

Computerpraktikum: Aufgabenblatt 4

- C.1** Testen Sie eine von Ihnen ausgewählte verfügbare AES-Implementierung mit den Referenzdaten des AES-256 aus dem Standard FIPS-197 (Stand: 26.11.2001), Appendix C.3, wovon die Eingangsdaten und der AES-Schlüssel hier noch einmal wiedergegeben sind:

Input = 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

Cipher Key = 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

Hinweis: Es soll getestet werden, ob die ausgewählte AES-Implementierung das AES-Chifftrat (“round[14].output” in FIPS-197, Appendix C.3, Seite 43) korrekt berechnet. Auf korrekte AES-256-Zwischenergebnisse braucht nicht getestet zu werden. Den hier referenzierten FIPS-197 Standard finden Sie auch im LEA-Kurs. Dieser Testvektor ist im überarbeiteten FIPS-197 Standard vom 9.5.2023 nicht mehr enthalten.

- C.2** In LEA finden Sie eine Binärdatei “chifftrat.jpg”, die mit einem AES-256 Schlüssel im Counter-Modus (CTR Modus) verschlüsselt worden ist. Konkret verwendet wurden der AES-256 Schlüssel

Key = FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

und der initiale Zähler

Counter = XX XX AA AA AA AA AA AA AA AA AA AA AA AA AA AA.

Die ersten zwei Bytes XX vom initialen Counter sind leider nicht mehr auffindbar.

- Schreiben Sie ein Programm mit Ihrer unter C.1 ausgewählten AES-256-Implementierung, um die fehlenden Bytes des Counters in Erfahrung zu bringen. Sie können davon ausgehen, dass die Klartextdatei eine jpg-Datei ist.
- Welchen Durchsatz – gemessen in Anzahl von AES-256 Operationen pro Sekunde – erreichen Sie mit Ihrer Implementierung?

Hinweise:

- Testvektoren für den AES-256 im Counter-Modus finden Sie unter https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/examples/AES_CTR.pdf. Dieses Dokument ist auch im LEA-Kurs.