Explicação do código – Implementação da Cifra de Hill em linguagem C

Gabriel Figueiredo Spaziante – R.A: 23008007

Para fazer uso da Cifra de Hill, inicialmente, é necessário fazer uma função na qual valide a mensagem para ser descriptografa adequadamente. Entre as medidas necessárias para validar a mensagem, podemos destacar: Tornar a mensagem válida retirando caracteres especiais, números e espaços. Tornar o número de caracteres par, pois a aplicação não funciona corretamente com os caracteres totais sendo ímpar.

Texto

Descrição gerada automaticamente

Linha 6 - A função cifraDeHill recebe os seguintes parâmetros: texto[] – que é o texto a ser recebido; matriz[2][2] – que é a matriz 2x2 da Cifra de Hill (usado para decodificar); textoCifrado – que é o resultado e onde será armazenado.

Linha 8 – strlen(texto) calcula o tamanho do texto.

Linha 10 – A função for divide o texto em blocos de dois caracteres, uma vez que a Cifra de Hill exige pares.

Linhas 12 e 13 – Converte os números (o par) para um valor numérico.

Linhas 15 e 16 – Aplica a matriz no primeiro e segundo número, respectivamente.

Linhas 19-24 - Verifica se o tamanho do texto é ímpar. Caso seja ímpar, int x = texto[tamanho - 1] - 'A' transforma a última letra em número e textoCifrado[tamanho - 1] = ((matriz[0][0] \* x) % 26) + 'A' aplica a matriz no último valor. textoCifrado[tamanho] = '\0'; Termina a string cifrada com o caractere nulo.

Texto

Descrição gerada automaticamente

Linhas 27-38 – A função void removerNumeros remove os números do texto. if (!isdigit(texto[i])) verifica se o caractere não é um número. texto[j++] = texto[i]; se não for número, copia o caractere para a posição j e incrementa j. texto[j] = '\0' termina a string sem números.

Linhas 40-51 – Repete a função anterior, mas aplica para caracteres especiais e espaços. if (isalpha(texto[i])) verifica se o caractere é uma letra.

Texto

Descrição gerada automaticamente

Linhas 53-72 - char texto[100] declara a variável para armazenar o texto a ser criptografado. char textoCifrado[100] declara a variável para armazenar o texto cifrado. int matriz[2][2] = {{6, 24}, {1, 16}}; define a chave da cifra de Hill, uma matriz 2x2. fgets(texto, sizeof(texto), stdin) lê a entrada do usuário e armazena na variável texto. texto[strcspn(texto, "\n")] = '\0' remove o caractere de nova linha ('\n') que pode ser incluído ao usar fgets. Linhas 64 e 65 aplicam as funções criadas anteriormente para remover números e caracteres especiais/espaços. Linha 67 aplica a função que irá cifrar o texto. Linha 69 imprime o resultado.