UNIVERSIDADE POSITIVO – UP
CURSO DE CIÊNCIAS DA COMPUTAÇÃO

CHAVES SIMÉTRICAS E CHAVES ASSIMÉTRICAS

YANN LUCAS SAITO DA LUZ

CURITIBA
2024

YANN LUCAS SAITO DA LUZ

CHAVES SIMÉTRICAS E CHAVES ASSIMÉTRICAS

Relatório escrito como requisito para conclusão da avaliação da atividade para composição de nota Bimestral da disciplina Criptografia e Segurança de Sistemas Computacionais da Universitário Positivo – UP.

Professor (a): Leandro Fabian Almeida Escobar.

CURITIBA

2024

RESUMO

Um algoritmo de criptografia representa uma fórmula matemática que sistematicamente converte dados em ciphertexts. Essa tecnologia também permite que os dados criptografados sejam revertidos em textos legíveis.

Há diferentes tipos de algoritmos que podem ser usados com a criptografia de dados simétrica e assimétrica.

Este artigo científico aborda os princípios da criptografia simétrica e assimétrica, apresentando suas diferenças, funcionamento e aplicações. Na criptografia simétrica, uma única chave é compartilhada entre emissor e receptor para codificar e decodificar os dados, proporcionando velocidade e eficiência, mas com uma camada de segurança limitada. Por outro lado, na criptografia assimétrica, são utilizadas duas chaves distintas e matematicamente associadas (chave pública e chave privada), oferecendo maior segurança, embora com uma complexidade e velocidade inferiores. Além disso, são discutidos seis dos algoritmos de criptografia mais comuns, incluindo DES, 3DES, AES, RSA, Twofish e RC4, destacando suas características e aplicações. Este artigo fornece uma visão abrangente das técnicas de criptografia, essenciais para garantir a segurança da informação em diversas aplicações digitais.

SUMÁRIO

1 INTRODUÇÃO

A criptografia é uma área fundamental na garantia da segurança da informação em sistemas computacionais, redes de comunicação e transações digitais. Com o aumento da dependência da sociedade em tecnologias digitais, a necessidade de proteger dados sensíveis contra acessos não autorizados tornou-se uma prioridade. Nesse contexto, a criptografia desempenha um papel crucial ao oferecer técnicas e algoritmos para codificar informações de maneira que apenas os destinatários autorizados possam decifrá-las.

Este relatório científico tem como objetivo explorar os princípios e aplicações da criptografia simétrica e assimétrica, dois dos principais paradigmas utilizados na proteção de dados digitais. Inicialmente, será apresentada uma visão geral dos conceitos básicos desses métodos, destacando suas diferenças fundamentais e os cenários em que são mais adequados. Em seguida, serão discutidos seis dos algoritmos de criptografia mais comuns, incluindo DES, 3DES, AES, RSA, Twofish e RC4, abordando suas características, funcionalidades e usos típicos.

Ao compreender os princípios e técnicas da criptografia, os profissionais de segurança da informação estarão mais bem preparados para implementar estratégias eficazes de proteção de dados e garantir a confidencialidade, integridade e autenticidade das informações transmitidas eletronicamente. Este relatório servirá como um recurso valioso para estudantes, pesquisadores e profissionais da área de segurança da informação interessados em aprimorar seus conhecimentos sobre criptografia e suas aplicações práticas.

2 O QUE SÃO AS CHAVES SIMÉTRICAS EM CRIPTOGRAFIA

Uma chave simétrica é uma única chave usada com as operações de um esquema de criptografia simétrica. Por exemplo, essa chave pode ser usada em um algoritmo de criptografia simétrica para criptografia e descriptografia.

No tipo de encriptação simétrica, o emissor e o receptor das informações utilizam uma chave simétrica idêntica para codificar e decodificar os dados transmitidos. Abaixo indicamos como se dá seu processo de funcionamento:

Quem envia e quem recebe os dados possuem a mesma chave criptográfica.

Utilizando essa chave secreta simétrica, o emissor criptografa os dados, transformando as informações textuais em um ciphertext ilegível.

É feito o envio dos dados criptografados através da internet.

O destinatário recebe os dados criptografados e decodifica eles com a mesma chave simétrica usada anteriormente, revelando as informações transmitidas.

Já que há apenas uma única chave, o processo de criptografia simétrica é mais ágil. Entretanto, apesar de ser eficiente, esse método não é tão seguro quanto a criptografia assimétrica de dados.

A codificação via chave simétrica é ideal em casos em que a prioridade é a velocidade e não a adição de uma camada extra de segurança. Muitas empresas costumam utilizar esse tipo de criptografia simétrica para proteger dados estacionários, como arquivos de contratos de trabalho de funcionários que são mantidos em um único local — como uma plataforma de armazenamento em nuvem.

