Mündliche Abiturprüfung / Mündliche Abschlussprüfung

Berufliches Gymnasium - Fach Informatik - Grundkurs / Klasse 12/13

Prüfender Fachlehrer (Autor der Aufgabe): David Jordan

Vorbereitungszeit: 20 min, Prüfungszeit 30 min

Kryptologie

1. Einordnung der Aufgabe in den Lehrplan, Taxonomie:

Der Wahlbereich der Kryptologie befindet sich im Lehrplan Informatik für berufsbildende Schulen, aus dem Jahr 2007, der 2009 in Kraft getreten ist. Informatik wird auf der Basis von 2 Wochenstunden im Grundkurs unterrichtet. Für jeden Wahlbereich stehen 4 Unterrichtsstunden zur Verfügung.

Übersicht über die Lernbereiche und Zeitrichtwerte

		Zeitrichtwerte
Klassenstufe 11		
Lernbereich 1:	Persönliches Informationsmanagement	36 Ustd.
Lernbereich 2:	Projekt zur Anwendung des Informationsmanagements	16 Ustd.
Lernbereiche mit Wahlpflichtcharakter		4 Ustd.
Wahlpflicht 1:	Wissensmanagementsysteme	
Wahlpflicht 2:	Multimedia	
Wahlpflicht 3:	Sicherungsverfahren für Informationen	
Jahrgangsstufen 12/13		
Lernbereich 1:	Informatische Modellierung fachrichtungsspezifischer Strukturen und Prozesse	26 Ustd.
Lernbereich 2:	Implementierung fachrichtungsspezifischer Modelle	26 Ustd.
Lernbereich 3:	Informatik als Wissenschaft	4 Ustd.
Lernbereich 4A:	Theoretische Informatik – Formale Sprachen und Automaten	22 Ustd.
Lernbereich 4B:	Technische Informatik – Simulation und Steuerung von Prozessen	22 Ustd.
Lernbereich 4C:	Praktische Informatik - Anwendungsentwicklung	22 Ustd.
Lernbereich 4D:	Angewandte Informatik – Nutzung von Branchensoftware	22 Ustd.
Lernbereich 5:	Informatikprojekt	18 Ustd.
Lernbereiche mit Wahlpflichtcharakter		4 Ustd.
Wahlpflicht 1:	Datenbankabfragen mit SQL	
Wahlpflicht 2:	Formale Sprache für Relationenalgebra	
Wahlpflicht 3:	Makros	
Wahlpflicht 4:	Datenaustausch zwischen Anwendungssoftware	
Wahlpflicht 5:	Kryptologie	

Abbildung 1: Lehrplan INF, Berufliches Gymnasium Sachsen (2007, S.16)

<Vorname> <Name>,
Didaktik der Informatik, Universität Leipzig

Mündliche Abiturprüfung / Mündliche Abschlussprüfung

Berufliches Gymnasium - Fach Informatik - Grundkurs / Klasse 12/13

Prüfender Fachlehrer (Autor der Aufgabe): David Jordan

Vorbereitungszeit: 20 min, Prüfungszeit 30 min

Kryptologie

Ziel im Wahlbereich Kryptologie ist es, dass die Schüler die zugrunde liegende Werteorientierung kennen und mindestens ein ausgewähltes Verschlüsselungsverfahren kennen und in seinen Grundzügen anwenden können.

Wahlpflicht 5: Kryptologie	**4 Ustd.**
Einblick gewinnen in Grundbedrohungen und Sicherheitsmechanismen - Verlust der Verfügbarkeit, Integrität und Vertraulichkeit als Grundbedrohungen - Authentifikation, Zugriffskontrolle, Vertraulichkeit, Datenintegrität, Sende- und Kommunikationsnachweis	⇒ Werteorientierung
Kennen eines ausgewählten Kryptologieverfahrens	Skytale von Sparta, Caesar- oder Vigenére-Chiffre, Pretty Good Privacy (PGP)

Abbildung 2: Lehrplan INF, Berufliches Gymnasium Sachsen (2007, S.24)

