ENE0090 - Segurança de Redes – 2024.2

Prof. João Gondim

Trabalho de Implementação 1

Cifra de Vigenère

Este trabalho explora a cifra de Vigenère, tendo duas partes: o cifrado/decifrador e o ataque de recuperação de senha por análise de frequência.

- Parte I: cifrador/decifrador

O cifrador recebe uma senha e uma mensagem que é cifrada segundo a cifra de Vigenère, gerando um criptograma, enquanto o decifrador recebe uma senha e um criptograma que é decifrado segundo a cifra de Vigenère, recuperando uma mensagem.

- Parte II: ataque de recuperação de senha por análise de frequência

Serão fornecidas duas mensagens cifradas (uma em português e outra em inglês) com senhas diferentes. Cada uma das mensagens deve ser utilizada para recuperar a senha geradora do keystream usado na cifração e então decifradas.

Para as frequências das letras use: https://pt.wikipedia.org/wiki/Frequ%C3%AAncia_de_letras

Observações:

1. Não é permitida a utilização de bibliotecas públicas, como OpenSSL, para primitivas de criptográficas de cifração e decifração assimétrica, e geração de chaves.
2. A pontuação máxima será auferida os trabalhos que realmente implementarem as duas partes
3. A avaliação será mediante apresentação do trabalho, com a verificação das funcionalidades e inspeção do código.
4. Implementação preferencialmente individual, podendo ser em dupla.
5. Linguagens preferenciais C, C++, Java e Python.

O que deve ser entregue: git com o código fonte e seu executável (se for o caso), descritivo (4 pg max) da cifra com sua implementação e do ataque e sua implementação.

Data de Entrega: 04/11/2024 - envio do link do git ou zip com os arquivos.

Apresentações: a partir de 04/11/2024