UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

JOÃO PEDRO RODRIGUES LEITE

SEGURANÇA EM COMUNICAÇÕES PÓS-QUÂNTICAS

TOLEDO

2025

JOÃO PEDRO RODRIGUES LEITE

SEGURANÇA EM COMUNICAÇÕES PÓS-QUÂNTICAS

Post-Quantum Communication Security

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Fábio Engel de Camargo

TOLEDO

2025

JOÃO PEDRO RODRIGUES LEITE

SEGURANÇA EM COMUNICAÇÕES PÓS-QUÂNTICAS

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 01/janeiro/2025

Nome completo e por extenso do Membro 1
Título (especialização, mestrado, doutorado
Nome completo e por extenso da instituição a qual possui vínculo

---

Nome completo e por extenso do Membro 2
Título (especialização, mestrado, doutorado
Nome completo e por extenso da instituição a qual possui vínculo

---

Nome completo e por extenso do Membro 3
Título (especialização, mestrado, doutorado
Nome completo e por extenso da instituição a qual possui vínculo

---

Nome completo e por extenso do Membro 4
Título (especialização, mestrado, doutorado
Nome completo e por extenso da instituição a qual possui vínculo

TOLEDO

2025

Espaço destinado à dedicatória (elemento opcional). Folha que contém o oferecimento do trabalho à determinada pessoa ou pessoas.
Exemplo:
Dedico este trabalho à minha família, pelos momentos de ausência.

AGRADECIMENTOS

Certamente estes parágrafos não irão atender a todas as pessoas que fizeram parte dessa importante fase de minha vida. Portanto, desde já peço desculpas àquelas que não estão presentes entre essas palavras, mas elas podem estar certas que fazem parte do meu pensamento e de minha gratidão.

Agradeço ao(a) meu(minha) orientador(a) Prof.(a) Dr. Fábio Engel de Camargo, pela sabedoria com que me guiou nesta trajetória.

Aos meus colegas de sala.

A Secretaria do Curso, pela cooperação.

Gostaria de deixar registrado também, o meu reconhecimento à minha família, pois acredito que sem o apoio deles seria muito difícil vencer esse desafio.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

Espaço destinado aos agradecimentos (elemento opcional). Folha que contém manifestação de reconhecimento a pessoas e/ou instituições que realmente contribuíram com o(a) autor(a), devendo ser expressos de maneira simples.

Não devem ser incluídas informações que nominem empresas ou instituições não nominadas no trabalho.

Se o aluno recebeu bolsa de fomento à pesquisa, informar o nome completo da agência de fomento. Ex: Capes, CNPq, Fundação Araucária, UTFPR, etc. Incluir o número do projeto após a agência de fomento. Este item deve ser o último.

Atenção: não utilizar este exemplo na versão final. Use a sua criatividade!

Primeira Lei: Um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum mal. Segunda Lei: Um robô deve obedecer as ordens que lhe sejam dadas por seres humanos, exceto nos casos em que tais ordens contrariem a Primeira Lei. Terceira Lei: Um robô deve proteger sua própria existência desde que tal proteção não entre em conflito com a Primeira e Segunda Leis (ASIMOV, Isaac, 1950) - observação: A referência deve ser incluída na lista de referências no final do trabalho.
(elemento opcional)

RESUMO

O resumo deve ressaltar de forma sucinta o conteúdo do trabalho, incluindo justificativa, objetivos, metodologia, resultados e conclusão. Deve ser redigido em um único parágrafo, justificado, contendo de 150 até 500 palavras. Evitar incluir citações, fórmulas, equações e símbolos no resumo. A referência no resumo é elemento opcional em trabalhos acadêmicos, sendo que na UTFPR adotamos por não incluí-la nos resumos contidos nos próprios trabalhos. As palavras-chave e as keywords são grafadas em inicial minúscula quando não forem nome próprio ou nome científico e separados por ponto e vírgula.

Palavras-chave: palavra-chave 1; palavra-chave 2; palavra-chave 3; palavra-chave 4; palavra-chave 5.

ABSTRACT

Seguir o mesmo padrão do resumo, com a tradução do texto do resumo e referência, se houver, para a língua estrangeira (língua inglesa).

