FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

Visualisierung der Funktionsweise des Advanced Encrytion Standard (AES)

Benutzerhandbuch

Claude Petry

Projektarbeit im Bachelor Studiengang Informatik

Bearbeitungszeitraum: Sommersemester 2007

Betreuer: Prof. Dr. A. Scheerhorn

Inhaltsverzeichnis

1 Zusammenfassung

Im Rahmen der Lehre im Bereich Angewandte Kryptographie wird der AES Algorithmus behandelt. Um das Verfahren für die Studenten anschaulicher darstellen zu können, wurde im Rahmen eines Praxisprojektes ein Animationstool entwickelt, das die bei der AES Ver- und Entschlüsselung ablaufenden Vorgänge visualisiert.

In diesem Benutzerhandbuch werden die wichtigsten Bedienoberflächen vorgestellt. Anschließend wird die Funktionsweise der Bedienelemente erklärt.

2 Systemvoraussetzungen und Installation

Dieses Tool wurde für Java 5.0 übersetzt. Zur Ausführung wird ein (bereits installiertes) Java Runtime Environment (JRE) oder Java Development Kit (JDK) vorausgesetzt.

Eine spezielle Installationsprozedur ist nicht erforderlich. Das Tool wird in Form einer JAR - Datei ausgeliefert und kann direkt ausgeführt werden. Ein Start über die Konsole ist ebenfalls möglich und kann wie gewohnt über den Befehlt „java –jar“ erfolgen.

3 Die Oberfläche

In diesem Kapitel werden Ein, Ausgabe und Hauptfenster vorgestellt, dies sind die wichtigsten Bedienoberflächen.

3.1 Eingabefenster

Das Eingabefenster dient zur Auswahl des Betriebsmodus (Verschlüsselung oder Entschlüsselung), sowie der Eingabe des Schlüssels und je nach Betriebsart des Klartext- resp. Chiffretext-Blockes.

Die Länge des Schlüssels kann über eine Combobox eingestellt werden und muss zur Länge des eingegebenen Schlüssels passen.

Die Eingabe des Schlüssels sowie der Klar- resp. Chiffretext-Blöcke erfolgt in hexadezimaler Form. Abstände zwischen den Byte-Gruppen sind erlaubt.

Beispiel mit Abständen:

```
32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
```

Beispiel ohne Abstände:

```
3243f6a8885a308d313198a2e0370734
```

Alternativ zur manuellen Eingabe können zuvor gespeicherte Startkonfigurationen über den Button „Load from file…“ eingelesen werden.

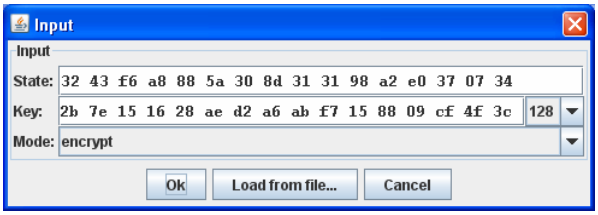

Abb. 1: Eingabefenster

3.2 Hauptfenster

Das Hauptfenster ist in drei Bereiche eingeteilt. Siehe hierzu Abbildung 2.

Links befindet sich der zur Ver- resp. Entschlüsselung passende Pseudocode. Die aktive Anweisung wird durch eine gelbe Zeilenmarkierung angezeigt.

Im rechten oberen Teil des Fensters werden die aktuellen Zustände der Daten und Schlüsselblöcke angezeigt.

Darunter befindet sich die Anzeigefläche für die Visualisierung der aktuellen Anweisung.

Zusätzlich stehen Buttons und Menüs zur Steuerung des Simulationsfortschrittes zur Verfügung.

