2. Aufgabenstellung:

Verfahren zur Gewährleistung von Vertraulichkeit

Vorwort:

Der Wunsch nach Geheimhaltung von Nachrichten ist mittlerweile so alt wie die Menschheit selbst. Damals wie heute verfolgte man das Ziel Nachrichten sicher zu verschlüsseln, damit sensible Informationen nicht von unberechtigten Personen eingesehen werden können. Nutzen Sie die bereitgestellten Folien und Materialien, um die von Ihnen ausgearbeiteten Inhalte geeignet zu präsentieren.

Aufgaben:

1) Überblick:
   a) (6 BE) Vervollständigen Sie das Schema zur Geheimhaltung von Nachrichten. (*Hinweis: Vervollständigen Sie das Schema auf Extrafolie 1.*)
   b) (10 BE) Beschreiben Sie, an welcher Stelle Sie **fünf** der folgenden sechs Chiffren und Verfahren in das Schema einordnen würden. Geben Sie jeweils eine kurze Begründung ihrer Entscheidung an.

   Brute-Force-Angriff | Digital Watermarking | Skytale | Fleißnersche Schablone | Semagramm | Caesar-Chiffre

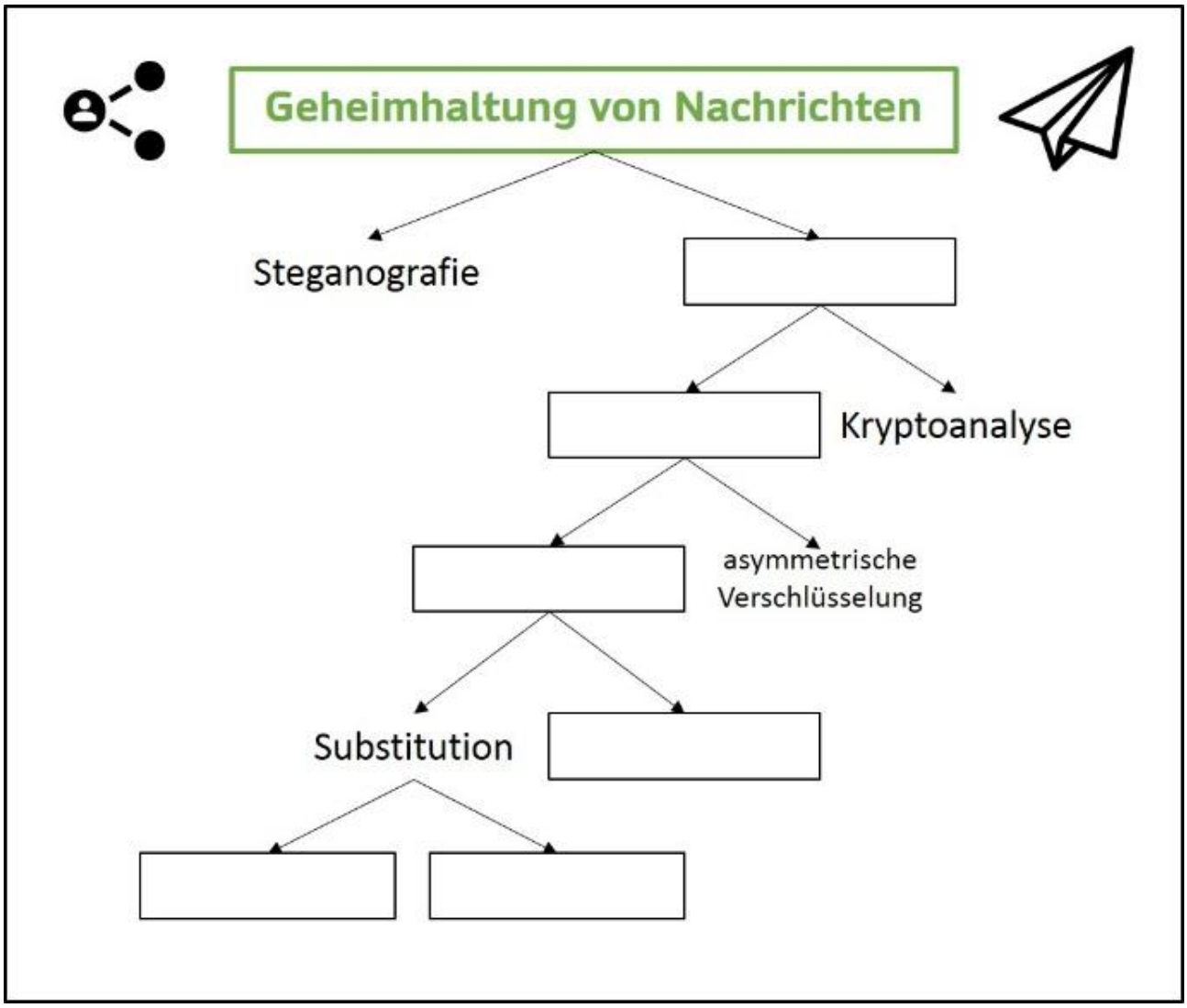
2) Die Gronsfeld-Chiffre verschlüsselt Texte mithilfe eines endlichen Schlüssels in Form einer natürlichen Zahl. Man schreibt die Ziffern des Schlüssels nacheinander über die einzelnen Buchstaben des Geheimtextes, solange bis man jeden Buchstaben markiert hat. Ist die Nachricht länger als der Schlüssel, beginnt man wieder mit der ersten Ziffer des Schlüssels. Ein Buchstabe im Geheimtext wird dann um die markierte Ziffer nach hinten im Alphabet verschoben, wodurch man den zugehörigen chiffrierten Buchstaben erhält.
   a) (3 BE) Chiffrieren Sie das Wort: „LUFTBALLON“ mit der Gronsfeld-Chiffre. Nutzen Sie den Schlüssel 1719 und das Alphabet $\Sigma = \{A; B; C; \ldots; Z\}$. (*Hinweis: Vervollständigen Sie dazu die Tabelle auf Extrafolie 2.)*
   b) (2 BE) Die Häufigkeitsanalyse ist ein altbewährtes Verfahren aus dem Bereich der Kryptoanalyse. Analysieren Sie die Tauglichkeit dieses Verfahrens zur Entschlüsselung der Gronsfeld-Chiffre.
   c) (6 BE) Beurteilen Sie die Sicherheit der Gronsfeld-Chiffre. Beziehen Sie die Caesar-Chiffre und die Vigenére-Chiffre in Ihre Argumentation mit ein.

