Curso de Extensão em Tecnologias Microsoft

INF0998 Programação segura (segurança de software)

Atividades práticas de criptografia aplicada

As seguintes ferramentas são usadas ao longo das tarefas:

- Cryptool Online https://www.cryptool.org/en/cto
- Cryptool para Windows https://www.cryptool.org/en/ct1
- JCryptool https://www.cryptool.org/en/jct/
- OpenPGP, GPG4win e Kleopatra https://www.openpgp.org/software
- OpenSSL (Usar o openssl da sua distribuição Linux preferida)

Atividades com CrypTool Online

Cifra de César

Acessar o site https://www.cryptool.org/en/cto/caesar.

Teste da cifra de César clássica

Na página indicada, realizar as seguintes tarefas.

- Digitar na caixa de texto Plaintext: “Teste de Cesar”.
- Ajustar a Chave (controle Key) para 3.
- Verificar o deslocamento resultante no alfabeto do Ciphertext.
- Visualizar na caixa de texto Ciphertext: “WHVWH GH FHVDU”.

Teste de outra cifra de César com deslocamento de um

A cifra de César é, na verdade, uma família de cifras de deslocamento simples. Esta atividade usa outro deslocamento.

- Ajustar a chave para 1.
- Verificar o deslocamento resultante no alfabeto do Ciphertext.
- Visualizar na caixa de texto Ciphertext: “UFTUF EF DFTBS”.

A cifra ROT13

Ainda na página indicada, realizar as tarefas.

- Ajustar a chave para ROT 13.
- Verificar o deslocamento resultante no alfabeto do Ciphertext.
- Visualizar na caixa de texto Ciphertext: “GRFGR QR PRFNE”.

Cifra de Vinegère

Realizar as seguintes tarefas para a cifra de Vigenere.

- Acessar o site https://www.cryptool.org/en/cto/vigenere.
- Digitar na caixa de texto Plaintext: “Teste de Vigenere”.
- Ajustar a Chave no campo de texto ke para “chave”
- Visualizar na caixa de texto Ciphertext: “Vlsoi fl Vdkguemi”.

Simulador da máquina Enigma

A máquina Enigma é um dispositivo eletromecânico de encriptação e decriptação usado durante a segunda guerra mundial.

Esta é a aparência da Enigma (vide imagem no link):

https://s2.glbimg.com/TWCzUx2XAQ7deE24oL11dyMP_u0=/e.glbimg.com/og/ed/f/original/2019/08/30/69714272_1347536952068161_513362189462011904_n.jpg

A máquina Enigma é um dispositivo eletromecânico de encriptação e decriptação usado durante a segunda guerra mundial. Esta atividade consiste em usar um simulador na máquina Enigma, que está disponível online no website da ferramenta CrypTool, no link: https://www.cryptool.org/en/cryptool-online.

Acessar o menu *Ciphers → Enigma (Step-by-Step),* ou acessar diretamente pelo link https://www.cryptool.org/en/cto/enigma-step-by-step.

São cinco seções da Enigma:

1. *Configuration* define os rotores;
2. *Key* define a chave;
3. *Input* é o texto claro de entrada;
4. *Encoding/Decoding Rounds* mostra as rodadas de encriptação/decriptação;
5. *Encoded* é a saída.

Entrar com texto claro “teste” e a chave “abc”, na configuração padrão, a encriptação é HVMSO. Experimentar livremente a simulação.

O algoritmo AES passo a passo

Esta atividade prática proporciona a visualização do funcionamento interno do algoritmo AES, passo-a-passo.

Acessar o site *https://www.cryptool.org/en/cto/aes-step-by-step.*

Na guia *Cipher*, fazer o seguinte.

- No campo *Configuration,* digitar uma chave hexadecimal de 16, 24 ou 32 bytes;
    - Por exemplo, uma chave de 128 bits (16 bytes) é 00112233445566778899aabbccddeeff;
- No campo *Input*, digitar uma sequência 16 bytes em hexadecimal como texto claro;
- No quadro *Encoding Rounds*, analisar os resultados das operações da rodada do AES para cada round (10, 12 ou 14);
- No campo *Encoded*, verificar o resultado da encriptação;
- No quadro *Decoding Rounds*, analisar os resultados da decriptação em cada rodada do AES;
- No campo Decoded, verificar o resultado da decriptação.

Uma animação do funcionamento do AES pode ser visualizada neste link https://www.cryptool.org/en/cto/aes-animation.

O algoritmo RSA passo a passo

Prática de uso do algoritmo RSA e visualização do funcionamento do RSA passo-a-passo.

Acessar o site https://www.cryptool.org/en/cto/rsa-step-by-step.

Na guia *Cipher*, fazer o seguinte.

- No quadro *Prime factors*, preencher com números primos os campos *1st prime p, 2nd prime q.*
    - Por exemplo, usar números primos pequenos de 2 dígitos;
    - Ver o resultado do cálculo do módulo *n = p*q;*
- No quadro *Public key*, escolher o valor da chave de encriptação *e;*
- No quadro *Secret key*, observar os valores calculados para *phi(n)*, *gcd(e,phi(n))* e para a chave de decriptação *d;*
- No quadro *Messages*
    - Digitar um número grande de 5 dígitos. Observar a mensagem de erros emitida. Se a mensagem for longa demais, a aplicação emitirá a mensagem de erro, por causa das restrições de tamanho do RSA. A mensagem dirá qual o limite de tamanho.
    - Digitar um número / mensagem menor que o limite indicado.
    - Visualizar o criptograma gerado.

Segurança de senhas

Análise de segurança de senhas para uso em mecanismos *Password-based Encryption (PBE).* A derivação de chaves criptográficas a partir de senhas para encriptação de outras chaves criptográficas é uma técnica comum de guarda segura de chaves armazenadas em arquivos.

Password Meter

Análise de segurança de senhas para uso em mecanismos *Password-based Encryption (PBE)* com a ferramenta CrypTool Online.

Acessar o site https://www.cryptool.org/en/cto/password-meter.

Digitar uma senha qualquer no campo *Password Meter.*

Ver a segurança da senha no quadro *Rating.*

- O quadro apresenta várias métricas e um valor total.
- A segurança é indicada qualitativamente em um código de cores.

Ver o resultado da análise no quadro *Details via zxcvbn.*

- Observar o tempo estimado para quebra da senha com ataques online e offline.
- Ver as observações e recomendações.
    - Ver o resultado da análise no quadro *Details via Stutz' Password-Score.*
- Observar o tempo estimado para quebra da senha;
- Observar a entropia da senha e outras informações.

Password Checker

Acessar o site https://www.cryptool.org/en/cto/password-check.

Digitar uma senha no campo *Password.*

- Observar o score da complexidade.
- Analisar as outras informações de segurança sobre a senha.

No final da página há uma legenda para os rótulos e classificações usados pela aplicação.

Password Generator

Acessar o site https://www.cryptool.org/en/cto/password-generator.

Selecionar as opções da política de geração de senha (*Lowercase characters, Uppercase characters, Numbers, Special characters, Hex characters only*).

- Fornecer o tamanho da senha a ser gerada.
- Clicar o botão *Generate Password*. A senha será gerada.
- Usar a senha nos testes anteriores e analisar os resultados.