Criptografia

Matheus Tiecher

Faculdade Iguaçu – Capanema – Paraná – Brasil

Mateus_tiecher@hotmail.com

Abstract. This article discusses the evolution of cryptography and its importance. It talks about symmetric key algorithms and asymmetric key algorithms (public), and their differences. It also explains the basics and how it works, demonstrates how and where it is used, and its importance and need to protect and communicate with security, privacy, integrity, and authenticity in this world of great technology.

Resumo. Neste artigo é abordado a evolução da criptografia e a sua importância. Fala sobre os algoritmos de chaves simétricas e algoritmos de chaves assimétricas (público), e as suas diferenças. Também explica os conceitos básicos e os funcionamentos da mesma, demonstra como e onde é usada, e a sua importância e necessidade para se proteger e para se comunicar com segurança, privacidade, integridade e autenticidade nesse mundo de grandes tecnologias.

Palavras chaves: Criptografia, simétrica e assimétrica, chaves criptográficas, história da criptografia.

1. Introdução:

A criptografia é um mecanismo de segurança e privacidade que embaralha as informações para que apenas as pessoas endereçadas possam visualizá-las. Usamos a criptografia diariamente na internet, as vezes sem ao menos perceber, ela está presente em quase todos os meios comunicativos, com algoritmos altamente complexos e com chaves de acesso.

A ideia básica da criptografia consiste em pegar um texto puro, ou seja, que ainda não tem criptografia e torná-lo um texto cifrado, para que isso aconteça é necessário que o texto puro passe por uma forma de transformação, nesse processo ele é parametrizado por uma chave, e a saída desse processo é a criptografia, ou seja, o texto cifrado.

2. História:

A necessidade de criptografar, cifrar informações, é muito antiga. Inicialmente foi usada pelos Romanos através da "Cifra de Cesar", usada nas guerras como tática militar por muitos anos, servia para passar ordens e mensagens aos exércitos de forma segura. Era um método simples e muito inteligente de criptografar e esconder mensagens importantes do exército inimigo.

Como toda tecnologia e inovação, a criptografia também evoluiu. Temos a criptografia clássica e a moderna, o marco que as separa é a chegada das novas tecnologias e da internet, então surge a necessidade de um mecanismo de defesa mais seguro para manter nossos dados mais confidenciais e protegidos. Com a importância de uma boa proteção de informação tornou-se algo indispensável em um sistema o uso da criptografia.

Um dos marcos da criptografia clássica é a Cifra de Cesar, que é um método muito simples de desordenar o alfabeto movendo-o para frente ou para trás quantas casas desejar, assim as letras ficariam desordenadas e apenas quem soubesse quantas casas foram andadas poderiam decifrar. Nos dias atuais essa criptografia não é mais segura, pois com alguns métodos de força bruta (tentativa e erro), ela poderia ser facilmente decifrada.

Do mesmo modo que a criptografia clássica, a criptografia moderna tem como objetivo a cifragem de dados e informações. Ela está presente em quase todos os meios comunicativos, com algoritmos altamente complexos e com chaves de acesso. Na criptografia moderna os algoritmos criptográficos podem ser divididos em algoritmos de chave simétrica e assimétrica (pública), a principal diferença entre elas são as chaves, pois a simétrica utiliza uma única chave,

tanto para cifrar como para decifrar enquanto na criptografia assimétrica são usadas duas chaves, uma pública que cifra e uma chave privada que decifra as informações.

3. O que é Criptografia?

Criptografar é a arte e a ciência de embaralhar dados e tornar textos ilegíveis, esconde e protege documentos e informações de pessoas indesejadas. A criptografia funciona da seguinte maneira: usa-se um texto puro e o embaralha, assim tornando-o ilegível, ou seja, um texto cifrado. Para decifrá-lo e torná-lo um texto puro novamente é necessário a chave de acesso que apenas a pessoa endereçada possui, assim, apenas o usuário endereçado poderá decifrar o texto cifrado.

A arte de solucionar mensagens cifradas é chamada de criptoanálise. E a de criar mensagens cifradas e solucioná-las é chamada coletivamente de criptologia.