Para que seja possível utilizar a mesma chave na criptografia e descriptografia é necessário o seu compartilhamento entre as partes envolvidas. Utilizamos esse tipo de criptografia quando queremos realizar comunicação ponto a ponto de modo seguro (VPNs, sistemas IoT, mensagens de chat, transferência de arquivos, dentre outros casos). Também é usado em sistemas corporativos ou controlados, em que as partes envolvidas podem compartilhar a mesma chave de forma segura (redes corporativas, comunicação entre servidores, sistemas de backup, dentre outros).

3 EXEMPLOS DE ALGORITIMOS DE CRIPTOGRAFIA QUE UTILIZAM CHAVE SIMÉTRICAS

Os algoritmos simétricos mais conhecidos são mais rápidos do que os algoritmos de chave pública mais conhecidos. Portanto, eles são preferenciais ao processar grandes quantidades de dados. Alguns dos algoritmos simétricos mais comuns são RC4, TRIPLE DES (Data Encryption Standard) e AES (Advanced Encryption Standard).

3.1 DATA ENCRYPTION STANDARD (DES)

Criado na IBM, o Data Encryption Standard (DES) foi um dos primeiros algoritmos criptográficos desenvolvidos. Ele é um algoritmo de tipo chave simétrica e era considerado o padrão federal de criptografia de dados dos Estados Unidos até 1999.

Devido a algumas preocupações com a segurança do método, novos algoritmos criptográficos modernos substituíram o já ultrapassado Data Encryption Standard. Isso porque suas chaves de 56 bits são muito curtas e, portanto, fáceis de serem decifradas por um computador moderno.

Antes de se tornar obsoleto, o DES era tipicamente utilizado para proteger transações financeiras eletrônicas. Seu uso na atualidade inclui treinamentos em criptografia e projetos de pesquisa.

3.2 TRIPLE DATA ENCRYPTATION STANDARD (3DES)

O algoritmo criptográfico 3DES (Triple Data Encryption Standard) é o sucessor do algoritmo DES original. Seu propósito inicial era de resolver os principais problemas do DES. Mais especificamente, a questão do tamanho pequeno da chave secreta (56 bits).

Assim como seu antecessor, o 3DES é um algoritmo criptográfico simétrico, e o tamanho das suas chaves é de 64 bits. Ele também foi desenvolvido a partir da mesma estrutura de códigos da Cifra Feistel.

O algoritmo simétrico 3DES utiliza um método de criptografia triplo, aplicando três vezes o algoritmo DES em cada bloco de dados. É assim que a chave do 3DES se torna mais longa e, portanto, significativamente mais difícil de decifrar.

3.3 ADVANCED ENCRYPTION STANDARD (AES)

O padrão de criptografia avançado — Advanced Encryption Standard (AES) — é um algoritmo simétrico mais recente. Ele substituiu o DES como o padrão criptográfico nacional dos EUA a partir da aprovação feita pelo Instituto Nacional de Padrões e Tecnologia, o NIST (National Institute of Standards and Technology).

A principal vantagem do AES sobre o DES é o tamanho das chaves geradas, cujo comprimento pode ser de até 256 bits, tornando-as mais difíceis de decifrar por usuários não autorizados. Além disso, o algoritmo de criptografia AES é mais rápido, já que é matematicamente mais eficiente.

Entre os algoritmos criptográficos simétricos, o AES é atualmente o mais popular. Seus principais usos incluem a segurança de redes Wi-Fi e a proteção de informações em plataformas de armazenamento de dados e em aplicativos móveis.

4 O QUE SÃO AS CHAVES ASSIMÉTRICAS EM CRIPTOGRAFIA

Também conhecida como criptografia de chave pública, o método assimétrico utiliza duas chaves diferentes, mas matematicamente associadas. Elas são chamadas de chave pública e chave privada.

A chave pública trata da criptografia dos dados e fica disponível para todo mundo. Os dados criptografados por ela só podem ser decodificados com a utilização da chave privada correspondente.

A chave privada, por sua vez, só pode ser gerada e usada pelos usuários legítimos que tenham a permissão de acesso às informações. Sendo assim, apesar de todos serem capazes de criptografar dados sensíveis, apenas o receptor específico a quem as informações foram destinadas pode revelá-las.

Abaixo listamos os passos que resumem o funcionamento das duas chaves num sistema de criptografia assimétrica:

Tanto o emissor quanto o receptor das informações geram seus pares de chaves assimétricas.

