Aufgaben

5.1. Wir betrachten das Verschlüsseln von Datensätzen in einer Datenbank mit AES. Jeder Datensatz hat eine Länge von 16 Bytes. Die Datensätze sind alle unabhängig voneinander gespeichert. Welcher Betriebsmodus ist hier zu empfehlen?

5.2. Diese Aufgabe beschäftigt sich mit der vollständigen Schlüsselsuche bei Blockchiffren mit einer Schlüssellänge von k Bit im CBC-Modus. Die Blocklänge n ist größer als die Schlüssellänge, d. h. $n > k$.

1. Wie viele Klartext-Chiffrat-Paare benötigt man, wenn die Chiffre im ECB-Modus betrieben wird? Wie viele Suchschritte werden maximal benötigt?
2. Die Chiffre wird nun im CBC-Modus betrieben, wobei dem Angreifer der Initialisierungsvektor IV bekannt ist. Beschreiben Sie die vollständige Schlüsselsuche für diesen Fall. Wie viele (i) Klartextblöcke und (ii) Geheimtextblöcke werden benötigt? Wie viele Suchschritte werden maximal durchgeführt?
3. Wie viele Klartext-Chiffrat-Paare werden benötigt, wenn der IV nicht bekannt ist?
4. Ist es merkbar schwerer, eine vollständige Schlüsselsuche gegen eine Chiffre im CBC-Modus relativ zum ECE-Modus durchzuführen?

5.3. In einem Firmennetzwerk werden alle Daten während der Übertragung mit AES-128 im CBC-Modus verschlüsselt. Der Schlüssel ist immer fest und der IV änderst sich einmal pro Tag. Bei der Übertragung werden jeweils Dateien verschlüsselt, wobei der IV am Anfang jeder Datei eingesetzt wird.

Durch einen Malware-Angriff kommen Sie in Besitz des AES-Schlüssels, Sie kennen aber nach wie vor nicht die IV. An einem Tag können Sie die verschlüsselte Version zweier Dateien mitschneiden. Von der einen Datei wissen Sie, dass diese nur den Wert `0xFF` enthält. Beschreiben Sie, wie Sie den unbekannten IV rekonstruieren und die zweite Datei dechiffrieren können.

5.4. Die Komplexität eines Brute-Force-Angriffs gegen den OFB-Modus steigt nicht an, wenn der IV geheim gehalten wird. Beschreiben Sie eine vollständige Schlüsselsuche, wenn der IV unbekannt ist. Welche Klar- und Geheimtexte müssen dem Angreifer bekannt sein?

5.5. Beschreiben Sie einen Angriff auf den OFB-Modus, wenn ein IV für alle Verschlüsselungen gleich bleibt.

5.6. Beschreiben Sie den OFB-Modus für den Fall, dass immer nur ein Byte an Klartext verschlüsselt wird, beispielsweise für die Verschlüsselung von Tastatureingaben. Als Chiffre wird AES verwendet. Für jede Verschlüsselung eines Bytes soll eine AES-Verschlüsselung ausgeführt werden. Zeichnen Sie ein Blockdiagramm des Schemas, in dem die Bitlängen (Busse) genau angegeben sind (vgl. Text am Ende von Abschnitt 5.1.4).

5.7. Wie so oft in der Kryptografie ist es einfach, ein anscheinend sicheres Verfahren durch kleine Änderungen zu schwächen. Wir betrachten den OFB-Modus mit AES, bei dem wir nur die acht höchstwertigen Bits (MSBs) des Ausgangs der Chiffre auf den Eingang rückkoppeln. Die verbleibenden 120 Bits werden mit dem Wert 0 aufgefüllt.

1. Zeichnen Sie ein Blockdiagramm des Verfahrens.
2. Warum ist das Schema schwach, wenn wir größere Klartexte von z. B. 100 kByte verschlüsseln? Wie viele Klartexte benötigt der Angreifer maximal, um das System vollkommen zu brechen?
3. Das rückgekoppelte Byte habe nun den Wert FB. Wird das Schema schwerer angreifbar, wenn wir den 128-Bit-Wert $FB, FB, \ldots, FB$ als Eingang für die Chiffre wählen, d. h. wir kopieren den Ausgang 16-mal und nutzen diesen als AES-Eingabe?

