Criptografia: Parte 03 (Cifragem de Cesar-1)

Mário Leite

...

Nas duas partes da **Introdução** foi dito que a chave é um elemento fundamental no processo de *codificar/decodificar* uma mensagem. Também foi dito que os algoritmos dos métodos criptográficos podem ser classificados em dois grandes grupos**:** os que adotam uma chave única (simétrica) para codificar e decodificar a mensagem (criptografia de chave simétrica) e os que adotam chave dupla (assimétrica): uma para codificar e outra para decodificar. Um exemplo clássico de "Criptografia de Chave Simétrica" é conhecido pela expressão "*Cifragem de Cesar*"; em homenagem ao imperador romano Caio Júlio Cesar, que governou Roma após o fim do período republicano até a sua morte em 44 a.C. Ele utilizava um tipo de codificação para enviar mensagens cifradas a seus generais nos campos de batalha, ou mesmo para fazer política com autoridades romanas. Na verdade, este tipo de codificação era bem simples; bem inocente se comparado com os métodos atuais de proteção de mensagens. O método de Cesar se resume no seguinte**:** uma letra é substituída por outra depois de um deslocamento de determinado tamanho; por exemplo, a letra "K" é substituída por "N"; a letra "P" por "S", e assim por diante, considerando um deslocamento de tamanho três; o padrão cesariano. Assim, com medo de que o mensageiro pudesse estar compactuado com o inimigo, Júlio Cesar fazia este tipo de substituição nas letras da mensagem de modo que só o destinatário pudesse saber o seu significado. Então, suponha que o imperador confiasse cegamente em um de seus generais e quisesse ordenar sua volta à Roma para uma missão secreta; observe como poderia ser essa mensagem:

Mensagem original: **`VOLTE A ROMA PARA VIGIAR BRUTUS`**
Mensagem cifrada: **`YROWH D URPD SDUD YLJLDU EUXWXV`**

Note que a codificação (*cifragem*)) ocorreu de forma bem simples: para decifrar cada letra da mensagem original ocorre a sua substituída pela terceira letra APÓS ela; no caso a letra "**V**" foi substituída por "**Y**", a letra "**O**" por "**R**", e assim por diante...

O modo como o general descobria o teor real da mensagem era através da "chave" que lhe era dada pelo imperador, da seguinte maneira: "CADA LETRA DEVE SER SUBSTITUÍDA PELA TERCEIRA LETRA ANTES DELA; DE TRÁS PARA FRENTE". Em resumo: é este o processo de *codificar/decodificar* uma mensagem por este método. E uma observação importante a respeito da "Cifragem de Cesar" é que, quando o final do alfabeto é atingido retorna-se ao início, mantendo o mesmo deslocamento. Por exemplo, a palavra **ZETA** seria cifrada como **CHWD**; **YVANOV** como **BYDQRY** e **PIXULECO** como **SLAXOHFR**. Veja os esquemas de *codificação/decodificação* da palavra "**VOLTE**" nas **figuras CCI.1** e **CCI.2, respectivamente**.

Continua com a "Cifragem de Cesar-2" (Parte 04)

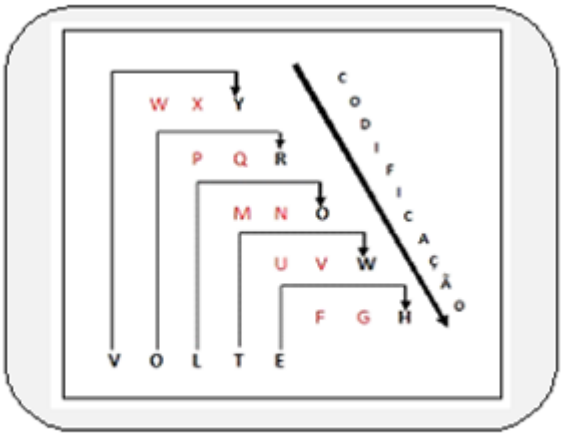

Figura CCI.1 - Codificação por Cifragem de Cesar

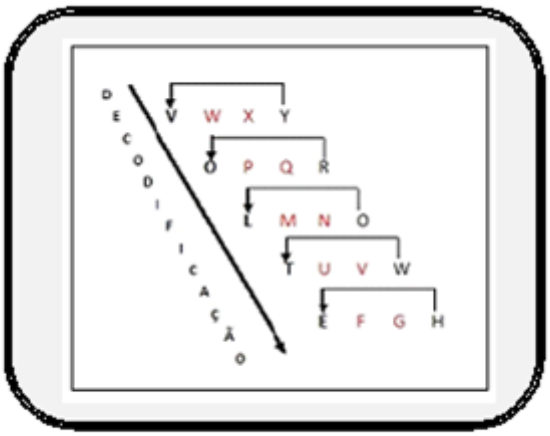

Figura CCI.2 - Decodificação por Cifragem de Cesar