Ambos enviam a chave pública para o outro.

Com a chave criptográfica pública do receptor, o emissor criptografa os dados e os envia ao destinatário.

Utilizando sua própria chave privada, o destinatário decodifica os dados criptografados transmitidos e assim revela as informações.

Caso o receptor queira enviar os dados de volta ao emissor, a criptografia das informações deve agora ser feita através da chave pública do emissor original. E assim o processo se repete.

Algumas tecnologias utilizam uma abordagem híbrida, que combina os métodos de criptografia de dados simétrico e assimétrico. Os certificados TLS (Transport Layer Security) são um exemplo desse tipo de tecnologia.

Serviços de abordagem híbrida utilizam a criptografia assimétrica de dados para proteger a chave simétrica. Desse modo, os indivíduos ou dispositivos envolvidos

na transmissão dos dados vão utilizar uma única chave secreta simétrica para codificar e decodificar as informações sensíveis, ao invés de fazer uso de uma chave pública e uma chave privada para cada etapa.

Sendo assim, a criptografia de dados assimétrica oferece uma camada adicional de segurança, porém é mais lenta — justamente devido a esses passos extras. A criptografia de chave pública costuma ser utilizada mais comumente na proteção de trocas de informações sensíveis na internet, como mensagens de email.

5 EXEMPLOS DE ALGORITIMOS DE CRIPTOGRAFIA QUE UTILIZAM CHAVE ASSIMÉTRICAS

As chaves assimétricas são lentas, e por isso não são indicadas para a criptografia de dados muito grandes, porém são adequadas para trabalhar com chaves. Alguns exemplos de algoritmos que utilizam as chaves assimétricas são: RSA, Twofish e RC4

5.1 RSA

O Rivest-Shamir-Adleman (RSA) é um dos primeiros algoritmos criptográficos assimétricos. Apesar de ser antigo, ele se mantém como uma opção popular, já que oferece um alto nível de segurança.

O RSA utiliza o método matemático de Fatoração Primária — uma espécie de decomposição em fatores primos — para gerar uma longa sequência de números a partir de combinações menores. Assim, a partir de longas strings, os cibercriminosos precisariam determinar quais são as pequenas strings de números primos para então descobrir a chave secreta.

O algoritmo criptográfico RSA utiliza tamanhos de chave significativamente maiores do que outras soluções de algoritmos de criptografia de chave pública. O RSA suporta chaves assimétricas de até 4096 bits, que são quase impossíveis de decifrar, mesmo com um computador moderno.

Esse algoritmo de chave pública costuma ser utilizado para proteger aplicações web, mensagens de email e blockchains de criptomoedas. Os certificados SSL e TLS também fazem uso do algoritmo RSA para executar seus processos de criptografia assimétrica.

5.2 TWOFISH

O Twofish é um algoritmo de criptografia simétrico que suporta chaves de comprimento de até 256 bits. Ele foi inicialmente desenvolvido para substituir o DES, mas seu desempenho com chaves de 128 bits ficou aquém do algoritmo de criptografia AES.

Apesar de um pouco mais lento, este algoritmo oferece um nível de segurança similar ao do AES. A principal vantagem do Twofish, entretanto, está na sua flexibilidade, já que esse algoritmo adequado pode ser utilizado numa ampla gama de casos e aplicativos.

O Twofish possibilita a compensação de desempenho de acordo com a relevância de diversos parâmetros, como velocidade de encriptação e capacidades de hardware. Sendo assim, isso faz com que o algoritmo criptográfico Twofish seja a solução ideal para aplicações com recursos limitados de armazenamento e memória RAM.

Apesar do Twofish não ser tão amplamente utilizado quanto o AES, alguns apps populares usam esse método de criptografia:

PGP (Pretty Good Privacy) – programa de criptografia que realiza autenticação, codificação e decodificação de emails.

KeePass – ferramenta do tipo gerenciador de senhas para armazenamento e criptografia.

TrueCrypt – software de criptografia de disco para programas freeware, protegendo seus dados.

Peazip – criador e extrator de arquivos em ficheiros. Programa de código aberto.

5.3 RC4

O Rivest Cipher (RC4) é um algoritmo de criptografia simétrico que utiliza um sistema de cifras de fluxo. Trata-se de um método de codificação que processa os dados um bite por vez.

Essa encriptação simétrica é conhecida por sua simplicidade e bom desempenho. Os casos em que sua utilização é mais comum incluem certificados SSL e TLS, protocolos de criptografia para Wi-Fi e proteção de navegadores, como o Microsoft Edge.

