UNIVERSIDADE
FEDERAL DO CEARÁ

Dupla: João Paulo de Araújo e Marcus Vinícius Martins Melo.

RELATÓRIO DO TRABALHO PRÁTICO ‘2’ DA DISCIPLINA DE CRIPTOGRAFIA

O trabalho consiste em implementar os modos de operação do algoritmo ***Advanced Encryption Standard***, (AES, ou Padrão de Criptografia Avançada, em português), CBC (Cypher Block Chaining - Criptografia de Blocos Encadeados) e CTR (Counter - Modo de Contador).

O modo de operação CBC, desenvolvido na linguagem C, é totalmente automatizado, sem a intervenção humana em seu funcionamento. O mesmo funciona realizando a expansão da chave, esta passada como parâmetro para o método, e o arquivo que se deseja encriptar. Como o CBC é similar ao ECB(***Eletronic Code Book***), já implementado como exemplo, as dificuldades em relação a implementação do mesmo não foram significativas. Por outro lado, o CTR, por necessitar de um número totalmente aleatório, que tem como propósito realizar a “confusão” no processo, impôs um grau de dificuldade mais elevado. Para contornar o problema, foi necessário inicializar o contador presente no modo, o que pode ocasionar problemas que podem facilitar ataques no corrente modo de operação. Porém, mesmo com as dificuldades expostas anteriormente, os graus de conhecimento adquirido com a elaboração do trabalho foram bastante significativos, enriquecendo a base de conhecimento em relação a aos modos de operação.