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

Kryptologie

Aufgabe 1:
Im Kloster Marienbrunnen in Sachsen herrscht eine strenge Schweigepflicht. Elektronische Kommunikationsmedien sind seit jeher verboten. Die beiden Ordensbrüder Thomas und Philipp haben jedoch ein brisantes Thema zu diskutieren, bei dem es um die Zukunft des Klosters geht. Aus Angst, dass ihre schriftliche Kommunikation abgefangen werden könnte, leihen sie sich in der Bibliothek ein Buch über Kryptologie aus.

a) Nennen Sie die beiden Teilgebiete der Kryptologie und beschreiben Sie kurz deren Aufgabengebiet.

b) Ihre erste Nachricht tauschen die Ordensbrüder, über mit Zitronensaft beschriebene Servietten aus. Nach dem Erhitzen steht auf der Serviette von Thomas:
whvw 3 (a b c d e f g h i j k l m n o p q r s t u v w x y z)
Dechiffrieren Sie zuerst die Nachricht. Nennen und charakterisieren Sie im Anschluss das eingesetzte Verfahren.

c) Einen Teil des Prozesses aus 1b) haben Thomas und Philipp thematisch sicher nicht dem Kryptologiebuch entnommen. Begründen Sie diese Aussage.

d) Um ihre Kommunikation sicherer zu machen chiffrieren die beiden ihre Nachrichten nun doppelt. Diskutieren Sie die Sinnhaftigkeit dieser Maßnahme.

Aufgabe 2:
Mittlerweile kennen und nutzen die beiden das sicherere Vigenere-Verfahren.

a) Entschlüsseln Sie, mit dem beiliegenden Vigenere-Quadrat, die untenstehende Nachricht und stellen Sie dar, warum das Verfahren sicherer ist, als das in Aufgabe 1.

Geheimtext:	w t l q a m
Schlüssel:	h i
Klartext:	_ _ _ _ _ _

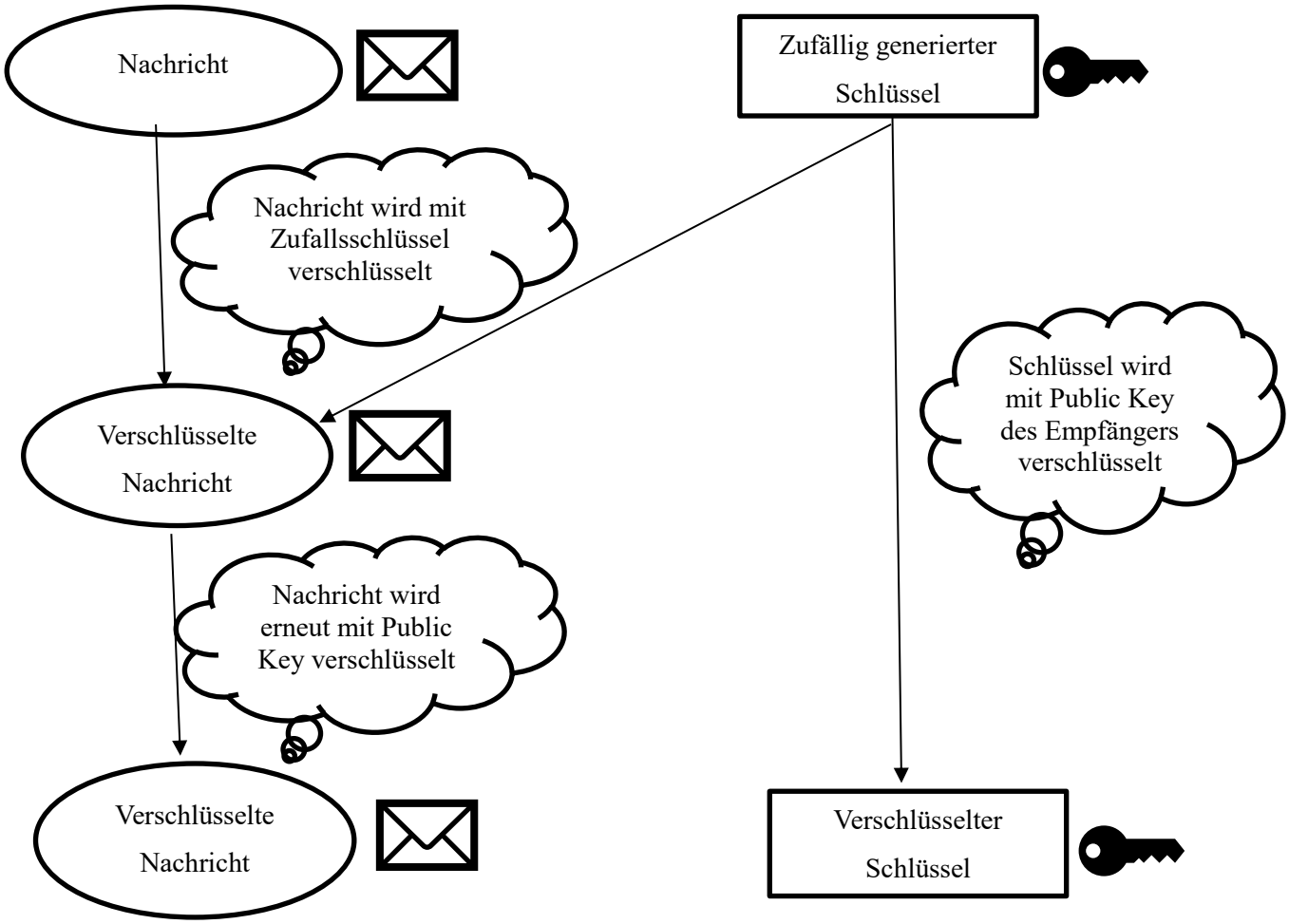
b) Nennen Sie eine Möglichkeit, um die Verschlüsselung in 2a) zu optimieren und begründen Sie ihre Antwort.

