Trabalho - Sistemas Criptográficos

Objetivo: Adquirir conhecimento teórico-prático sobre os diversos sistemas que utilizam criptografia através de uma pesquisa bibliográfica e implementação do sistema criptográfico.

Requisitos: 1) Realizar uma pesquisa bibliográfica que aborde os seguintes assuntos:

- Introdução: Contextualização, problema e objetivo ou ideia principal do sistema criptográfico
- Fundamentação teórica:
  - Conceitos básicos (conceitos matemáticos necessários ao entendimento dos cálculos de cifragem).
  - Estrutura, tamanho de bloco, geração de chaves, número de rotações.
  - História (incluindo a(s) RFC's que padronizam o sistema)
  - Exemplo(s) de aplicação(ões) que utilizam o sistema criptográfico
- Criptoanálise: tipos de ataques que o sistema pode sofrer e/ou relatos de quebra do sistema.
- Materiais e métodos
  - Hadware/Software/Ferramenta utilizadas.
  - Exemplo(s) ilustrativos do funcionamento.
- Considerações Finais
- Referências Bibliográficas utilizadas

2) Documentar a pesquisa e formato de artigo modelo SBC entre 5 e 6 páginas no máximo.

3) Implementar uma aplicação do sistema criptográfico em Linguagem Java
O código deve ser comentado e o funcionamento do sistema (os pacotes em Java utilizados que contém os cálculos do sistema criptográfico devem ser mostrados e explicados).

Forma de entrega: Pelo sistema acadêmico

- Artigo
- Arquivos compactados (projeto e executável) da aplicação.

Grupos: 3 alunos no máximo.

Data da entrega 25/06/2019 até às 12:00h e apresentação (de 15 minutos max.):

25/06/2019

- 3DES (Vinicius 2x, Igor)
- AES (Rafaela, Suela e Ana Paula Cunha)
- Blowfish (Julio, Augusto e Renato)
- RC5 (Pedro, Tales e Lucas)
- RSA (Elias, Maria Eduarda e Rodrigo Souza)
- Skipjack (Rodrigo Cesar, Bruna e Luis)

27/06/2019

- EL Gamal (Saulo, Rodrigo e Fernanda)
- ECC (Elliptic Curve Cryptography) (Flavia, Luis Eduardo, Luis Nogueira)
- Argon2: https://tools.ietf.org/html/draft-josefsson-argon2 (Italo e Mateus)
- Blake2: https://tools.ietf.org/html/rfc7693 (Nara, Patrícia e Ana Laura)
- IDEA (Ana Paula, Jonatan e Kimberly)

Avaliação: Domínio do tema durante a apresentação;
Qualidade do artigo: formatação, objetividade e clareza;
Atendimento aos requisitos e a forma de entrega.

Considerações Finais:

Este é um trabalho que envolve programação, portanto aqueles que possuem dificuldades, devem estudar o assunto procurando livros, tutoriais e outros materiais que complementem sua deficiência em programação por conta própria; Trabalhos plagiados ou feitos por terceiros valerão zero.