Criptografia: Parte 1 (Introdução-1)

Mário Leite

...

A mercadoria mais valiosa desde há muito tempo, e principalmente a partir do Século XX é, sem sombra de quaisquer dúvidas, a Informação; ou, mais precisamente: os *dados* que são transformados em Informação com o objetivo final de se obter o Conhecimento.

Desde há muito tempo o homem tem se preocupado em proteger suas mensagens enviadas para algum destinatário, empregando métodos de proteção que variam desde a ocultação até a modificação textual da mensagem, de modo que somente o emissor (aquele que a emite) e o receptor (aquele que a recebe) saibam do que, efetivamente, se trata. Um exemplo muito simples e bastante corriqueiro no nosso dia a dia é o uso do caixa eletrônico de um banco**:** ao digitar a senha aparecem asteriscos no lugar dos caracteres digitados; é uma forma simples do cliente proteger seus dados. Até o imperador romano Caio Júlio César já utilizava um método de codificar as mensagens que enviava a seus generais nos campos de batalha; ele não confiava no mensageiro.

Um tipo de proteção de texto conhecido como esteganografia (derivada do grego: steganos=encoberto e *graphéin=escrita*) foi muito usado durante as guerras entre gregos e persas no Século V a.C. Um exemplo deste tipo de proteção era o de raspar a cabeça do mensageiro e escrever a mensagem em sua cabeça; após o cabelo crescer ele era enviado ao destinatário. A mensagem ficava oculta na cabeça dele, e só poderia ser conhecida pelo destinatário que tinha a "chave" para decifrar o seu conteúdo: "RASPE A CABEÇA DO MENSAGEIRO". Embora este tipo de proteção pudesse funcionar, o inimigo poderia interceptar o mensageiro e resolver "dar uma geral" nele, incluindo a raspagem de seu cabelo; e assim a mensagem seria revelada. Durante a Segunda Guerra Mundial os alemães utilizaram este método de proteger as suas mensagens com o famoso "microponto", que consistia em fotografar a mensagem, reduzi-la a um ponto no papel e colocar esse "microponto" no final de um texto qualquer sem ligação com a verdadeira mensagem. Assim, caso o papel fosse interceptado pelo inimigo a mensagem estaria segura pois, somente o destinatário sabia a "chave" para encontrar o tal microponto e como ampliá-lo para descobrir o verdadeiro sentido da mensagem.

Outro tipo de proteção é a Criptografia, que altera o texto da mensagem original através de *substituição* e/ou *transposição* dos caracteres. O termo "criptografia" é originário do grego (*kryptós=escondido* e *gráphen=escrita*) e pode ser entendido como "*estudo dos princípios e técnicas pelas quais a informação pode ser transformada de sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário*". Na prática, o que se deseja é transformar um texto legível em algo ilegível. Então, o objetivo final da criptografia é dar segurança a um texto confidencial, tornando a informação nele contida inacessível para aquelas pessoas não autorizadas a conhecê-la. Tecnicamente, existem dois termos empregados na proteção de mensagens: **Cifragem** e **Codificação**. A **figura I.**1 mostra que estes dois termos são duas formas de fazer substituições no texto original da mensagem, que por sua vez é uma das duas formas de Criptografia.

Continua com a "Introdução-2" (Parte2)

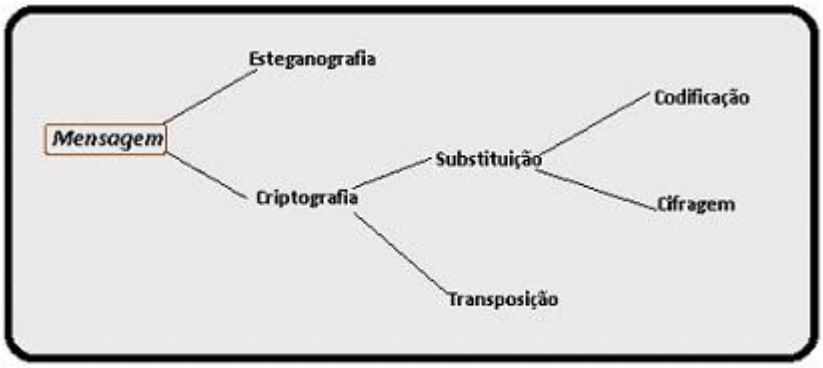

Figura I.1 - Processo de codificação de uma imagem