Vorbemerkungen und Abgabe

Das Übungsblatt bietet einen Überblick über die Aufgaben, die in dem aktuellen Online-Test zu bearbeiten sind. Wir erwarten, dass Sie alle Aufgaben die nicht als optional gekennzeichnet sind eigenständig lösen. Das Aufgabenblatt dient dazu, dass Sie vor dem Lösen des Tests bereits einen Überblick über den Inhalt der Übung bekommen und sich darauf vorbereiten können. Es müssen 75% (aufgerundete Punkte) der möglichen Punkte der jeweiligen Aufgabenblätter erworben werden, damit der Test als bestanden gilt. In den Aufgaben behandeln wir ausgewählte Detailaspekte, die Inhalte aus der Vorlesung erweitern bzw. vertiefen. Im Übungsbetrieb werden die Aufgaben, deren Lösungen und die zugrundeliegenden Inhalte besprochen. Zusätzlich werden die optionalen Aufgaben und gegebenenfalls weitere Präsenz-Aufgaben vorgestellt und besprochen. Der Inhalt aller Aufgaben ist klausurrelevant.
Der Besuch der Vorlesung ist für das Verständnis der Inhalte und die erfolgreiche Teilnahme an der Klausur essenziell. Die Termine finden Sie unter **https://www.inf.uni-hamburg.de/de/inst/ab/svs/courses/master/vis.html**
Die Abgabe erfolgt online unter **https://lernen.min.uni-hamburg.de/mod/quiz/view.php?id=4709**; Falls das System nicht erreichbar ist, wenden Sie sich notfalls per E-Mail an schwarz@informatik.uni-hamburg.de.

Moderne Kryptographie

One-Time-Pad (1 Punkt)
Gegeben sei eine mit einem One-Time-Pad verschlüsselte Nachricht. Welche Information kann ein*e Angreifer*in aus der Nachricht ableiten, wenn er*sie diese abfangen kann?
Wählen Sie eine oder mehrere Antworten:

1. Die Entropie der originalen Nachricht.
2. Den Inhalt der originalen Nachricht.
3. Die Länge der originalen Nachricht.

Feistel (1 Punkt)
Welche der folgenden Eigenschaften lässt sich dem Feistel-Verfahren zuordnen?

1. Einwegeigenschaft
2. Bijektivität
3. Falltüreigenschaft
4. Indeterministische Cipher-Texte

Feistel (2 Punkte)
Sie haben eine Binärzahl gegeben, die mit dem Feistel-Verfahren verschlüsselt wurde. Es wurden 3 Runden durchlaufen, der Schlüssel ist k = 13 und F ist ein AND. Berechnen Sie den ursprünglichen Klartext.
Die verschlüsselte Binärzahl lautet: 00001111

One-Time-Pad - Anwendung (2 Punkte)
Ihnen sind eine Reihe verschlüsselter deutscher Substantive in die Hände gefallen. Sie gehen davon aus, dass der*die Urheber*in fahrlässigerweise alle Wörter mit dem selben One-Time-Pad byteweise verschlüsselt hat. Versuchen Sie den Schlüssel zu ermitteln, indem Sie einen geeigneten Angriff implementieren.
Hinweis: Passwort und Substantive sind ASCII-Codiert (Alphabet = A,B,C, ... ,Z)
Die Schlüsseltexte (der 6 Substantive) in Dezimalschreibweise lauten:
09 00 04 10
10 20 28 09
10 16 02 02
10 20 05 08
26 26 03 00
28 16 03 17

Visuelle Kryptographie - Theorie (2 Punkte)
Auf wie viele Folien kann bei visueller Kryptographie das Geheimnis theoretisch maximal verteilt werden?

1. 2
2. beliebig viele
3. 4

Das Verfahren der visuellen Kryptographie bei 2 erzeugten Folien pro Secret hat Ähnlichkeiten zu einem anderen bekannten kryptographischen Verfahren. Welchem?

