

AES

-

Abschlussprojekt Modul „Assemblerprogrammierung“

von Konstantin Blechschmidt & Tim M. Kretzschmar

Daten:

TASM; Prozessor .486 ; DOS-Box Version 0.74

Was geht

Grafik

Mausklicken um Modi zu wechseln

Eingabe/Ausgabe (Klartext (ASCII) und Hexadezimal)

Beenden über „ESC“ aus dem Hauptmenü heraus

Schlüsselexpansion & Schlüssel anwenden

SBOX-Substitution & inverse Version

ShiftRow & die inverse Version

ShiftColumn

Kompilieren, Debugger starten und einfaches starten per Batch-Datei

Was geht nicht

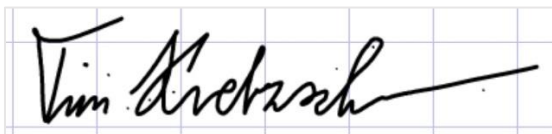
Inverses ShiftColumn (haben wir leider nicht zum Laufen bekommen...)

mgl. Quelle:

<https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf>

Eidesstattliche Erklärung:

Hiermit bestätigen wir, Konstantin Blechschmidt & Tim M. Kretzschmar, dass wir dieses Programm „AES – in TASM umgesetzt“ selbstständig und nur unter Angabe der genutzten Quellen erstellt und getestet haben.



Tim M. Kretzschmar (Wermsdorf, 03.08.2021)



Konstantin Blechschmidt (Schkeuditz, 03.08.2021)