

Mündliche Abiturprüfung Informatik (Sachsen) - Thema: Informationssicherheit

Aufgabe 1: Kryptografische Verfahren

- **1a) Nennen** Sie eine Definition für die folgenden Verschlüsselungsverfahren: symmetrische Verschlüsselung und asymmetrische Verschlüsselung. **[2 BE]**
- **1b) Vergleichen** Sie symmetrische und asymmetrische Verfahren hinsichtlich ihrer Stärken und Schwächen im Kontext zu deren Anwendungsbereich. Nennen sie je 2 Stärken und Schwächen für die Verschlüsselungsverfahren **[5 BE]**
- **1c) Erläutern** Sie das Vigenère-Verschlüsselungsverfahren anhand der Verschlüsselung der folgenden Wortgruppe "WorldHello" mit dem Schlüsselwort "badec". Gehen Sie dabei auf die Funktionsweise und die mathematischen Grundlagen ein. **[8 BE]**

Vignère-Tabelle zur Bearbeitung der Aufgabe 1c)

Klartext

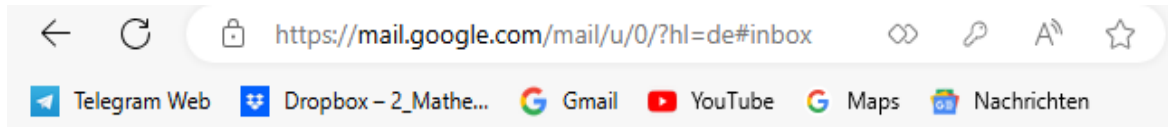
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Verschlüsselungstext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	F	G	H	I	J	K	L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

- **1d) Beurteilen** Sie die Aktualität des Vigenère-Verschlüsselungsverfahrens im Kontext moderner Datensicherheit und ob es heutzutage noch relevant ist. **[3 B]**

Aufgabe 2: Daten- und Informationssicherheit

- **2a) Beschreiben** sie 2 Vorgehensweisen der Backup-Erstellung zur Sicherung von Daten **[2 BE]**
- **2b)** Sie nutzen Ihren Webbrowser, um Ihre E-Mails abzurufen. In der Adressleiste des Browsers sehen Sie ein Schloss-Symbol und **https://** am Anfang der Webadresse. **Erläutern** Sie, welches Protokoll hier verwendet wird und inwiefern, es zur Gewährleistung der Informationssicherheit Ihrer E-Mails beiträgt, beziehen sie sich dabei auf die Informationssicherheitsanforderungen. **[8 BE]**

Angabe: Bild einer Browserleiste



Aufgabe 3: Datenschutz und Datensicherheit im gesellschaftlichen Kontext

Wählen sie eine der untenstehenden Aufgaben zur Bearbeitung aus!

- **3a) Positionieren** Sie sich zur folgenden Aussage: „Im digitalen Zeitalter sind die Grundprinzipien des Datenschutzes überholt und behindern den technologischen Fortschritt.“ **[4 BE]**
- **3b) Diskutieren** Sie die gesellschaftlichen Auswirkungen von Datenschutz-verletzungen und erörtern Sie Maßnahmen zur Stärkung der Datensicherheit. **[4 BE]**

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

Aufgabe Nr.	Sachverhalt	AB1	AB2	AB3
1a		2	0	0
1b		0	4	1
1c		4	4	0
1d		0	2	1
2a		2	0	0
2b		2	6	0
3a		0	0	4
3b		0	0	4
	Summe BE Gesamt	10	16 32	6

Not e	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
BE	32	30	28	27	25	24	22	20	19	17	16	14	10	6	2	1=>