3) Diffie-Hellman Schlüsselaustausch:
   a) (2 BE) Beschreiben Sie den Nutzen des Diffie-Hellman Schlüsselaustauschs.
   b) (7 BE) Stellen Sie den Ablauf beim Diffie-Hellman Schlüsselaustausch mithilfe von Farben auf einer Folie dar und erläutern Sie diese.

4) (5 BE) Seit dem Anschlag in Wien vom 02. November 2020 arbeiten die EU-Regierungen an einem Entwurf, welcher besagt, dass z. B. die Betreiber von WhatsApp zukünftig einen Generalschlüssel zur Beobachtung von fragwürdigen Chats für EU-Regierungen und Sicherheitsdienste hinterlegen müssen. Diese Maßnahme solle der Sicherheit der Bevölkerung dienen. Bewerten Sie, ob die Maßnahme im Einklang zu den Anforderungen an Informationssicherheit steht.

Extrafolie 1

Schema zu Aufgabe 1a:



Extrafolie 2

Zu Aufgabe 2a:

Schlüssel:										
Klartext:	L	U	F	T	B	A	L	L	O	N
Ergebnis:										

		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
Key	0	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	Geheimtext
	1	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	
	2	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	
	3	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	
	4	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	
	5	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	
	6	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	
	7	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	
	8	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	
	9	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	

Abbildung 1: Verschiebung des Alphabets[4]

[4] Quelle: https://www.cryptool.org/assets/img/gronsfeld.jpg

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

Aufgabe Nr.	Sachverhalt	AB1	AB2	AB3
1a	Das Schema zur Geheimhaltung von Nachrichten soll um fehlende Fachbegriffe ergänzt werden, indem die zu prüfende Person sechs Lücken füllt.	6	0	0
1b	Es sollen fünf von sechs möglichen Verfahren und Chiffren begründet in das obige Schema zugeordnet werden.	0	10	0
2a	Es soll ein gegebenes Wort anhand einer Beschreibung der Gronsfeld-Chiffre verschlüsselt werden.	3	0	0
2b	Es soll analysiert werden, ob das Verfahren der Häufigkeitsanalyse zielführend bei der Entschlüsselung der Gronsfeld-Chiffre ist.	0	2	0
2c	Es soll die Sicherheit der Gronsfeld-Chiffre beurteilt werden. Hierbei sollen die Caesar- und die Vigenére-Chiffre mit in die Argumentation einbezogen werden. *(Hinweis: 1 BE AB1 gibt es auf die bloße Aussage, dass die Gronsfeld-Chiffre nicht sicher ist.)*	1	0	5
3a	Der Nutzen des Diffie-Hellman Verfahrens soll beschrieben werden.	2	0	0
3b	Die zu prüfende Person soll den Ablauf des Diffie-Hellman Schlüsselaustauschs mit verschiedenen Farben darstellen. Mathematische Hintergründe werden dabei nicht verlangt.	0	7	0
4	Es soll bewertet werden, ob die Einführung eines Generalschlüssels (für Regierungen) zur Beobachtung von „fragwürdigen“ Nachrichten und Chats im Einklang zu den Anforderungen an Informationssicherheit steht.	0	5	0
	Summe BE	12	24	5
	Gesamt	41		

