notebook

December 18, 2024

1 Simplified - DES

A criptografia por deslocamento, é uma das técnicas de criptografia mais antigas já criadas. Ela consiste em substituir cada letra de uma mensagem por outra, deslocando-a no alfabeto por um número fixo de posições. Esse número, chamado de chave de deslocamento, deve ser um inteiro, geralmente entre 1 e 25 no caso do alfabeto latino, para evitar que o deslocamento seja redundante (chaves iguais a 0 ou 26 resultam no texto original).

No funcionamento da cifra, cada letra é convertida para um índice numérico correspondente à sua posição no alfabeto (A = 0, B = 1, ..., Z = 25). Em seguida, o valor da chave é somado a esse índice, e o resultado passa por uma operação de módulo 26, garantindo que o índice resultante permaneça dentro do intervalo válido para o alfabeto. A nova posição determina a letra substituta. Por exemplo, com uma chave de deslocamento de 3, a letra "A" se torna "D", "B" se torna "E", e assim por diante.

Embora historicamente usada para proteger mensagens confidenciais, a Cifra de César oferece pouca segurança no contexto atual, especialmente com a utilização dos computadores no auxlio desta quebra, pois pode ser facilmente quebrada por força bruta (testando todas as chaves possíveis) ou análise de frequência.

A seguir, iremos desenvolver um código que implementará uma Criptografia por Deslocamento. O programa será capaz de gerar uma chave de deslocamento que define o número de posições a serem alteradas no alfabeto, criptografar a mensagem original com base na chave gerada e também será capaz de descriptografar tanto utilizando a chave de deslocamento tanto quanto sem esta chave utilizando apenas análise de frequência das letras no português.

[ ]:

1.1 Código para Geração das sub chaves K1 e K2

Para o estudo da criptografia por deslocamento, utilizaremos a primeira página do livro:"A Revolução dos Bixos" por George Orwell. Da edição da Gaveta do Povo. A escolha foi motivada pela necessidade que para a quebra de um texto por análise de frequência, é importante ter um grande volume de palavras escritas de forma coerente e ortograficamente corretas. Assim, nada melhor que um livro para nos fornercer esses dados.

Mas para isso é necessário uma série de filtragens para tornar o texto livre de acentuação, caracteres especiais e letras como "ç".

Assim, vamos desenvolver a seguinte função para a leitura e tratamento do nosso texto a ser cifrado:

1.1.1 Função de Permutação P10

Para o estudo da criptografia por deslocamento, utilizaremos a primeira página do livro:"A Revolução dos Bixos" por George Orwell. Da edição da Gaveta do Povo. A escolha foi motivada pela necessidade que para a quebra de um texto por análise de frequência, é importante ter um grande volume de palavras escritas de forma coerente e ortograficamente corretas. Assim, nada melhor que um livro para nos fornercer esses dados.

Mas para isso é necessário uma série de filtragens para tornar o texto livre de acentuação, caracteres especiais e letras como "ç".

Assim, vamos desenvolver a seguinte função para a leitura e tratamento do nosso texto a ser cifrado:

1.1.2 Função para o Deslocamento Circular a Esquerda

Para o estudo da criptografia por deslocamento, utilizaremos a primeira página do livro:"A Revolução dos Bixos" por George Orwell. Da edição da Gaveta do Povo. A escolha foi motivada pela necessidade que para a quebra de um texto por análise de frequência, é importante ter um grande volume de palavras escritas de forma coerente e ortograficamente corretas. Assim, nada melhor que um livro para nos fornercer esses dados.

Mas para isso é necessário uma série de filtragens para tornar o texto livre de acentuação, caracteres especiais e letras como "ç".

Assim, vamos desenvolver a seguinte função para a leitura e tratamento do nosso texto a ser cifrado:

1.1.3 Função de Permutação P8

Para o estudo da criptografia por deslocamento, utilizaremos a primeira página do livro:"A Revolução dos Bixos" por George Orwell. Da edição da Gaveta do Povo. A escolha foi motivada pela necessidade que para a quebra de um texto por análise de frequência, é importante ter um grande volume de palavras escritas de forma coerente e ortograficamente corretas. Assim, nada melhor que um livro para nos fornercer esses dados.

Mas para isso é necessário uma série de filtragens para tornar o texto livre de acentuação, caracteres especiais e letras como "ç".

Assim, vamos desenvolver a seguinte função para a leitura e tratamento do nosso texto a ser cifrado:

1.1.4 Executando as Funções para Geração de K1 e K2