PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Bacharelado em Ciência da Computação

Arthur Braga de Campos Tinoco
Arthur Gonçalves de Moraes

Criptografia: Algoritmos e perspectivas para o futuro

Belo Horizonte

2024

Arthur Braga de Campos Tinoco
Arthur Gonçalves de Moraes

Criptografia: Algoritmos e perspectivas para o futuro

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 tem por objetivo apresentar, de maneira resumida, a revisão bibliográfica que fundamenta o presente artigo.

> Sem dúvida já lhes perguntaram muitas vezes para que serve a matemática, e se essas delicadas construções que tiramos inteiras de nosso espírito não são artificiais, concebidas por nosso capricho. Entre os que fazem essa pergunta, devo fazer uma distinção; os práticos reclamam de nós apenas um meio de ganhar dinheiro. Estes não merecem resposta; é a eles, antes, que conviria perguntar para que serve acumular tantas riquezas e se, para ter tempo de adquiri-las, é preciso negligenciar a arte e a ciência, as únicas que podem nos proporcionar espíritos capazes de usufruí-las, *et propter vitam vivendi perdere causas* (POINCARE, 2011)

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

O artigo *Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities*, publicado no *IEEE Acecess* de 2020 por Vishal A. Thakor, Mohammad Abdur Razzaque e Muhammad R. A. Khandaker, apresenta como problemática a implementação da criptografia em dispositivos IoT, dado os seus recursos físicos e lógicos limitados. O artigo tem por objetivo comparar os algoritmos existentes em termos de:

- Custos de implementação
- Performace de hardware e software
- Resistência a ataques

> IoT is becoming more common and popular due to its wide range of applications in various domains. They collect data from the real environment and transfer it over the networks. There are many challenges while deploying IoT in a real-world, varying from tiny sensors to servers. Security is considered as the number one challenge in IoT deployments,

> as most of the IoT devices are physically accessible in the real world and many of them are limited in resources (such as energy, memory, processing power and even physical space). (THAKOR MOHAMMAD ABDUR RAZZAQUE, 2020)

2.2 Square root computation in finite fields

O artigo *Square root computation in finite fields*, publicado no periódico *Designs, Codes and Cryptography* de 2024 por Ebru Adiguzel-Goktas e Enver Ozdemir, tem como problemática encontrar raízes quadradas em campos (corpos) finitos, por meio de três algoritmos práticos amplamente utilizados.

> In this paper, we present a review of three widely-used practical square root algorithms. We then describe a unifying framework where each of these well-known algorithms can be seen as a special case of it. The framework with singular curves offers a broad perspective to compare and further improve the existing methods in addition to offering a new avenue for square root computation algorithms in finite fields. (ADIGUZEL-GOKTAS, 2024)

2.3 Private simultaneous messages based on quadratic residues

O artigo *Private simultaneous messages based on quadratic residues*, publicado no periódico *Designs, Codes and Cryptography* de 2023 por Kazumasa Shinagawa, Reo Eriguchi, Shohei Satake e Koji Nuida tem por objetivo desenvolver um protocolo PSM (*Private Simultaneous Messages*) mais eficiente para funções simétricas (QR-PSM).

> Private Simultaneous Messages (PSM) model is a minimal model for secure multiparty computation. Feige, Kilian, and Naor (STOC 1994) and Ishai (Cryptology and Information Security Series 2013) constructed PSM protocols based on quadratic residues. In this paper, we define QR-PSM protocols as a generalization of these protocols. A QR-PSM protocol is a PSM protocol whose decoding function outputs the quadratic residuosity modulo p of what is computed from messages. We design a QR-PSM protocol for any symmetric function $f : \{0,1\}^n \longrightarrow \{0,1\}$ of communication complexity $O(n^2)$.(SHINAGAWA REO ERIGUCHI, 2023)

2.4 Criptografia e Teoria dos Números

O livro *Criptografia e Teoria dos Números*, de Framilson José Ferreira Carneiro, apresenta a evolução da criptografia ao longo da historia, seus aspectos básicos e a apresentação dos conceitos matemáticos necessários para a compreensão do método RSA.

