# Klausurersatzleistung GK inf3 Informatik 12/2 – Kryptologie

*Die Verwendung der eigenen Unterrichtsaufzeichnungen sowie aller Programme auf dem Rechner ist gestattet. Die Nutzung des Internets und Kommunikation zwischen den Rechner/Nutzern jedoch nicht.*

## Anwendung Caesar-Verfahren (A 🡪 D)

* 1. Ordnen Sie dem Caesar-Verfahren die zugehörigen Eigenschaftswerte *monoalphabetisch* bzw. *polyalphabetisch*, *symmetrisch* bzw. *asymmetrisch* zu. (2)
	2. Julius Caesar will den Klartext „BEREITSCHAFT?“ verschlüsselt senden.
	Bestimmen Sie den Geheimtext. (1)
	3. Geben Sie das Sicherheitsziel an, das Caesar mit seinem Verfahren verfolgte. (1)
	4. Caesar empfängt die verschlüsselte Antwort „DANCAOPAHHP“ und kann sie nicht mit seinem Originalverfahren entschlüsseln. Er vermutet, dass der Sender eine falsche „Verschiebung“ verwendet hat.
		1. Geben Sie die Anzahl der Versuche an, die er im schlimmsten Fall durchführen muss? (1)
		2. Bestimmen Sie den Klartext. Wie haben Sie ihn ermittelt? (2)
	5. Begründen Sie, dass das Caesar-Verfahren nicht dem Prinzip Kerckhoffs genügt. (1)

## Anwendung Gronsfeld-Verfahren und One-Time-Pad

Ende des 17. Jahrhundert entwickelte Feldmarschall Gronsfeld-Bronkhorst eine Variante der Vigenère-Chiffre. Er benutzte als Schlüssel eine Ziffernfolge und eine reduzierte Vigenère-Tabelle. Es zeigte sich, dass man das Verfahren analog zur Vigenère-Chiffre brechen konnte.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 |
| 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 |
| 1 | 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 |
| 2 | 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 |
| 3 | 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 |
| 4 | 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 |
| 5 | 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 |
| 6 | 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 |
| 7 | 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 |
| 8 | 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 |
| 9 | 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 |

* 1. Begründen Sie, dass es sich um ein polyalphabetisches, symmetrisches Verfahren handelt. (2)
	2. Polyalphabetische Verfahren galten 300 Jahre als sicher. Begründen Sie, dass diese nicht über die Häufigkeitsverteilung der Klartextbuchstaben gebrochen werden können. (1)
	3. Verschlüsseln Sie mit dem Schlüssel 815 den Klartext „KAISER“. (1)
	4. Ermitteln Sie aus dem Geheimtext „DDJHNGV“, der mit dem Schlüssel 815 verschlüsselt wurde, den Namen des Kaisers. (1)
	5. Ein Kryptologe will das Gronsfeld-Verfahren zu einem One-Time-Pad machen. Er setzt die Schlüssellänge gleich der Klartextlänge.
		1. Geben Sie die zwei weiteren Bedingungen an, die ein One-Time-Pad erfüllen muss. (2)
		2. Zeigen Sie, dass sich der Geheimtext „YBER“ in die Klartexte „EINS“ und „ACHT“, jedoch nicht in den Klartext „ZWEI“ überführen lässt. (3)
		3. Beurteilen Sie, ob das Verfahren bei Einhaltung der drei One-Time-Pad-Bedingungen 100% sicher ist. (2)
1. **Anwendung Asymmetrisches Verfahren ASYM**

Alice und Bob besitzen für den ASYM-Kodierer verschiedene Schlüssel. Einige liegen beim Trust Center und wurden von dort bereits an Alice und Bob übermittelt.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Alice** |  | **Bob** |
|  | **Weibliches Profil****Bob: BGF****+: APB****-: PAF** |  | **Männliches Profil****Alice: APB****+: BGF****-: FDB** |
| **A** | Alice verschlüsselt die Nachricht „EIN.UHR“ mit dem ➀ Schlüssel von ➁ zu ➂ und sendet diese an Bob. | 🡪 | Bob entschlüsselt die empfangene Nachricht mit dem ➃ Schlüssel von ➄ zu ➅. |
| **B** | Alice prüft die digitale Signatur der Nachricht „JA OU“ von Bob. | 🡨 | Bob verschlüsselt die Antwort „JA“ mit seinem privaten Schlüssel zu „OU“. Anschließend sendet er „JA OU“ an Alice. |

* 1. Geben Sie den Vorteil der asymmetrischen im Vergleich zur symmetrischen Verschlüsselung an. (1)
	2. Geben Sie den öffentlichen und den privaten Schlüssel von Alice an. (1)
	3. Geben Sie die Schlüssel an, die im Trust-Center liegen sollten. (1)
	4. Ordnen Sie für die Zeile A zu
		1. die Symbole ➀ und ➃ den Begriffen „öffentlichen“ bzw. „privaten“. (1)
		2. die Symbole ➁ und ➄ den Namen „Alice“ bzw. „Bob“. (1)
		3. die Symbole ➂ und ➅ dem ermittelten Klar- bzw. Geheimtext. (2)
	5. Erläutern Sie die Aussage: „Bob verwendet für seine Antwort in der Zeile B das Prinzip der digitalen Signatur, um die Sicherheitsziele Authentizität und Integrität zu erreichen.“ (3)
	6. Prüfen Sie für Alice in Zeile B die digitale Signatur der Nachricht „JA OU“ von Bob. (2)
	7. Wie wird sichergestellt, dass jeder Kommunikationspartner dem Trust Center vertraut? (1)