AES etwas genauer betrachtet

Um diesen Abschnitt bearbeiten zu können, solltest du mit den wesentlichen Begriffen der modernen symmetrischen Kryptoverfahren vertraut sein.

Schlüssellänge und Rundenzahl

Die **Blocklänge** des AES beträgt **128 Bit**. Die AES-Schlüssellänge kann wahlweise auf 128, 192 oder 256 Bit festgelegt werden, die Rundenzahl hängt von der gewählten Schlüssellänge ab:

Schlüssellänge	Rundenzahl
128 Bit	10
192 Bit	12
256 Bit	14

Klartextblock als Matrix

Alle Operationen werden auf einer 4×4 Byte Matrix ausgeführt, dazu werden die 128Bit des Klartextblocks wie folgt angeordnet:

Rundenaufbau

Wir betrachten nur den AES mit 128Bit Schlüssellänge und 10 Runden.

Der AES verfügt über die folgenden Operationen, die im Ablauf der Runden zum Einsatz kommen und auf der 4×4 Byte Matrix ausgeführt werden:

- SubBytes
- ShiftRow
- MixColumn
- AddRoundKey

Die mathematischen Details der Operationen beleuchten wir an dieser Stelle nicht.

Der Ablauf ist wie folgt:

(A1)

Wieviele Rundenschlüssel sind nötig? Wie viel (Bit/Byte) Schlüsselmaterial muss bei der Schlüsselaufbereitung erzeugt werden? Ein Rundenschlüssel ist 16Byte lang.

Beobachte die Schlüsselaufbereitung im Cryptool. Klappe die Abschnitte `Schlüssel` und `Erweiterter Schlüssel` aus. Ändere anschließend den Wert für den Schlüssel und beobachte, was im Feld erweiterter Schlüssel geschieht.

Überprüfe, ob die Menge des Schlüsselmaterials beim erweiterten Schlüssel mit deinen eigenen Überlegen übereinstimmt.

Was macht SubBytes?

Die Rundenfunktion „SubBytes“ dient zur **kryptographischen Konfusion** und ist mit einer S-Box realisiert. Die AES S-Box ist eine feste Zuordnungstabelle, in der für jeden Byte-Wert von 00 bis FF (0-255) festgelegt ist, durch welchen anderen Byte-Wert ein Eingabebyte ersetzt werden soll.

Bei der Ersetzung wird nun jedes Byte der 4×4 Matrix durch seine entsprechende Ersetzung ersetzt. Im Cryptool kann man die AES S-Box sehen:

Dabei sind 2 Hexadezimale Stellen jeweils ein Byte und man zählt vom Beginn der S-Box an von 00 bis FF (von 0 bis 255), damit ergeben sich folgende Ersetzungen:

```
00 -> 63
01 -> 7c
02 -> 77
...
fe -> bb
ff -> 16
```

(A2)

Mache dir zunächst noch einmal klar, dass 2 hexadezimale Ziffern 8 Bit, also ein Byte repräsentieren.

Hilfestellung

Arbeite im Cryptool zunächst mit dem Schlüssel `00000000 00000000 00000000 00000000` und der Eingabe `00010203 04050607 08091011 fcfdfeff`.

Das hat zur Folge, dass die erste Anwendung von **AddRoundKey** auf den Eingabetext - bevor die Runden beginnen - keine Auswirkung auf die Bitfolge hat, auf die die S-Box angewandt wird.

Mache dir klar, dass die Eingabe zählt von 0 beginnend für hoch zählt (12Bytes weit), beziehungsweise von 255 beginnend abwärts zählt (4Bytes weit)

`496e666f 20697374 20746f6c 6c21210a` [1)]

[1)]
Zusatzfrage: Welcher Text ist in dieser Eingabe codiert?