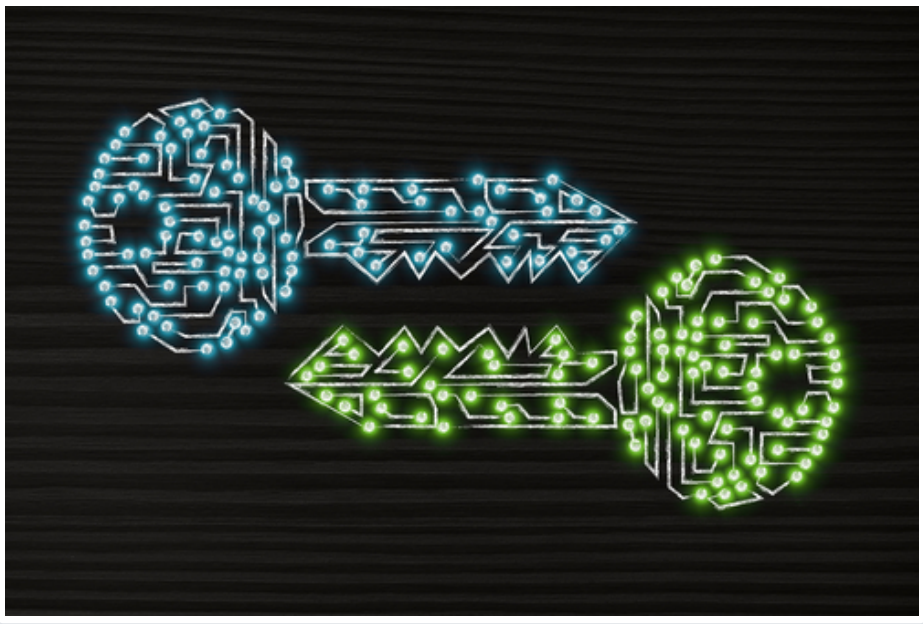
CRIPTOGRAFIA

Nesta webaula vamos apresentar a abrangência tecnológica da criptografia e mostrar a aplicação de algoritmos de criptografia.

A CRIPTOGRAFIA FAZ PARTE DO DIA A DIA DE TODOS

Os dados de seu dispositivo móvel são armazenados com criptografia; o acesso online ao seu banco é feito usando um canal seguro com criptografia; a sua comunicação com amigos e familiares com *WhatsApp*, por exemplo, é protegida por criptografia, e ninguém consegue escutar as mensagens ou ter acesso a elas no meio do caminho.



Fonte: Shutterstock.

A CRIPTOGRAFIA É UTILIZADA PELAS EMPRESAS

Como profissional de segurança, você pode utilizar a criptografia para melhorar a segurança da sua empresa.

- Criptografia dos dados armazenados no notebook.
- Conexão remota do home office utilizando VPN para proteger a comunicação pela internet.
- Criptografia do banco de dados para proteger as informações de vendas armazenadas.
- Criptografia das conexões ao website de vendas online usando HTTPS/TLS/SSL.

Fonte: Shutterstock.

