PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Bacharelado em Ciência da Computação

Arthur Braga de Campos Tinoco
Arthur Gonçalves de Moraes

Criptografia: Uma Revisão da Literatura e Comparação de Implementações

Belo Horizonte

2024

Arthur Braga de Campos Tinoco
Arthur Gonçalves de Moraes

Criptografia: Uma Revisão da Literatura e Comparação de Implementações

Projeto de Pesquisa apresentado na disciplina Trabalho Interdisciplinar III - Pesquisa Aplicada do curso de Ciência da Computação da Pontifícia Universidade Católica de Minas Gerais.

Belo Horizonte

2024

RESUMO

A criptografia, derivada do grego kryptos ("escrita secreta"), é o conjunto de técnicas utilizadas para ocultar o significado de mensagens, tornando-as acessíveis apenas para destinatários específicos. Desde a antiguidade, com exemplos como os hieróglifos egípcios e a cifra de César, a criptografia tem sido fundamental para a proteção de informações confidenciais. Com o avanço da matemática e da computação, especialmente em teoria dos números e álgebra linear, a criptografia evoluiu, culminando em algoritmos modernos como o RSA, amplamente utilizado em segurança digital. Este artigo explora a evolução histórica da criptografia, suas aplicações contemporâneas, e a importância contínua de desenvolver métodos criptográficos mais seguros e eficientes para proteger dados pessoais e sigilosos em uma sociedade altamente conectada.

Palavras-chave: Criptografia, cifra de César, algoritmo RSA, segurança digital, teoria dos números, álgebra linear, proteção de dados, história da criptografia.

SUMÁRIO

1 INTRODUÇÃO

Criptografia, derivada do grego *kryptos* ('escrita secreta'), trata-se dos conjunto de princípios e técnicas utilizados para ocultar o significado de uma determinada mensagem, tornando-a legível somente a pessoas especificas. Sendo isto oriundo da necessidade de de se enviar a mensagem a dois ou mais pontos sem que fossem interceptadas ou alteradas, a invenção da criptografia data desde a antiguidade.

> A criptografia é tão antiga quanto à própria escrita, podendo ser encontrada no sistema de escrita Hieroglífica dos egípcios, onde era usada para esconder o significado real do texto e dar-lhe um caráter mais solene. Vários povos da antiguidade, dentre eles, gregos, hebreus, persas e árabes a utilizavam para tentar impedir que informações confidenciais, caso caíssem em mãos inimigas fosse interpretadas. (CARNEIRO, 2017)

Em se tratando do aspecto histórico, pode-se citar *a cifra de César* como exemplo de criptografia que data da antiguidade . Trata-se de um cifra de substituição baseada no deslocamento de caracteres do alfabeto, então, por exemplo, se aplicada a cifra de cesar com deslocamento de três casas, a palavra 'criptografia' se torna 'fulswrjudild'.

O desenvolvimento da matemática e da computação, sobretudo de ramos como a teoria dos números e álgebra linear, levou a um amadurecimento da criptografia. Um exemplo emblemático que ressalta tal importância é o algoritmo de RSA (*Rivest-Shamir-Adleman*), que é o algoritmo de chave pública mais utilizado no mundo, sendo ele presente em aplicações como o SSH (*Secure Shell*) ou *OpenPGP*, inteiramente baseado na aritmética modular.

Criptografia é por muitas vezes considerado um campo considerado obscuro dado a sua natureza matemático-formal, sobretudo em técnicas modernas, necessitando de uma exposição sobre seus problemas, fundamentos e métodos de resolução.

É de extrema importância conduzir estudos sobre criptografia, visando encontrar mais seguras e eficientes soluções para esse tópico tão importante na realidade altamente conectada em que vivemos, no que diz respeito à proteção de dados pessoais, assim como a de dados sigilosos de governos e empresas.

1.1 Objetivos

Este projeto tem por objetivo conduzir estudos sobre os métodos de criptografia em diferentes cenários.

1.1.1 Objetivos específicos

Os objetivos específicos deste projeto são:

1. Avaliar quais são os métodos de criptografia mais seguros, levando em consideração o contexto e o tipo de criptografia.
2. Avaliar quais são os pontos fracos de diferentes métodos de criptografia em diferentes cenários.
3. Analisar quais são os métodos de criptografia mais adequados para diferentes cenários.

2 REVISÃO BIBLIOGRÁFICA

Este capítulo apresenta a revisão bibliográfica acerca de alguns tópicos relacionados a criptografia.

2.1 Criptografia simetrica e assimetrica

Criptografia simétrica é aquela que demanda de uma única chave para criptografar e descriptografar os dados, enquanto as criptografias assimetricas demandam de duas chaves, sendo uma utilizada para criptografar os dados e outra para descriptografar.