Keywords: keyword 1; keyword 2; keyword 3; keyword 4; keyword 5.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, avanços consideráveis na pesquisa e desenvolvimento de tecnologia quântica têm levantado questões sobre a segurança dos sistemas de criptografia convencional. O poder de processamento das informações dos computadores quânticos, por realizarem operações em paralelo e explorarem os princípios da superposição e emaranhamento, representa uma ameaça significativa à criptografia convencional utilizada atualmente para proteger dados sensíveis em comunicações digitais. Enquanto a criptografia convencional depende da complexidade computacional para proteger os dados, os computadores quânticos podem potencialmente quebrar esses algoritmos em um tempo muito menor, comprometendo a confidencialidade e integridade das comunicações digitais (**??**). Computadores quânticos atualmente encontram-se em estágios iniciais de desenvolvimento e aplicação. Empresas e instituições de pesquisa ao redor do mundo estão trabalhando ativamente para construir e aprimorar esses sistemas. Alguns exemplos notáveis incluem os esforços da IBM, Google, Microsoft, Intel, Rigetti Computing, entre outros, bem como instituições acadêmicas e laboratórios de pesquisa governamentais (**??**). Embora os computadores quânticos ainda estejam longe de serem tão poderosos e amplamente disponíveis como os computadores clássicos, há avanços significativos sendo feitos nessa área. Esses avanços têm implicações profundas para vários campos, incluindo a criptografia.

Diante do cenário de avanços na pesquisa e desenvolvimento de tecnologia quântica e das preocupações crescentes com a segurança dos sistemas de criptografia convencional, surge um problema de destaque: a estratégia conhecida como “armazenar agora, decifrar depois” (*store now, decrypt later*). Essa abordagem baseia-se na aquisição e armazenamento a longo prazo de dados criptografados atualmente ilegíveis, aguardando possíveis avanços na tecnologia de decifragem que permitiriam sua leitura no futuro, em uma data hipotética referida como Y2Q (uma alusão ao Y2K *problem*, ou *bug* do milênio) (**??**). Esta estratégia, que espera explorar futuras quebras na criptografia para acessar informações previamente inacessíveis, é o problema principal abordado nesta proposta de trabalho. A partir dessa problemática, propõe-se um estudo sobre os métodos atualmente disponíveis para mitigar os riscos associados à estratégia “armazenar agora, decifrar depois". Em suma, os métodos criptográficos atuais enfatizam a adoção de algoritmos de “criptografia pós-quântica” (CPQ), oferecendo uma abordagem resistente à ameaça iminente dos avanços na computação quântica.

A segurança das comunicações digitais é essencial para a proteção da privacidade, integridade e autenticidade das informações. Diante da chegada dos computadores quânticos, a busca por soluções criptográficas pós-quânticas torna-se uma necessidade, visando garantir a segurança dos dados em um ambiente de ameaças em constante evolução.

O principal desafio deste projeto consiste na identificação e apresentação das novas técnicas criptográficas capazes de resistir aos potenciais ataques quânticos, e na compreensão dos fundamentos teóricos subjacentes a essas técnicas. A complexidade dos algoritmos

de criptografia pós-quântica apresenta um desafio significativo, exigindo um entendimento de conceitos matemáticos e computacionais.

Este trabalho pretende contribuir para uma maior compreensão dos desafios e soluções na área da segurança da informação em um contexto pós-quântico. Ao identificar e apresentar os algoritmos de criptografia pós-quântica existentes, espera-se fornecer uma conscientização em relação à importância da proteção das comunicações digitais em um ambiente de ameaças em constante evolução.

1.1 Objetivos

A seguir são apresentados os objetivos geral e específicos que regem esta proposta.

1.1.1 Objetivo Geral

O objetivo geral desta proposta de TCC é apresentar um estudo sobre as soluções de criptografia pós-quântica disponíveis para assegurar a segurança das comunicações digitais frente aos desafios impostos pela computação quântica. Este estudo visa o entendimento das tecnologias criptográficas que são projetadas para serem resilientes contra os métodos de quebra que computadores quânticos podem oferecer, uma vez que se tornem operacionais. Para tanto, o trabalho focará na revisão e apresentação dos algoritmos de criptografia pós-quântica mais relevantes e nos princípios que garantem sua eficiência. O trabalho pretende abordar algoritmos já estabelecidos e também, possivelmente, aqueles ainda em desenvolvimento, proporcionando uma visão ampla do estado atual da criptografia pós-quântica e suas potenciais aplicações práticas para proteger informações críticas em um futuro próximo.

