

**FCT – Faculdade de Ciências e Tecnologia**

**DMC – Departamento de Matemática e Computação**

**Bacharelado em Ciência da Computação**

**Pesquisa e construção de um algoritmo de criptografia**

**Lucas Cronemberger Domingues**

Orientador: Prof. Dr. Ronaldo Toshiaki Oikawa

Presidente Prudente, julho de 2024

1. **INTRODUÇÃO**

Criptografia é a ciência e a arte de transformar informações de maneira que apenas partes autorizadas possam acessá-las e entendê-las. Desde os tempos antigos, quando mensagens secretas eram escritas em códigos simples, até os complexos algoritmos matemáticos utilizados hoje, a criptografia tem sido uma ferramenta essencial para garantir a confidencialidade, integridade e autenticidade das informações.

No contexto moderno, a criptografia é fundamental para a segurança da informação em um mundo digital. Ela protege dados em trânsito, como comunicações via internet, e dados em repouso, como arquivos armazenados em discos rígidos e outros dispositivos de armazenamento. A criptografia é utilizada em uma variedade de aplicações, incluindo transações bancárias online, comunicação por e-mail, autenticação de usuários e proteção de informações sensíveis de empresas e governos.

1. **DES (Data Encryption Standard)**

O Data Encryption Standard (DES) foi desenvolvido pela IBM nos anos 1970 e adotado pelo National Institute of Standards and Technology (NIST) como um padrão federal dos EUA em 1977. DES foi projetado para fornecer um nível elevado de segurança para dados confidenciais em uma era de crescente digitalização.

DES é um algoritmo de criptografia simétrica, o que significa que a mesma chave é usada tanto para criptografar quanto para descriptografar dados. DES opera em blocos de 64 bits de dados, transformando-os através de 16 rodadas de substituições e permutações complexas controladas por uma chave de 56 bits. Cada rodada envolve processos como expansão, substituição, permutação e chave XOR.

Embora DES fosse considerado seguro na época de sua adoção, a chave de 56 bits tornou-se um ponto fraco significativo com o avanço da capacidade computacional. Ataques de força bruta (testar todas as combinações possíveis de chaves) tornaram-se práticos, comprometendo a segurança do algoritmo. Em 1999, um grupo conseguiu quebrar uma chave DES em menos de um dia.

Devido às suas limitações de segurança, o uso de DES foi amplamente descontinuado em favor de algoritmos mais robustos. A introdução de Triple DES (3DES) e, posteriormente, do Advanced Encryption Standard (AES) foi uma resposta direta às vulnerabilidades do DES.

1. **3DES (Triple Data Encryption Standard)**

Triple DES, ou 3DES, foi desenvolvido para melhorar a segurança do DES sem a necessidade de um novo algoritmo radicalmente diferente. Foi padronizado em 1995 como uma forma de estender a vida útil do DES diante de suas vulnerabilidades crescentes.

3DES aplica o algoritmo DES três vezes a cada bloco de dados, usando duas ou três chaves diferentes. Existem três variações principais de 3DES:

* EDE (Encrypt-Decrypt-Encrypt): Usa duas chaves (k1, k2) e executa uma criptografia com k1, uma descriptografia com k2, e outra criptografia com k1.
* EEE (Encrypt-Encrypt-Encrypt): Usa três chaves diferentes (k1, k2, k3) e aplica o DES em três etapas de criptografia consecutivas.
* EEE com duas chaves: Usa duas chaves (k1, k2) e executa três criptografias consecutivas, mas reutiliza k1 para a terceira etapa.

Ao aplicar DES três vezes, 3DES efetivamente aumenta o tamanho da chave para até 168 bits (ou 112 bits se duas chaves forem usadas), oferecendo uma proteção muito maior contra ataques de força bruta. No entanto, isso também resulta em uma operação mais lenta e um uso intensivo de recursos computacionais.

Embora mais seguro que o DES, 3DES também está sendo gradualmente substituído pelo AES, que é mais eficiente e oferece um nível de segurança ainda maior. Muitos sistemas que ainda utilizam 3DES estão migrando para AES.

1. **Blowfish**

Blowfish foi criado por Bruce Schneier em 1993 como uma alternativa gratuita e segura ao DES e outros algoritmos existentes na época. Foi projetado para ser rápido e flexível, sendo adaptável a diferentes comprimentos de chave.