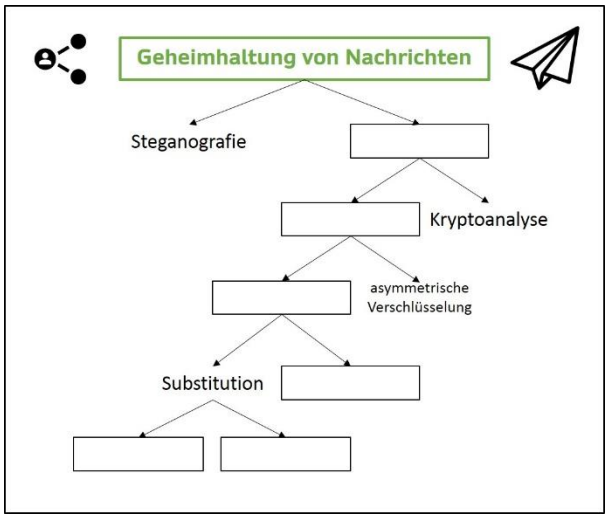
NP	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
BE	39	37	35	33	31	29	27	25	23	20	18	15	11	7	4

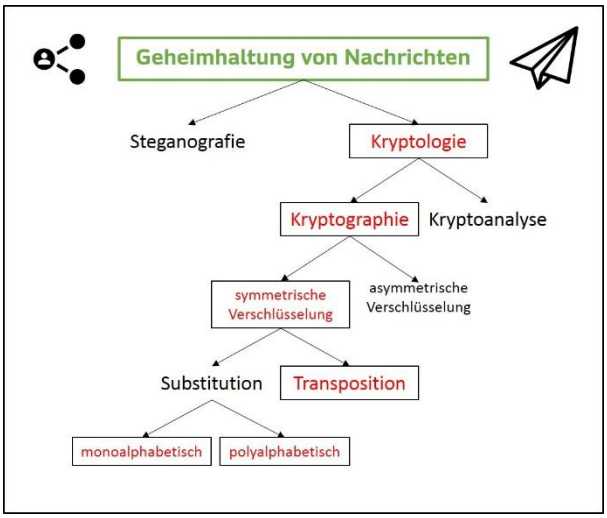
4. Musterlösung mit Angabe der Zuordnung der einzelnen BE:

Verfahren zur Gewährleistung von Vertraulichkeit: Musterlösung

1) Überblick:

a) Vervollständigen Sie das folgende Schema zur Geheimhaltung von Nachrichten.





[6 BE]

b) Beschreiben Sie, an welcher Stelle Sie **fünf** der folgenden sechs Chiffren und Verfahren in das Schema einordnen würden. Geben Sie jeweils eine kurze Begründung ihrer Entscheidung an.

Brute-Force-Angriff | Digital Watermarking | Skytale | Fleißnersche Schablone | Semagramm | Caesar-Chiffre

Verfahren / Chiffre	Zuordnung	Begründung
Brute-Force-Angriff	Kryptoanalyse	Verfahren zur Entschlüsselung von Chiffren (monoalphabetische Substitution)
Digital Watermarking	Steganografie	Verstecken von Informationen in Trägermedien (z.B. Bild, Video)
Skytale	Transposition	Form der Verschlüsselung, bei der jeder Buchstabe seine Bedeutung behält (Schlüssel wird durch die Anzahl der Windungen beschrieben)
Fleißnersche Schablone	Transposition	Form der Verschlüsselung, bei der jeder Buchstabe seine Bedeutung behält (Schlüssel in Form einer Schablone)
Semagramm	Steganografie	Verstecken einer Nachricht in einem Medium (z. B. Nutzung verschiedener Schriftarten)
Caesar-Chiffre	monoalphabetische Substitution	Buchstaben bekommen anhand einer Verschiebung des Alphabets eine neue Bedeutung

[10 BE]

2)

a) Chiffrieren Sie das Wort: „LUFTBALLON“ mit der Gronsfeld-Chiffre. Nutzen Sie den Schlüssel 1719 und das Alphabet $\Sigma = \{A; B; C; \ldots; Z\}$.

Schlüssel:	1	7	1	9	1	7	1	9	1	7
Klartext:	L	U	F	T	B	A	L	L	O	N
Ergebnis:	M	B	G	C	C	H	M	U	P	U

- 1 BE auf die komplett richtige Schlüssel-Zeile
- Je 1 BE auf 5 richtig chiffrierte Buchstaben

[3 BE]

b) Die Häufigkeitsanalyse ist ein altbewährtes Verfahren aus dem Bereich der Kryptoanalyse. Analysieren Sie die Tauglichkeit dieses Verfahrens zur Entschlüsselung der Gronsfeld-Chiffre.