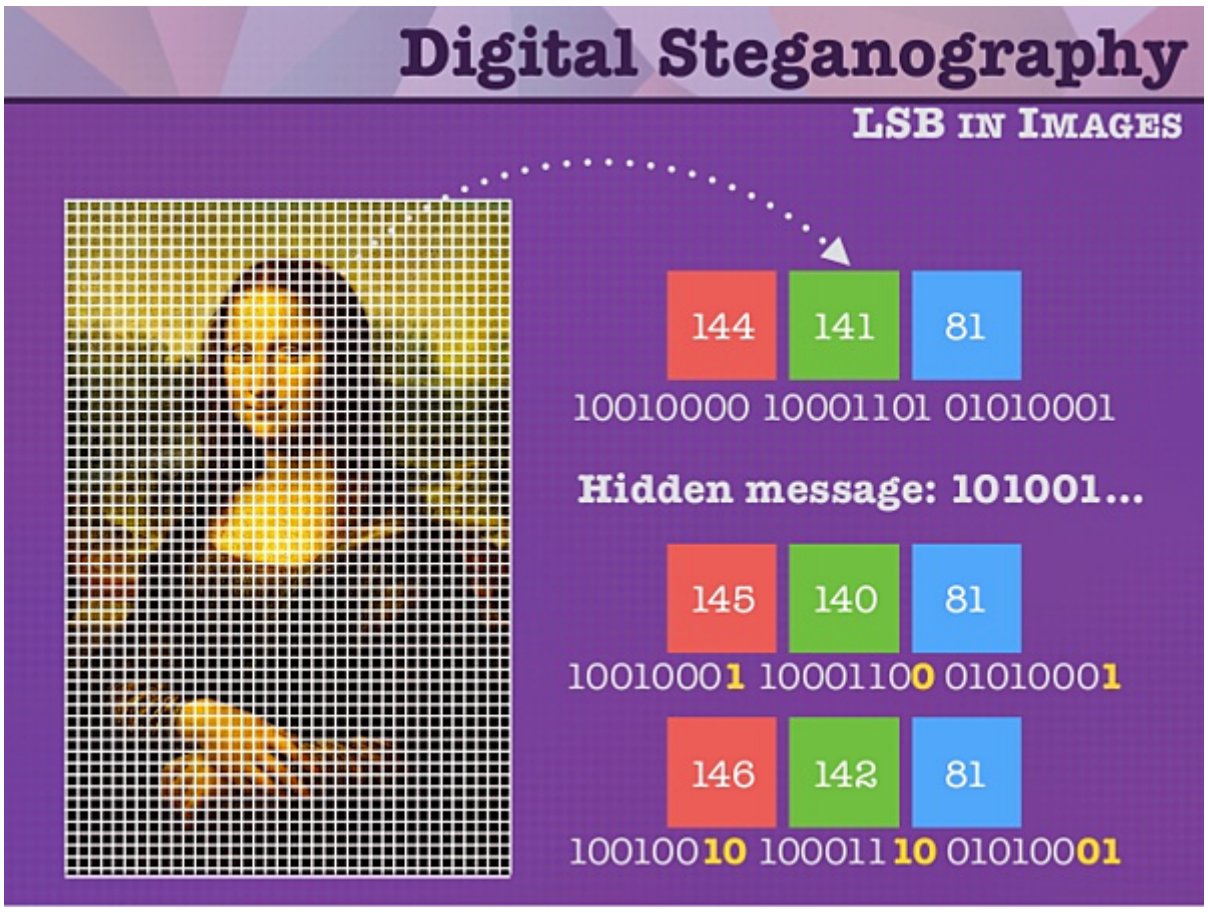
O QUE É CRIPTOGRAFIA?

Criptografia é ocultar o significado das mensagens, e não ocultar a mensagem em si. Esta é a esteganografia.

- No caso da criptografia, em caso de a mensagem ser interceptada, o conteúdo está protegido.

- Já no caso da esteganografia, a mensagem está oculta.

Exemplo da esteganografia



Fonte: Switchfast.

TESTES

Vamos ver como funciona a esteganografia ocultando um texto em uma imagem.

- Você pode testar passo a passo utilizando a ferramenta *OpenPuff*, disponível em: https://bit.ly/3sXBqBq. Acesso em: 16 nov. 2020.
- Você pode testar alguns algoritmos de criptografia em uma ferramenta online chamada *Online Cryptography Tools*, disponível em: https://bit.ly/3tZNVh4. Acesso em: 2 nov. 2020.

