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**	