1. AES
2. RSA
3. One-Time-Pad
4. CBC

Visuelle Kryptographie - Anwendung (2 Punkte)
Sie haben zwei Folien gegeben, die Schlüssel eines visuellen Kryptographieverfahrens darstellen. Geben Sie das Geheimnis an, das verschlüsselt wurde. (Die Folien finden sich in dem Ordner zur Aufgabe 2 im moodle)

Gütekriterien (1 Punkt)
Kreuzen Sie die richtige(n) Lösung(en) an.

1. Um eine lineare Verschlüsselungsfunktion zu brechen, kann ein Gleichungssystem aufgestellt und gelöst werden.
2. Output-Zeichen können als lineare Input-Zeichen beschrieben werden, wenn ihre Verschlüsselungsfunktion linear ist.
3. Das strikte Avalanche-Kriterium ist erfüllt, wenn sich bei der Änderung eines Input-Zeichen 50% der Output-Zeichen ändern.
4. Die Erfüllung der Gütekriterien sorgt für hinreichende Sicherheit der symmetrischen Chiffren.

5. Der Grad der Vollständigkeit wird mit $\frac{k}{n}$ angegeben, d.h. im Mittel hängen k Output-Zeichen von n Input-Zeichen ab.

Symmetrische Konzelationssysteme (1 Punkt)
Kreuzen Sie die richtige(n) Lösung(en) an.

1. Der*die Empfänger*in erhält den Schlüsseltext c über einen unsicheren Kanal und entschlüsselt ihn mithilfe einer Dekodierungsfunktion *dec* und dem Schlüssel k.
2. Die Entschlüsselungsfunktion *dec* beschreibt die Abbildung von Paaren aus Schlüsseltexten und Schlüsseln auf Nachrichten.
3. Für alle k aus dem möglichen Schlüsselraum K ist die Abbildung der Verschlüsselungsfunktion *enc* surjektiv.
4. Der Verschlüsselungsalgorithmus *enc* bzw. Entschlüsselungsalgorithmus *dec* dürfen öffentlich bekannt sein.
5. Sender*innen und Empfänger*innen erhalten den gemeinsamen Schlüssel k über einen unsicheren Kanal.
6. Die Schlüsselgenerierung für Schlüssel k muss in einem Vertrauensbereich stattfinden.

Triple-DES (4 Punkte)
Um der Kritik des DES bezüglich seiner zu geringen Schlüssellänge von 56 Bit zu begegnen, wurde Triple-DES (3-DES) vorgeschlagen. Dabei wird mit zwei 56 Bit langen Schlüsseln k_1 und k_2 gearbeitet und beim Verschlüsseln entweder $encrypt(k_1) \rightarrow decrypt(k_2) \rightarrow encrypt(k_1)$ (EDE-Modus) oder $encrypt(k_1) \rightarrow encrypt(k_2) \rightarrow encrypt(k_1)$ (EEE-Modus) ausgeführt.

1. Warum begnügt man sich bei Triple-DES aus Sicherheitsgründen nicht mit zwei Verschlüsselungen? Gehen Sie von einem Known-plaintext-Angriff aus. Geben Sie die Ziffer der Antwort an, die Sie für richtig halten.

   a) Der Sicherheitsgewinn wäre nur 1 Bit (durch Anwendung eines Meet-in-the-Middle-Angriffs).

   b) Bei zwei Verschlüsselungen würden sich die Verschlüsselungseffekte gegenseitig aufheben.

   c) Der Sicherheitsgewinn ist in der Praxis nur halb so groß, wie die Summe der Schlüssellängen und dadurch immer noch zu kurz.

2. Welchen Modus benutzt man bevorzugt bei Triple-DES?

   a) EDE-Modus

   b) EEE-Modus

3. Berechnen Sie die theoretische und die effektive Schlüssellänge des Triple-DES unter einem Known-plaintext-Angriff mit drei 56-Bit-Schlüsseln, d.h. $encrypt(k_1) \rightarrow encrypt(k_2) \rightarrow encrypt(k_3)$.
   Geben Sie das Ergebnis als 2 hoch x an, wobei x eine natürliche Zahl ist.
   2 hoch _____