> Para estudar matemática é preciso perseverança. A frustração faz parte do processo de aprendizagem, e e importante não desistir. À medida que se vai adquirindo mais intimidade com a disciplina e seus conteúdos, tudo se torna mais simples. (CARNEIRO, 2017)

3 METODOLOGIA

Este capítulo .... Apresentar uma classificação da pesquisa.

3.1 Atividades a serem realizadas

Esta seção apresenta ....

3.1.1 Atividade 1: xxxx

Descrição

3.1.2 Atividade 2: xxxx

Descrição

3.1.3 Atividade n: xxxx

Descrição

3.2 Cronograma

Esta seção apresenta ... (Tabela 1).

Tabela 1 – Cronograma

	Meses 1-3	**Meses 4-6**	**Meses 7-9**	**Meses 10-11**
Pesquisa asdads	X	X		
Coleta de dados		X	X	
sdfsdf	X		X	X
nova linha	X		X	X

4 PRIMEIRO CAPÍTULO DE EXEMPLO

A seguir serão apresentados alguns comandos do LaTex usados comumente para formatar textos de dissertação baseados na normalização da PUC (2011).

Para as citações a norma estabelece duas formas de apresentação. A primeira delas é empregada quando a citação aparece no final de um parágrafo. Neste caso, o comando cite é usado para formatar a citação em caixa alta, como é mostrado no exemplo a seguir. (DUATO; YALAMANCHILI; LIONEL, 2002).

Outra forma de apresentação da citação é a que ocorre no decorrer do texto, essa situação é exemplificada na próxima frase. Conforme Bjerregaard e Mahadevan (2006), o estudo mencionado revela progressos no desempenho dos processadores. Para a formatação da citação em caixa baixa deve ser usado o comando citeonline.

Nas citações que aparecem mais de uma referência as mesmas devem ser separadas por vírgulas, como neste exemplo. (KEYES, 2008; ZHAO, 2008; GANGULY et al., 2011). Se houver necessidade de especificar a página ou que foi realizada uma tradução do texto deve ser feito da seguinte maneira. (SASAKI et al., 2009, p. 2, tradução nossa). A citação direta deve ser feita de forma semelhante. "[...] A carga de trabalho de um sistema pode ser definida como o conjunto de todas as informações de entrada." (MENASCE; ALMEIDA, 2002, p. 160).

O arquivo dissertacao.bib mostra exemplos de representação para vários tipos de referências (artigos de conferências, periódicos, relatórios, livros, dentre outros). Cada um desses tipos requer uma forma diferente de representação para que a referência seja formatada conforme as exigências da normalização.

4.1 Primeira seção

Para gerar a lista de siglas automaticamente deve ser usado o pacote *acronym*. Para tanto, toda vez que uma sigla for mencionada no texto deve ser usado o comando ac{sigla}. Dessa forma, se for a primeira ocorrência da sigla a mesma será escrita por extenso conforme descrição feita no arquivo lista-siglas.tex. Caso contrário, somente a sigla será mostrada. Ex

4.1.1 Primeira subseção

As enumerações devem ser geradas usando o pacote *compactitem*. Cada item deve terminar com um ponto final. Abaixo um exemplo de enumeração é apresentado:

a) Coletar e analisar.
b) Configurar e simular.
c) Definir a metodologia.
d) Avaliar o desempenho.
e) Analisar e avaliar características.

