßnahme zur Gewährleistung der Verfügbarkeit von Informationen Datensicherung	Kontext persönlicher Datensicherung cloudbasierte Speicher Komplettsicherung, differentielle und inkrementelle Sicherung ➔ Kl. 9, LB 3
Sich positionieren zu Problemen der Informationssicherheit und zum Datenschutz	Aufgreifen einer aktuellen gesellschaftlichen Fragestellung Notwendigkeit kryptographischer Verfahren, Prinzipien des Datenschutzes Steganografie, Bildforensik ⇒ Medienbildung ⇒ Verantwortungsbereitschaft

Max Herzler,
Didaktik der Informatik, Universität Leipzig

2. Aufgabenstellung (so wie sie dem Prüfling vorgelegt wird):

Mündliche Abiturprüfung

Fach Informatik – Grundkurs

Prüfender Fachlehrer (Autor der Aufgabe): Max Herzler

Vorbereitungszeit: 20 min, Prüfungszeit 30 min

Informationssicherheit und Verschlüsselungsverfahren

Bearbeiten Sie die folgenden Aufgaben zum Thema Informationssicherheit und Verschlüsselungsverfahren. Zugelassene Hilfsmittel sind ein *grafikfähiger Taschenrechner, ein dokumentenechter Stift sowie bereitgestelltes Papier* für ihre Notizen. Für die Bearbeitung der Aufgaben haben Sie insgesamt **20 Minuten** Zeit. Stellen Sie dann ihre Ergebnisse innerhalb der ersten 15 Minuten der mündlichen Abiturprüfung vor.

1. Aufgabe – Datensicherheit

Die Datensicherheit beschäftigt sich mit Maßnahmen zum allgemeinen Schutz von Daten jeglicher Art. Die zentralen Ziele der Datensicherheit lauten *Verfügbarkeit, Vertraulichkeit, Integrität* und *Authentizität*.

a) *Erläutern* Sie die vier zentralen Ziele der Datensicherheit. 4 BE

b) *Entscheiden und begründen* Sie für die folgenden Fallbeispiele, welches Ziel der Datensicherheit verletzt wird: 4 BE

   i. Nach einem Phishing-Angriff verbreitet ein Hacker über den Account des Opfers Peter Müller vermehrt Werbung auf Social-Media.

   ii. Nachdem Nina online Konzertkarten gekauft hat, geht die Bestellung durch einen Absturz des Servers verloren. Die Tickets werden nicht versandt, obwohl sie das Geld bereits bezahlt hat.

c) *Diskutieren* Sie einen möglichen Lösungsansatz für Fall i. aus Aufgabe 1b). 2 BE

2. Aufgabe – RSA-Verschlüsselung

Die RSA-Verschlüsselung gilt heute als gängige Verschlüsselungsmethode.

a) *Begründen* Sie, warum es sich bei der RSA-Verschlüsselung um ein asymmetrisches Verschlüsselungsverfahren handelt. *Erläutern* Sie die grundlegenden Rollen des öffentlichen und des privaten Schlüssels. 3 BE

b) *Stellen* Sie an einem *selbstgewählten* Beispiel die Erstellung eines Schlüsselpaars (inklusive

Berechnung der Werte p, q, n, φ(n) *dar*. *Erläutern* Sie, welche Eigenschaften die Werte erfüllen müssen. Für die Werte e und d müssen lediglich die Eigenschaften erläutert werden (keine Berechnung notwendig). 7 BE

c) *Berechnen* Sie die Verschlüsselung des Werts „14“ mithilfe des öffentlichen Schlüssels (e, n) = (7, 35). 2 BE

d) *Beurteilen* Sie, ob es sich bei der RSA-Verschlüsselung um ein sicheres Verfahren handelt und ob die Verschlüsselung geeignet für die Anwendung in der Praxis ist. 3 BE

3. Tabellarisches Erwartungsbild mit Angaben der jeweils erreichbaren BE und der Zuordnung zu den Anforderungsbereichen:

Aufgabe Nr.	Sachverhalt	AB1	AB2	AB3
1. a	Ziele der Datensicherheit erläutern	4	0	0
1. b	Fallbeispiele verschiedenen Kriterien zuordnen	0	4	0
1. c	Einen Lösungsansatz diskutieren.	0	0	2
2. a	Begründung Asymmetrie und Rolle des Schlüsselpaars	3	0	0
2. b	Erstellung eines Schlüsselpaars	0	7	0
2. c	Berechnung der Verschlüsselung	0	2	0
2. d	Beurteilung des RSA-Verfahrens	0	0	3
	Summe BE	7	13	5
	Gesamt	25		

