Modul 114: LB1 Teil 2

Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Name	
Vorname	
Klasse	
Prüfungsdatum	

Mögliche Punkte	40
Erreichte Punkte	
Note	

Rahmenbedingungen

- **Prüfungszeit:** 60 Minuten
- **Berechnung der Note:** (Punkte · 5 / Maximale Punktzahl) + 1

Prüfungsregeln

- Ausser einer persönlichen **zweiseitigen Zusammenfassung** dürfen keine schriftlichen Unterlagen benützt werden.
- Jegliche Arten von Prüfungen oder deren Musterlösungen sind auf der Zusammenfassung nicht erlaubt.
- Der Taschenrechner darf verwendet werden.
- Jeglicher Informationsaustausch unter den Kandidatinnen und Kandidaten ist nicht erlaubt.
- Es sind sämtliche Notizen und Zusammenfassungen mit der Probe abzugeben.

1. Allgemeine Fragen

1.1 Ordnen Sie folgende Begriffe den richtigen Aussagen zu.

Beachten Sie:
Zu **einem** Begriff hat es keine korrekte Aussage.
Zwei Aussagen können keinem Begriff zugeordnet werden.
(1 Punkt pro korrekte Aussagenzeile, keine Abzüge, maximal 13 Punkte)

Begriffe

a)	ASCII	b)	100kB
c)	Hamming-Code	d)	RSA
e)	3MB	f)	Unicode
g)	Huffman-Code	h)	XOR
i)	Redundanz	j)	10GB
k)	Hamming-Abstand	l)	D

Antwort	Aussage
	Ungefähre Grösse eines gewöhnlichen Word-Dokuments.
	Ein asymmetrisches Verschlüsselungsverfahren.
	Produziert einen Code mit minimaler Redundanz.
	Ein 7 Bit - Code
	Ein 8 Bit - Code
	Ein symmetrisches Verschlüsselungsverfahren.
	Möglicher CAESAR-Schlüssel.
	Jedes Zeichen wird mit 16 Bit codiert.
	Anteil der nicht verwendeten Kombinationen eines Codes.
	Ein Mittel zur automatischen Korrektur von Übertragungsfehlern.
	Ungefähre Grösse einer Spielfilm-Datei.
	Damit werden Klartext und Schlüssel zum Chiffrat verknüpft.
	Ungefähre Grösse einer MP3-Audiodatei (1 Song).

2. Dateitypen und Dateigrössen

2.1 Geben Sie drei Dateitypen für Textdateien an (3 Punkte).

2.2 Aus wie vielen Bits besteht ein Kilobyte (2 Punkte).

2.3 Wie lange dauert theoretisch ein Backup von 100MB Daten, wenn das Speichermedium eine Schreibgeschwindigkeit von 1Mb/s aufweist (4 Punkte)?

3. Verlustfreie Kompression

3.1 Erstellen Sie einen Huffman-Codebaum und codieren Sie damit folgende Zeichenfolge:

FUENF FEINE FREUNDE

Bestimmen Sie die Länge der entstandenen Bitfolge und berechnen Sie die Kompressionsrate gegenüber dem Originaltext in Unicode (6 Punkte).

Huffman-Codebaum:

Bitfolge:

Kompressionsrate:

4. Verlustbehaftete Kompression

4.1 Nennen Sie zwei psychoakustische Phänomene und begründen Sie, warum diese zur Reduktion von Audiodateien genutzt werden können (4 Punkte).

5. Verschlüsselung

5.1 Verschlüsseln Sie den Klartext BURGDORF mit dem Caesar-Schlüssel C (2 Punkte).

5.2 Berechnen Sie die fehlenden Parameter und Verschlüsseln Sie die Nachricht mit dem RSA-Verfahren (6 Punkte):

Primzahl p:	7	
Primzahl q:	13	
Öffentlicher Schlüssel e:	5	
Privater Schlüssel d:	29	
Modulzahl n:		_____ _____
Geheime Modulzahl phi(n):		_____ _____
Verschlüsseln Sie die Nachricht „11“		__ __

Wie würden Sie diese verschlüsselte Nachricht entschlüsseln? Sie sollen die Berechnung nicht durchführen sondern lediglich die korrekten Zahlen als Formel dazu notieren

__ _____