Atividade da classe - Criando códigos

# Objetivos

Neste laboratório, você criará e criptografará mensagens usando ferramentas online.

Parte 1: Procure uma ferramenta online de codificação e decodificação.

Parte 2: Criptografar uma mensagem e enviá-la por e-mail para seu parceiro de laboratório.

Parte 3: descriptografar o texto cifrado.

# Histórico/Cenário

Códigos secretos foram usados há milhares de anos. Gregos antigos e espartanos usavam uma foice (rima com a Itália) para codificar mensagens. Romanos usaram uma cifra de César para criptografar mensagens. Há algumas centenas de anos, os franceses usaram a cifra de Vigenère para codificar mensagens. Hoje, existem muitas maneiras pelas quais as mensagens podem ser codificadas.

Existem vários algoritmos de criptografia que podem ser usados para criptografar e descriptografar mensagens. As Redes Privadas Virtuais (VPNs) são comumente usadas para automatizar o processo de criptografia e descriptografia.

Neste laboratório, você e um parceiro de laboratório usarão uma ferramenta on-line para criptografar e descriptografar mensagens.

# Recursos necessários

* PC com acesso à Internet

# Instruções

## Procure uma ferramenta de codificação e decodificação online.

Existem muitos tipos diferentes de algoritmos de criptografia usados em redes modernas. Um dos mais seguros é o algoritmo de criptografia simétrica Advanced Encryption Standard (AES). Vamos usar este algoritmo em nossa demonstração.

* + 1. Em um navegador da Web, pesquise **criptografar AES on-line**. Várias ferramentas diferentes serão listadas nos resultados da pesquisa.
    2. Explore os diferentes links fornecidos e escolha uma ferramenta. No nosso exemplo, usamos a ferramenta disponível em:

<http://aesencryption.net/>

## Criptografe uma mensagem e envie-a por e-mail para o seu parceiro de laboratório.

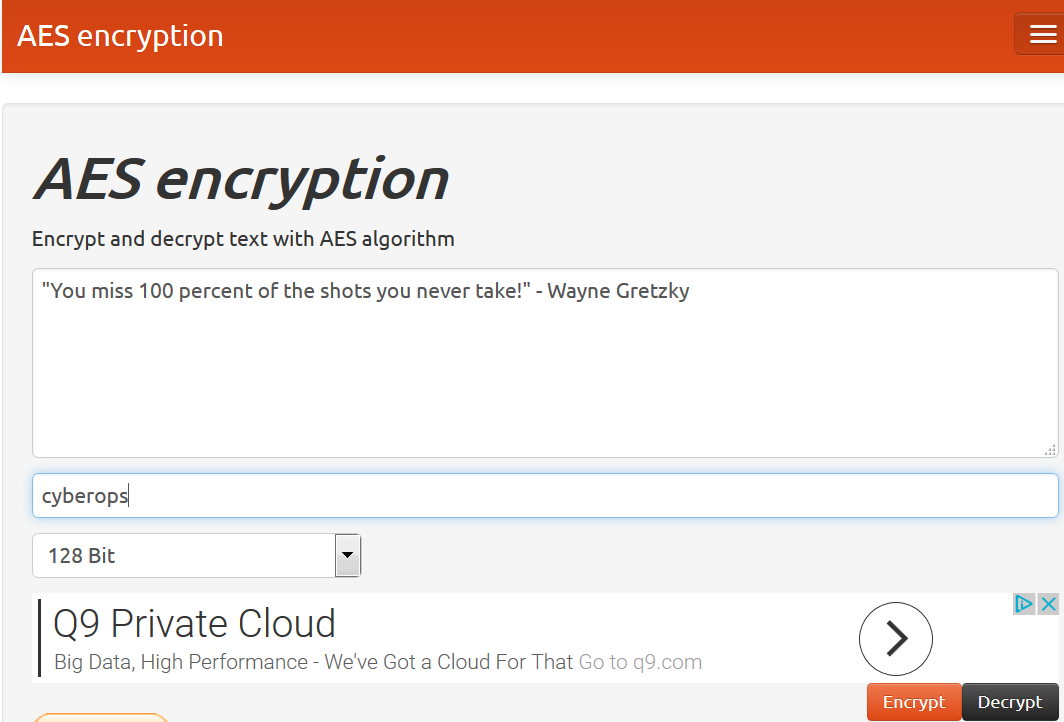
Nesta etapa, cada parceiro de laboratório criptografará uma mensagem e enviará o texto criptografado para o outro parceiro de laboratório.

**Observação:** As mensagens não criptografadas são chamadas de texto simples, enquanto as mensagens criptografadas são chamadas de texto cifrado.

* + 1. Insira uma mensagem de texto simples de sua escolha na caixa de texto. A mensagem pode ser muito curta ou longa. Certifique-se de que seu parceiro de laboratório não veja a mensagem de texto simples.

