EXEMPLOS HISTÓRICOS E ALGORITMOS DE CRIPTOGRAFIA

Jhonatan de Lima Alves dos Santos – 824215769

Sistemas computacionais e segurança

Prof. Robson Calvetti

Universidade São Judas Tadeu - 2025

Introdução

- A criptografia é um método utilizado para proteger informações, tornando-as inacessíveis para pessoas não autorizadas. Seu objetivo principal é garantir a segurança dos dados, evitando que sejam lidos ou alterados sem permissão.
- Desde os tempos antigos, a criptografia tem sido usada para ocultar mensagens importantes, como em guerras e comunicações sigilosas. Com o avanço da tecnologia, os métodos de criptografia se tornaram mais sofisticados e são amplamente utilizados na proteção de senhas, transações bancárias e comunicações na internet.
- Neste trabalho, serão apresentados exemplos históricos do uso da criptografia e os principais algoritmos de criptografia simétrica e assimétrica utilizados atualmente.

Exemplos históricos do uso de criptografia

- A criptografia tem sido utilizada ao longo da história para garantir a segurança das informações. Dois exemplos notáveis são:
- **Cifra de Vigenère**: Desenvolvida no século XVI, a cifra de Vigenère é um método de criptografia polialfabética que utiliza uma palavra-chave para alterar os deslocamentos de caracteres no texto cifrado. Por muito tempo, foi considerada inviolável até que, no século XIX, Charles Babbage e Friedrich Kasiski desenvolveram métodos para quebrá-la (STALLINGS, 2020).
- **Máquina SIGABA**: Utilizada pelos Estados Unidos na Segunda Guerra Mundial, a SIGABA foi uma máquina de criptografia mais avançada que a Enigma alemã, sendo considerada inviolável durante o conflito. Sua segurança derivava da complexidade de suas engrenagens e da forma como gerava chaves criptográficas (KAHN, 1996).

Algoritmos de criptografia simétrica utilizados atualmente

- Na criptografia simétrica, a mesma chave é utilizada tanto para cifrar quanto para decifrar a informação. Dois dos algoritmos mais utilizados atualmente são:
- **AES (Advanced Encryption Standard)**: Criado para substituir o DES (Data Encryption Standard), o AES é um dos algoritmos mais seguros e amplamente adotados em sistemas de proteção de dados, como redes Wi-Fi e transações bancárias (NIST, 2001).
- **ChaCha20**: Desenvolvido por Daniel J. Bernstein, esse algoritmo de fluxo é utilizado em aplicações modernas, incluindo o protocolo TLS e sistemas operacionais como Android (BERNSTEIN, 2008).

Algoritmos de criptografia assimétrica utilizados atualmente

- A criptografia assimétrica utiliza um par de chaves – uma pública e uma privada – para garantir a segurança da comunicação. Dois dos algoritmos mais comuns são:
- **RSA (Rivest-Shamir-Adleman)**: Amplamente utilizado para assinaturas digitais e trocas de chaves seguras, sendo um dos padrões da segurança digital (RIVEST; SHAMIR; ADLEMAN, 1978).
- **ECDSA (Elliptic Curve Digital Signature Algorithm)**: Baseado em criptografia de curvas elípticas, é um algoritmo eficiente para assinaturas digitais, sendo mais seguro que o RSA para chaves menores (NIST, 2013).

Conclusão

- A criptografia desempenha um papel fundamental na proteção das informações, garantindo sigilo, autenticidade e integridade dos dados. Desde os métodos históricos, como a Cifra de Vigenère e a Máquina SIGABA, até os modernos algoritmos simétricos e assimétricos, sua evolução tem acompanhado as necessidades de segurança da sociedade.
- Atualmente, algoritmos como **AES, ChaCha20, RSA e ECDSA** são amplamente utilizados em diversas aplicações, como transações bancárias, comunicação digital e segurança de redes. Com o avanço da tecnologia, novos desafios surgem, exigindo o aprimoramento contínuo das técnicas criptográficas para garantir a proteção contra ataques cada vez mais sofisticados.
- Dessa forma, a criptografia continua sendo um dos pilares essenciais da segurança da informação, assegurando que dados sensíveis permaneçam protegidos no mundo digital.

Referências

- BERNSTEIN, Daniel J. *ChaCha, a variant of Salsa20*. 2008. Disponível em: https://cr.yp.to/chacha.html. Acesso em: 26 mar. 2025.
- KAHN, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner, 1996.
- NIST. *Advanced Encryption Standard (AES)*. FIPS PUB 197, National Institute of Standards and Technology, 2001. Disponível em: https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Acesso em: 26 mar. 2025.
- NIST. *Digital Signature Standard (DSS)*. FIPS PUB 186-4, National Institute of Standards and Technology, 2013. Disponível em: https://csrc.nist.gov/publications/fips/fips186-4/fips-186-4.pdf. Acesso em: 26 mar. 2025.
- RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Leonard. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, v. 21, n. 2, p. 120-126, 1978.
- STALLINGS, William. *Criptografia e segurança de redes: princípios e práticas*. 7. ed. São Paulo: Pearson, 2020.