c) Ein Drittes Ordensmitglied hat durch Zufall die Schlüssellänge herausgefunden und ist sich nun sicher, die Verschlüsselung knacken zu können. Positionieren Sie sich zu dieser Annahme.

Aufgabe 3:
Mittlerweile finden solch klassische Verschlüsselungsverfahren, wie sie die Mönche in Aufgabe 1 und 2 benutzt haben, kaum noch Anwendung, da sich ihre Sicherheit meist auf den dahinter liegenden Algorithmus beschränkt.

a) Nennen Sie den Namen des Prinzips, welches diese Veränderung maßgeblich einläutete und erklären Sie kurz dessen Inhalt.

b) Ein klassisches modernes Hybrid-Verfahren ist das PGP Verfahren, wie es hier nicht ganz korrekt skizziert ist. Zeigen Sie die Stelle, an der das Schema nicht stimmt und stellen Sie knapp den korrekten Ablauf dar.



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

Aufgabe Nr.	Sachverhalt	AB1	AB2	AB3
1a)	Teilgebiete der Kryptologie	3		
1b)	Caesar Chiffre anwenden + charakterisieren		4	
1c)	Abgrenzung Steganographie			1
1d)	Doppelte Chiffrierung			3
2a)	Vigenere anwenden		4	
2b)	Verbesserung Vigenere Verfahren		3	
2c)	Vigenere knacken		3	
3a)	Kerckhoffs Prinzip	3		
3b)	PGP korrigieren		3	
	Summe BE	6 (22%)	17 (63%)	4 (15%)
	Gesamt	27		

4. Musterlösung mit Angabe der Zuordnung der einzelnen BE:

Kryptologie – Musterlösung

1 a) *Erklärung Teilgebiete:* Kryptografie und Kryptoanalyse (1BE)
Verschlüsseln von Nachrichten (1BE) / Brechen von Verschlüsselungen bzw. Schlüsseln (1BE)

1 b) *Dechiffrierte Nachricht*: Test (1BE).
Name: Caesar Chiffre (1BE)
Charakterisierung: Monoaphabetisches Verfahren (1BE), jeder Buchstabe wird mit EINEM FESTEN Buchstaben ersetzt. (1BE)

1 c) Zitronensaft ist keine Verschlüsselung, sondern wäre eine Form von Steganographie. Thematisch hat dieses Verfahren nichts mit Kryptografie zu tun. (1BE)

