Prüfungsaufgaben Kryptographie

mündliche Abiturprüfung - Grundkurs Informatik

Kryptographie taucht im Grundkurs vor allem im LB 4 auf. Zudem gibt es im LB 3 noch einen kleinen Teil zu Identifizierung und Authentifizierung.

Übertragen der Kenntnisse zur Sicherheit von Informationen auf die Umsetzung in Rechnernetzen	⇒ Medienbildung ➔ LB 4
- Transportwegverschlüsselung	TLS, VPN
- Identifizierung und Authentifizierung	Zwei-Faktor-Authentifizierung, Authentifizierung mit biometrischen Merkmalen

Lernbereich 4: Informationssicherheit	**10 Ustd.**
Kennen von Anforderungen an die Informationssicherheit	Datensicherheit, Datensicherung, Datenschutz
- Vertraulichkeit	
- Integrität	
- Authentizität	
- Verfügbarkeit	
Kennen der Grundprinzipien kryptographischer Verfahren zur Gewährleistung der Vertraulichkeit von Informationen	Schlüsselpaar, Einweg- und Falltürfunktion ➔ LB 3
- symmetrisch	
- asymmetrisch	
- hybrid	
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	Kontext persönlicher Datensicherung cloudbasierte Speicher
Datensicherung	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

mündliche Abiturprüfung
Grundkurs Informatik

Prüfer (Autor der Aufgaben):	Valentin Heckmann
Vorbereitungszeit:	20 min
Prüfungszeit:	30 min (inkl. 15 min Vorstellung der vorbereiteten Inhalte)

Thema: Kryptographie

Aufgabe 1: Verschlüsselungsverfahren

a) Beschreiben Sie die Funktionsweise von Symmetrischen Verschlüsselungsverfahren.
(2 BE)

b) Beschreiben Sie die Funktionsweise von Asymmetrischen Verschlüsselungsverfahren.
(2 BE)

c) Nennen Sie je einen Vor- und einen Nachteil von symmetrischen und asymmetrischen Verschlüsselungsverfahren, welche die beiden Verfahren voneinander abgrenzen.
(2 BE)

d) Bei Messenger-Anwendungen werden meist hybride Verschlüsselungen verwendet.
Beschreiben Sie den Ablauf einer hybriden Verschlüsselung bei einem Messenger.
Begründen Sie, warum bei Messengern gerade hybride Verschlüsselungen gut geeignet sind.
(10 BE)

Aufgabe 2: Das Kerckhoffs-Prinzip

Das Kerckhoffs-Prinzip besagt, dass die Sicherheit von kryptographischen Verfahren nur von der Geheimhaltung des Schlüssels abhängen darf, nicht aber von der Geheimhaltung des Verfahrens selber.
Nehmen Sie begründet Stellung zu diesem Prinzip.
(4 BE)

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

Aufgabe Nr.	Sachverhalt	AFB 1	AFB 2	AFB 3
1 a	Beschreiben symmetrischer Verschlüsselungsverfahren	2		
1 b	Beschreiben asymmetrischer Verschlüsselungsverfahren	2		
1 c	Vorteile von symmetrischen und asymmetrischen Verschlüsselungsverfahren.	2		
1 d	hybride Verschlüsselungen bei Messengern		10	
2	Stellung nehmen zu Kerckhoffs Prinzip			4
	Summe BE je AFB	6	10	4
	Summe BE gesamt		**20**	

Musterlösung

Aufgabe 1: Verschlüsselungsverfahren

a) Beschreiben Sie die Funktionsweise von Symmetrischen Verschlüsselungsverfahren. (2 BE)

Symmetrische Verschlüsselungsverfahren verwenden denselben Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln der Daten. (1 BE)

Der Sender verwendet den Schlüssel, um die Nachricht in eine unleserliche Form zu verschlüsseln, und der Empfänger verwendet denselben Schlüssel, um die Nachricht wieder in ihre ursprüngliche Form zu entschlüsseln. (1BE)

b) Beschreiben Sie die Funktionsweise von Asymmetrischen Verschlüsselungsverfahren. (2 BE)