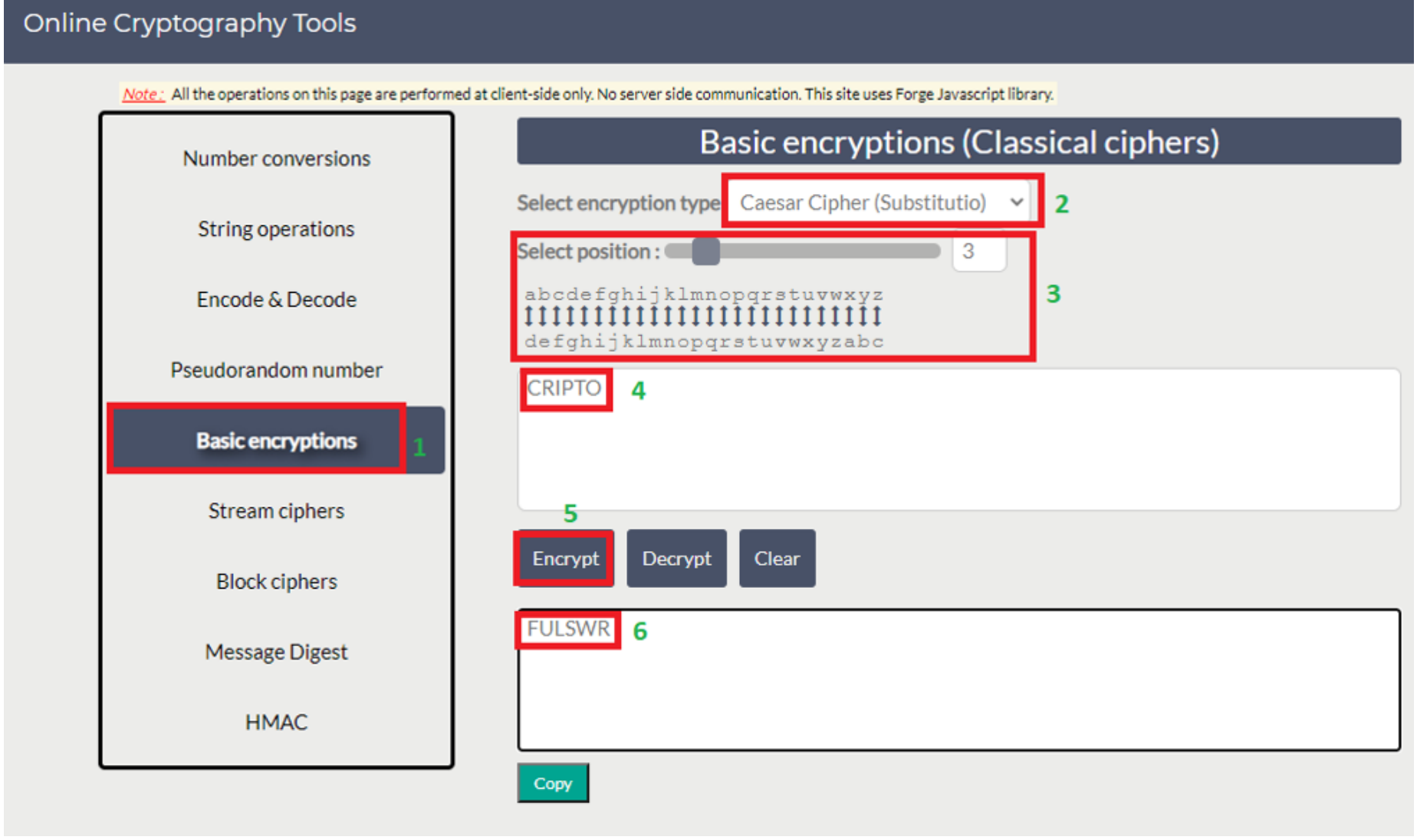
A ferramenta *Online Cryptography Tools* contém exemplos desde a cifras simples, como a Cifra de César, como criptografia de chave simétrica e *hash*.

A seguir temos um exemplo de aplicação da Cifra de César.