1.1.2 Objetivos Específicos

Os objetivos específicos desta proposta de TCC incluem:

- Identificar e catalogar os principais algoritmos de criptografia pós-quântica que estão atualmente em uso ou em fase de desenvolvimento, descrevendo suas bases teóricas, características e contextos de aplicação.
- Identificar as principais técnicas empregadas pelos algoritmos de criptografia pós-quântica.
- Apresentar uma comparação sobre os algoritmos de criptografia pós-quântica entre si em termos de complexidade computacional e praticabilidade, utilizando critérios de avaliação para determinar suas vantagens e limitações.

- Elaborar recomendações para desenvolvedores web, tendo em visto as deficiências nos atuais algoritmos de criptografia, frente a potenciais aplicações práticas de computadores quânticos.

1.2 JUSTIFICATIVA

A relevância do problema abordado nesta proposta de trabalho reside na importância crescente da segurança da informação em um cenário onde avanços na computação quântica ameaçam comprometer os sistemas de criptografia convencionais. A possibilidade iminente de que computadores quânticos possam quebrar algoritmos de criptografia existentes representa uma ameaça significativa à confidencialidade e integridade das comunicações digitais atuais.

Dentre as contribuições deste trabalho, espera-se primeiramente, identificar e apresentar as novas técnicas criptográficas capazes de resistir aos potenciais ataques quânticos, proporcionando uma compreensão dos desafios e soluções na área da segurança da informação em um contexto pós-quântico. Além disso, o estudo dessas técnicas pode proporcionar informações importantes para o desenvolvimento de sistemas web seguros.

Quanto ao estágio de desenvolvimento dos conhecimentos referentes ao tema, embora os computadores quânticos ainda estejam em estágios iniciais de desenvolvimento e aplicação, os avanços significativos na pesquisa e desenvolvimento de tecnologia quântica nos últimos anos destacam a importância de antecipar e preparar-se para os desafios que esses avanços podem trazer para a segurança da informação.

Por fim, este trabalho tem o potencial de sugerir recomendações para desenvolvedores web, considerando as deficiências nos atuais algoritmos de criptografia frente às potenciais aplicações práticas de computadores quânticos. Ao identificar e descrever os principais algoritmos de criptografia pós-quântica, bem como suas características e contextos de aplicação, pretende-se oferecer orientações práticas para a implementação de medidas de segurança mais robustas e resilientes no ambiente digital.

Assim, considerando a relevância do problema, as contribuições esperadas, o estágio de desenvolvimento dos conhecimentos referentes ao tema e a possibilidade de sugerir recomendações práticas, justifica-se a realização deste trabalho de TCC.

1.3 Estrutura do trabalho

Este trabalho está estruturado da seguinte forma...

2 REFERENCIAL TEÓRICO

A computação quântica é uma área da ciência da computação e da física que utiliza os princípios da mecânica quântica para realizar operações. Diferentemente dos computadores clássicos, que usam bits binários (0 ou 1) para processar informações, os computadores quânticos utilizam qubits, que podem existir em superposição de estados. Isso significa que um qubit pode ser 0, 1 ou ambos ao mesmo tempo, permitindo que os computadores quânticos processem uma quantidade exponencialmente maior de informações em paralelo.

2.1 História da Computação Quântica

A história da computação quântica começa na década de 1980, com a contribuição de diversos cientistas que perceberam o potencial dos sistemas quânticos para realizar cálculos. Alguns dos principais pioneiros desse campo incluem Richard Feynman, David Deutsch, Peter Shor e Lov Grover.

Em 1981, durante uma conferência sobre física da computação no MIT (Massachusetts Institute of Technology), Richard Feynman propôs a ideia de que os computadores clássicos não eram capazes de simular sistemas quânticos de forma eficiente. Ele sugeriu a necessidade de um novo tipo de computador que fosse baseado em princípios quânticos (**??**). Essa ideia de Feynman foi fundamental para o desenvolvimento inicial da computação quântica, pois abriu caminho para a exploração de conceitos e tecnologias que poderiam aproveitar o poder dos fenômenos quânticos.

Em 1985, o físico britânico David Deutsch formalizou a ideia de um computador quântico universal. Ele introduziu o conceito de uma máquina de Turing quântica, demonstrando que um computador quântico poderia simular qualquer sistema físico, inclusive computadores clássicos (**??**). Deutsch começou a explorar algoritmos quânticos que poderiam ser mais eficientes do que os clássicos, estabelecendo as bases teóricas para futuros desenvolvimentos na área.