4. Musterlösung mit Angabe der Zuordnung der einzelnen BE:

Informationssicherheit und Verschlüsselungsverfahren - Musterlösung

1. Aufgabe – Datensicherheit

Die Datensicherheit beschäftigt sich mit Maßnahmen zum allgemeinen Schutz von Daten jeglicher Art. Die zentralen Ziele der Datensicherheit lauten *Verfügbarkeit, Vertraulichkeit, Integrität* und *Authentizität*.

a) *Erläutern* Sie die vier zentralen Ziele der Datensicherheit. 4 BE

→Verfügbarkeit bedeutet, dass Daten und Systeme für autorisierte Benutzer jederzeit zugänglich und nutzbar sind, wann immer sie benötigt werden. [1]

→Vertraulichkeit bedeutet, dass Informationen nur für autorisierte Personen zugänglich sind und vor unbefugtem Zugriff geschützt werden. [1]

→Integrität bedeutet, dass Daten vor unbefugter oder unabsichtlicher Veränderung geschützt sind und ihre Korrektheit und Vollständigkeit gewährleistet ist. [1]

→Authentizität bedeutet, dass die Echtheit einer Identität oder einer Information sichergestellt wird, d.h., dass die Quelle und der Inhalt vertrauenswürdig und unversehrt sind. [1]

b) *Entscheiden und begründen* Sie für die folgenden Fallbeispiele, welches Ziel der Datensicherheit verletzt wird: 4 BE

i. Nach einem Phishing-Angriff verbreitet ein Hacker über den Account des Opfers Peter Müller vermehrt Werbung auf Social-Media.

→z.B. Authentizität [1] (andere auch möglich – Begründung wichtig!)

→Der Phishing-Angriff führt dazu, dass ein Hacker die Identität von Peter Müller übernimmt und seinen Account missbraucht, um Werbung zu verbreiten. Dadurch wird die Authentizität des Accounts von Peter Müller untergraben, da nun nicht mehr sichergestellt werden kann, dass Nachrichten und Posts tatsächlich von ihm stammen. [1]

ii. Nachdem Nina online Konzertkarten gekauft hat, geht die Bestellung durch einen Absturz des Servers verloren. Die Tickets werden nicht versandt, obwohl sie das Geld bereits bezahlt hat.

→z.B. Verfügbarkeit [1] (andere auch richtig – Begründung wichtig)

→Der Serverabsturz verhindert den ordnungsgemäßen Zugriff und die Verarbeitung der Transaktion, was bedeutet, dass das System zum Zeitpunkt des Absturzes nicht verfügbar war und somit die Transaktion nicht korrekt abgeschlossen werden konnte. Das führt dazu, dass trotz Bezahlung keine Tickets versandt werden. [1]

c) *Diskutieren* Sie einen möglichen Lösungsansatz für Fall i. aus Aufgabe 1b). 2 BE

→Bewertet werden sowohl der Ansatz als auch dessen Erläuterung. [2]

→Beispiele für mögliche Lösungsansätze bei i:

- 2-Faktor-Authentifizierung
- Sensibilisierung und Schutz vor Phishing-Angriffen
- Überwachung von Kontenaktivitäten

2. Aufgabe – RSA-Verschlüsselung

Die RSA-Verschlüsselung gilt heute als gängige Verschlüsselungsmethode.

a) *Begründen* Sie, warum es sich bei der RSA-Verschlüsselung um ein asymmetrisches Verschlüsselungsverfahren handelt. *Erläutern* Sie die grundlegenden Rollen des öffentlichen und des privaten Schlüssels. 3 BE

→zum Ver- und Entschlüsseln werden verschiedene Schlüssel verwendet (im Gegensatz zum symmetrischen Verfahren, bei dem der Schlüssel gleich ist) [1]

b) *Stellen* Sie an einem *selbstgewählten* Beispiel die Erstellung eines Schlüsselpaars (inklusive Berechnung der Werte p, q, n, φ(n) *dar*. *Erläutern* Sie, welche Eigenschaften die Werte erfüllen müssen. Für die Werte e und d müssen lediglich die Eigenschaften erläutert werden (keine Berechnung notwendig). 7 BE

