Aufgabenblatt der Lernkontrolle: InfSi1_V05

Name der Lernkontrolle:	InfSi1_V05
Beschreibung:	
Startzeitpunkt:	22. March 2016 12:50:00
Endzeitpunkt:	08. April 2016 23:59:00
Maximale Punktezahl:	50
Anzahl Fragen:	21
Anzahl eigene Teilnahmen:	1
Teilnehmer:	Rico Akermann (rakerman@hsr.ch)
Startzeitpunkt Teilnahme:	28. July 2016 22:15:29
Endzeitpunkt Teilnahme:	28. July 2016 22:45:31
Benötigte Zeit:	00:30:02
Punkte:	4/50 (8%)

Frage 1: Bei welchem Verfahren zeigt die Autokorrelation der verschlüsselten Zeichenfolge des Märchentextes "Ali Baba und die 40 Räuber" Periodizitäten?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Caesar
◉	◉	Vigenère

Frage 2: Der Informationsgehalt eines Symbols, welches mit der Wahrscheinlichkeit 1/68 vorkommt, beträgt ...

Richtige Antwort	Deine Antwort	Fragetext
O	O	5.1 Bit
O	O	6 Bit
◉	O	6.09 Bit
O	◉	7.2 Bit
O	O	8 Bit

Frage 3: An der Entschlüsselung von Enigma-Meldungen im 2. Weltkrieg war folgende Person massgeblich beteiligt:

Richtige Antwort	Deine Antwort	Fragetext
O	O	Auguste Kerckhoffs
O	O	Claude Shannon
◉	◉	Alain Touring
O	O	Gilbert Vernam

Frage 4: Wie viele mögliche Schlüssel gibt es beim Caesar-Code?

Richtige Antwort	Deine Antwort	Fragetext
◉	O	26
O	O	26^2
O	◉	26!

Frage 5: Wie viele mögliche Schlüssel gibt es beim Vigenère-Code mit n Zeichen bzw. Buchstaben Schlüssellänge?

Richtige Antwort	Deine Antwort	Fragetext
O	O	26
O	◉	26^2
O	O	26!
◉	O	26^n

Frage 6: Angreifer können das Chiffrat eines Textes am besten entschlüsseln, wenn ...

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	der Klartext viel Redundanz enthält.
O	O	die Entropie des Klartexts 4.7 Bit beträgt.
O	O	alle Zeichen des Chiffrats gleich häufig auftreten.

Frage 7: Das Vigenère Verschlüsselungsverfahren ...

Richtige Antwort	Deine Antwort	Fragetext
✗	✗	ist ein Transpositionsverfahren.
✓	✓	is ein Substitutionsverfahren.
✗	✓	verwendet monoalphabethische Verschlüsselung.
✓	✗	verwendet polyalphabethische Verschlüsselung.

Frage 8: Unter Berücksichtigung des Zusammenhangs aufeinanderfolgender Zeichen beträgt die Entropie englischer Texte etwa ...

Richtige Antwort	Deine Antwort	Fragetext
O	O	8 Bit
O	O	5 Bit
O	◉	3 Bit
◉	O	2 Bit

Frage 9: Dass die Sicherheit eines Verschlüsselungssystems einzig und allein von der Sicherheit des geheimen Schlüssels abhangen soll, wurde gefordert von ...

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	Auguste Kerckhoffs
O	O	Claude Shannon
O	O	Alain Touring
O	O	Gilbert Vernam

Frage 10: Welche Werte liefert die Autokorrelation einer zufälligen Buchstabenfolge bestehend aus 100 Zeichen (nur Grossbuchstaben) bei der Verschiebung um mindestens ein Zeichen?

Richtige Antwort	Deine Antwort	Fragetext
O	O	etwa 7% Übereinstimmungen
O	O	etwa 4% Übereinstimmungen
◉	O	etwa 1% Übereinstimmungen
O	◉	periodisch kleine und dann wieder grössere Werte

Frage 11: Welche Aussagen treffen zu "Steganographie" zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Steganographie wird auch mit "bedeckt schreiben" umschrieben.