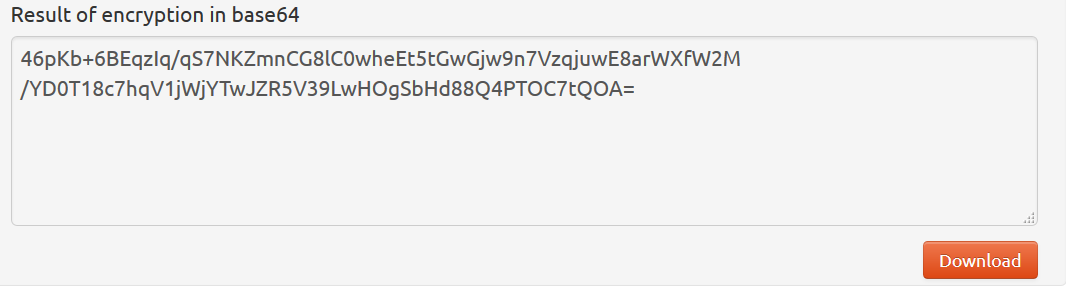
Uma chave secreta (ou seja, senha) geralmente é necessária para criptografar uma mensagem. A chave secreta é usada junto com o algoritmo de criptografia para criptografar a mensagem. Só alguém com conhecimento da chave secreta seria capaz de decifrar a mensagem.

* + 1. Digite uma chave secreta. Algumas ferramentas podem solicitar que você confirme a senha. No nosso exemplo, usamos a chave secreta do **cyberops**.



* + 1. Em seguida, clique em **Criptografar**.

Na janela Resultado da criptografia em base64, texto aleatório é exibido. Esta é então uma mensagem criptografada.

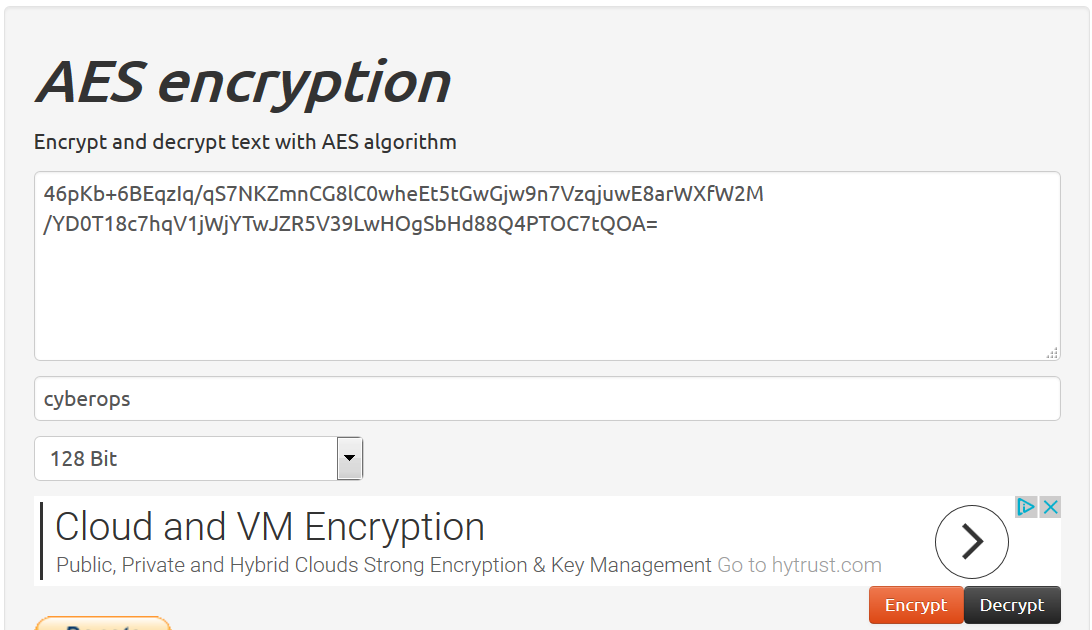


* + 1. Copie ou baixe a mensagem resultante.
    2. Envie a mensagem criptografada para seu parceiro de laboratório.

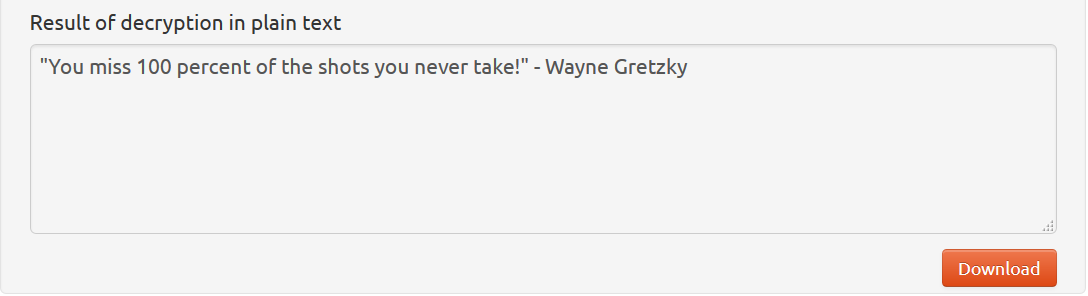
## Descriptografar o texto cifrado.

O AES é um algoritmo de criptografia simétrica Isso significa que as duas partes que trocam mensagens criptografadas devem compartilhar a chave secreta com antecedência.

* + 1. Abra o e-mail do seu parceiro de laboratório.
    2. Copie o texto cifrado e cole-o na caixa de texto.
    3. Insira a chave secreta pré-compartilhada.



* + 1. Clique em **Descriptografar** e a mensagem de texto não criptografado original deve ser exibida.



### Pergunta:

O que acontece se você usar uma chave secreta errada?

Digite suas respostas aqui.

Fim do documento