Apresentação do Curso

Em todos os tempos a **Informação** tem sido uma arma muito poderosa nas tomadas de decisão e controle; seja individualmente, seja para as empresas ou para os governantes. Deste modo, a preservação e integridade de seu conteúdo é de fundamental importância, e não deve ser do conhecimento de pessoas não autorizadas. Portanto, a proteção dos dados que geram a informação, ou mesmo a informação em si, devem ser protegidos a todo custo.

E quando se fala em informação dois atores têm que ser considerados: o que emite a informação (*emissor*) e aquele que a recebe (*receptor*). Então, ao emitir (enviar) uma mensagem o emissor deve enviá-la com um certo "segredo" para despistar de pessoas não autorizadas. Este "segredo" está na maneira de como a mensagem é enviada, protegendo-a de olhares curiosos. Colocar um "segredo" em uma mensagem é codificá-la de maneira que só ambos, emissor e receptor, possam conhecer seu conteúdo; e isto é feito inserindo uma "chave" nela, para protegê-la.

Neste minicurso serão apresentadas técnicas de proteção de mensagens e como criar as chaves de codificação/decodificação de mensagens. Serão estudados três tipos de proteção de mensagens: *Cifragem de Cesar*, *Cifra de Vigenère* e *Método RSA*. O primeiro é baseado no sistema de chave simples monoalfabética, o segundo no sistema de chave simples polialfabética e o terceiro no sistema de chaves duplas.

Este minicurso é sequencial e exposto em doze arquivos *pdf*; cada um representando uma parte do curso. Portanto, deve ser seguido na sequência sugerida, de modo que: ***UM ARQUIVO SÓ DEVE SER LIDO E ESTUDADO DEPOIS DE O ANTERIOR TER SIDO INTEGRALMENTE LIDO, ESTUDADO E COMPREENDIDO***.

1) **Criptografia - Parte I (Introdução-1)**
2) **Criptografia - Parte II (Introdução 2)**
3) **Criptografia - Parte III (Cifragem de Cesar-1)**
4) **Criptografia - Parte IV (Cifragem de Cesar-2)**
5) **Criptografia - Parte V (Cifra de Vigenère-1)**
6) **Criptografia - Parte VI (Cifra de Vigenère-2)**
7) **Criptografia - Parte VII (Cifra de Vigenère-3)**
8) **Criptografia - Parte VIII (Método RSA-1)**
9) **Criptografia - Parte IX (Método RSA-2)**
10) **Criptografia - Parte X (Método RSA-3)**
11) **Criptografia - Parte XI (Método RSA-4)**
12) **Criptografia - Parte XII (Método RSA-5)**