INSTITUTO FEDERAL DE SÃO PAULO
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FELIPPE MARQUES DA SILVA DE ALMEIDA

CRIPTOGRAFIA

SÃO PAULO - SP
MAIO/2023

FELIPPE MARQUES DA SILVA DE ALMEIDA

CRIPTOGRAFIA

Trabalho apresentado ao Instituto Federal de São Paulo, como requisito para a disciplina de Segurança da Informação.

Professor (a): Miguel Molina

SÃO PAULO - SP

MAIO /2023

Sumário

Criptografia

A criptografia é uma técnica utilizada para proteger informações confidenciais, garantindo que apenas as partes autorizadas possam ter acesso a elas. A criptografia é uma área da segurança da informação que tem sido amplamente estudada e aplicada em diversos setores, incluindo governos, empresas e organizações.

O principal objetivo da criptografia é garantir a confidencialidade, integridade e autenticidade das informações. A confidencialidade refere-se à proteção das informações contra acesso não autorizado, enquanto a integridade refere-se à proteção contra alterações não autorizadas nas informações. A autenticidade refere-se à proteção contra falsificação de informações.

Existem várias técnicas de criptografia disponíveis, mas a mais comum é a criptografia de chave simétrica, que utiliza a mesma chave para cifrar e decifrar as informações. A chave é compartilhada entre as partes autorizadas e é mantida em segredo para garantir a confidencialidade das informações.

A criptografia de chave assimétrica é outra técnica comum, que utiliza um par de chaves – uma pública e outra privada. A chave pública é compartilhada entre as partes, enquanto a chave privada é mantida em segredo pelo proprietário. As informações cifradas com a chave pública só podem ser decifradas com a chave privada correspondente.

A criptografia é amplamente utilizada em diversos setores, incluindo finanças, governos, militares e comércio eletrônico. A criptografia também é utilizada em redes de computadores, para proteger as informações que são transmitidas entre as máquinas.

Apesar de ser uma técnica muito útil, a criptografia não é infalível. Os sistemas de criptografia podem ser quebrados, principalmente se a chave for descoberta ou se o algoritmo

utilizado for vulnerável. Portanto, é importante que as organizações continuem a investir em tecnologias de criptografia mais avançadas e mantenham suas chaves seguras.

Em resumo, a criptografia é uma técnica importante para garantir a segurança das informações confidenciais. A criptografia permite que as informações sejam compartilhadas de forma segura entre as partes autorizadas, garantindo a confidencialidade, integridade e autenticidade das informações.

Algoritmos de Criptografia

Existem diversos algoritmos de criptografia disponíveis, cada um com suas próprias características e níveis de segurança. Alguns dos principais algoritmos de criptografia incluem:

AES (Advanced Encryption Standard): é um algoritmo de chave simétrica amplamente utilizado, que oferece alto nível de segurança. O AES é capaz de cifrar e decifrar grandes quantidades de dados em alta velocidade.

RSA (Rivest-Shamir-Adleman): é um algoritmo de chave assimétrica que utiliza um par de chaves – uma pública e outra privada – para cifrar e decifrar informações. O RSA é amplamente utilizado em aplicações de comércio eletrônico, autenticação e assinatura digital.

Blowfish: é um algoritmo de chave simétrica rápido e seguro, que é amplamente utilizado em aplicações de segurança de rede e criptografia de arquivos.

DES (Data Encryption Standard): é um algoritmo de chave simétrica que foi amplamente utilizado em décadas passadas, mas que agora é considerado inseguro devido a vulnerabilidades descobertas. Ele foi substituído pelo AES.

3DES (Triple DES): é um algoritmo de chave simétrica que utiliza três vezes o DES para aumentar a segurança. Embora ainda seja utilizado em algumas aplicações, o 3DES está sendo gradualmente substituído pelo AES.

ECC (Elliptic Curve Cryptography): é um algoritmo de chave assimétrica que oferece alto nível de segurança com chaves menores em comparação com outros algoritmos de chave assimétrica. O ECC é amplamente utilizado em aplicações de segurança de dispositivos móveis e de Internet das Coisas.

