CIC0201 - Segurança Computacional – 2023/2

Prof. João Gondim

Trabalho de Implementação 2 - Cifra de bloco e modo de operação CTR

Este trabalho explora a cifra de bloco AES e o modo de operação CTR (contador), tendo três partes: implementação da cifra, do modo de operação e teste.

https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard)

- Parte I: implementação do AES (bloco= 128 bits, chave 128 bits)

A cifra AES deve ser implementada (cifração e decifração) de forma a ser possível especificar o número de rodadas que se deseja executar. Assim, deve-se implementar a rodada básica da cifra e também as manipulações específicas das rodadas inicial e final.

- Parte II: implementação do modo de operação CTR

O modo CTR deve ser implementado para a cifra AES conforme especificada acima.

- Extra 1: Implemente o modo de cifração autenticada GCM - contador de Galois

Para checar a corretude da implementação, pode-se usar o openssl – apenas para verificação.

- **Testes**

O trabalho deve ser testado conforme segue: 0) cifre e decifre um arquivo

Extra 2:

1) tire uma selfie

2) cifre a selfie no modo CTR com 1, 5, 9 e 13 rodadas do AES implementado na parte 1. Renderize os resultados de cada execução e anexe ao relatório as imagens indicando o número de rodadas.

O que deve ser entregue:

- Relatório com:
  - descrição da cifra e do modo implementado
  - descrição da sua implementação da cifra e do modo
  - selfie e resultados dos Testes
- o código fonte

Observações:

1. Não é permitida na implementação a utilização de bibliotecas públicas, como OpenSSL, para primitivas criptográficas de cifração e decifração simétrica, e geração de chaves.
2. A pontuação máxima será conferida os trabalhos que realmente implementarem as duas partes e os testes, além de entregar o relatório (2-4 pg).
3. A avaliação será mediante apreciação do relatório, da execução das funcionalidades e inspeção do código. Se necessário, serão agendadas apresentações para esclarecimentos.
4. Implementação preferencialmente individual, podendo ser em dupla, em C, C++, Java e Python.

Data de Entrega: 30/10/2023, as instruções para envio seguirão oportunamente.