PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *12.05.2025*
***Abgabe**: bis FR 09.05. 17:00 an uhl@cs.sbg.ac.at*

24.) Zum CBC Betriebsmodus von Blockciphern: Erklären sie, (i) warum die angegebene Entschlüsselungsformel tatsächlich funktioniert, (ii) wie es zu den beschriebenen Plaintextfehlern nach dem Auftreten eines 1-Bit Ciphertextfehler kommt und (iii) warum CBC self-recovering ist.

25.) Implementieren sie (natürlich unter zu-Hilfenahme einer AES realisierenden Library) ECM und CBC unter AES selbst und bestätigen sie experimentell das beschriebene Verhalten von CBC bei Ciphertextfehlern. Vergleichen sie weiters ihre ECM und CBC Varianten mit den Varianten die die Library zur Verfügung stellt bzgl. der benötigten Rechenzeit.

26.) Implementieren sie (natürlich unter zu-Hilfenahme einer AES realisierenden Library) zusätzlich OFB, CFB und CTR selbst und führen sie Experimente zum Laufzeitverhalten aller fünf Modi durch (wieder bzgl. des Vergleichs von Laufzeitverhalten ihrer Versionen mit den zur Verfügung gestellten). Variieren sie insbesondere für CFB die Menge der aus der verschlüsselten Queue entnommenen bits pro Verschlüsselungsvorgang des Blockciphers (ich habe darauf in der VO bereits hingewiesen).

VIEL ERFOLG !!