**WP Informatik – Jahrgang 9**

**Klassenarbeit zum UV 9.3 Sichere Kommunikation mit Kryptographie**

**Die ausführliche schriftliche Ausarbeitung auf dieser ersten Seite der Beispiel­arbeit dient der Veranschaulichung der Bezüge zum Kernlehrplan. Diese müssen nicht notwendigerweise schriftlich fixiert werden.**

**Kompetenzerwartungen:**

Bei der Bearbeitung der Aufgabe werden auch **übergeordnete Kompetenzerwartungen** des Kernlehrplans erfüllt, welche sich in ihrer Komplexität nicht einzelnen Aufgabenteilen zuordnen lassen.

Die Schülerinnen und Schüler

* analysieren informatische Sachverhalte,
* bewerten informatische Sachverhalte mithilfe begründeter Kriterien,
* implementieren Modelle mit geeigneten Werkzeugen,
* erläutern Modelle und deren Implementierung,
* analysieren und bewerten Informatiksysteme und Anwendungen unter dem Aspekt der zugrunde liegenden Modellierung,
* beurteilen Modelle, Implementierungen und die verwendeten Werkzeuge hinsichtlich der Eignung zur Erfassung eines Sachverhalts,
* wählen geeignete Darstellungsformen aus.

Diese Klassenarbeit nimmt Bezug auf folgende **inhaltsfeldbezogene konkretisierte Kompetenzerwartungen:**

Die Schülerinnen und Schüler

* codieren und decodieren Daten mithilfe eines vorgegebenen Verfahrens oder im Rahmen einer Anwendung (MI) [a, b, c],
* interpretieren Daten in unterschiedlichen Darstellungsformen hinsichtlich der dargestellten Information (DI) [a, b, c],
* erläutern und verwenden elementare Datentypen im Kontext einer Anwendung (A) [a, b, c],
* begründen die Auswahl einer geeigneten Darstellungsform für Daten im Kontext einer konkreten Problemstellung (A) [d],
* erläutern und verwenden grundlegende Operationen für den Zugriff auf strukturierte Daten (MI) [b],
* beurteilen die Problemangemessenheit verwendeter Algorithmen (A) [d],
* wählen geeignete Werkzeuge zur Lösung gegebener Problemstellungen aus (A) [a, b, c, d, e],
* erläutern das Recht auf informationelle Selbstbestimmung und Möglichkeiten zur Umsetzung (A) [f],
* testen die Sicherheit einfacher Verschlüsselungsverfahren (A) [c, d],

**Überprüfungsformen für Klassenarbeiten**

Im Kernlehrplan werden in Kapitel 3 „Lernerfolgsüberprüfungen und Leistungsbewertung“ mögliche Überprüfungsformen von Klassenarbeiten beschrieben. In der vorliegenden Klassen­arbeit werden folgende Überprüfungsformen eingesetzt:

* Darstellungs- und Dokumentationsaufgabe [a, e],
* Entscheidungs- und Bewertungsaufgabe [f],
* Gestaltungs- und Konstruktionsaufgabe [b],
* Analyse- und Parameteraufgabe [c],
* Optimierungsaufgabe [d].

**Hinweise zum Umgang mit diesem Material:**

Die Klassenarbeit ist für 45 Minuten konzipiert.

Es werden folgende Arbeitsmittel benötigt: kariertes Papier

Alice und Bob sind Freunde und möchten sich geheime Botschaften zuschicken.

1. Zunächst schreibt Bob an Alice „Ich möchte Dir geheime Botschaften senden“ und verwendet dazu die Methode der Skytale. Warum ist die Botschaft für andere Personen nicht leicht zu verstehen? Erläutere, wie Alice die Botschaft entschlüsseln kann.
2. Da offenbar ein Kundiger doch das Verschlüsselungsverfahren „geknackt“ hat, wechselt Alice zum Cäsar-Verfahren und Alice schreibt an Bob zurück „Wir gehen heute Abend ins Kino und sehen uns den Film ‘Zurück in die Zukunft‘ an“.
Alice und Bob haben sich darauf geeinigt, ein A mit dem ersten Buchstaben des aktuellen Wochentages zu verschlüsseln. Der Sendetag der Botschaft ist ein Freitag.
Wie lautet Alices verschlüsselter Text?
Welche Zeichen müssen als Sonderfälle in Alices Botschaft behandelt werden?
3. Mike will unbedingt herausfinden, was Bob und Alice sich mitzuteilen haben. Er hat die verschlüsselte Nachricht aus b) abgefangen. Beschreibe Mikes weiteres Vorgehen!
4. Alice und Bob sind sich immer noch nicht sicher, ob ihre geheimen Botschaften auch geheim bleiben. Beschreibe eine weitere Maßnahme, die ihre Kommunikationssicherheit erhöhen kann. Gib eine Begründung für die erhöhte Sicherheit dieser Maßnahme.
5. Zu guter Letzt entscheiden sich Alice und Bob für ein modernes asymmetrisches Verschlüsselungsverfahren, da sie gehört haben, dass das sehr sicher sein soll. Als ihr kompetenter Sicherheitsberater erläuterst Du ihnen an einem kleinen Diagramm, wie man das asymmetrische Verschlüsselungsverfahren anwendet.
6. Elke sagt: „Alice und Bob dürfen überhaupt keine verschlüsselten Nachrichten über das Internet austauschen. Das ist Heimlichtuerei. Mike hat vollkommen Recht, wenn er die verschlüsselten Nachrichten entschlüsseln will.“
Nimm begründet Stellung zu Elkes Aussage.

Erlaubte Hilfsmittel: Cäsar-Scheibe