Criptografia

Arthur Braga de Campos Tinoco
Arthur Gonçalves de Moraes

Objetivo

Conduzir estudos sobre os métodos de criptografia em diferentes cenários

Objetivos específicos:

- Avaliar quais são os métodos de criptografia mais seguros
- Avaliar quais são os pontos fracos de diferentes métodos de criptografia em diferentes cenários
- Analisar quais são os métodos de criptografia mais adequados para diferentes cenários

Revisão Bibliográfica

O estudo e comparação dos algoritmos de criptografia é de extrema importância para garantir a segurança dos dados.

O uso de métodos de criptografia em dispositivos IoT, por exemplo, enfrenta diversos desafios (capacidade computacional, disponibilidade de energia, etc) que devem ser considerados na implementação de um algoritmo. [1]

Trabalhos Relacionados

Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities [1]

Private simultaneous messages based on quadratic residues [2]

Square root computation in finite fields [3]

Referências

[1] THAKOR, Vishal A.; RAZZAQUE, Mohammad Abdur; KHANDAKER, Muhammad R. A. Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities. IEEE Access, [S.l.], v. 9, p. 28177-28193, 2021. Disponível em: https://doi.org/10.1109/ACCESS.2021.3052867. Acesso em: 16 maio 2024.

[2] SHINAGAWA, Kazumasa; ERIGUCHI, Reo; SATAKE, Shohei; NUIDA, Koji. Private simultaneous messages based on quadratic residues. Designs, Codes and Cryptography, [S.l.], v. 91, n. 12, p. 3915–3932, Aug. 2023. Disponível em: http://dx.doi.org/10.1007/s10623-023-01279-5. Acesso em: 16 maio 2024.

[3] ADIGUZEL-GOKTAS, Ebru; OZDEMIR, Enver. Square root computation in finite fields. 2024. Disponível em: https://arxiv.org/abs/2206.07145. Acesso em: 16 maio 2024.