✗	✗	Eine mit Steganographie verarbeitete Nachricht, kann nur bei Kenntnis des richtigen Schlüssels gelesen werden
✓	✗	Bei der Steganographie benötigt man ein Hostfile.
✓	✓	Steganographie spielt bei der Copyright Protection eine wichtige Rolle.

Frage 12: Security by Obscurity heisst, ...

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	dass die Sicherheit auf der Geheimhaltung von Systemeigenschaften, Verfahren und Systemdesign basiert.
O	O	dass die Sicherheit darauf beruht, dass sehr komplexe Verfahren eingesetzt werden.
O	O	dass möglichst undurchsichtige, nicht erratebare Passwörter verwendet werden.

Frage 13: Bei welchem Verfahren ist die typische Buchstabenhäufigkeit einer Sprache im Chiffrat weniger klar ersichtlich?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Caesar
◉	◉	Vigenère

Frage 14: 8 zufällig gewählte Hex-Zeichen haben einen Informationsgehalt von...

Richtige Antwort	Deine Antwort	Fragetext
O	O	4 Bit
O	O	16 Bit
◉	O	32 Bit
O	◉	64 Bit
O	O	128 Bit

Frage 15: Bei einem System wird eine Geheimzahl (z.B. der PIN-Code) aus einer völlig zufällig gewählten Kombination mit vier Zeichen erstellt. Für die vier Zeichen steht der Zeichensatz 0, ..., 9 zu Verfügung, d.h. es sind Geheimcodes zwischen "0000" und "9999" möglich. Welche Entropieangabe liegt am nächsten bei der Entropie der daraus abgeleiteten Binärschlüssels?

Richtige Antwort	Deine Antwort	Fragetext
O	O	10 Bit
◉	O	13 Bit
O	O	20 Bit
O	O	40 Bit

Frage 16: Das Caesar Verschlüsselungsverfahren ...

Richtige Antwort	Deine Antwort	Fragetext
✗	✓	ist ein Transpositionsverfahren.
✓	✗	ist ein Substitutionsverfahren.
✓	✗	verwendet monoalphabethische Verschlüsselung.
✗	✗	verwendet polyalphabethische Verschlüsselung.

Frage 17: Wer gilt als Begründer der Informationstheorie und hat die Einheit zum Informationsgehalt definiert?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Auguste Kerckhoffs
◉	O	Claude Shannon
O	O	Alain Touring
O	◉	Gilbert Vernam

Frage 18: Der Informationsgehalt eines einzelnen Zeichens ist dann am höchsten, ?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	wenn das Zeichen sehr selten vorkommt.
O	O	wenn das Zeichen gleich häufig vorkommt, wie alle anderen Zeichen.
O	O	wenn das Zeichen sehr häufig vorkommt.

Frage 19: Die Entropie (bzw. der mittlere Informationsgehalt) einer zufällig gewählten Zeichenfolge ist dann am höchsten, ...

Richtige Antwort	Deine Antwort	Fragetext
O	◉	wenn einige Zeichen sehr selten vorkommen.
◉	O	wenn alle Zeichen gleich häufig vorkommen.
O	O	wenn einige Zeichen sehr häufig vorkommen.

Frage 20: Welche Teile eines Kryptosystems müssen geheim gehalten werden?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Verschlüsselungsalgorithmus
O	O	Entschlüsselungsalgorithmus
◉	◉	Schlüssel
O	O	Systemaufbau

Frage 21: Beim One-Time-Pad Verschlüsselungsverfahren ...

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	ist der Schlüssel gleich lang wie der Klartext.
✗	✗	müssen alle Klartextzeichen gleich häufig auftreten.
✓	✓	darf der Schlüssel nicht mehrfach verwendet werden.
✗	✗	wird der Schlüssel nach jeweils 1000 Zeichen gewechselt.