Em 1994, Peter Shor desenvolveu um algoritmo quântico que revolucionou o campo da criptografia. O algoritmo de Shor é capaz de fatorar grandes números inteiros em tempo polinomial, o que representa uma ameaça à segurança de muitos sistemas criptográficos baseados em fatoração, como o RSA (**??**). Essa descoberta destacou o enorme potencial dos computadores quânticos para resolver problemas que são praticamente insolúveis para computadores clássicos, mostrando uma das aplicações mais promissoras da computação quântica.

Em 1996, Lov Grover apresentou um algoritmo quântico para pesquisa em banco de dados, que é quadraticamente mais rápido do que qualquer algoritmo clássico equivalente (**??**). O algoritmo de Grover é especialmente relevante para problemas de busca não estruturada, oferecendo melhorias significativas na eficiência e exemplificando como a computação quântica pode ser aplicada para resolver problemas complexos de forma mais rápida e eficaz.

2.1.1 Comparação com a computação clássica

A comparação entre a computação quântica e a computação clássica revela diferenças fundamentais na forma como essas duas abordagens processam informações e resolvem problemas. A compreensão dessas diferenças é essencial para compreender o potencial dos computadores quânticos em relação aos computadores clássicos.

A diferença mais básica entre computadores quânticos e clássicos reside na forma como eles representam e processam informações. Como já mencionado anteriormente, os computadores clássicos utilizam bits, que são unidades de informação binária representadas por 0 ou 1. Cada bit pode estar em um desses dois estados, e a computação clássica se baseia na manipulação de grandes conjuntos de bits para realizar cálculos.

Por outro lado, os computadores quânticos usam qubits (bits quânticos). Um qubit pode estar em um estado de 0, 1, ou qualquer superposição de ambos os estados ao mesmo tempo, graças ao fenômeno quântico da superposição. Essa capacidade de estar em múltiplos estados simultaneamente permite que os computadores quânticos processem uma quantidade exponencialmente maior de informações em paralelo, o que os torna potencialmente muito mais poderosos para certas tarefas.

Devido à capacidade dos computadores quânticos de realizar operações em muitos estados simultaneamente, eles são especialmente adequados para resolver problemas que envolvem um grande espaço de possibilidades. Algoritmos quânticos, como o de Shor para fatoração de números inteiros e o de Grover para busca em bases de dados, demonstram como os computadores quânticos podem superar os limites dos algoritmos clássicos em termos de velocidade de execução e eficiência.

Os computadores clássicos são altamente eficientes para a maioria das tarefas diárias e continuam a ser a melhor escolha para muitas aplicações. No entanto, para problemas específicos que envolvem grandes espaços de solução ou fenômenos quânticos intrinsecamente complexos, os computadores quânticos oferecem vantagens significativas.

Apesar de suas capacidades, os computadores quânticos enfrentam desafios significativos em termos de correção de erros e estabilidade. Os qubits são altamente sensíveis a interferências externas, o que pode levar à decorrência e erros nos cálculos. Em contraste, os computadores clássicos são mais estáveis e possuem técnicas bem estabelecidas de correção de erros. Desenvolver formas de mitigar os erros quânticos é um dos principais desafios na construção de computadores quânticos práticos e de larga escala.

Os computadores quânticos ainda estão em fases iniciais de desenvolvimento, com protótipos atualmente limitados a algumas dezenas ou centenas de qubits. No entanto, a percepção de que eles são apenas um projeto científico foi superada; agora, eles são um projeto de engenharia em desenvolvimento. Não resta dúvida de que esses sistemas não apenas funcionarão, mas também se tornarão viáveis comercialmente e práticos no futuro (**??**). À medida que a tecnologia avança, espera-se que os computadores quânticos revolucionem campos como a

criptografia, a simulação de materiais e a otimização complexa, oferecendo soluções para problemas que são atualmente intratáveis com computadores clássicos.

2.1.2 Fundamentos da Computação Quântica

A computação quântica explora fenômenos quânticos únicos, como a superposição e o emaranhamento, que não têm equivalentes na computação clássica. A superposição permite que os qubits existam em múltiplos estados simultaneamente, o que aumenta exponencialmente o espaço de estado que pode ser explorado durante os cálculos. O emaranhamento cria uma ligação entre qubits, de modo que o estado de um qubit pode instantaneamente influenciar o estado de outro, independentemente da distância entre eles. Juntas, essas propriedades possibilitam a execução de operações em uma escala muito maior do que seria possível em sistemas clássicos.

