Criptografia: Parte 2 (Introdução-2)

Mário Leite

...

Com foi explicado na **Parte 1** (*Introdução-1*) a **Informação** é uma das mercadoras mais valiosas atualmente; com certeza, a mais valiosa. As empresas que não protegem seus **Dados** - potencialmente matéria prima de suas Informações - podem perder competitividade, ou até mesmo desaparecer do mercado. Uma forma moderna e bem eficiente de proteger os *Dados/Informações* é a Criptografia. O ato de criptografar (encriptar) uma mensagem é fazer alterações no seu texto de modo que somente o destinatário poderá saber o seu verdadeiro conteúdo quando descriptografar (decriptar) a mensagem. Para decriptar a mensagem o destinatário tem que conhecer a "chave" que faz esta operação. E mesmo não sendo um processo de decriptar, no sentido mais formal do termo, "*RASPE A CABEÇA DO MENSAGEIRO*" (*vide **Parte I** da Introdução*), para conhecer a mensagem, que era a "chave" para o receptor. Por exemplo, Leônidas (receptor) deveria conhecer a mensagem que fora enviada por sua esposa Gorgo (emissor) durante a batalha das Termópilas. Então, "chave" é um termo fundamental na Criptografia. Os métodos e algoritmos criptográficos podem ser divididos em dois grandes grupos em função do tipo de chave adotado: **Criptografia de Chave Única** (chave simétrica) e **Criptografia de Chave Dupla** (chaves assimétricas). Dentro do grupo de chave simétrica alguns exemplos podem ser citados, como: **Cifragem de Cesar**, **Cifra de Vigenère**, **AES**, **Serpent**, **RC4**, **IDEA**, etc. No grupo de Chaves Assimétrica temos: **RSA**, **DSS**, **El Gamal**, **Diffie-Hellman**, etc. A utilização de um ou de outro método varia de acordo com a importância avaliada para a informação contida na mensagem! Supondo que a mensagem seja: "*ENCONTRO DUAS DA TARDE ESTACIONAMENTO SHOPPING CENTER BRASIL*", qual seria o método criptográfico a ser utilizado para proteger esta mensagem? É claro que vai depender muito do "valor" (importância) da mensagem para ambos: emissor e receptor. Se este "encontro" fosse um encontro normal entre duas pessoas normais, poderia ser aplicada uma criptografia de chave única (simétrica); mas se o encontro fosse entre dois espiões, com segredos de estado comprometedores, então o "valor" da mensagem seria muito alto e a proteção teria que ser baseada numa criptografia de chave dupla (assimétrica).

Mas... afinal, qual é a diferença entre chave simétrica e chave assimétrica? Para uma explicação bem simples e objetiva, suponha que exista um quarto sem janelas e com apenas uma porta onde está guardado "algo"; se esse "algo" não for muito valioso, então pode existir uma única chave que abre e fecha a porta: uma chave única (simétrica). Mas, se o "algo" guardado for muito valioso, é mais seguro ter duas chaves (assimétrica): uma só para abrir e outra só para fechar. Em ambos os casos é necessário ter chave (uma ou duas) para ter acesso ao "algo" dentro desse quarto.

Situação 1: Para o caso de se ter uma única chave e com uma característica: *girando-a na fechadura para a esquerda abre a porta; girando para a direita fecha a porta*. Então, depois de colocar o "algo" dentro do quarto o dono da casa (emissor) fecha o quarto girando a chave para a direita, e a entrega ao seu filho para que ele possa entrar no quatro para ver o "algo" quando quiser. Assim, o ato de fechar a porta girando a chave para a direita seria ENCRIPTAR o "algo"; e quando o filho (receptor) fosse abrir a porta com a mesma chave, girando-a para a esquerda, seria o ato de DECRIPTAR para ver o "algo". Nesta situação, mesmo tendo que girar a chave na fechadura para a direita ou para a esquerda, ambos (emissor e receptor) usam a mesma chave: uma chave única, simples.

Situação 2: No caso de o “algo” ser muito valioso o dono da casa resolve colocar uma porta especial que requer duas chaves: uma só para fechar e outra só para abrir. Então, neste caso, o dono da casa fecharia a porta com uma chave **F** e daria uma outra chave **A** para o filho abri-la quando fosse necessário. Ao fechar a porta com a chave **F** seria como se o pai (emissor) estivesse ENCRIPTANDO o “algo”; e ao abrir a porta com a chave **A** seria como se o filho (receptor) estivesse “DECRIPTANDO” para ver o “algo” que estava protegido. Mas, em ambos os casos, não importa para que lado as chaves são giradas; o fato é que uma chave só fecha a porta e a outra só a abre. No jargão da Criptografia de chave assimétrica a chave para encriptar é chamada de “**chave pública**” e a chave para decriptar é a “**chave privada**”. Isto pode ser visto na **figura II.1**.

Continua com a “Cifragem de Cesar-1” **(Parte 3)**

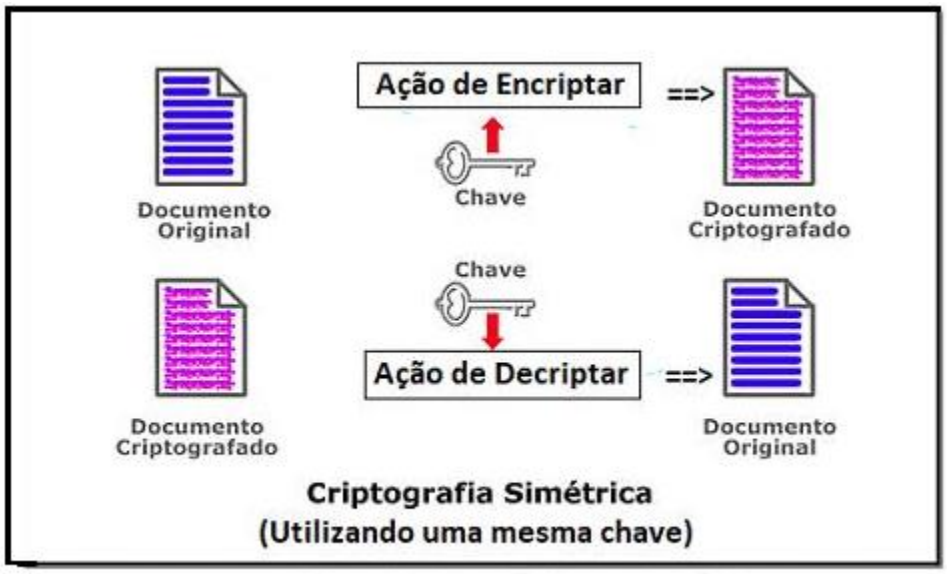

Figura II.1 - Criptografia de Chave Simétrica

Figura II.2 - Criptografia de Chave Assimétrica