Mündliche Abiturprüfung / Mündliche Abschlussprüfung
Fach Informatik - Grundkurs / Klasse 12

Prüfender Fachlehrer (Autor der Aufgabe): _____

Vorbereitungszeit: 20 min, Prüfungszeit 30 min, Hilfsmittel: Taschenrechner

Datenschutz und Kryptografie

1. Einordnung der Aufgabe in den Lehrplan, Taxonomie:

Die nachfolgende Prüfungsaufgabe ist im sächsischen Lehrplan im Lernbereich 3: Sicherheit von Informationen für den Grundkurs 11/12 einzuordnen. Punkte, die thematisch Teil der Aufgabe sind, wurden farblich hervorgerufen:

Lernbereich 3: Sicherheit von Informationen	**12 Ustd**
Kennen von Anforderungen an die Informationssicherheit - Vertraulichkeit - Integrität - Authentizität - Verbindlichkeit/Anerkennung	Recht auf informationelle Selbstbestimmung ⇒ Werteorientierung
Einblick gewinnen in die Kryptologie im gesellschaftlichen Kontext - Kryptographie - Kryptoanalyse	Notwendigkeit und Missbrauch kryptographischer Verfahren ⇒ Empathie und Perspektivwechsel Verschlüsselung und Entschlüsselung an Beispielen
Kennen von Verfahren zur Gewährleistung der Vertraulichkeit - symmetrische Verfahren - asymmetrische Verfahren - nicht kryptographische Verfahren	klassische Verfahren: Cäsar-Chiffre, Vigenere-Verschlüsselung, Prinzip der Enigma Verfahren mit geheimem Schlüssel: DES, AES, SSL RSA-Verfahren, ElGamal Steganographie
Kennen von Verfahren zur Gewährleistung der Integrität und Authentizität	One-Way-Hash Funktion elektronische Unterschrift
Beherrschen der Nutzung von Verfahren zur Gewährleistung der Sicherheit von Informationen	Maßnahmen und Strategien zum Datenschutz, zur Datensicherheit und gegen Datenmissbrauch Einsatz von Werkzeugen Umsetzung einfacher Verfahren mit einer Programmierumgebung

Stephan Wedekind
Didaktik der Informatik, Universität Leipzig

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

Datenschutz und Kryptografie

1. Aufgabe (5 Punkte)

a) Beim Datenschutz geht es um den Schutz von sogenannten personenbezogenen Daten. Stellen Sie kurz dar, was personenbezogene Daten sind und in welcher Rechtsvorschrift deren Nutzung geregelt. Beschreiben Sie was in diesem Zusammenhang das „Recht auf Vergessen werden“ bedeutet? (3 BE)

Abbildung © GDD

b) Erläutern Sie anhand der Karikatur warum personenbezogenen Daten geschützt werden sollten. (3 BE)

2. Aufgabe (9 Punkte)

Verschlüsselungsverfahren lassen sich in symmetrische und asymmetrische Verfahren unterteilen.

a) Erläutern Sie beiden Typen von Verfahren an jeweils einem selbstgewählten Beispiel und gehe auf je ein Vor- und Nachteil ein. (6 BE)

b) Erkläre wann vor allem hybride Verschlüsselungsverfahren zum Einsatz kommen. (3 BE)

3. Aufgabe (11 Punkte)

a) Das RSA -Verfahren spielt in der Kryptografie eine bedeutende Rolle. Nutzen Sie die Parameter in der rechten Box und geben Sie einen öffentlichen und privaten Schlüssel nach dem RSA Verfahren an. (5 BE)

$$p = 11,\ \ q = 13,\ \ e = 7$$
$$721 = 1\ mod\ (\varphi(n))$$

b) Verschlüsseln Sie die Zahl 8 mit dem öffentlichen Schlüssel aus Teilaufgabe a).

c) Nehmen Sie Stellung zu folgender Aussage: „Der Parameter e ist prinzipiell frei wählbar. Wichtig ist nur, dass er stets kleiner als $\varphi(n)$ 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)	Definition Personenbezogene Daten, DSGVO, Recht auf Vergessen	3	0	0
1.b)	Schutz personenbezogener Daten	0	3	0
2.a)	Erläutern Verschlüsselungsverfahren	2	4	0
2.b)	Erklären Grundprinzip der hybriden Verschlüsselung	0	3	0
3.a)	Berechnung, Anwendung	0	5	0
3.b)	Zahl verschlüsseln	1	0	1
3.c)	Stellung nehmen zur Aussage	0	0	3
	Summe BE	6	15	4
		24 %	60 %	16 %
	Gesamt	25		

4. Musterlösung mit Angabe der Zuordnung der einzelnen BE:

Datenschutz und Kryptografie

1. Aufgabe (5 BE)

a) Beim Datenschutz geht es um den Schutz von sogenannten personenbezogenen Daten. Stellen Sie kurz dar, was personenbezogene Daten sind und in welcher Rechtsvorschrift deren Nutzung geregelt ist. Beschreiben Sie was in diesem Zusammenhang das „Recht auf Vergessen werden“ bedeutet? (3 BE)