De todo modo, o RC4 não é mais tão utilizado devido ao seu baixo nível de segurança. Apesar desse algoritmo criptográfico suportar chaves secretas de até 2048 bits, diversos estudos identificaram vulnerabilidades de segurança significativas no RC4.

Múltiplas variantes de criptografia foram desenvolvidas para resolver essas fragilidades, como os algoritmos Spritz, RC4A, RC4A+ e o VMPC (Variably Modified Permutation Composition).

6 CRIPTOGRAFIA SIMÉTRICA VS. ASSIMÉTRICA

A encriptação simétrica é um dos dois principais métodos de encriptar dados em sistemas de computadores modernos. O outro é a encriptação assimétrica, também conhecida como criptografia de chave pública. A principal diferença entre esses métodos é o fato de os sistemas assimétricos usarem duas chaves, e não apenas uma como no sistema de encriptação simétrica. Uma das chaves pode ser compartilhada publicamente (chave pública), enquanto a outra deve ser mantida em segredo (chave privada).

O uso de duas chaves ao invés de uma também produz uma variedade de diferenças funcionais entre a encriptação simétrica e assimétrica. Algoritmos assimétricos são mais complexos e mais lentos que os simétricos. Como as chaves pública e privada empregadas na encriptação assimétrica estão matematicamente relacionadas, as próprias chaves devem ser consideravelmente mais longas para fornecer um nível semelhante de segurança oferecido por chaves simétricas mais curtas.

7 CONCLUSÃO

A criptografia desempenha um papel essencial na proteção da informação em ambientes digitais, proporcionando uma camada de segurança vital contra ameaças cibernéticas. Neste relatório, exploramos os princípios e aplicações da criptografia simétrica e assimétrica, destacando suas características, diferenças e usos típicos. Desde a eficiência e velocidade da criptografia simétrica até a robustez e segurança da criptografia assimétrica, cada paradigma oferece vantagens e limitações que devem ser consideradas na implementação de sistemas de segurança da informação.

Além disso, discutimos seis dos algoritmos de criptografia mais comuns, incluindo DES, 3DES, AES, RSA, Twofish e RC4, examinando suas características e aplicações específicas. Esses algoritmos representam ferramentas poderosas para proteger dados sensíveis em uma variedade de cenários, desde transações financeiras online até comunicações de dados confidenciais.

Como a segurança da informação continua sendo uma preocupação crescente na era digital, é fundamental que os profissionais de segurança da informação estejam familiarizados com os princípios e práticas da criptografia. Ao entender os conceitos fundamentais e os algoritmos disponíveis, os profissionais podem tomar decisões informadas sobre as estratégias de proteção de dados mais adequadas para suas necessidades específicas.

Em última análise, a criptografia desempenha um papel central na construção de sistemas de segurança robustos e confiáveis, garantindo a confidencialidade, integridade e autenticidade das informações digitais. À medida que continuamos a avançar no mundo digital, a compreensão e a aplicação eficaz da criptografia serão essenciais para proteger nossos dados e preservar a confiança na era da informação..

REFERÊNCIAS

CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA: CONFIRA A DIFERENÇA, 2023. Disponível em: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/criptografia-simetrica-e-assimetrica/. Acesso em: 16 de abril de 2024.

CRIPTOGRAFIA-DIFERENCAS-SIMETRICA-ASSIMETRICA-HOMOMORFICA, 2023. Disponível em: https://www.alura.com.br/artigos/criptografia-diferencas-simetrica-assimetrica-homomorfica. Acesso em: 16 de abril de 2024.

WHAT-IS-SYMMETRIC-KEY-CRYPTOGRAPHY, 2022. Disponível em: https://academy.binance.com/pt/articles/what-is-symmetric-key-cryptography. Acesso em: 16 de abril de 2024.

SYMMETRIC-KEYS, 2023. Disponível em: https://learn.microsoft.com/pt-br/windows/win32/seccrypto/symmetric-keys. Acesso em: 16 de abril de 2024.

ASYMMETRIC ENCRYPTION SCHEMES, 2023. Disponível em: https://typeset.io/papers/asymmetric-encryption-schemes-q9jsu8dw. Acesso em: 16 de abril de 2024.

BASIC CRYPTOGRAPHY: ASYMMETRIC KEY ENCRYPTION, 2021. Disponível em: https://typeset.io/papers/basic-cryptography-asymmetric-key-encryption-1oxudevy. Acesso em: 16 de abril de 2024.

O QUE É CRIPTOGRAFIA: ENTENDA COMO ELA FUNCIONA, QUAIS OS DIFERENTES TIPOS E MAIS INFORMAÇÕES, 2022. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-criptografia. Acesso em: 16 de abril de 2024.