Asymmetrische Verschlüsselungsverfahren verwenden zwei verschiedene, aber mathematisch miteinander verbundene Schlüssel: einen öffentlichen Schlüssel zum Verschlüsseln der Daten und einen privaten Schlüssel zum Entschlüsseln der Daten. (1 BE)
Der öffentliche Schlüssel kann frei verteilt werden, während der private Schlüssel geheim gehalten wird. Nur der private Schlüssel kann die mit dem öffentlichen Schlüssel verschlüsselten Daten entschlüsseln. (1 BE)

c) Nennen Sie je einen Vor- und einen Nachteil von symmetrischen und asymmetrischen Verschlüsselungsverfahren, welche die beiden Verfahren voneinander abgrenzen. (2 BE)

	Symmetrische Verschlüsselung	**Asymmetrische Verschlüsselung**
Vorteil	schnell	keine Probleme mit dem Austausch von Schlüsseln, da der public key öffentlich bekannt sein kann
Nachteil	der Schlüssel muss erst sicher ausgetauscht werden	rechenintensiver und langsamer

d) Bei Messenger-Anwendungen werden meist hybride Verschlüsselungen verwendet. Beschreiben Sie den Ablauf einer hybriden Verschlüsselung bei einem Messenger. Begründen Sie, warum bei Messengern gerade hybride Verschlüsselungen gut geeignet sind.

Beschreibung des Ablaufes:
Person 1 möchte einen Chat mit Person 2 anfangen

Person 1 erstellt Schlüssel für hybride Verschlüsselung für den Chat
1 BE

Person 1 verschlüsselt den erstellten Schlüssel mit dem public Key von Person 2 (asymmetrisch)
1 BE

Person 1 verschickt die (symmetrisch) verschlüsselte Nachricht und den (asymmetrisch) verschlüsselten Schlüssel an Person 2
1 BE

Person 2 entschlüsselt den asymmetrisch verschlüsselten Schlüssel für das symmetrische Verfahren mit ihrem private Key (asymmetrisch)
1 BE

Person 2 entschlüsselt die Nachricht mit dem jetzt entschlüsselten Schlüssel (symmetrisch)
1 BE

Person 2 kann ab jetzt Antworten an Person 1 mit dem symmetrischen Schlüssel verschlüsseln (ab jetzt nur noch symmetrisch)
1 BE

Begründung:
Für die eigentlichen Chatnachrichten sind symmetrische Verschlüsselungsverfahren am besten geeignet (1 BE), da diese schnell ablaufen (1 BE).
Für die Erstellung der Verbindung ist allerdings ein asymmetrisches Verschlüsselungsverfahren nötig (1 BE), da somit die beiden Personen nicht am selben Ort sein müssen, um den symmetrischen Schlüssel festzulegen (1 BE).

Aufgabe 2: Das Kerckhoffs-Prinzip

Das Kerckhoffs-Prinzip besagt, dass die Sicherheit von kryptographischen Verfahren nur von der Geheimhaltung des Schlüssels abhängen darf, nicht aber von der Geheimhaltung des Verfahrens selber.

Nehmen Sie begründet Stellung, ob dieses Prinzip in der heutigen Zeit sinnvoll ist. (4 BE)

Ja, das Kerckhoffs-Prinzip ist sinnvoll (1BE)

Mögliche Begründungen:
- Praktikabilität (in der Praxis oft unmöglich, das Verfahren geheim zu halten)
- Transparenz und Überprüfbarkeit (Vertrauen schaffen)
- erhöhte Sicherheit (oft überprüfte Verfahren sind tendenziell sicherer
- Kompatibilität zwischen Systemen durch offene Standards
- Wiederbenutzbarkeit (nur neue Schlüssel benötigt)
- Sicherheitsnachweise (Vergleichbarkeit nur bei bekannten Systemen möglich)

(3 BE für sinnvolle Begründungen)

Hinweise zur Umsetzung

Es wird kein besonderes Material benötigt. Die Schüler*innen sollten in der Vorbereitungszeit lediglich Schmierpapier zur Verfügung gestellt bekommen.

Erklärung der Freigabe zur Nachnutzung der Aufgabe:

Hiermit erkläre ich, Valentin Heckmann, 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)