Cifra de César

Vamos utilizar como senha a palavra “CRIPTO” e substituir cada letra da palavra avançando três letras no alfabeto. Por exemplo, a letra “C” vamos substituir por “F”, a letra “R” será alterada pela letra “U”, a letra “I” pela letra “L”, a letra “P” pela letra “S”; “T” pela letra “W” e “O” por “R”. Para testar o exemplo siga os passos enumerados na imagem da figura:

Cifra de César e as substituições feitas com uma chave 3 na palavra teste



Fonte: elaborada pelo autor.

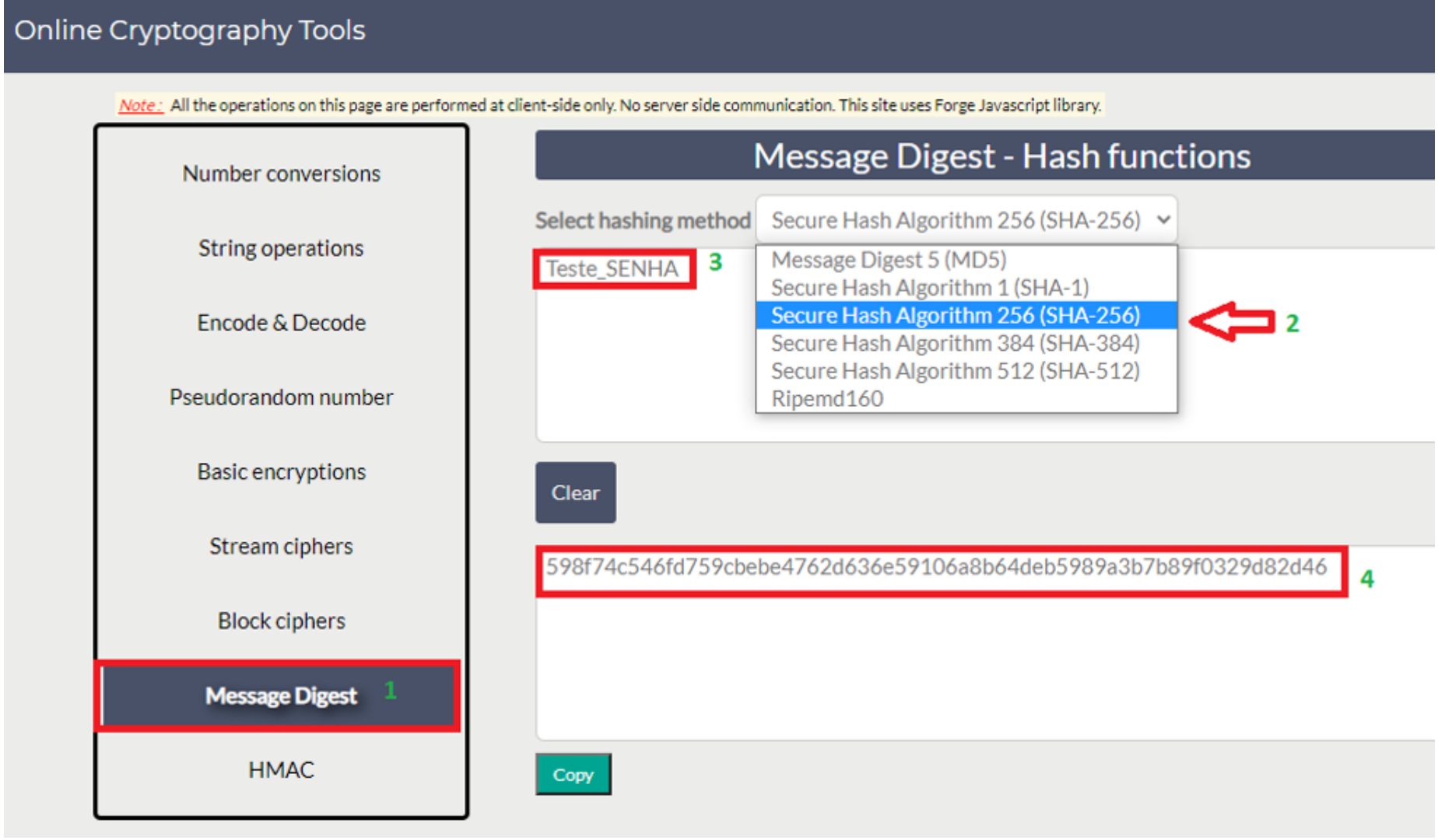
1. Ao acessar o site, vá em Basic encryptions.
2. Em Select encryption type, selecione a Caesar Cipher (Cifra de César).
3. Em Select Position, selecione o número de posições que será avançado no alfabeto para substituição das letras. No caso foi selecionado o número 3, o que corresponde a quantidade letras a se avançar e a serem substituídas no alfabeto. Observe que no caso a letra “a” será trocada por “d”, “b” por “e”.
4. No passo 4, incluímos a palavra “CRIPTO”
5. E clicamos em Encrypt.
6. Será criptografada e gerada abaixo a palavra correspondente “FULSWR”.

