

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

Parte 1: 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.

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

<http://aesencryption.net/>

Parte 2: 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.

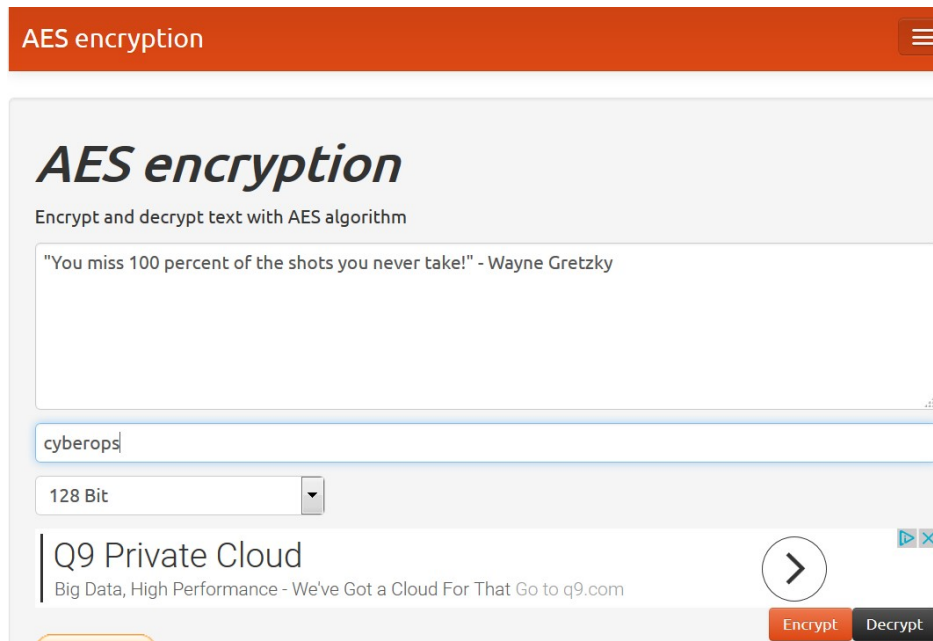
Observação: As mensagens não criptografadas são chamadas de texto simples, enquanto as mensagens criptografadas são chamadas de texto cifrado.

- 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.

Atividade da classe - Criando códigos

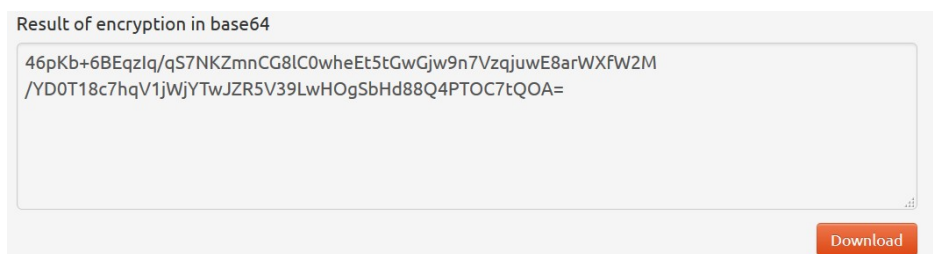
Uma chave secreta (ou seja, senha) geralmente é necessária para criptografar uma mensagem. A chave secreta é usada junto com o algoritmo de criptografia para criptografar a mensagem. Só alguém com conhecimento da chave secreta seria capaz de decifrar a mensagem.

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



- c. Em seguida, clique em **Criptografar**.

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



- d. Copie ou baixe a mensagem resultante.
- e. Envie a mensagem criptografada para seu parceiro de laboratório.

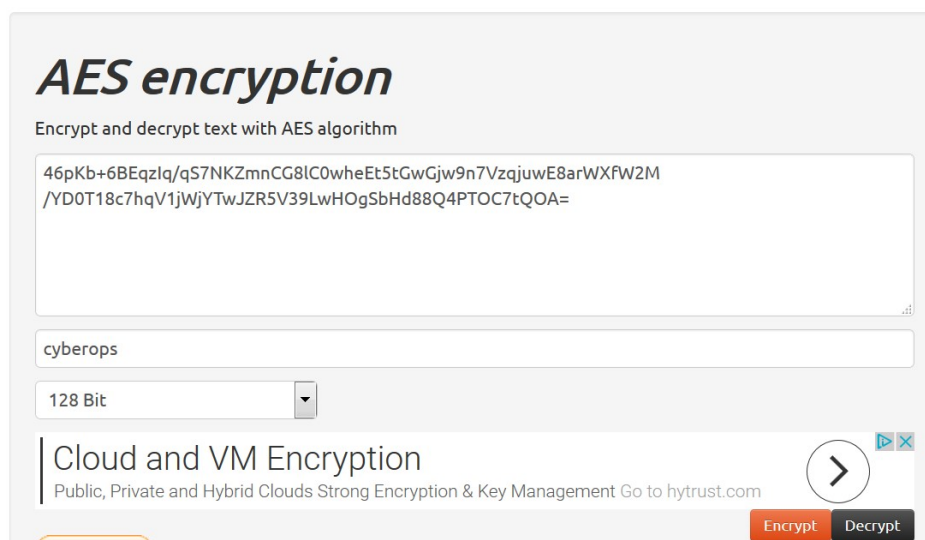
Parte 3: Descriptografar o texto cifrado.

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.

- a. Abra o e-mail do seu parceiro de laboratório.
- b. Copie o texto cifrado e cole-o na caixa de texto.

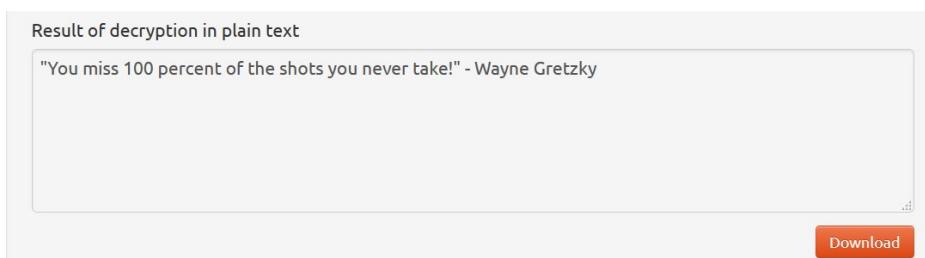
Atividade da classe - Criando códigos

- c. Insira a chave secreta pré-compartilhada.



The screenshot shows a web interface titled "AES encryption" with the subtitle "Encrypt and decrypt text with AES algorithm". It features a large text area containing a long alphanumeric string: "46pKb+6BEqzIq/qS7NKZmnCG8lC0wheEt5tGwGjw9n7VzqjuwE8arWXPW2M/YD0T18c7hqV1jWjYTwJZR5V39LwHOGSbHd88Q4PTOC7tQOA=". Below this is a text input field with the word "cyberops". A dropdown menu is set to "128 Bit". At the bottom, there is a navigation bar with the text "Cloud and VM Encryption" and "Public, Private and Hybrid Clouds Strong Encryption & Key Management Go to hytrust.com". On the right side of the navigation bar, there is a circular arrow icon and two buttons labeled "Encrypt" and "Decrypt".

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



The screenshot shows the result of the decryption process. It features a text area with the message: "You miss 100 percent of the shots you never take!" - Wayne Gretzky. Below the text area is a button labeled "Download".

O que acontece se você usar uma chave secreta errada?