Cifra de Vigenère

João José Costa Gondin

Descrição da implementatação e método de quebra da cifra

Neste documento nos ateremos à descrever minuciosamente a implementação do método de quebra da cifra de Vigenère (ataque de kasiski) por meio da linguagem de programação C. Apresentando de forma superficial a implementação do método de cifração em si, dado que esse por suposto não é a principal funcionalidade e habilidade requerida para esse trabalho. Funcionando de certa forma como função auxiliar.

Comentários gerais

Neste trabalho optou-se por fazer-se a conversão de todos os caracteres maiúsculos para minúsculos e também por não tratar caracteres fora da faixa de a à z, mantendo-os assim em suas posições originais no momento da decifração da mensagem. Decidiu-se também fazer uma abordagem que não leva em conta demasiadas funções, se atendo assim apenas ao necessário para uma boa organização do código. Por motivos evidentes as implementações das funções “Preenche_tabua” e “menu” não serão comentadas.

Função “Cifra”

Primeiramente a função “Cifra” pede o texto ao qual se quer cifrar e a chave a ser usada para tal. Logo em seguida faz o tratamento tanto do texto quanto da chave (transformando caracteres maiúsculos em minúsculos sem levar em consideração caracteres fora da faixa de a à z), posteriormente finda o algoritmo combinando chave e texto através do método de vigenère e imprimindo na tela o resultado.

Função “Decifra”

Por motivos de organização tanto o texto a ser decifrado quanto a chave de decifração são solicitadas em trechos de código da função “main” e então repassadas para a função “Decifra”. Essa então faz o tratamento tanto do texto quanto da chave (transformando caracteres maiúsculos em minúsculos sem levar em consideração caracteres fora da faixa de a à z). A posteriori começa o processo de decifração cruzando o texto cifrado com a chave referente ao mesmo e com auxílio da tabela alfabética preenchida pela função “Preenche_tabua”, ao final o algoritmo imprime na tela o resultado.

Função “Ataque”

Primeiramente a função “Ataque” solicita o texto o qual será analisado, a fim de se descobrir sua chave de cifra. Logo em seguida o texto é tratado (transformando caracteres maiúsculos em minúsculos sem levar em consideração caracteres fora da faixa de a à z), então usasse um vetor para copiar o conteúdo relevante do texto fornecido, com o intuito de facilitar sua análise. A partir daí começasse a procurar trincas de letras idênticas consecutivas. Quando duas das referidas cadeias de caracteres idênticas são encontradas sabe-se que o espaço entre elas é um possível múltiplo da chave de cifra, então iniciasse um processo de sucessivas divisões (de dois até trinta, pois estimou-se por arbitrariedade que trinta era o maior tamanho de chave possível) para inferir os possíveis tamanhos de palavra chave. Depois de realizado tal processo em todo o texto cifrado e guardado os candidatos a tamanho de chave de forma propícia em um vetor, faz-se uma seleção dos três tamanhos de chave mais prováveis. Agora dentre as opções é escolhido o tamanho de chave de forma conveniente, pois se por exemplo, a chave usada para cifrar o texto tem tamanho oito, no processo descrito anteriormente os tamanhos dois e quatro terão um auto índice de inferência e isso deve ser levado em consideração, pois é lógico que é melhor ter uma chave duplicada do que correr o risco de não pegá-la inteira (todos os caracteres). Com o fim de tal processo é hora de inferir o idioma o qual o texto original foi escrito. O algoritmo fará isso com base nos slices criados com fundamentação no tamanho encontrado para a chave, o código criará estatísticas para cada letra presente no slice e o comparará com as estatísticas de letras tanto no idioma português quanto no idioma inglês. Como as estatísticas das letras estão deslocadas como em uma cifra de César, é necessário transladar os índi

ces dos slices até se encontrar a melhor correspondência (isso é feito simultaneamente com os dois idiomas), esse processo é viabilizado por uma subtração entre o conteúdo dos índices do vetor do referido idioma e o slice em questão. Encontrando a melhor correspondência para cada idioma comparasse as duas análises para saber qual a mais provável e marcasse uma variável de controle, esse processo é feito em todos os slices do texto. Ao final, as variáveis de controle referentes aos idiomas em questão são comparadas e a decisão de em que idioma o texto original foi escrito é tomada. Finalmente refazemos tal processo, agora apenas com o idioma original do texto e guardando a translação do slice para saber como o mesmo foi deslocado e qual a correspondência estatísticas das letras. Esse algoritmo é repetido até que acabe todos os slices e a palavra chave usada para cifrar o texto em questão seja revelada, ao final o algoritmo apresenta a chave encontrada e chama a função “Decifra” passando para a mesma como argumento a chave de cifra e o texto cifrado.