**Princípios Básicos**

Encriptação ou cifragem é a conversão de dados legíveis para um formato ilegível (texto cifrado) por pessoas não-autorizadas, usando uma chave e um algoritmo criptográfico.

Seu objetivo é proteger a privacidade ao armazenarmos dados ou trocarmos informações com outras pessoas.

O receptor da mensagem encriptada pode decriptá-la e ler seu conteúdo, no formato original.

Desencriptação ou decriptação é o processo inverso da encriptação, ou seja, a transformação de dados encriptados (ilegíveis) em dados legíveis, usando uma chave e um algoritmo criptográfico (cifra).

**Criptoanálise**

Criptoanálise é o processo de transformação de dados cifrados (encriptados) em dados legíveis (decriptados) sem que se conheça a chave de encriptação.

Portanto, trata-se de “quebrar” a encriptação dos dados para obter acesso ao conteúdo das mensagens, porém com o intuito de descobrir falhas nos algoritmos para torná-los mais seguros, validá-los ou descartá-los.

Um exemplo clássico de criptoanálise foi realizada com o [**algoritmo de criptografia de redes wireless WEP**](http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf).

**Requerimentos de Segurança em Comunicações**

Há quatro princípios básicos que todo sistema de segurança em comunicações deve seguir. São eles:

* Autenticação
* Integridade
* Confidencialidade
* Não-Repúdio

**Integridade**

Um dos conceitos mais importantes é o da Integridade, que diz respeito ao conteúdo das informações trocadas entre transmissor e receptor.

Deve-se garantir que o conteúdo da mensagem chegue íntegro a seu destino, ou seja, que não seja alterado de nenhuma forma no meio do caminho.

**Autenticação**

Outro princípio importante é o da Autenticação.

A autenticação assegura que a mensagem foi realmente originada pelo remetente, e não por outra pessoa. Assim podemos ter certeza de quem enviou a mensagem.

**Confidencialidade**

Confidencialidade significa que a informação não está disponível para pessoas e processos que não tenham autorização para acessá-la e utilizá-la. Somente pessoas autorizadas podem ter acesso à informação transmitida ou armazenada.

**Não-Repúdio**

Deve-se também evitar que uma mensagem, após ter sido enviada, seja repudiada pelo transmissor – ele não poderá negar que a transmitiu.

Para isso podemos utilizar, por exemplo, assinaturas digitais – técnica que estudaremos ao longo do curso.

**Chaves (Keys)**

Uma chave é um valor matemático que determina como uma mensagem em texto plano será criptografada para produzir um texto cifrado, e ela também é necessária para que possamos recuperar a mensagem original.

A segurança de um sistema de criptografia deve residir em suas chaves, e os algoritmos devem ser sempre de conhecimento público.

A chave é um número secreto usado por um algoritmo de criptografia para alterar o texto plano e convertê-lo em texto cifrado, e é gerada aleatoriamente.

Se mesma chave for usada para encriptar e decriptar os dados, temos uma chave simétrica.

A chave é necessária pois manter o algoritmo em segredo não é efetivo – os invasores invariavelmente quebram o algoritmo (descobrem seu funcionamento).

Um exemplo histórico disso é o [**algoritmo RC4, que foi postado na Internet em 1994**](https://en.wikipedia.org/wiki/RC4#Security) por hackers anônimos.

**Características de uma chave**

**Comprimento da chave:** número de bits na chave (às vezes bytes).

**Espaço de chaves**: coleção de todos os valores matemáticos possíveis que tenham o mesmo comprimento de uma chave. Na prática, é o tamanho da chave, medido em bits.

Uma chave de comprimento ***n*** gera um espaço de chaves de***2n*** valores distintos. Uma chave de 64 bits portanto tem um intervalo de 0 a 264 combinações possíveis. Cada bit adicional dobra o tempo necessário para quebrar a chave – ou seja, chaves maiores dificultam o trabalho de um invasor.

http://www.bosontreinamentos.com.br/seguranca/introducao-a-criptografia/