Vorbemerkungen und Abgabe

Das SVS-Übungsblatt besteht aus Pflicht-Aufgaben und optionalen Aufgaben. Nur die Pflicht-Aufgaben müssen von Ihnen abgegeben werden. Wir erwarten, dass Sie diese eigenständig lösen. In den optionalen Aufgaben behandeln wir ausgewählte Detailaspekte, die Inhalte aus der Vorlesung erweitern bzw. vertiefen. Die optionalen Aufgaben müssen nicht abgegeben werden. Die Auseinandersetzung mit diesen Aufgaben ist jedoch u. U. zur Beantwortung der Pflicht-Aufgaben erforderlich, in jedem Fall aber eine gute Vorbereitung auf die Klausur. Nur die Pflicht-Aufgaben werden korrigiert und für den Erhalt des Übungsscheins herangezogen (50%-Regel). 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://svs.informatik.uni-hamburg.de/submission/for/vis17-7**; bitte nicht per E-Mail abgeben! Abgaben müssen exakt eine PDF-Datei umfassen und können bis zum Ablauf der Frist mittels eines Zugriffscodes (VISxx-xxxx-xxxx-xxxx-xxxx), der beim 1. Hochladen angezeigt wird, beliebig oft aktualisiert werden. Eine spätere Abgabe ist nicht möglich. Wird kein Zugriffscode angezeigt wird, war das Hochladen wahrscheinlich nicht erfolgreich. Versuchen Sie es in diesem Fall erneut. Falls das System nicht erreichbar ist, können Sie zur Wahrung der Frist ihre Lösung notfalls per E-Mail an ezimmer@informatik. . . schicken. Die Bewertungen sind rechtzeitig vor den Übungen (spätestens am Tag der Übung morgens) ebenfalls online einsehbar. Bitte bringen Sie ggf. selbst einen Ausdruck Ihrer Lösung zum Übungstermin mit.

Kryptografie

Aufgabe 1 (Pflicht; 6 Punkte): Triple-DES

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 $E(k_1) \rightarrow D(k_2) \rightarrow E(k_1)$ (EDE-Modus) oder $E(k_2) \rightarrow E(k_2) \rightarrow E(k_1)$ (EEE-Modus) ausgeführt. Gehen Sie im Folgenden davon aus, dass DES eine effektive Sicherheit bietet, die der Schlüssellänge entspricht.

a) Warum begnügt man sich bei 3-DES aus Sicherheitsgründen nicht mit zwei Verschlüsselungsoperation $E(k_1) \rightarrow E(k_2)$? Überlegen Sie sich, wie ein Angreifer zum Entziffern einer solchermaßen verschlüsselten Nachricht vorgehen würde und bestimmen Sie dabei die effektive Sicherheit des Verfahrens. Vergleichen Sie diese mit der Sicherheit, die durch die Verwendung von zwei 56 Bit langen Schlüsseln „versprochen“ wird.

b) Warum sind bei 3-DES schon *zwei* verschiedene Schlüssel ausreichend und nicht erst drei verschiedene? Berechnen Sie dazu zuerst die Schlüssellänge und die effektive Sicherheit des oben dargestellten 3-DES mit zwei 56-Bit-Schlüsseln. Ermitteln Sie dann die Schlüssellänge und effektive Sicherheit einer 3-DES-Implementierung, welche drei verschiedene 56-Bit-Schlüssel

verwendet, d.h. $E(k_1) \rightarrow E(k_2) \rightarrow E(k_3)$. Gehen Sie dabei davon aus, dass Chosen-Plaintext-Angriffe nicht möglich sind.

c) Was ändert sich in Teilaufgabe b), wenn Chosen-Plaintext-Angriffe erlaubt sind, der Angreifer sich also beliebige Klartexte verschlüsseln lassen kann, ohne dabei den Schlüssel zu bekommen (optionale Teilaufgabe).

Aufgabe 2 (Optional): Unsicherheit des Electronic-Codebook-Modus

Eine einfache, jedoch unsichere, Technik zum Betrieb einer Blockchiffre ist der Electronic-Codebook-Modus (ECB-Modus).

a) Informieren Sie sich über den ECB-Modus. Inwiefern stellt dessen Funktionsweise ein Sicherheitsproblem dar?

b) Demonstrieren Sie die problematische Funktionsweise des ECB-Modus anschaulich, indem Sie ein Programm schreiben, welches eine einfache Windows-Bitmap-Grafik einliest, den Bildinhalt mit dem AES-Verfahren im ECB-Modus verschlüsselt und wieder als Bitmap ausgibt. Rufen Sie zum Vergleich die Verschlüsselung noch einmal im CBC-Modus auf und vergleichen Sie die erhaltenen Resultate. Informieren Sie sich dazu über das Datenformat von BMP-Dateien. Überlegen Sie sich, welche Bedingungen die Bitmap-Grafik erfüllen muss, damit besonders anschauliche Ergebnisse erzielt werden.