5.8. In dem Abschnitt zum CFB-Modus wird eine Variante beschrieben, welche einzelne Bytes verschlüsselt. Zeichnen Sie ein Blockdiagramm für diesen Modus und benutzen Sie AES als Chiffre. Geben Sie die Busweiten (d. h. Anzahl der Bits) jeder Verbindung in dem Diagramm an.

5.9. AES wird im Counter Mode zur Verschlüsselung einer Datei der Größe 1 TB benutzt. Was ist die maximale Länge des IV?

5.10. In manchen Anwendungen können Fehler während der Datenübertragung auftreten, die sich je nach Betriebsmodus unterschiedlich auswirken. In dieser Aufgabe untersuchen wir das Zusammenspiel zwischen Übertragungsfehlern und den verschiedenen Betriebsmodi. Wir nehmen einfache Bitfehler an, d. h. bei der Übertragung wird ein Bit des Chiffrats von "0" auf "1" gekippt oder umgekehrt.

1. Es tritt ein Bitfehler in Chiffratblock y_i auf. Welche Klartextblöcke von Bob, dem Empfänger, sind davon betroffen?
2. Wir nehmen wiederum einen Übertragungsbitfehler in Block y_i an. Welche Klartextblöcke von Bob sind betroffen, wenn der CBC-Modus verwendet wird?
3. Diesmal betrachten wir einen Fehler in dem Klartextblock x_i, den Alice verschlüsselt. Welche Klartextblöcke von Bob sind betroffen, wenn der CBC-Modus eingesetzt wird?
4. Wir betrachten den CFB-Modus bei dem jeweils 8 Bit verschlüsselt werden. Es tritt ein Bitfehler während der Übertragung auf. Wie weit pflanzt sich dieser Fehler bei Bob fort? Beschreiben Sie genau, welche Veränderungen in den Klartexten auftreten.
5. Erstellen Sie eine Tabelle mit den Betriebsmodi, die beschreibt, wie ein Bitfehler in Block y_i die Klartexte in den fünf Betriebsmodi ECB, CBC, CFB, OFB und CTR beeinflusst. Unterscheiden Sie zwischen einzelnen Bitfehlern und ganzen Blöcken, die betroffen sind.

5.11. Neben einfachen Bitfehlern kann auf Übertragungskanälen auch der Fall auftreten, dass Bits gar nicht übertragen werden oder zusätzliche Bits eingefügt werden.

Dies führt in den meisten Fällen dazu, dass die Ver- und Entschlüsselung nicht mehr synchron verlaufen und alle nachfolgenden Chiffrate inkorrekt entschlüsselt werden. Ein Sonderfall ist der CFB-Modus, bei dem nur ein Bit rückgekoppelt wird. Zeigen Sie, dass Ver- und Entschlüsselung nach $\kappa + 1$ Schritten wieder synchronisiert sind, wobei $\kappa + 1$ die Blockgröße der Chiffre ist.

5.12. In dieser Aufgabe versuchen wir eine Kostenabschätzung für einen Angriff auf 2DES zu erstellen, d. h. DES mit Zweifachverschlüsselung:

$$2DES(x) = DES_{K_2}(DES_{K_1}(x))$$

1. Zunächst betrachten wir eine naive vollständige Schlüsselsuche ohne Abspeichern von Zwischenergebnissen. Es muss der gesamte Schlüsselraum, der von K_1 und K_2 gebildet wird, durchsucht werden. Wie teuer ist eine Spezialmaschine, die 2DES in einer Woche brechen kann (Worst-case-Betrachtung)?
   Wir nehmen hierzu spezielle ICs, sog. ASICs, an, die 10^7 Schlüssel pro Sekunde testen können und \$5 das Stück kosten. Wir nehmen einen Overhead von 50% für den Bau der Maschine an.
2. Wir betrachten nun den Meet-in-the-Middle-Angriff, welcher ein Time-Memory-Tradeoff-Angriff ist.
   - Wie viele Einträge müssen in der Tabelle abgespeichert werden?
   - Wie viele Bytes müssen pro Eintrag gespeichert werden?
   - Wie teuer ist eine Suchmaschine, die den Schlüssel innerhalb einer Woche findet? Man beachte, dass für das Anlegen der Tabelle auch der gesamte Schlüsselraum einmal durchlaufen werden muss. Wir nehmen an, dass für das Anlegen der Tabelle (Phase 1) und die Suche in Phase 2 die gleiche Spezialmaschine verwendet wird.