→p und q sind zwei verschiedene Primzahlen [1]

→$n\ mit\ n = p \cdot q$ [1]

→$\varphi(n)\ mit\ \varphi(n) = (p-1) \cdot (q-1)$ [1]

→$e\ mit\ e$ ist teilerfremd zu $\varphi(n)$ [1]

→$d\ mit\ d \cdot e = 1\ mod\ n$ [1]

→öffentlicher Schlüssel (e, n) und privater Schlüssel (d, n) [1]

→schlüssige Beschreibung [1]

c) *Berechnen* Sie die Verschlüsselung des Werts „14“ mithilfe des öffentlichen Schlüssels (e, n) = (7, 35). 2 BE

→$c \equiv m^e\ mod\ n\ \ (mit\ n = 35, e = 7, m = 7\ und\ c\ gesucht.$ [1]

→$c = 28$ [1]

d) *Beurteilen* Sie, ob es sich bei der RSA-Verschlüsselung um ein sicheres Verfahren handelt und ob die Verschlüsselung geeignet für die Anwendung in der Praxis ist. 3 BE

→Beleuchtung dreier der folgenden (oder auch weiteren sinnvollen) Aspekte [3]

→positiv:

- einfache Schlüsselgenerierung, aber sehr hoher Rechenaufwand zur Entschlüsselung ohne bekannte Schlüssel
- Verfahren wird sicherer, desto länger die Schlüssel sind
- Sicherheit des Verfahrens hängt nicht von der Geheimhaltung des Verfahrens ab
- kann für das Senden von Nachrichten in unsicheren Netzwerken verwendet werden
- wenig aufwendige Schlüsselverwaltung

→negativ:

- hoher Rechenaufwand zur Ver- und Entschlüsselung großer Texte → in der Praxis hybride Verfahren
- wird eventuell in Zukunft durch Quantencomputer mit hoher Rechenleistung unsicher

5. Hinweise zur Umsetzung

Bei der Auswahl dieser Aufgabe ist zu beachten:

- Es sollte ein (nicht unbedingt grafikfähiger) Taschenrechner zu Verfügung gestellt werden.
    - Dabei ist vorher zu überprüfen, dass keinerlei Notizen oder selbstgeschriebene Programme auf dem Gerät vorhanden sind.
- Dem Prüfling sollte in der Prüfung eine Tafel mit Kreide, ein Overheadprojektor oder ähnliches zur Verfügung gestellt werden, um die Rechenwege darzustellen.
- Die Aufgaben sind insgesamt nicht nach Schwierigkeit sortiert, sowohl Aufgabe 1 als auch Aufgabe 2 erfüllen die Anforderungsbereiche 1, 2 und 3.
- Es ist darauf zu achten, dass in Aufgabe 1 c) nur *ein* Fallbeispiel aus Aufgabe 1 b) betrachtet werden soll. Gegebenenfalls sollte man intervenieren, wenn der Prüfling die Aufgabe für beide Beispiele bearbeitet.

6. Anhang: Abbildungen:

Benotungsschlüssel:

BE	Prozent (mindestens)	Notenpunkte	entspricht Note
24 – 25	95%	15	1
23	90%	14	
22	85%	13	
20 – 21	80%	12	2
19	75%	11	
18	70%	10	
17	65%	09	3
15 – 16	60%	08	
14	55%	07	
13	50%	06	4
12	45%	05	
10 – 11	40%	04	
9	35%	03	5
8	30%	02	
7	25%	01	
0 – 6	0%	00	6

bestanden	nicht bestanden

7. Quellenangabe, Abbildungsnachweise:

-

8. Erklärung der Freigabe zur Nachnutzung der Aufgabe:

Hiermit erkläre ich, Max Herzler, diese Aufgabe unter Wahrung des Urheberrechts erstellt zu haben.

Ich stelle diese Aufgabe zur Nachnutzung nach Lizenz CC BY-NC (Namensnennung, Bearbeitung, nicht kommerziell) zur Verfügung.

Unterschrift des Autors / elektron. Signatur