Complementando a superposição e o emaranhamento, a interferência quântica é outro princípio crucial que permite manipular as probabilidades dos estados dos qubits. Por meio da interferência, é possível reforçar as soluções corretas de um problema enquanto cancela as incorretas. Essa propriedade é explorada em algoritmos quânticos para aumentar a eficiência na resolução de problemas complexos, como a busca em grandes bases de dados ou a simulação de sistemas moleculares. Assim, a interferência atua em conjunto com a superposição e o emaranhamento para amplificar o poder de computação dos qubits.

Para implementar esses conceitos, transformações condicionais e portas quânticas são fundamentais na manipulação precisa dos qubits. Portas como CNOT, Toffoli e Fredkin permitem realizar operações complexas, controlando o estado de um qubit com base no estado de outros, de forma semelhante às portas lógicas em circuitos digitais clássicos. A porta CNOT é essencial para criar o entrelaçamento de qubits, onde o estado de um qubit depende do estado de outro, mesmo que estejam separados por grandes distâncias. A porta Toffoli, por sua vez, pode realizar qualquer operação lógica necessária, enquanto a porta Fredkin oferece flexibilidade adicional ao permitir a troca dos estados dos qubits. Essas portas são a base para implementar a interferência e o emaranhamento em algoritmos práticos.

No entanto, a física quântica impõe restrições aos tipos de transformações que podem ser feitas. Todas as transformações de estado quântico, e portanto todos os portões quânticos e computações quânticas, devem ser reversíveis. Isso significa que cada transformação pode ser desfeita, permitindo uma manipulação mais eficiente dos dados. Na computação clássica, muitas operações são irreversíveis, levando à perda de informações e à necessidade de operações adicionais para gerenciar esses dados. A reversibilidade das operações quânticas evita esses problemas, resultando em um processamento mais eficiente e sustentável. Dessa forma, a reversibilidade não apenas otimiza a eficiência do processamento de informações, mas também aproveita ao máximo as propriedades fundamentais dos qubits.

2.1.3 Criptografia quântica

A criptografia quântica nos últimos anos tem sido alvo de muita pesquisa, tendo em vista que a tecnologia quântica representa uma ameaça significativa à criptografia tradicional. Os computadores quânticos possuem um poder de processamento que realizam operações em pararelo e exploram os princípios da superposição e emaranhamento, e isso poderá comprometer a segurança dos dados nas comunicações digitais. A criptografia tradicional utiliza como princípio algoritmos matemáticos, já a criptografia quântica utiliza propriedades quânticas da luz para realizar tarefas criptográficas (**??**). Essa ideia, que inicialmente foi apresentada por Stephen Wiesner na década de 1970, é baseada no princípio da incerteza de Heisenberg (**??**). A criptografia quântica aproveita propriedades como o comportamento duplo da luz (onda e partícula) e a interdependência instantânea entre elétrons de um par. Enquanto a criptografia clássica é segura enquanto o algoritmo de encriptação for seguro, mas é vulnerável a engenharia reversa e *hacking*, a criptografia moderna busca melhorar essas limitações usando chaves mais complexas e computação matemática avançada. Algoritmos de computação quântica, como o de Shor, podem quebrar muitos dos algoritmos criptográficos atuais em tempo significativamente menor. A criptografia quântica oferece segurança incondicional, mesmo contra adversários quânticos, e não depende da complexidade matemática, mas de princípios físicos quânticos.(**??**).

Conforme citado por Cameron R. Argetsinger a computação quântica pode ser o que vai salvar o mundo como o que vai acabar com o planeta, tudo depende de quem está manipulando essa tecnologia. Grupos criminosos já estão trabalhando nisso. O conceito de "*store now, decrypt later*" (também referido como "*harvest now, decrypt later*", ou "*steal now, decrypt later*") refere-se à prática de interceptar e armazenar dados criptografados atualmente, com a expectativa de que avanços futuros na tecnologia de computação quântica permitirão decifrar esses dados (**??**).

No contexto desta proposta de TCC, é de fundamental importância a tese de doutorado de **??**.A tese discute como a segurança das conexões TLS, que utilizam o protocolo ACME (*Automated Certificate Management Environment*), pode se tornar vulnerável à medida que computadores quânticos desenvolvem a capacidade de quebrar os algoritmos criptográficos atualmente em uso. Para enfrentar esse desafio, a criptografia pós-quântica (CPQ) é apresentada como uma solução viável, baseada em problemas matemáticos que são considerados resistentes tanto para computadores clássicos quanto para quânticos (**??**). Este trabalho fornece uma base para explorar soluções de segurança que protejam a confidencialidade dos dados em um cenário de computação quântica.