Aufgabe 3 (Pflicht; 6 Punkte): Cipher-Block-Chaining-Modus

Beim Cipher-Block-Chaining-Betriebsmodus wird ein Klartextblock M_i vor der Anwendung der Verschlüsselungsfunktion mit dem unmittelbar vorher erzeugten Chiffretextblock C_{i-1} durch die XOR-Operation verknüpft. Die erzeugten Chiffretextblöcke hängen dadurch von ihren Vorgängern ab. Bei der Verschlüsselung des allerersten Klartextblocks, M_1, verwendet der Sender der Nachricht für C_0 einen von ihm gewählten Initialisierungsvektor (IV).

Gehen Sie bei der Beantwortung der folgenden Fragen davon aus, dass eine moderne Blockchiffre, z.B. AES, eingesetzt wird. Überlegen Sie sich im folgenden jeweils die Antworten auf folgende Fragen: Welche Teile des Schlüsseltextes bzw. des Klartextes verändern sich durch die Änderung beim Ver- bzw. Entschlüsseln? Inwiefern sind die Auswirkungen für die Vertraulichkeit bzw. Integrität von Bedeutung?

a) Wie unterscheiden sich zwei Schlüsseltexte, die mit demselben Schlüssel erzeugt wurden und denselben Klartext enthalten, jedoch mit unterschiedlichen IVs erzeugt wurden?

b) Wie unterscheiden sich zwei Schlüsseltexte, wenn sie sich lediglich an einer Stelle im ersten Klartextblock unterscheiden (also ein Bit gekippt wird) und ansonsten völlig identisch sind (bei gleichem IV und Schlüssel)?

c) Welche Auswirkung hat es beim Entschlüsseln, wenn durch einen Übertragungsfehler ein Bit im zweiten Schlüsseltext-Block bei der Übertragung verändert wird?

d) Welche Auswirkung hat es beim Entschlüsseln, wenn durch einen Übertragungsfehler ein Bit im Initialisierungsvektor verändert wird?

Aufgabe 4 (Optional): Hybrides Kryptosystem

Ihr Ziel ist es, Daten vor der Übertragung über das Netzwerk mit einem geeigneten Verschlüsselungsverfahren zu übertragen.

Warum ist ein hybrides Kryptosystem einem rein symmetrischen bzw. einem rein asymmetrischen Verfahren üblicherweise vorzuziehen?

Aufgabe 5 (Optional): Das Diffie-Hellman-Schlüsselaustauschprotokoll

Das Diffie-Hellman(-Merkle)-Schlüsselaustauschprotokoll (DH-Protokoll) ermöglicht es zwei Kommunikationspartnern durch den Austausch von Nachrichten über einen unsicheren Kanal einen symmetrischen Sitzungsschlüssel zu etablieren, der von passiven Angreifern nicht ermittelt werden kann.

Beim ursprünglichen DH-Protokoll, das auch als „anonymes“ DH-Protokoll bezeichnet wird, wird kein Schlüsselserver verwendet. Die Kommunikationspartner tauschen dabei erst im Moment des Schlüsselaustauschs sämtliche Protokollnachrichten über den unsicheren Kanal aus.

a) Stellen Sie den Ablauf des anonymen DH-Protokolls zwischen den beiden Teilnehmern Alice und Bob mit passend gewählten kleinen Zahlen dar.

b) Erläutern Sie, auf welcher mathematischen Annahme die Sicherheit des DH-Protokolls basiert. Welche weiteren Annahmen macht man über den Angreifer (Angreifermodell)?

c) Schutz vor aktiven Angreifern ist möglich, wenn die Kommunikationspartner einige Parameter bzw. Protokollnachrichten vorab über einen sicheren Kanal ausgetauscht haben, der vom Angreifer nicht kontrolliert werden kann. Die eigentliche Schlüsselvereinbarung erfolgt dann später über den unsicheren Kanal in Anwesenheit eines aktiven Angreifers. Welche Nachrichten müssen vorab ausgetauscht worden sein, damit aktive Angriffe verhindert werden?

Aufgabe 6 (Pflicht; 6 Punkte): Sicherheit des RSA-Verfahrens

a) Auf welcher mathematischen Annahme basiert die Sicherheit des geheimen Schlüssels beim RSA-Verfahren? Stellen Sie zur Erläuterung anhand eines Beispiels mit kleinen Zahlen dar, welche Informationen ein Angreifer besitzt und wie er anhand dieser Informationen eine verschlüsselte Nachricht entschlüsseln könnte, wenn die oben angesprochene Annahme nicht gelten würde.

b) Auf der SVS-Website unter **https://svs.informatik.uni-hamburg.de/teaching/vis/rsa.zip** finden Sie ein ZIP-Archiv, in dem sich zwei Textdateien befinden. Die eine Textdatei enthält einen mit dem RSA-Verfahren verschlüsselten Text. Der Text wurde zunächst ASCII-kodiert und dann zeichenweise verschlüsselt und mit einem Zeilenumbruch getrennt abgespeichert, d.h. jedes verschlüsselte Zeichen steht in einer eigenen Zeile. In der zweiten Textdatei finden sie den Exponenten sowie den Modulus des zugehörigen öffentlichen Verschlüsselungsschlüssels ebenfalls durch einen Zeilenumbruch getrennt. Erläutern Sie kurz aber präzise, welche Möglichkeiten Sie haben, um an den Klartext zu gelangen. Setzen Sie eine der Möglichkeiten praktisch um. Geben Sie den Klartext sowie den Quelltext Ihrer praktischen Umsetzung ab.