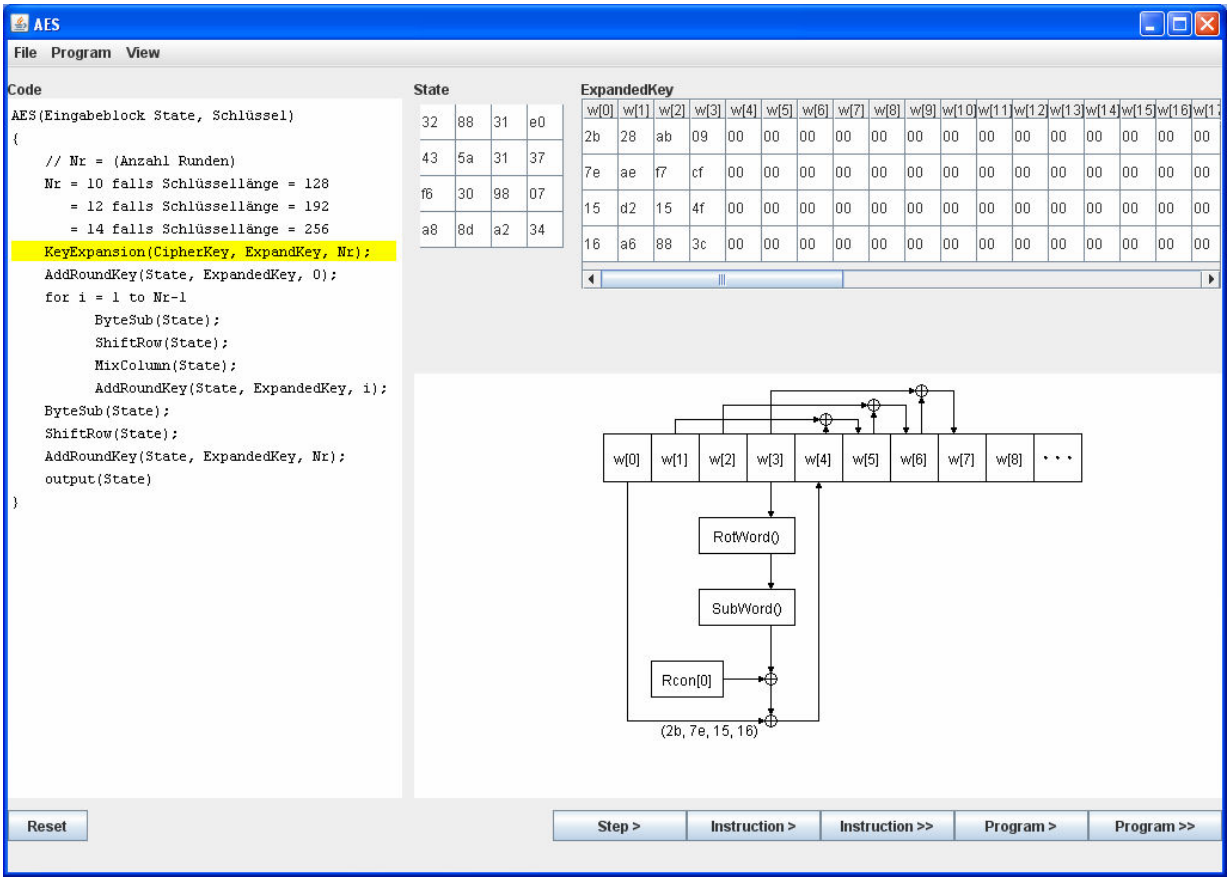

Abb. 2: Hauptfenster

3.3 Ausgabefenster

Im Ausgabefenster wird unter „Output“ der aus der Ver- resp. Entschlüsselung resultierende Datenblock (Chiffretext resp. Klartext) angezeigt.

Zusätzlich werden unter „Input“ noch mal die Eingabedaten (Datenblock, Schlüssel, Schlüssellänge und Betriebsmodus) wiederholt.

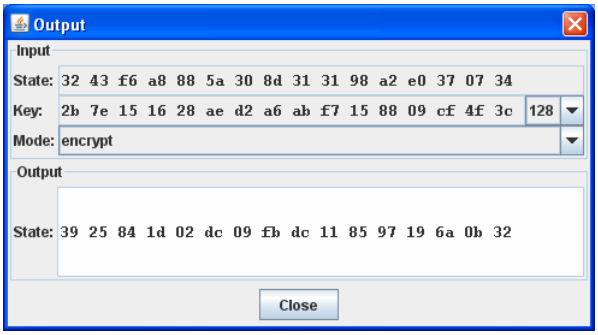

Abb. 3: Ausgabefenster

4 Programmstart und Simulation

Beim Start des Programms wird das Eingabefenster angezeigt. Es kann nun wahlweise, wie in Kapitel 3.2 beschrieben, eine Startkonfiguration eingegeben oder aus einer Datei geladen werden.

Anschließend kann die Simulation gestartet werden. Hierzu stehen die Schaltflächen am unteren Rand des Hauptfensters zur Verfügung. Siehe hierzu Abbildung 2.

Durch betätigen der Schaltfläche „Instruction >“ kann die aktuelle Anweisung mit zugehöriger Animation ausgeführt werden.

Der „Step >“ - Button ermöglicht das schrittweise Visualisieren der einzelnen Schritte einer Anweisung. Bei jedem Betätigen wird ein Schritt abgearbeitet.

Wird der „Program >“ - Button gedrückt, läuft die Simulation unter dazu passender Animation bis zum Ende ab.

Eine laufende Animation, die durch „Instruction >“ oder „Program >“ gestartet wurde, kann durch die Schaltfläche „Stop“ angehalten werden. Ein Fortsetzen ist dann mit Hilfe der Funktionen „Step“, „Instruction“ und „Program“ möglich.

Die Simulation kann zurückgesetzt werden, indem der „Reset“ – Button betätigt wird. Dies führt dazu dass die Startzustände wiederhergestellt und die Ausführung auf die erste Anweisung zurückgeführt wird.