2.2 Algoritmo RSA

O algoritmo RSA (Rivest-Shamir-Adleman) é um algoritmo de criptografia assimetrica baseado na facilidade de encontrar números primos grandes e a dificuldade de fatorar o produto de dois números primos grandes. O procedimento para gerar a chave pública e privada pode ser descrito da seguinte forma (CORMEN CHARLES E. LEISERSON, 2024):

- Selecione aleatoriamente dois números primos grandes p e q, tais que $p \neq q$.
- Calcule $n = pq$.
- Selecione um inteiro ímpar pequeno e tal que e seja primo com $\phi(n)$, que é igual a $(p-1)(q-1)$.
- Calcule d como o inverso multiplicativo de $e \mod \phi(n)$.
- Divulgue o par $P = (e, n)$ como a chave pública RSA do participante.
- Mantenha o par $S = (d, n)$ em segredo como a chave secreta RSA do participante.

2.3 Corpos finitos

Um corpo, segundo (ZAHN, 2022), é "um conjunto não vazio K munido de duas operações binárias, chamadas adição $+ : K \times K \to K, (a, b) \to a + b \in K$ e multiplicação $\cdot : K \times K \to K, (a, b) \to a \cdot b \in K$ que satisfazem os seguintes axiomas:

- Associatividade: $\forall x, y, z \in K$,

  $A1 : (x + y) + z = x + (y + z)$,
  $M1 : (x \cdot y) \cdot z = x \cdot (y \cdot z)$

- Comutatividade: $\forall x, y \in K$,

  $A2 : x + y = y + x$,
  $M2 : x \cdot y = y \cdot x$

- Elemento Neutro:

  $A3 : \exists 0 \in K$ tal que $x + 0 = x, \forall x \in K$
  O elemento 0 chama-se zero
  $M3 : \exists 1 \in K$ tal que $1 \neq 0, x \cdot 1 = x, \forall x \in K$
  O elemento 1 chama-se um

- Simétrico:

  $A4 : \forall x \in K, \exists -x \in K$ tal que $x + (-x) = 0$

- Inverso Multiplicativo:

  $M4 : \forall x \neq 0, x \in K, \exists x^{-1} \in K$ tal que $x \cdot x^{-1} = 1$

- Distributividade: $\forall x, y, z \in K$ tem-se

  $D1 : x \cdot (y + z) = x \cdot y + x \cdot z$
  $D2 : (x + y) \cdot z = x \cdot z + y \cdot z$

Portanto, um corpo finito é um corpo de tamanho finito, em que sua cardinalidade é sempre a potência de um número primo.

2.4 Curvas elipticas

Uma curva eliptica é, segundo (AUMASSON, 2018), uma curva no plano, isto é, um grupo de pontos com coordenadas x e y tal que, a equação da curva define todos os pontos pertencentes a ela. A equação da curva tipicamente utilizada em criptografia se encontra na forma $y^2 = x^3 + ax + b$ (também conhecida como forma de Weierstrass), onde as constantes a e b definem a forma da curva.

3 METODOLOGIA

Este capítulo apresenta a metodologia utilizada na pesquisa de abordagem quantitiva.

3.1 Atividades a serem realizadas

As atividades iniciam-se com a coleta de artigos, que em sequência passaram por um processo de filtragem e o mais adequados serão escolhidos. Após essa etapa de levantamento bibliográfico é feita uma análise metrica dos dados apresentados, o que possibilita uma avaliação dos algorítimos.

3.1.1 Atividade 1: Coleta de artigos

Primeiro define-se as bases de dados a serem utilizadas (IEE ACCESS e Designs, Codes and Cryptography). Após, é realizada a coleta de artigos que estejam relacionados a criptografia.

3.1.2 Atividade 2: Filtragem dos artigos

Os artigos selecionados previamente são filtrados por termos (algorithms, comparision, research), data de publicação (2019-2024) e pela leitura do resumo.

3.1.3 Atividade 3: Análise métrica

Análise dos resltados apresentados nos artigos, classificando os algoritimos quanto sua performace e gasto de energia.

3.1.4 Atividade 4: Avaliação dos algoritimos

Uma nova classificação dos algoritimos levando em conta os resulatdos anteriores e sua melhor aplicação em diferentes áreas da compuitação com base na sua disponibilidade de energia e poder computacional.

3.2 Cronograma

(Tabela 1).

Tabela 1 – Cronograma

	Meses 1-3	**Meses 4-6**	**Meses 7-9**	**Meses 10-11**
Coleta dos artigos	X	X		
Filtragem		X	X	
Análise métrica		X	X	X
Avaliação dos algoritimos				X

REFERÊNCIAS

ADIGUZEL-GOKTAS, E. O. E. Square root computation in finite fields. Designs, Codes and Cryptography, 2024.

AUMASSON, J.-P. Serious Cryptography. [S.l.]: No Starch Press, Inc., 2018.

CARNEIRO, F. J. F. Criptografia e Teoria dos Números. [S.l.]: Editora Ciência Moderna Ltda., 2017.

CORMEN CHARLES E. LEISERSON, R. L. R. C. S. T. H. Algoritmos: Teoria e prática. [S.l.]: GEN | Grupo Editorial Nacional S.A., 2024.

SHINAGAWA REO ERIGUCHI, S. S. K. N. K. Private simultaneous messages based on quadratic residues. Designs, Codes and Cryptography, 2023.

THAKOR MOHAMMAD ABDUR RAZZAQUE, M. R. A. K. V. A. Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities. IEEE Access, 2020.

ZAHN, M. Análise real. [S.l.]: Editora Blucher, 2022.