Técnicas de Criptografia

Encriptação Simétrica e Assimétrica

# Ana Cristina Xavier

## *Centro Universitário Euro Americano*

Brasília, DF

## Abstract

## Introdução

### A.

## Segurança de computadores

Neste capítulo entraremos na parte básica de alguns conceitos cruciais para o melhor entendimento do desenvolvimento deste artigo.

### A. Conceitos De segurança De Computadores

### O Manual de Segurança de Computadores da NIST [NIST95] define o termo segurança de computadores da seguinte forma:

### Segurança de computadores: a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).

### Essa definição introduz três objetivos principais que são o coração da segurança de computadores:

### Confidencialidade e Privacidade: a confidencialidade assegura que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados e a privacidade assegura que os indivíduos controlem ou influenciem quais informações relacionadas a eles podem ser obtidas e armazenadas, da mesma forma que como, por quem e para quem essas informações são passíveis de ser reveladas.

### Integridade de dados sistema: a integridade de dado assegura que as informações e os programas sejam modificados somente de uma maneira especificada e autorizada. A integridade do sistema assegura que o mesmo

execute as suas funcionalidades de forma ilesa, livre de manipulações deliberadas ou inadvertidas do sistema.

### Disponibilidade: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.

A segurança da informação é utilizada no desenvolvimento de mecanismos ou algoritmos específicos de segurança, pois ela considera potenciais ataques e para garantir os itens citados acima existem técnicas que são aplicadas para auxiliar em uma melhor performance em proteger os sistemas e dados de uma ou mais organização.

### Autenticação: autenticação refere-se a um serviço que garante que uma comunicação é autêntica.

Controle de acesso relacionado a segurança da informação tem a ver com a capacidade de limitar e dominar o acesso aos sistemas e aplicações por meio de links de comunicação. [1]

## Criptografia

### Este capítulo abordará um dos principais conceitos que se tratam de criptografia e termos relacionados.

Criptografia é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e a compreenda. Criptoanálise é a arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise é chamada ataque. Criptologia é a ciência que reúne a criptografia e a criptoanálise. [2]

Cifrar é o ato de transformar dados em alguma forma ilegível. A intenção é de garantir a privacidade, conservando a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados. [2]

Decifrar é o processo inverso, ou seja, transforma os dados criptografados na sua forma original, inteligível. [2]

Para cifrar ou decifrar uma mensagem, é preciso obter informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia que foi usado, a mesma chave pode ser utilizada tanto para criptografar como para descriptografar mensagens, enquanto outros mecanismos utilizam senhas diferentes.

## Algoritmos

Os processos de cifragem e de decifragem estão definidos em algoritmos, que é a especificação de um procedimento padronizado, expresso por uma sequência finita e lógica de regras formais, que se destina à obtenção de um determinado fim. Tais algoritmos são um conjunto de complexas fórmulas ou operações matemáticas sobre determinados dados normais, com a intensão de transformá-los em dados cifrados. Sendo assim, deve existir também um algoritmo que faça o caminho inverso, capaz de reconverter os dados cifrados nos dados normais originais anteriores.

Na literatura pode-se encontrar vários algoritmos com diferentes técnicas, portadoras de especificidades e aspectos próprios. Em pesquisas relacionadas a essas técnicas para e elaboração deste artigo, foram apontadas como relevantes atualmente a criptografia simétrica e criptografia assimétrica que veremos mais à frente.

## Chaves

Agora que sabemos qual a principal função dos algoritmos de cifragem e decifragem podemos entender o como as chaves são importantes para a criptografia.

Esses algoritmos sempre se utilizam de uma sequência de bits especial, de um determinado tamanho planejado, como uma variável necessária e indispensável ao desempenho de sua tarefa. Essa sequência de bits é chamada de chave que possibilita todo o processo de criptografia.

Utilizando o algoritmo de cifragem é capaz de ter uma codificação individualizada, única e exclusiva para cada conjunto específico de dados sobre os você utilize. Sendo assim, o uso da chave é que o algoritmo de decifragem poderá realizar o caminho inverso, decodificando os dados cifrados.

A chave, numa analogia, seria algo como uma exclusiva e específica rota, traçada por um determinado caminho de um mapa que contivesse muitos bilhões de caminhos, a guiar o algoritmo em seus procedimentos de cifragem e decifragem. De onde o algoritmo sai e onde o algoritmo chega, guiado pela rota única definida no mapa, não se pode saber, a menos que se tivesse acesso ao mapa contendo a indicação do caminho seguido. [3]

#### REFERENCES

1. William Stalling (livro)
2. Carla Rocha Guimarães Uberlândia, dezembro 2001. (artigo)
3. GIUSTOZZI, Corrado. La crittografia a chiave pubblica e l'algoritmo RSA: terminologia crittografica, não paginado [<http://www.interlex.it/docdigit/corrado1.htm>]