   Für eine grobe Kostenabschätzung nehmen wir an, dass 10 GByte Festplattenspeicher \$8 kosten, wobei 1 GByte = 10^9 Byte.
3. Wann fallen die Kosten unter \$1 Million, wenn wir das Mooresche Gesetz annehmen? (Da die Speicherkosten ständig fallen, kann man die Aufgabe an aktuelle Preise anpassen.)

5.13. Anstatt seltsame Experimente an Erdenbürgern vorzunehmen, hinterlassen Außerirdische nach ihrem letzten Besuch auf unserem Planeten eine Schlüsselsuchmaschine, die besonders gut für AES geeignet ist. Mit ihr kann man Schlüsselräume von 128, 192 und sogar 256 Bit innerhalb weniger Tage durchsuchen. Wie viele Klartext-Chiffrat-Paare benötigt man, damit inkorrekte Schlüssel mit einer hohen Wahrscheinlichkeit ausgeschlossen werden können?

Bemerkung: Da sowohl Außerirdische als auch Suchmaschinen für solche Schlüssellängen extrem unwahrscheinlich sind, ist diese Aufgabe reine Fiktion.

5.14. Gegeben seien einige Klartext-Chiffrat-Paare und das Ziel ist, ein System anzugreifen, welches Mehrfachverschlüsselung verwendet.

1. Ein Verschlüsselungssystem E soll angegriffen werden, welches Dreifachverschlüsselung mit AES-192 durchführt, d. h. die Blockgröße beträgt $n = 128$ Bit und die Schlüssellänge $k = 192$ Bit. Der korrekte Schlüssel sei K. Wie viele Tupel (x_i, y_i) mit $y_i = e_K(x_i)$ werden benötigt, damit ein *false positive* Schlüssel K' mit einer Wahrscheinlichkeit von $Pr(K' \neq K) = 2^{-20}$ auftritt?
2. Was ist die maximale Schlüssellänge einer Chiffre mit Blockgröße $n = 80$, die mit Zweifachverschlüsselung, d. h. $l = 2$, betrieben wird, damit die Fehlerwahrscheinlichkeit eines inkorrekten Schlüssels K' den Wert $Pr(K' \neq K) = 2^{-10} = 1/1024$ hat?
3. Was ist die Erfolgswahrscheinlichkeit für die Schlüsselsuche mit vier gegebenen Klartext-Chiffrat-Paaren für AES-256 ($n = 128$, $k = 256$), der mit Zweifachverschlüsselung eingesetzt wird?

Man beachte, dass dies rein theoretische Aufgaben sind, da es technisch vollkommen ausgeschlossen ist, Schlüsselräume mit 2^{128} oder mehr Elementen zu durchsuchen.

5.15. 3DES kann mit etwa 2^{2k} DES-Verschlüsselungen und 2^k Speicherzellen gebrochen werden, wobei $k = 56$ ist. Beschreiben Sie den entsprechenden Angriff. Wie viele Paare (x, y) sollten zur Verfügung stehen, damit die Wahrscheinlichkeit eines inkorrekten Schlüsseltripels (k_1, k_2, k_3) für die Praxis ausreichend niedrig ist?

5.16. In dieser Aufgabe haben Sie die Möglichkeit, ein Kryptoverfahren zu brechen. Es ist bekannt, dass es in der Kryptografie viele Fallstricke gibt. Diese Aufgabe ist ein gutes Beispiel für ein starkes Verschlüsselungsverfahren, welches durch eine geringfügige Modifikation sehr schwach wird.

In dem Abschnitt zu Key Whitening wurde gezeigt, dass diese Technik gut geeignet ist, um Blockchiffren robuster gegen Brute-Force-Angriffe zu machen. Im Folgenden betrachten wir eine Variante von DES mit Key Whitening, die wie DESA nennen:

$$DESA_{k,k_1}(x) = DES_k(x) \oplus k_1$$

Obwohl das Schema stark dem regulären Key Whitening ähnelt, ist es kaum stärker als DES. Ihre Aufgabe ist es zu zeigen, dass eine vollständige Schlüsselsuche kaum schwerer als im Falle des regulären DES ist. Wir können annehmen, dass dem Angreifer einige Klartext-Chiffrat-Paare zur Verfügung stehen.