Klassenarbeit: Sicherheit von Informationen

Diese Klassenarbeit richtet sich an die Schülerinnen und Schüler der 11./12. Klasse am Gymnasium zum Thema Sicherheit von Informationen.

Tabelle zur Beschreibung der Aufgabe

Bereiche	Information und Daten Begründen und Bewerten
Klassenstufe:	11 - 12
Schwierigkeit:	AI
Medien:	
Medien:	Einzeln
Bearbeitungsdauer:	0
Quellen:	
Author:	KPSI

Aufgabenstellung

Teilaufgabe 1

Aufgabentyp	Bestimmungsaufgabe
Punkte	3

Was ist Kryptologie?

Erwartungshorizont

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen sowei der Analyse kryptografischer Verfahren zum der Bewertung ihrer Stärken und Schwächen. (1 Punkt)

Die Kryptologie teilt sich in zwei Teilbereiche:

1. Kryptografie (Verschlüsselung von Informationen) (1 Punkt)

2. Kryptoanalyse (Analyse und Bewertung der Sicherheit von Kryptoverfahren gegen unbefugte Angriffe) (1 Punkt)

Klassenarbeit: Sicherheit von Informationen

Teilaufgabe 2

Aufgabentyp	Bestimmungsaufgabe
Punkte	6

Nennen Sie die allgemeinen Anforderungen an die Informationssicherheit **(4)** und erklären Sie **zwei** der Anforderungen kurz!

Erwartungshorizont

Vertraulichkeit: Lesen des eigentlichen Inhalts für Unbefugte "praktisch" unmöglich machen

Integrität: Eigenschaft, dass die Nachricht nicht verändert wurde

Authentizität: Die Identität des Absenders einer Nachricht muss für den Empfänger nachprüfbar sein und umgekehrt

Verbindlichkeit/Nichtabstreitbarkeit: Der Empfänger kann den Nachweis erbringen, dass der Sender die Nachricht mit identischen Inhalt abgeschickt hat. (Leugnen Zwecklos) **Punktevergabe:**

Pro Anforderung 1 Punkt

Pro Erläuterung 1 Punkt

Teilaufgabe 3

Aufgabentyp	Bestimmungsaufgabe
Punkte	8

In der Kryptoanalyse gibt es symetrische und asymetrische Verschlüsselungsverfahren!

1. Erklären Sie den Unterschied zwischen diesen beiden Verschlüsselungsverfahren!

2. Nennen Sie je **zwei** Vor- und Nachteile dieser Verfahren!

Klassenarbeit: Sicherheit von Informationen

3. Nennen Sie je **ein** Beispiel für symetrische und asymetrische Verfahren!

4. Was ist ein hybrides Verfahren?

Erwartungshorizont

Ein **asymetrisches Kryptosystem** ist ein Kryptosystem, dass im Gegensatz zu einem symetrischen Kryptosystem verschiedene Schlüssel zur Ver- und Entschlüsselung verwendet.

Vorteile: Geheimnis klein; keine Schlüsselvermittlung --> öffentlicher Schlüssel

Nachteile: langsam; öffentlicher Schlüssel echt?; nicht bewiesene Sicherheit

Beispiel: RSA

Ein **symetrisches Kryptosystem** ist ein Kryptosystem, welches im Gegensatz zu einem asymetrischen Kryptosystem den gleichen Schlüssel zur Ver- und Entschlüsselung verwendet.

Vorteile: schnell; einfach

Nachteile: Schlüsselvergabe; selber Schlüssel zur Ver- und Entschlüsselung

Beispiel: Cäsar

Punkteverteilung:

(1.) ein Punkt auf die Erklärung des Unterschiedes

(2.) je ein Punkt pro Vor- und Nachteil

(3.) je Beispiel ein Punkt

(4.) ein Punkt Erklärung

Teilaufgabe 4

Aufgabentyp	Analyseaufgabe
Punkte	3

Verschlüsseln Sie das Wort **INFORMATIK** mit der **Cäsar - Chiffre** und dem **Schlüssel 6** !

Schreiben Sie zunächst das Geheimtextalphabet unter das Klartextalphabet!

Klartextalphabet: 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

Klassenarbeit: Sicherheit von Informationen

Erwartungshorizont

Klartextalphabet: 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

Geheimtextalphabet: 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

INFORMATIK --> OTLUXSGZOQ

Punkteverteilung:

Erkennen des Schlüssels (Verwenden der MEthode) --> 1 Punkt

Verwenden des Schlüssels --> 1 Punkt

Lösungswort --> 1 Punkt

Teilaufgabe 5

Aufgabentyp	Analyseaufgabe
Punkte	3

Verschlüsseln Sie das Wort INFORMATIK mit der **Vignere - Chiffre** und dem **Schlüssel ABC!**

Erwartungshorizont

INFORMATIK --> IOHOSOAUKK

Punktevergabe

Erkennen des Schlüssels (Verwenden der Methode) --> 1 Punkt

Verwenden des Schlüssels --> 1 Punkt

Lösungswort --> 1 Punkt Bitte Beachten!

In den Anhang der Aufgabe muss unbedingt das Vignere - Quadrat da sonst die Lösung der Aufgabe sehr schwierig wird.

Teilaufgabe 6

Klassenarbeit: Sicherheit von Informationen

Aufgabentyp	Bestimmungsaufgabe
Punkte	3

Was ist Steganographie und welche Ziele **(2)** verfolgt es?

Erwartungshorizont

1. Steganographie ist das Verstecken von Botschaften! Ziele:

Prüfung des Ursprungs von Gütern und Dokumenten (durch Wasserzeichen)

Nachweis von Veränderung der Ware beziehungsweise des Dokuments

Punkteverteilung

Was ist Steganographie --> 1 Punkt

2 Ziele --> je einen Punkt

Teilaufgabe 7

Aufgabentyp	Analyseaufgabe
Punkte	10

1. **Verschlüsseln** Sie die Zahl **65** mit dem **RSA - Verfahren (p=11; q=17**)!

2. **Entschlüsseln** Sie danach den Geheimtext wieder!

Erwartungshorizont

p = 11 und q = 17 --> n = 187 //1Punkt

(p - 1) = 10 und (q - 1) = 16 //1Punkt

Klassenarbeit: Sicherheit von Informationen

besitzen die Primfaktoren 2 und 5
//2Punkte

Wahl von e: z.B. e=
7
//1Punkt

öffentlicher Schlüssel:
(7;187) //1Punkt

d=(x(p-1)(q-1)+1) / e für x = 1: d = 23
//1Punkt

geheimer Schlüssel:
(23;187) //1Punkt

Verschlüsselung: z = 657 mod 187 = 142 //1Punkt

Entschlüsselung: a = 14223 mod 187 = 65 //1Punkt