# Aufgabenblatt der Lernkontrolle: InfSi1_V06

| | |
|---|---|
| **Name der Lernkontrolle:** | InfSi1_V06 |
| **Beschreibung:** | |
| **Startzeitpunkt:** | 05. April 2016 18:38:00 |
| **Endzeitpunkt:** | 18. April 2016 18:38:00 |
| **Maximale Punktezahl:** | 57 |
| **Anzahl Fragen:** | 18 |
| **Anzahl eigene Teilnahmen:** | 1 |
| **Teilnehmer:** | Rico Akermann (rakerman@hsr.ch) |
| **Startzeitpunkt Teilnahme:** | 28. July 2016 23:00:28 |
| **Endzeitpunkt Teilnahme:** | 28. July 2016 23:39:02 |
| **Benötigte Zeit:** | 00:38:34 |
| **Punkte:** | 3/57 (5%) |

**Frage 1: Wenn man die Länge eines Schlüssels um ein Bit erhöht ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | verdoppelt sich die Sicherheit des Systems. |
| ✗ | ✗ | verdoppelt sich der Informationsgehalt des Schlüssels. |
| ✓ | ✗ | nimmt der Informationsgehalt des Schlüssels um ein Bit zu. |
| ✗ | ✗ | wird die Sicherheit des Systems vier mal grösser. |

**Frage 2: Welche der folgenden Begriffe beschreiben AES?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✓ | Stream Cipher |
| ✓ | ✗ | Block Cipher |
| ✓ | ✓ | Advanced Encryption Standard |
| ✗ | ✗ | American Encryption Standard |

**Frage 3: Welche Parameter müssen der Sender und der Empfänger beim Einsatz von Block Codes miteinander absprechen? (Der Algorithmus sei festgelegt.)**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | Blocklänge |
| ✓ | ✓ | Paddingverfahren |
| ✓ | ✗ | Schlüssellänge |
| ✓ | ✗ | Datenrate |

**Frage 4: Bei welchem Block Cipher Betriebsmodus können Periodizitäten im Klartext erhalten bleiben?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | O | Electronic Codebook (ECB) Mode |
| O | O | Cipher Block Chaining (CBC) |
| O | O | Cipher Feedback Mode (CFB) |
| O | ◉ | Counter Mode (CTR) |

**Frage 5: Welche Parameter müssen der Sender und der Empfänger beim Einsatz von Stream Ciphers miteinander absprechen? (Der Algorithmus sei festgelegt.)**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | Blocklänge |
| ✗ | ✗ | Paddingverfahren |
| ✓ | ✓ | Schlüssellänge |
| ✓ | ✓ | Datenrate |

**Frage 6: Bei der Verschlüsselung eines deutschen Textes mit DES oder AES wird die Häufigkeit der Ciphertext-Bytes untersucht. Welche Aussage trifft zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | Die Häufigkeit der Buchstaben ist auch im Chiffrat zu erkennen. |
| ◉ | ◉ | Alle Ciphertext-Bytes treten etwa gleich häufig auf. |

**Frage 7: Welche EXOR-Inputs führen auf den Output "1"?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | 0 (+) 0 |
| ✓ | ✓ | 1 (+) 0 |
| ✓ | ✓ | 0 (+) 1 |
| ✗ | ✗ | 1 (+) 1 |

**Frage 8: Bei DES (CBC) wird im Cryptool X.923-Padding verwendet. Der letzte Datenblock enthalte nur die drei Bytes AA BB CC. Welche Aussagen treffen auf das in diesem Fall durchgeführte Padding zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✓ | Die drei Bytes werden nach der Verschlüsselung auf 8 Bytes ergänzt. |
| ✓ | ✓ | Der zu verschlüsselnde Datenblock lautet AA BB CC 00 00 00 00 03. |
| ✓ | ✓ | Beim Entschlüsseln wird das Padding wieder entfernt. |
| ✗ | ✗ | Der zu verschlüsselnde Datenblock lautet AA BB CC 00 00 00 00 00. |

**Frage 9: Welche der folgenden Verfahren sind Symmetric Key Verfahren?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✗ | RSA |
| ✗ | ✓ | DH |
| ✓ | ✗ | AES |
| ✓ | ✗ | DES |

**Frage 10: AES steht für ...**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ◉ | ◉ | Advanced Encryption Standard |
| O | O | American Encryption Standard |
| O | O | Adopted Encryption Security |
| O | O | Algorithmic Enctyption Security |

**Frage 11: Welche (effektive) Schlüssellänge muss bei einer Brute Force Attacke Triple-DES-Verschlüsselung "verarbeitet" bzw. durchprobiert werden?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 56 Bit |

| | | |
|---|---|---|
| O | O | 64 Bit |
| ⊙ | O | 112 Bit |
| O | ⊙ | 128 Bit |
| O | O | 192 Bit |

**Frage 12: Die maximale Entropie einer Zeichenkette bestehend aus zufällig gewählten, mit Wahrscheinlichkeit 1/26 auftretenden Buchstaben beträgt ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✗ | ld(26) |
| ✓ | ✗ | 4.7 Bit |
| ✓ | ✗ | log(26)/log(2) |
| ✗ | ✓ | ld(1/26) |
| ✗ | ✗ | 5 Bit |

**Frage 13: Beim Einsatz von Block Codes im Cipherblock Chaining (CBC) Modus ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✗ | ✓ | könnte der Sender die Verschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✓ | ✓ | könnte der Empfänger die Entschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✗ | ✗ | führen gleiche Klartextblöcke immer auf die gleichen Ciphertextblöcke. |
| ✓ | ✓ | müssen sich Sender und Empfänger auf denselben Initialisierungsvektor einigen. |

**Frage 14: Was ergibt die Verknüpfung y = a EXOR b EXOR a ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | ⊙ | 1 |
| O | O | a |
| ⊙ | O | b |
| O | O | 0 oder 1 abhängig von a |

**Frage 15: Welche (effektive) Schlüssellänge wird bei "normaler" DES-Verschlüsselung verwendet?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ⊙ | O | 56 Bit |
| O | O | 64 Bit |
| O | O | 112 Bit |
| O | ⊙ | 128 Bit |
| O | O | 192 Bit |

**Frage 16: Welche Aussagen treffen auf einen Pseudo Random Number Generator (PRNG) zu?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✓ | PRNG wird in Stream Cipher Verfahren eingesetzt |
| ✓ | ✗ | PRNG liefert Sequenzen, welche siche irgendwann wiederholen |

**Frage 17: Beim Einsatz von Block Codes im Electronic Codebook (ECB) Modus ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| ✓ | ✗ | könnte der Sender die Verschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |
| ✓ | ✗ | könnte der Empfänger die Entschlüsselungsgeschwindigkeit durch Parallelisierung erhöhen. |

| | | |
|---|---|---|
| ✓ | ✓ | führen gleiche Klartextblöcke immer auf die gleichen Ciphertextblöcke. |
| ✗ | ✗ | müssen sich Sender und Empfänger auf denselben Initialisierungsvektor einigen. |

**Frage 18: Bei AES beträgt die Schlüssellänge mindestens ?**

| Richtige Antwort | Deine Antwort | Fragetext |
|---|---|---|
| O | O | 56 Bit |
| O | ◉ | 64 Bit |
| O | O | 112 Bit |
| ◉ | O | 128 Bit |
| O | O | 196 Bit |