Diffie-Hellman: é um algoritmo de troca de chaves que permite que duas partes estabeleçam uma chave compartilhada sem que a chave seja transmitida pela rede. O Diffie-Hellman é amplamente utilizado em aplicações de segurança de rede e criptografia de mensagens.

Em resumo, os algoritmos de criptografia desempenham um papel fundamental na proteção de informações confidenciais. A escolha do algoritmo de criptografia dependerá das necessidades de segurança específicas de cada aplicação, levando em consideração o nível de segurança necessário, a velocidade de processamento e outras considerações. É importante manter-se atualizado sobre os avanços em criptografia para garantir a segurança das informações.

PKI(Public Key Infrastructure)

É uma infraestrutura de chave pública que fornece serviços de segurança de chave pública, como autenticação, confidencialidade, integridade e não repúdio. A PKI é baseada em criptografia assimétrica, que utiliza um par de chaves - uma pública e outra privada - para proteger as informações.

A PKI utiliza uma Autoridade Certificadora (AC) para emitir certificados digitais que contêm informações de identidade de usuários, dispositivos e serviços. Esses certificados são usados para autenticar a identidade dos usuários e para garantir a confidencialidade e integridade das informações trocadas.

Os certificados digitais emitidos pela AC contêm a chave pública do usuário ou dispositivo e as informações de identidade do titular do certificado, como nome, endereço de e-mail, data de validade e outros detalhes relevantes. Esses certificados são geralmente armazenados em um repositório de certificados digitais para que possam ser acessados e validados conforme necessário.

A PKI é amplamente utilizada em aplicações de segurança, como comércio eletrônico, assinatura digital, autenticação e autorização em redes de computadores, e proteção de dados sensíveis. A PKI é uma ferramenta poderosa para garantir a segurança das informações e proteger a privacidade dos usuários.

No entanto, a implantação da PKI pode ser complexa e envolver vários componentes, incluindo a geração de chaves, a emissão de certificados, a revogação de certificados e a gestão do ciclo de vida dos certificados. Além disso, a segurança da PKI depende da segurança das chaves privadas, que devem ser protegidas adequadamente para evitar o acesso não autorizado.

Certificado Digital

Um certificado digital é um arquivo eletrônico que contém informações de identidade de uma pessoa, empresa ou dispositivo, além de sua chave pública. Os certificados digitais são emitidos por uma Autoridade Certificadora (AC) confiável e são usados para autenticar a identidade dos usuários, garantir a confidencialidade e integridade das informações trocadas e permitir a assinatura digital de documentos eletrônicos.

Um certificado digital geralmente contém informações como o nome do titular, o nome da empresa ou organização, o número do documento de identificação, o número de registro de contribuinte (CNPJ/CPF), a chave pública do titular e a data de validade do certificado. Essas informações são verificadas pela AC antes da emissão do certificado.

Os certificados digitais são amplamente utilizados em diversas aplicações, incluindo:

1.Comércio eletrônico: para autenticar a identidade dos usuários e garantir a segurança das transações financeiras;

2. Assinatura digital: para permitir a assinatura eletrônica de documentos, tornando-os legalmente válidos;

3. Autenticação de usuários: para permitir o acesso a sistemas e aplicativos, autenticando a identidade dos usuários;

4. Proteção de dados sensíveis: para proteger informações confidenciais, como dados de saúde, dados bancários e outras informações pessoais.

Os certificados digitais são armazenados em um repositório de certificados, que pode ser acessado por

aplicativos e sistemas para autenticar a identidade dos usuários e garantir a segurança das informações trocadas. A revogação de certificados também é possível, caso ocorra uma falha de segurança ou se o certificado se tornar obsoleto.

Em resumo, os certificados digitais são uma ferramenta essencial para garantir a segurança e privacidade das informações na era digital. Eles fornecem uma maneira segura de autenticar a identidade dos usuários, garantir a confidencialidade e integridade das informações e permitir a assinatura digital de documentos eletrônicos.