A criptografia é um mecanismo de segurança e privacidade que usamos diariamente na internet, as vezes sem ao menos perceber (Criptografia em E-mails e mensagens). O uso da mesma é altamente importante e necessário, pois sem ela suas informações estariam vulneráveis na rede.

Atualmente existem dois tipos de criptografia: a simétrica e a assimétrica, tanto uma como a outra funcionam através de chaves para cifrar e para decifrar. A Criptografia Simétrica tende a ser mais rápida, porém menos segura, pois ela usa a mesma chave tanto para cifrar como para decifrar o arquivo. Já com a Criptografia Assimétrica são usadas duas chaves, a chave pública da pessoa endereçada para cifrar a informação e a chave privada da pessoa endereçada para decifrá-la, tendo assim uma grande segurança de que apenas a pessoa endereçada poderá decifrar essa criptografia e visualizar a informação.

Criptografia de chave simétrica: também chamada de criptografia de chave secreta ou única, ela usa a mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados, seu ponto negativo é que ela não é tão segura

quanto a chave assimétrica, porém ela é mais rápida. Os algoritmos de chave simétrica desfiguram os bits em uma séria de rodadas parametrizados pela chave para transformar o texto puro no texto cifrado. É necessário que haja uma pré comunicação combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Criptografia de chaves assimétricas: também conhecida como criptografia de chave pública, são usadas duas chaves distintas, a chave pública da pessoa endereçada para cifrar a informação e a chave privada da pessoa endereçada para decifra-la, tendo assim uma grande segurança de que apenas a pessoa endereçada poderá decifrar essa criptografia e visualizar a informação. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. A chave de decodificação não pode ser derivada a partir da chave de codificação. Essas propriedades tornam possível divulgar a chave pública. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

Com a chegada da internet e das novas tecnologias a criptografia tornou-se algo extremamente essencial e importante para nossa proteção e privacidade. Para entender a importância da criptografia, veja alguns lugares que em que ela está presente: e-mails, assinatura digital, transações bancárias, backups, servidores, trocas de informações e dados em geral.

Muitas empresas estão apostando caro na criptografia e na sua segurança, com software e algoritmos altamente potentes. Tudo isso para manter suas informações seguras e longe de pessoas indesejadas. A Google por exemplo, confia tanto em usa criptografia e no seu sistema que chegou a colocar uma recompensa de 200 mil dólares para quem achasse bugs e falhas de segurança no seu Android.

4. Conclusão:

Por fim, nota-se que o uso da criptografia é algo extremamente importante e essencial nos dias atuais, pois sem ela nossas informações e dados estariam vulneráveis a pessoas mal intencionadas e indesejadas. Várias empresas estão apostando caro nessa tecnologia, pois mantes suas informações seguras e longe de invasores é algo extremamente necessário. Quero ainda acrescentar que serão produzidos mais artigos sobre o assunto para dar sequências de como se manter protegido e também sobre o funcionamento das chaves de criptografia, dos certificados digitais e dos principais softwares usados.

5. Referencias:

Tanenbaum, (2003). Redes de Computadores / Andrew S. Tanenbaum. 1. Redes de computadores. I. Título.

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

PPL Ware no comments. disponivel em: <https://pplware.sapo.pt/informacao/conhea-a-historia-da-criptografia/>. Acesso em - 21/11/2017 as 23:59.

PPL Ware no comments. disponivel em: <https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/> - 22/11/2017 as 23:50.

Aperte F5 disponivel em: <http://www.apertef5.com.br/criptografia-o-que-e-e-para-que-serve/> - 23/11/2017 as 09:10.

Olhar Digital disponivel em: <https://olhardigital.com.br/fique_seguro/noticia/google-pagara-r-650-mil-a-quem-conseguir-hackear-o-android/68713> - 27/11/2017 as 09:30.

Google Sites disponível em:

<https://sites.google.com/site/kryptosgraphein/criptografiamoderna> - 02/12/2017 as 15:30.