Blowfish é um algoritmo de chave simétrica que usa tamanhos de chave variáveis entre 32 e 448 bits, com um tamanho de bloco fixo de 64 bits. O algoritmo divide a entrada de dados em blocos e os criptografa por meio de uma série de operações, incluindo expansão de chave, substituição e permutação. Blowfish usa 16 rodadas de processamento, onde cada rodada é uma combinação de funções de substituição (S-box) e permutação.

Blowfish é conhecido por sua resistência a muitos tipos de ataques criptoanalíticos, incluindo ataques de força bruta, graças ao seu comprimento variável de chave. No entanto, o tamanho fixo do bloco de 64 bits torna-o menos adequado para algumas aplicações modernas que requerem tamanhos de bloco maiores para maior segurança.

Blowfish tem sido amplamente utilizado em diversas aplicações, especialmente em software de segurança como ferramentas de criptografia de arquivos e protocolos de segurança de rede. Apesar de sua popularidade, muitos sistemas agora preferem usar algoritmos como AES, que oferecem blocos maiores de 128 bits e são mais eficientes para hardware e software modernos.

1. **AES (Advanced Encryption Standard)**

O Advanced Encryption Standard (AES) foi desenvolvido em resposta às limitações do DES e foi adotado como padrão pelo NIST em 2001. O algoritmo foi criado por dois criptógrafos belgas, Joan Daemen e Vincent Rijmen, e originalmente nomeado Rijndael.

AES é um algoritmo de criptografia simétrica que suporta chaves de 128, 192 e 256 bits, com blocos de dados fixos de 128 bits. O algoritmo é estruturado em várias rodadas de processamento (10, 12 ou 14, dependendo do tamanho da chave), cada uma composta por operações de substituição, permutação e mistura. As rodadas incluem quatro etapas principais: SubBytes, ShiftRows, MixColumns e AddRoundKey.

AES é amplamente considerado um dos algoritmos de criptografia mais seguros disponíveis atualmente. Seu design robusto o torna resistente a todos os ataques criptoanalíticos conhecidos, incluindo ataques de força bruta. Com tamanhos de chave maiores, a segurança do AES aumenta exponencialmente.

AES é amplamente adotado em uma variedade de aplicações, desde a segurança de dados pessoais até a proteção de informações governamentais classificadas. É o padrão de facto para criptografia de dados em muitas indústrias, incluindo finanças, saúde e tecnologia da informação.

1. **SAFER (Secure And Fast Encryption Routine)**

SAFER é uma família de algoritmos de criptografia simétrica desenvolvida por James Massey para a Cylink Corporation nos anos 1990. O objetivo era criar um algoritmo seguro e eficiente para criptografia de dados.

Existem várias versões do SAFER, incluindo SAFER K, SAFER SK, e SAFER+, cada uma com diferentes tamanhos de chave e número de rodadas. O algoritmo opera em blocos de dados, tipicamente de 64 ou 128 bits, e utiliza uma série de operações aritméticas e de substituição para transformar os dados de entrada. As versões mais modernas, como SAFER+, foram desenvolvidas para melhorar a segurança e o desempenho.

SAFER é conhecido por sua resistência a ataques criptoanalíticos, como criptoanálise diferencial e linear. As versões mais recentes, como SAFER+, incorporam melhorias que aumentam ainda mais sua robustez contra vários tipos de ataques.

Embora não seja tão amplamente adotado quanto AES ou até mesmo Blowfish, o SAFER tem sido utilizado em várias aplicações, incluindo sistemas de autenticação e dispositivos de hardware onde a eficiência é crucial. A família SAFER também tem sido popular em dispositivos móveis e sistemas embarcados devido ao seu design eficiente.

Works Cited

[1] Patil, Priyadarshini, et al. “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish.” *Procedia Computer Science*, vol. 78, 1 Jan. 2016, pp. 617–624, www.sciencedirect.com/science/article/pii/S1877050916001101, <https://doi.org/10.1016/j.procs.2016.02.108>. Accessed 3 July 2024.

[2] Srivastava, Shipra, et al. “Review on Quantum Safe Algorithms Based on Symmetric Key and Asymmetric Key Encryption Methods.” *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 28 Apr. 2022, ieeexplore.ieee.org/abstract/document/9823437, <https://doi.org/10.1109/icacite53722.2022.9823437>. Accessed 3 July 2024.