ATIVIDADE 4

2 Exemplos históricos do uso de criptografia

a) Cifra de Playfair: Criada em 1854 por Charles Wheatstone, mas popularizada por Lord Playfair, essa cifra substitui pares de letras por outros pares, tornando-a mais complexa que a Cifra de César. Exemplo:
"ENCONTRO SECRETO"
Pares de letras: "EN", "CO", "NT", "RO", "SE", "CR", "ET", "O/"
Texto cifrado: "RXABRSANHTBSLXDA"

b) Cifra de Hill: Desenvolvida em 1929 por Lester S. Hill, essa cifra usa álgebra linear para criptografar mensagens, sendo uma das primeiras a usar matemática em criptografia.Exemplo:
"DADOS"
Conversão para números (A=0, B=1, etc.): "3 0 3 18 18"
Pares de números: "(3, 0)", "(3, 18)", "(18,/)"
Texto cifrado: "11 9 11 12 2" que traduzido para letras fica "LJLMC"

2 Algoritmos de criptografia com chaves simétricas utilizados atualmente

a) AES (Advanced Encryption Standard): Um dos algoritmos mais populares e seguros atualmente, usado em diversas aplicações, como Wi-Fi e VPNs.

b) DES (Data Encryption Standard): Embora considerado obsoleto devido ao seu tamanho de chave curto, o DES foi um padrão importante na criptografia por muitos anos.

2 algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente

a) RSA (Rivest-Shamir-Adleman): Um dos primeiros algoritmos de chave pública, amplamente utilizado em aplicações como e-mail seguro e transações online.

b) ECC (Elliptic Curve Cryptography): Um algoritmo mais recente que oferece segurança semelhante ao RSA com chaves menores, tornando-o ideal para dispositivos móveis e outras aplicações com recursos limitados.