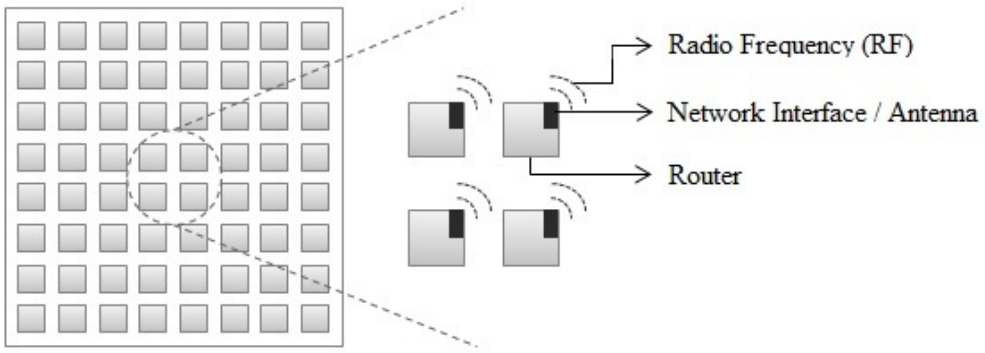
4.2 Segunda seção

Para referenciar um capítulo, seção ou subseção basta definir um label para o mesmo e usar o comando ref para referênciá-lo no texto. Exemplo: Como pode ser visto no Capítulo 4 ou na Seção 4.1.

5 SEGUNDO CAPÍTULO DE EXEMPLO

As figuras devem ser apresentadas pelos comandos abaixo. O parâmetro *width* determina o tamanho que a figura será exibida. No parâmetro *caption* o texto que aparece entre colchetes será o exibido no índice de figuras e o texto contido entre chaves será exibido na legenda da figura. Para citar a figura o comando ref deve ser usado juntamente com o label, como é mostrado nesse exemplo da Figura 1.

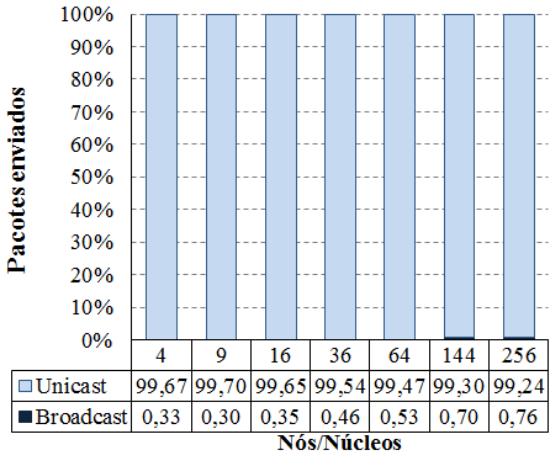
Figura 1 – Principais componentes de WiNoCs



Fonte: (OLIVEIRA et al., 2011)

Os comandos abaixo são usados para apresentação de gráficos. A diferença está apenas na definição do tipo “grafico“ que permite a adição dos itens no índice de gráficos de forma automática. Os parâmetros são semelhantes aos usados para representação de figuras. O parâmetro *width* determina o tamanho do gráfico. O texto entre colchetes no *caption* será o exibido no índice de gráficos e o texto contido entre chaves será exibido na legenda.

Gráfico 1 – Percentual de pacotes enviados



Fonte: Dados da pesquisa

Um exemplo de criação de tabela é mostrado a seguir. As colunas são separadas por elementos & e as linhas por duas barras invertidas. Os comandos *hline* e | definem a criação de linhas e colunas para separar os conteúdos, respectivamente. A tabela pode ser referenciada usando o comando ref juntamente com o label, como na Tabela 2.

Tabela 2 – Parâmetros definidos por classe

Benchmark	Parâmetro	Classe S	Classe W	Classe A	Classe B	Classe C	Classe D
BT	*Grid*	12^3	24^3	64^3	102^3	162^3	408^3
CG	Linhas	1400	7000	14000	75000	150000	1500000
EP	Pares	2^{24}	2^{25}	2^{28}	2^{30}	2^{32}	2^{36}
FT	*Grid*	64^3	$128^2 * 32$	$256^2 * 128$	$512 * 256^2$	512^3	$2048 * 1024^2$
IS	Chaves	2^{16}	2^{20}	2^{23}	2^{25}	2^{27}	2^{31}
LU	*Grid*	12^3	33^3	64^3	102^3	162^3	408^3
MG	*Grid*	32^3	128^3	256^3	256^3	512^3	1024^3
SP	*Grid*	12^3	36^3	64^3	102^3	162^3	408^3