Um die Animation von Simulationsschritten zu überspringen können die Schaltflächen „Instruction >>“ und „Program >>“ genutzt werden. Die Arbeitsweise ähnelt der der „Instruction >“ und „Program >“ Buttons, jedoch werden die Wartezyklen in den Animationen unterdrückt.

Nach Ablauf des Simulationsprogramms wird das Ausgabefenster angezeigt. Das Ergebnis der Ver- resp. Entschlüsselung kann dann im Bereich „Output“ abgelesen werden.

5 Speichern und Laden

Über die Menüeinträge „Save“ und „Open“ im Hauptfenster sowie die Schaltfläche „Load from file“ im Eingabefenster wird ein Speichern und Laden der Startzustände sowie des Betriebsmodus ermöglicht. Nach Betätigung erscheint ein Dateidialog. (siehe hierzu Abbildung 4) Nach Bestätigen der Dateieingabe wird der Dialog geschlossen und das Speichern resp. Laden durchgeführt.

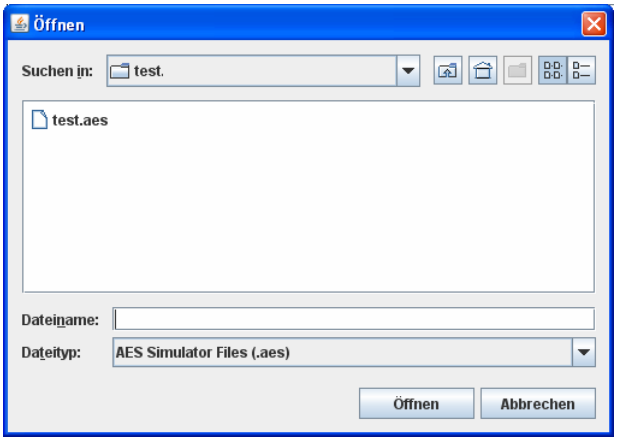

Abb. 4: „Öffnen“-Dialog

6 Einstellungen

Im „View“ – Menü stehen zwei Einstellungen zum Anzeigeformat zur Verfügungen. Es können Zeichensatzgröße und Anzeigeformat umgestellt werden.

6.1 Zeichensatzgröße

Der Dialog zur Änderung der Zeichensatzgröße kann über den Menüpunkt „View“ – „Font Size“ aufgerufen werden. Es erscheint das in Abbildung 5 abgebildete Eingabefenster. Die eingegebene Zeichensatzgröße muss zwischen 3 und 16 liegen.

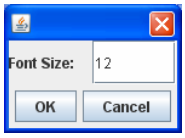

Abb. 5: Dialog Zeichensatzgröße

6.2 Zahlenformat

Im „View“ – Menü kann über die Menüpunkte „HEX“ und „Decimal“ zwischen hexadezimaler und dezimaler Anzeigeform gewählt werden.

7 Sonderfunktionen

Über das „View“ – Menü können zwei zusätzliche Fenster (Die S-Box Matrix und ein GF(256) Multiplikationsrechner) eingeblendet werden.

7.1 Anzeigen der S-Box

Über den Menüeintrag „View“ – „ByteSub Matrix (S-Box)“ kann die S-Box angezeigt werden. Hierzu öffnet sich das in Abbildung 6 dargestellte Fenster.

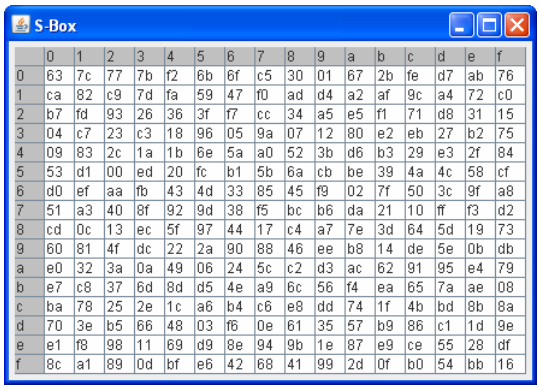

Abb. 6: S-Box Fenster

7.2 Multiplikation in GF(256)

Der Multiplikationsrechner lässt sich über den Menüeintrag „View“ – „GF(256) Multiplikator“ öffnen. Die Eingabe erfolgt über die zwei dafür vorgesehenen Felder. Nach Betätigen des „Calculate“ – Buttons wird das Produkt im Ausgabefeld angezeigt. Alle Ein- und Ausgaben erfolgen in zweistelliger hexadezimaler Form.

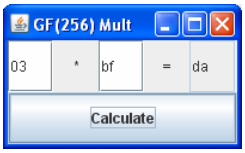

Abb. 7: GF(256) Multiplikation

8 Anhang

8.1 Links

[L01] http://java.sun.com/javase/downloads/index.jsp, Java SE Downloads