Die Häufigkeitsanalyse kann zur Entschlüsselung von monoalphabetischen Chiffren verwendet werden, da hierbei jeder Buchstabe des Alphabets eine eindeutigen neuen Buchstaben erhält. Wie aber aus der Beschreibung hervor geht, handelt es sich bei der Gronsfeld-Chiffre um eine **polyalphabetische Substitution**. So wird im Lösungswort z. B. u zu d und u zu b. Da jeder Buchstabe mehrere Bedeutungen hat, wäre eine **Häufigkeitsanalyse nicht zielführend**.

[2 BE]

c) Beurteilen Sie die Sicherheit der Gronsfeld-Chiffre. Beziehen Sie die Caesar-Chiffre und die Vigenére-Chiffre in Ihre Argumentation mit ein.

Im Vergleich zur Caesar-Chiffre ist die Gronsfeld-Chiffre **deutlich sicherer**, da es sich um **polyalphabetische Substitution** handelt. Somit kann einem Verschlüsselten Buchstaben kein eindeutiger Buchstabe des Geheimtextes zugeordnet werden.

Im Vergleich zur Vigenére-Chiffre ist die Gronsfeld-Chiffre **weniger sicher**. Dies hängt damit zusammen, dass der Key einer Vigenére-Chiffre, bei konstanter Schlüssellänge, **mehr Kombinationen von Zeichen** anbietet als ein Key der Gronsfeld-Chiffre. Es folgt ein Beispiel der Länge 4:

Vigenére: $26 \times 26 \times 26 \times 26$ Möglichkeiten (26 Buchstaben)

Gronsfeld: $10 \times 10 \times 10 \times 10$ Möglichkeiten (Ziffern 0 bis 9)

Da die **Vigenére Chiffre als allgemein unsicher** zählt, und die Gronsfeld-Chiffre ein Spezialfall der Vigenére Chiffre ist, ist die **Gronsfeld-Chiffre nicht sicher.**

[6 BE]

3) Diffie-Hellman Schlüsselaustausch:

a) Beschreiben Sie den Nutzen des Diffie-Hellman Schlüsselaustauschs.

Das Diffie-Hellman Verfahren dient der geheimen **Bestimmung eines gemeinsamen Schlüssels**, **ohne** den gemeinsamen Schlüssel an sich **auszutauschen** (vgl.Witt, 2014, S. 175).

[2 BE]

b) Stellen Sie den Ablauf beim Diffie-Hellman Schlüsselaustausch mithilfe von Farben auf einer Folie dar und erläutern Sie diese.

- **1 BE:** Alice und Bob besitzen einen öffentlichen und jeweils einen privaten Schlüssel.
- **1 BE:** Beide kombinieren die beiden Schlüssel zu einem Schlüsselpaar.
- **2 BE:** Beide Tauschen die „Mischung“ aus, wobei man nicht auf zugrundeliegende private Schlüssel schlussfolgern kann.
- **1 BE:** Beide kombinieren die Mischung mit dem eigenen privaten Schlüssel.
- **2 BE:** Beide erhalten den gleichen gemeinsamen Schlüssel, da jeweils beide privaten Schlüssel mit dem öffentlichen Schlüssel kombiniert wurden.

[7 BE]

4) Seit dem Anschlag in Wien vom 02. November 2020 arbeiten die EU-Regierungen an einem Entwurf, welcher besagt, dass z. B. die Betreiber von WhatsApp zukünftig einen Generalschlüssel zur Beobachtung von fragwürdigen Chats für EU-Regierungen und Sicherheitsdienste hinterlegen müssen. Diese Maßnahme solle der Sicherheit der Bevölkerung dienen. Bewerten Sie, ob diese Maßnahmen im Einklang zu den Anforderungen an Informationssicherheit stehen.

- **Vertraulichkeit:** Die Regierungen sind nicht der berechtigte Empfänger jeder Nachricht.
- **Integrität:** Da hier die Rede von „Beobachtung“ ist, sollte diese bestehen bleiben.
- **Verbindlichkeit:** Die Urheberschaft von Nachrichten wird nicht durch den Generalschlüssel beeinflusst.
- **Authentizität:** Die bloße Beobachtung hat keinen Einfluss auf die Überprüfbarkeit der Identität des Absenders einer Nachricht.

Die Maßnahme eines Generalschlüssels zur Beobachtung „fragwürdiger Chats“ **verletzt die Anforderung der Vertraulichkeit**. Somit steht Nutzung eines **Generalschlüsseln nicht im Einklang** mit den Anforderungen an Informationssicherheit.

[5 BE]