PESQUISA: CRIPTOGRAFIA

UNIVERSIDADE SÃO JUDAS TADEU – CAMPUS MOOCA

CIÊNCIAS DA COMPUTAÇÃO

RAFAELA MARIA DA SILVA – ATIVIDADE MINISTRADA POR PROFESSOR ROBSON CALVETTI.

SÃO PAULO

2025

**Cifra de Bifid**

- Criada pelo criptográfico francês Felix Delastelle em 1895.

- Combina substituição e transposição para tornar a criptografia mais difícil de quebrar. Ela transforma as letras em números e reorganiza os números antes de convertê-los de volta em letras.

Exemplo:   
Primeiro passo: Crie uma chave em forma de tabela 5x5 onde será escrito o alfabeto.

Tabela

O conteúdo gerado por IA pode estar incorreto.

Segundo passo: Escreva a sequência de letras da esquerda para direita, e de baixo para cima: dbewkcziahpymgfxvoustnrlq, essa chave será nosso código.

Terceiro passo: Mensagem codificada (PERIGO)

Escreva a frase da seguinte maneira:

P E R I G O

Quarto passo: Então, preencha cada espaço com as respectivas linhas e colunas que as letras da mensagem se encontram.

P E R I G O

3 1 5 2 3 4

1 3 3 3 4 3

Quinto passo: Em seguida, você deverá escrever os números na sequência de baixo para

cima e da esquerda para a direita.

3 1 5 2 3 4 1 3 3 3 4 3

Sexto passo: Agrupar os números do novo código 2 a 2.

3 1 5 2 3 4 1 3 3 3 4 3

3 5 3 1 3 4

1 2 4 3 3 3

Último passo: Ao final do processo, você terá uma sequência completa de números escritos na forma x/y. É então o momento de transformá-los em letras, conforme a tabela já criada.

3 1 5 2 3 4

1 3 3 3 4 3

P E R I G O

Obs: Sua tradução somente será possível por alguém que possua a tabela de  
transcrição.

**Cifra de Rail Fence**

- Criado no século XIX

- Usado como técnica de transposição

- Os caracteres são escritos numa matriz usando um padrão fixo em zigue-zague e a saída é o texto lido horizontalmente. O rail fence admite várias variações, como a linha que a primeira letra começa e o número de linhas usadas. Por exemplo, usando um rail fence com duas linhas:  
Texto: São judas  
Matriz:

S - O - U - A -

- A - J - D - S

Texto cifrado: SOUAAJDS

- Usada para mensagens militares e comunicação entre espiões.

**Criptografia Simétrica**

1 – AES (Advanced Encryption Standard)

O AES funciona protegendo dados por meio de criptografia simétrica, onde a mesma chave é usada para criptografar e descriptografar informações.

No caso do WhatsApp, ele usa AES em combinação com outros protocolos para garantir criptografia de ponta a ponta. Isso significa que:

- Quando uma mensagem é enviada, ela é criptografada com AES para que apenas o destinatário tenha a chave necessária para decodificá-la.

- Enquanto trafega pela internet, a mensagem permanece segura e ilegível para terceiros, incluindo hackers ou até mesmo o próprio WhatsApp.

- Quando a mensagem chega ao destinatário, ela é descriptografada com a chave correspondente e exibida normalmente.

2 – Blowfish

O Blowfish é um algoritmo de criptografia simétrica que divide os dados em blocos de 64 bits e usa uma chave de até 448 bits para proteger informações. Ele é rápido e eficiente, sendo usado principalmente em sistemas de segurança.

Em uma VPN por exempl**o**, o Blowfish pode ser utilizado para criptografar o tráfego de internet.

- O usuário envia dados para o servidor VPN.

- O algoritmo Blowfish criptografa os pacotes antes de serem transmitidos.

- O servidor VPN descriptografa os pacotes com a mesma chave e os encaminha ao destino.

- As respostas seguem o mesmo processo, garantindo segurança na comunicação.

**Criptografia Assimétrica**

1 - RSA (Rivest-Shamir-Adleman)

Um dos mais conhecidos e amplamente adotados para segurança na internet, incluindo assinatura digital e criptografia de emails.

Exemplo com RSA em emails:

- Você quer enviar um email criptografado para um amigo.

- Seu amigo tem um par de chaves RSA: uma pública e outra privada.

- Você usa a chave pública do seu amigo para criptografar o email.

- Apenas o seu amigo, que tem a chave privada correspondente, pode descriptografar e ler a mensagem.

2 - ECC - Elliptic Curve Cryptography

A criptografia de curva elíptica (ECC - Elliptic Curve Cryptography) é muito usada para garantir segurança em comunicações digitais com chaves menores e mais eficientes que o RSA.

Exemplo autenticação segura em um site

Imagine que você está acessando o site do seu banco através do navegador:

- Quando você digita a URL, seu navegador inicia uma conexão segura com o servidor do banco.

- O servidor usa ECC para enviar uma chave pública ao seu navegador.

- O navegador usa essa chave para criptografar informações sensíveis, como seus dados de login, antes de enviá-los.

- O servidor, que possui a chave privada correspondente, descriptografa seus dados e autentica sua identidade.

- Assim, ninguém pode interceptar e roubar suas credenciais durante a comunicação.

Bibliografia: [Cifras de Transposição | WikiSEC](https://wiki.imesec.ime.usp.br/books/criptografia/page/cifras-de-transposi%C3%A7%C3%A3o)

[Criptografia - Cifra de Bifid | Passei Direto](https://www.passeidireto.com/arquivo/72412800/criptografia-cifra-de-bifid)