1 d) *Diskussion Sinnhaftigkeit*: Sinnhaftigkeit fraglich (1BE), da doppelte Verschlüsselungen wie einfache Verschlüsselung, mit den beiden addierten Verschiebungen, wirkt. Beispiel: 1x4 und 1x7 → 1x11 (1BE). Außerdem mögliche Spezialfälle wie 16 und 10 → Verschlüsselung in den eigenen Klartext. (1BE)

2 a) *Dechiffrierte Nachricht*: pleite (2BE)
Begründung Sicherheit: Verfahren ist sicherer, da polyalphabetische Verschlüsselung (1BE). Gleiche Buchstaben werden in unterschiedliche Buchstaben verschlüsselt, abhängig vom Schlüsselwort. (1BE).

2 b) *Vorschlag um Verfahren sicherer zu machen*: Längeren Schlüssel benutzen (1BE), bewirkt geringere Wiederholungen (1BE) und ist somit schwerer zu knacken. (1BE)
Mögliche weitere Denkansätze: Vielleicht sogar gleich langen Schlüssel (One-Time-Pad)? Problem des Austausches des Schlüssels.

2 c) *Knackbarkeit Vigenere*: Ja das ist möglich (1BE). Zusammenfassen der Buchstaben mit gleicher Chiffrierung durch gleichen Buchstaben (1, 1+l, 1+2l, 1+3l….wobei l =Schlüssellänge).(1BE) Danach Häufigkeitsanalyse. (1BE). Nennt sich Kasiski Test.

3a) Kerckhoffs Prinzip (1BE). Verfahrenssicherheit muss sich auf Schlüssel begründen (1BE) und nicht auf den zugrunde liegenden Algorithmus. (1BE)

3b) *Korrektur Grafik PGP:* Nachricht wird nicht mit Public Key verschlüsselt (1BE), nur der zufällige Schlüssel. (1BE) Viel zu zeitintensiv in der Praxis, außerdem wäre es dann kein Hybrid-Verfahren mehr. (1BE) Hybrid beschreibt eben die Mischung aus synchronen und asynchronen Verfahren.

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

Aufgabe 2 ist mit dem beigefügte Vigenere-Quadrat (extra Blatt) zu lösen.

		Text																								
		A	B	C	D	**E**	F	**G**	**H**	**I**	J	K	L	**M**	**N**	O	P	Q	R	**S**	T	U	V	W	X	Y	Z
Schlüssel	**A**	A	B	C	D	E	F	**G**	H	**I**	J	K	L	M	N	O	P	Q	R	**S**	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	**L**	M	N	O	P	Q	**R**	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	**O**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	**C**	D	E	F	**G**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Geheimtext

Abbildung 3: Vigenere-Quadrat

6. Quellenangabe und Abbildungsnachweise:

Birrer, A. (2017). *Die Caesar-Verschüsselung.* Zugriff am 18.6.2018. Verfügbar unter https://www.swisseduc.ch/informatik/daten/kryptologie_geschichte/caesar.html

Birrer, A. (2017). *Die Vigenère-Verschüsselung*. Zugriff am 18.6.2018. Verfügbar unter https://www.swisseduc.ch/informatik/daten/kryptologie_geschichte/vigenere.html

Pretty Good Privacy (31.3.2018). Zugriff am 18.6.2018. Verfügbar unter https://de.wikipedia.org/wiki/Pretty_Good_Privacy

Sächsischen Staatsinstitut für Bildung und Schulentwicklung (2007). *Lehrplan Berufliches Gymnasium – Informatik* (Sächsisches Staatsministerium für Kultus, Hrsg.). Zugriff am 18.6.2018. Verfügbar unter https://www.schule.sachsen.de/lpdb/web/downloads/lp_bgy_informatik_2007.pdf?v2

Verschlüsselung (18.6.2018). Zugriff am 18.6.2018. Verfügbar unter https://de.wikipedia.org/wiki/Verschl%C3%BCsselung

Vigenère-Chiffre (14.6.2018). Zugriff am 18.6.2018. Verfügbar unter https://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre

7. Erklärung der Freigabe zur Nachnutzung der Aufgabe:

Hiermit erkläre ich David , Jordan 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)