Teste outros exemplos de algoritmos criptográficos e selecione mais posições a serem avançadas no alfabeto.

Outro exemplo de algoritmo de criptografia é a que utiliza funções *hash*. Funções de *hash* são utilizadas para verificação da integridade. Estes algoritmos realizam um cálculo matemático nas mensagens ou nos documentos. O receptor recebe a mensagem juntamente com o *hash* e utiliza o mesmo algoritmo para calcular o *hash* da mensagem recebida. O *hash* recebido e o *hash* calculado devem ser comparados, e devem ser iguais, o que garante a integridade da mensagem ou do documento. Alguns exemplos de funções de *hash* são o MD5 e a família SHA (SHA-1, SHA-256 e SHA-512). É importante ressaltar que o MD5 e o SHA-1 não devem mais ser utilizados na prática, pois são susceptíveis a ataques de colisão. Neste ataque, mensagens diferentes podem gerar o mesmo *hash*, impossibilitando a validação da integridade.

■ Você pode testar exemplos de funções *hash* na ferramenta *Online Cryptography Tool*s, disponível em: https://bit.ly/3e4KXSM. Acesso em: 2 nov. 2020.

O exemplo a seguir ilustra a saída para o algoritmo SHA-256 utilizando também a ferramenta *Online Cryptography Tools*.



Fonte: elaborada pelo autor.

1. Ao acessar o site, vá em Message Digest.
2. Em Select hashing method, clique e será apresentada uma lista de algoritmos com função *hash*, selecione a opção Secure Hash Algorithm 256 (SHA-256), ele irá converter o texto que você digitar no campo em sua respectiva *hash* de tamanho de 256 bits.
3. Digite o texto que você e você vai visualizar a *hash* de 256 bits.
4. Você conseguirá visualizar a hash da palavra “Teste_Senha”. Observe que foi gerado uma *hash* com 256 bits, tamanho fixo e se você alterar as letras para maiúsculas ou minúsculas ou quaisquer letras da palavra no campo 3, a *hash* também será alterada, porém, o tamanho é fixo. Cada palavra fase sempre vai conter uma *hash* única.

Teste você mesmo! Crie uma mensagem cifrada com chave 5 e depois teste utilizando a ferramenta.

PROTOCOLOS QUE USAM CRIPTOGRAFIA

- TLS é o protocolo padrão da internet atualmente, em substituição ao SSL, que possui muitas falhas de segurança.
- HTTPS é o uso do HTTP protegido por TLS/SSL.
- VPN é um túnel virtual nos moldes do TLS, para comunicação remota ou entre empresas que se comunicam por uma rede pública e não confiável.
- IPSec é um dos protocolos mais utilizados por VPNs.

A criptografia tem um papel importante para a proteção de dados armazenados, ainda mais em um mundo em que as informações estão distribuídas em datacenters de empresas, dispositivos de usuários e nuvem.

Pesquise mais