



Studio Shodwe

CYBER SECURITY



RAFAEL EXPEDITO PRADO
DA SILVA





EXEMPLOS HISTÓRICOS DO USO DE CRIPTOGRAFIA

Exemplo 1: A Criptografia de Júlio César

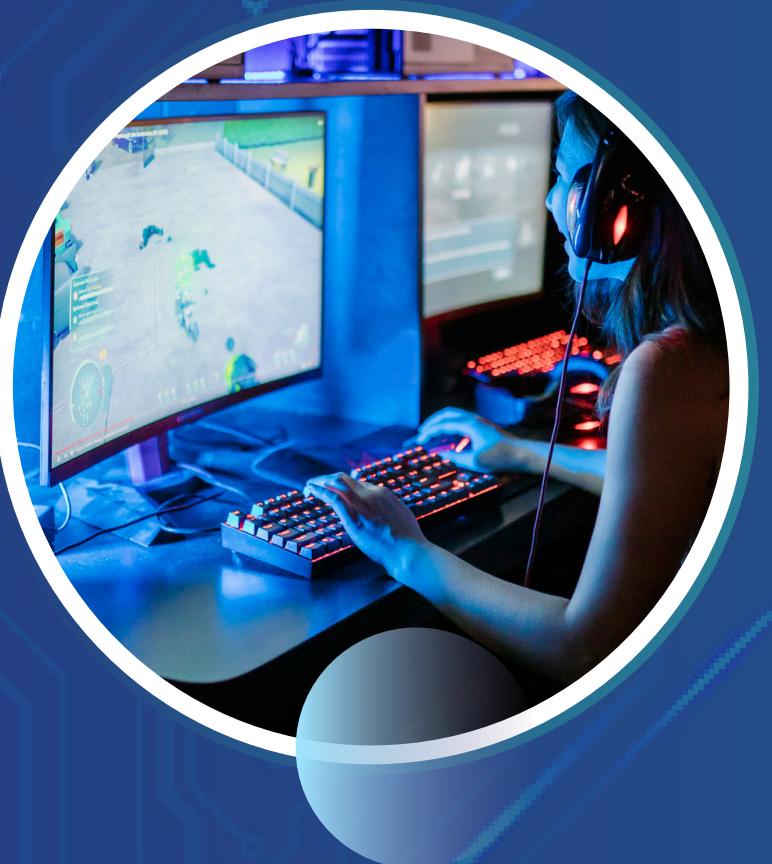
- Descrição: A criptografia de Júlio César, também conhecida como cifra de César, é uma das técnicas de criptografia mais antigas. Júlio César usava essa cifra para enviar mensagens secretas a seus generais, deslocando cada letra do alfabeto um número fixo de posições. Por exemplo, com um deslocamento de 3, a letra A se tornaria D, B se tornaria E, e assim por diante.

Exemplo 2: A Máquina Enigma

- Descrição: Durante a Segunda Guerra Mundial, a Alemanha usou a máquina Enigma para codificar suas comunicações militares. A máquina utilizava um sistema complexo de rotores e plugboards para criar uma cifra que mudava constantemente, tornando extremamente difícil para os aliados decifrar as mensagens. O trabalho de Alan Turing e sua equipe em Bletchley Park foi crucial para quebrar o código da Enigma.



ALGORITMOS DE CRIPTOGRAFIA COM CHAVES SIMÉTRICAS



Algoritmo 1: AES (Advanced Encryption Standard)

Descrição: O AES é um dos algoritmos de criptografia simétrica mais utilizados atualmente. Ele opera em blocos de 128 bits e suporta chaves de 128, 192 e 256 bits. É amplamente utilizado em aplicações de segurança, como em redes sem fio e em sistemas de armazenamento de dados.



Algoritmo 2: DES (Data Encryption Standard)

Descrição: Embora o DES tenha sido considerado inseguro para muitas aplicações modernas devido ao seu tamanho de chave de 56 bits, ele ainda é um exemplo importante de criptografia simétrica. O DES foi amplamente utilizado em sistemas de segurança até que o AES se tornasse o padrão.





Algoritmo 1: RSA (Rivest-Shamir-Adleman)

- Descrição: O RSA é um dos algoritmos de criptografia assimétrica mais conhecidos e utilizados. Ele se baseia na dificuldade de fatorar grandes números primos. O RSA é amplamente utilizado para a troca segura de chaves e na assinatura digital.

Algoritmo 2: ECC (Elliptic Curve Cryptography)

- Descrição: A criptografia de curva elíptica (ECC) é uma abordagem moderna que oferece um nível de segurança equivalente ao RSA, mas com chaves muito menores. Isso a torna ideal para dispositivos com recursos limitados, como smartphones e IoT (Internet das Coisas).

ALGORITMOS CRIPTOGRAFIA COM CHAVES ASSIMÉTRICAS

