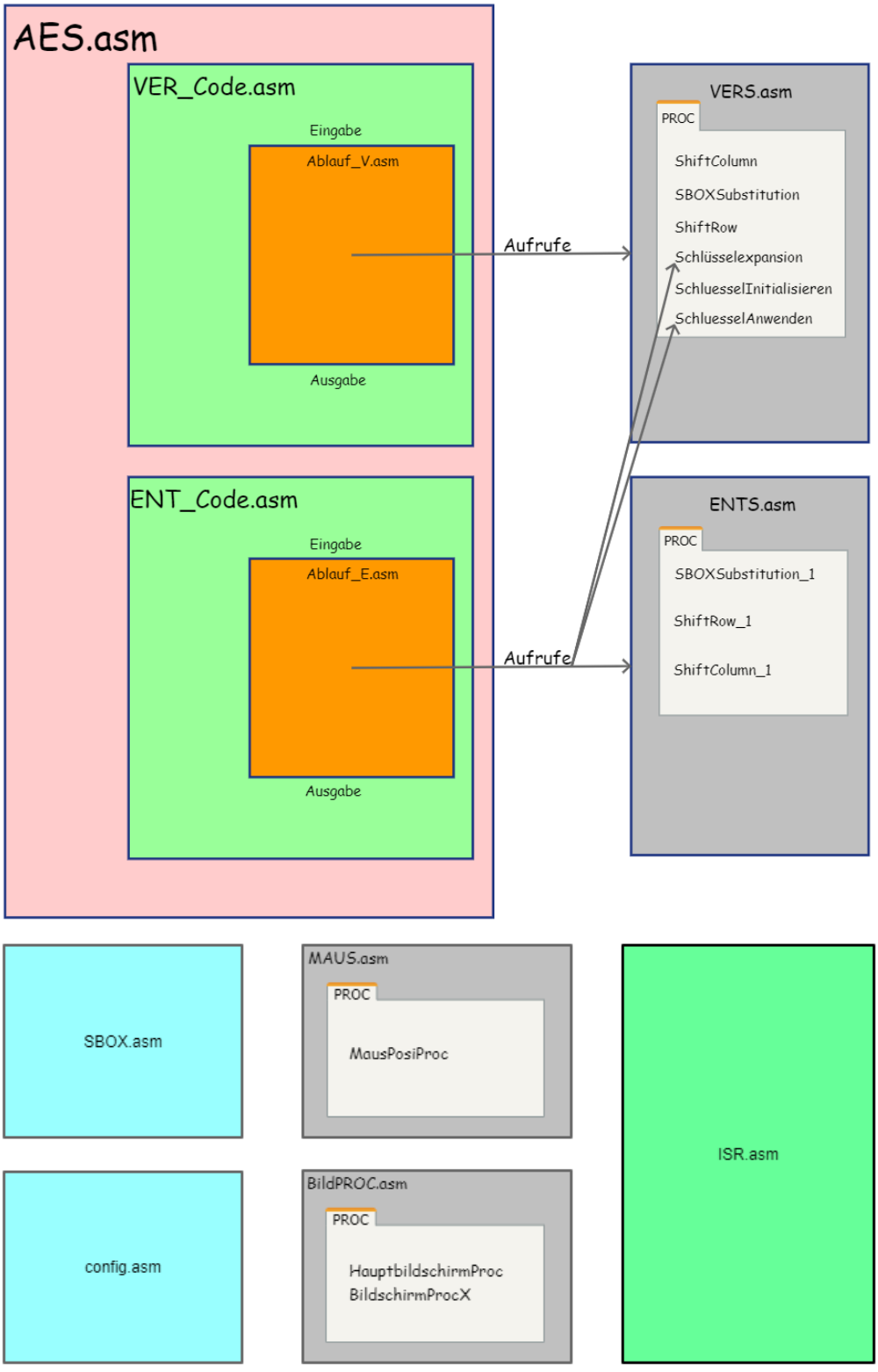
AES

-

Abschlussprojekt Modul „Assemblerprogrammierung“

von Konstantin Blechschmidt & Tim M. Kretzschmar



Unser Programm kann ich 2 Hauptbereiche mit je 2 Unterbereichen aufgeteilt werden.

I. Verschlüsselung

a) graphische Ein/Ausgabe Klartext und Ausgabe des Chiffretextes im Bildschirm + Schlüssel

b) Abarbeitung der Verschlüsselung unter Hilfenahme der PROC`s aus der VERS.asm

II. Entschlüsselung

c) graphische Ein/Ausgabe Chiffretext und Ausgabe des Klartextes im Bildschirm + Schlüssel

d) Abarbeitung der Entschlüsselung unter Hilfenahme der PROC`s aus der ENTS.asm und teilweise VERS.asm

Jede PROC und Programmteil ist im Kopfbereich der ASM Datei und Handbuch näher beschrieben.

Eine möglichst klare Erläuterung der jeweiligen Befehlszeilen befindet sich ebenfalls in den ASM-Dateien als Kommentar.

Leider können wir die echte Version von AES nicht vorzeigen, da es uns nicht möglich war, die inverse ShiftColumn zu implementieren. Die Verrechnung mit der inversen C-Matrix aus E, D, B, 9 (alles hexadezimale Werte) haben wir programmiert, aber das Ergebnis war nach mehreren Versuchen immer noch falsch leider.

Aus diesem Grund befindet sich unter dem Quelltext von der Ablauf_E.asm und Ablauf_V.asm der auskommentierte Code, der für den Ablauf nach AES-Standard vorgesehen wäre. Der nicht auskommentierte Code drüber soll die verfügbaren und nutzbaren Aspekte von AES anwenden, also dem Nutzer eine Verschlüsselung bieten, die AES-ähnlich ist.

Die schon kompilierte AES.EXE beinhaltet diese AES-ähnliche Umsetzung.

Bezüglich der Variablen, existieren die *config.asm* und *SBOX.asm*. Dort kann in den Kommentaren Näheres zu deren Einsatz erfahren, sowie eine Übersicht im Handbuch unter dem entsprechenden Absatz eingesehen werden.