CIC0201 - Segurança Computacional – 2021/1

Prof. João Gondim – Monitor: Gutemberg

Trabalho de Implementação 2

Cifra de bloco e modos de operação

Este trabalho explora a cifra de bloco AES e os modos de operação ECB e CTR (contador), tendo três partes: implementação da cifra, dos modos de operação e teste.

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

- Parte I: implementação do AES

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 dos modos de operação ECB e CNT

Os modos ECB e CNT devem ser implementados para a cifra AES conforme especificada acima.

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

- **Testes**

O trabalho deve ser testado conforme segue:

1) tire uma selfie

2) cifre a selfie no modo ECB com 1, 5, 9 e 13 rodadas do AES implementado na parte 1. Renderize os resultados de cada execução e gere o hash correspondente.

3) repita 2) para o modo CTR

O que deve ser entregue:

- Relatório com:
  - descrição da cifra e dos modos implementados
  - descrição da sua implementação da cifra e dos modos
  - selfie e resultados dos Testes
- o código fonte e seu executável

Observações:

1. Não é permitida na implementação a utilização de bibliotecas públicas, como OpenSSL, para primitivas de criptográficas de cifração e decifração (as)simétrica, e geração de chaves.
2. A pontuação máxima será conferida os trabalhos que realmente implementarem as duas partes e os testes, e entregar o relatório.
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.
5. Linguagens preferenciais C, C++, Java e Python.

Data de Entrega: 15/09/2021, por email até 23:59h.