Abbildung 1 © GDD

- *Personenbezogene Daten sind Daten, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen **(1 BE)***
- *die Verwendung solcher Daten ist in der DSGVO europaweit geregelt **(1 BE)***
- *eine betroffene Person das Recht hat, das Löschen aller sie betreffenden Daten zu fordern, wenn die Gründe für die Datenspeicherung entfallen **(1 BE)***

b) Erläutern Sie anhand der Karikatur warum personenbezogenen Daten geschützt werden sollten. **(3 BE)**

- *Personenbezogene Daten ermöglichen die Identifikation von Personen **(1 BE)***
- *Personen sind vor Datenmissbrauch zu schützen **(1 BE)***
- *die Karikatur zeigt auf ironische Weise, wie Daten bei einem Einstellungsgespräch missbraucht werden **(1 BE)***

2. Aufgabe (9 BE)

Verschlüsselungsverfahren lassen sich in symmetrische und asymmetrische Verfahren unterteilen.

a) Erläutern Sie beiden Typen von Verfahren an jeweils einem selbstgewählten Beispiel und gehe auf je ein Vor- und Nachteil ein. (6 BE)

Symmetrische Verfahren:
- *Codierung und Decodierung mit demselben Schlüssel*
- *Beispiele: Cäsar-Chiffre, Vigenere Verschlüsselung, Prinzip der Enigma **(1 BE)***
- *Vorteil: nur ein Schlüssel und sehr einfach in der Anwendung **(1 BE)***
- *Nachteil: alle nutzen den gleichen Schlüssel → Sicherheitsproblem **(1 BE)***

Asymmetrische Verfahre:
- *Codierung mit öffentlichem Schlüssel, Decodierung mit privatem Schlüssel*
- *Beispiel: RSA Verfahren **(1 BE)***

- *Vorteil: Notwendigkeit der Schlüsselverteilung entfällt **(1 BE)***
- *Nachteil: oftmals komplizierter und zeitintensiver in der Anwendung **(1 BE)***

b) Erklären Sie das Grundprinzip hybrider Verschlüsselungsverfahren und warum sie zum Einsatz kommen. (3 BE)
- *Große Datenmengen werden symmetrisch verschlüsselt. Anschließend wird der verwendete Schlüssel mit einem asymmetrischen Verfahren verschlüsselt **(1 BE)***
- *Die symmetrisch verschlüsselten Daten werden zusammen mit dem asymmetrisch verschlüsselten Schlüssel übertragen **(1 BE)***
- *Die Kombination von symmetrischen und asymmetrischen Verfahren bringt den Vorteil, dass Effizienz und sicherer Schlüsselaustausch kombiniert werden **(1 BE)***

3. Aufgabe (11 Punkte)

a) Das RSA -Verfahren spielt in der Kryptografie eine bedeutende Rolle. Nutzen Sie die Parameter rechts in der Box und geben Sie einen öffentlichen und privaten Schlüssel nach dem RSA Verfahren an. (5 BE)

$p = 11,\ q = 13,\ e = 7$
$721 = 1\ mod\ (\varphi(n))$

Berechnung von n	$n = p * q$	$n = 11 * 13 = 143$
Berechnung von $\varphi(n)$	$\varphi(n) = (p-1) * (q-1)$	$\varphi(143) = (11-1) * (13-1)$ $= 10 * 12$ $= \mathbf{120}$
Berechnung von d	$d * e = 1\ mod\ (\varphi(n))$	$d * 7 = 721$ $\rightarrow d = 721:7 = \mathbf{103}$
öffentlicher Schlüssel	(n, e)	$(120, 7)$
privater Schlüssel	(p, q, d)	$(11, 13, 103)$

Für jede Zeile 1 BE

b) Verschlüsseln Sie die Zahl 8 mit dem öffentlichen Schlüssel aus Teilaufgabe a)

*Für Ansatz und Ergebnis **je 1 BE**:*

Ansatz und Ergebnis:
$8^7 = \mathbf{2097152} \equiv 32\ mod\ (120)$

Rechnung:
$\frac{2097152}{120} \approx 17476{,}266$
$17476 * 120 = 2097120$
$2097152 - 2097120 = 32$

c) Nehmen Sie Stellung zu folgender Aussage: „Der Parameter e ist prinzipiell frei wählbar. Wichtig ist nur, dass er stets kleiner als $\varphi(n)$ ist.“ (3 BE)

- *Aussage ist falsch **(1 BE**), weil*
    - *ggT(e, $\varphi(n)$) = 1 (**1 BE**) → e ist nicht frei wählbar, $\varphi(n)$ darf kein Vielfaches von e sein (alle gerade Zahlen, sind nicht erlaubt)*
    - *e darf nicht kleiner oder gleich 1 sein: 1 < e < $\varphi(n)$ **(1 BE)***

5. Hinweise zur Umsetzung (benötigte Arbeitsmittel, ggf. Software auf dem Prüfungsrechner, …):

Bei der Auswahl dieser Aufgabe ist zu beachten:

- Der/die SchülerIn benötigt einen Taschenrechner
- Für die Präsentation der Lösung sollte eine Folie für den OHP bereitgelegt werden

5. Anhang: Abbildungen:

6. Quellenangabe, Abbildungsnachweise, …:

Quelle: https://www.gdd.de/downloads/materialien/cartoons

7. Erklärung der Freigabe zur Nachnutzung der Aufgabe:

Hiermit erkläre ich Stephan Wedekind 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)