Fonte: Adaptado de (NPB, 2011)

6 OBSERVAÇÕES IMPORTANTES

Este documento foi compilado em ambiente linux (Ubuntu 10.04) usando o programa Kile - an Integrated LaTeX Environment - Version 2.0.85. Para correta formatação os seguintes arquivos do pacote *abntex* devem ser alterados.

a) Arquivo abnt.cls
   No Ubuntu o arquivo fica armazenado em */usr/share/texmf/tex/latex/abntex*. Comentar a linha 967: Linha comentada para reduzir o espaçamento entre o topo da página e o título. Alterar a linha 1143: Parâmetro alterado de 30pt para -30pt para reduzir o espaçamento entre o top da página e o título do apêndice. Alterar a linha 985: Parâmetro alterado de 0pt para -30pt para reduzir o espaçamento entre o top da página e o título. Alterar a linha 991: Parâmetro alterado de 45pt para 30pt para reduzir o espaçamento entre o texto e o título.
b) Arquivo acronym.sty
   No Ubuntu o arquivo fica armazenado em */usr/share/texmf-texlive/tex/latex/acronym*. Alterar a linha 225: Inserir o separador – entre acrônimo/descrição e remover o negrito com o *normalfont*.

REFERÊNCIAS

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

BJERREGAARD, T.; MAHADEVAN, S. A survey of research and practices of network-on-chip. **Computing Surveys**, ACM, New York, USA, v. 38, n. 1, p. 1–51, Jun. 2006. ISSN 0360-0300.

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

DUATO, J.; YALAMANCHILI, S.; LIONEL, N. **Interconnection networks**: an engineering approach. San Francisco: Morgan Kaufmann Publishers, 2002. 515 p. ISBN 1558608524.

GANGULY, A. et al. Scalable hybrid wireless network-on-chip architectures for multi-core systems. **Journal Transactions on Computers**, IEEE Computer Society, Los Alamitos, USA, v. 60, n. 10, p. 1485–1502, 2011. ISSN 0018-9340.

KEYES, R. W. Moore's law today. **Circuits and Systems Magazine**, IEEE Computer Society, Los Alamitos, USA, v. 8, n. 2, p. 53–54, 2008.

MENASCE, D. A.; ALMEIDA, V. A. F. **Planejamento de capacidade para serviços na web**: métricas, modelos e métodos. Rio de Janeiro: Campus, 2002. 472 p. ISBN 8535211020.

NPB. **NAS Parallel Benchmarks**. Disponível em http://www.nas.nasa.gov/publications/npb.html. Acesso em jun. 2011.

OLIVEIRA, P. A. C. et al. Performance evaluation of winocs for parallel workloads based on collective communications. In: IADIS APPLIED COMPUTING, 8., 2011, Rio de Janeiro, Brasil. **Proceedings...** Rio de Janeiro: IADIS Applied Computing, 2011. p. 307–314.

POINCARE, H. O Valor da Ciência. [S.l.]: Contraponto Editora Ltda., 2011.

SASAKI, N. et al. A single-chip ultra-wideband receiver with silicon integrated antennas for inter-chip wireless interconnection. **Journal of Solid-State Circuits**, IEEE Computer Society, Los Alamitos, USA, v. 44, n. 2, p. 382–393, Feb. 2009. ISSN 0018-9200.

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.

ZHAO, D. Ultraperformance wireless interconnect nanonetworks for heterogeneous gigascale multi-processor SoCs. In: 2TH WORKSHOP ON CHIP MULTIPROCESSOR, MEMORY SYSTEMS AND INTERCONNECTS, 3., 2008, Beijing, China. **Proceedings...** Beijing: CMP-MSI, 2008. p. 1–3.