A criptografia pós-quântica (CPQ), portanto, é uma resposta à ameaça que a computação quântica representa para os métodos criptográficos atuais. Conforme abordado na pesquisa de **??**, a padronização de algoritmos de CPQ pelo NIST, como Dilithium, Falcon e SPHINCS+, busca garantir a segurança mesmo na era da computação quântica. Além disso, a transição para CPQ é desafiadora e complexa devido a questões de desempenho das aplicações e proto-

colos de rede, e a confiança nos novos algoritmos pós-quânticos, por esse motivo, Giron sugere a CPQ híbrida que fará uma transição mais suave à criptografia quântica.

No estudo realizado por **??**, a computação quântica não só transforma os paradigmas da segurança da informação, mas também impõe a necessidade de desenvolvimento contínuo de novos algoritmos que possam resistir aos ataques quânticos. A maior parte dos algoritmos de criptografia tradicionais é baseada na segurança matemática e que computadores convencionais não conseguiriam resolver. Um desses algoritmos é o RSA, sua base é cima de fatoração de números primos. Sua complexidade torna a quebra desse algoritmo altamente improvável na computação convencional, mas a estimativa é que um processador quântico com a capacidade de 6000 qubit levaria apenas 2 semanas para quebrá-lo (**??**).

3 TRABALHOS RELACIONADOS

Apresente aqui os trabalhos similares ao seu trabalho ou que são importantes para o entendimento do seu trabalho...

(ATENÇÃO -)

Atenção

Veja com o seu orientador se você vai ter este capítulo e se este vai ter nome, talvez ele seja uma seção de outro capítulo...

TEXTO TEXTO

4 MATERIAIS E MÉTODOS

Esta seção descreve os procedimentos adotados para alcançar os objetivos propostos no trabalho. Os métodos são estruturados em tópicos, cada um correspondendo a um subproduto do objetivo geral.

- Revisão Bibliográfica
  - Coleta de referências: Realizar uma busca em bases de dados acadêmicas, como IEEE Xplore, Google Scholar e ACM Digital Library, para identificar artigos, teses e relatórios técnicos sobre computação quântica e algoritmos criptográficos pós-quânticos.
  - Análise de conteúdo: Analisar e resumir os conteúdos coletados, focando nos fundamentos teóricos, características e contextos de aplicação dos algoritmos.
- Identificação das principais técnicas de criptografia pós-quântica.
  - Revisão de literatura: Examinar mídias especializadas e artigos recentes para identificar as técnicas comuns e emergentes em criptografia pós-quântica.
  - Documentação: Registrar as técnicas identificadas, destacando suas principais características e benefícios.
- Comparação de algoritmos de criptografia pós-quântica.
  - Definição de critérios de avaliação: Estabelecer critérios para avaliação dos algoritmos, como complexidade computacional, robustez contra ataques quânticos e praticabilidade.
  - Comparar: Utilizar os critérios definidos para comparar os algoritmos catalogados.
  - Elaboração de tabelas e gráficos: Apresentar os resultados da análise comparativa de forma visual, utilizando tabelas e gráficos para facilitar a interpretação dos dados.
- Recomendações para desenvolvedores web.
  - Elaboração de recomendações: Desenvolver recomendações práticas para os desenvolvedores web, baseadas nas análises e comparações realizadas anteriormente.

5 ALGORITMOS DE CRIPTOGRAFIA PÓS-QUÂNTICOS

6 RESULTADOS

Este capítulo apresenta o que foi obtido como resultado do trabalho, que, em princípio, é o sistema desenvolvido. Se não for um sistema, como, por exemplo, uma solução na área de redes, neste capítulo é reportada a solução proposta. Neste caso, a divisão do capítulo em seções é realizada, se necessária, de acordo com o trabalho.

O capítulo pode conter seções de acordo com o tipo de sistema e a necessidade de documentação mais extensa de determinados aspectos. Caso o trabalho se refira à comparação entre tecnologias ou dados obtidos como resultados do uso do sistema, além da descrição do sistema, há os dados obtidos com os testes e a discussão desses dados. Nesse caso haverá uma seção para os dados obtidos desses testes e as discussões.

6.1 Escopo do sistema

Apresenta o escopo do sistema (contendo entre dois ou cinco parágrafos) de forma bastante sucinta, considerando aspectos técnicos e conceituais. O escopo define o que é o sistema, consistindo das funcionalidades e características que o sistema deve conter. É importante apresentar também o escopo negativo, ou seja, as funcionalidades e características que o sistema não irá conter. Exemplo:

O sistema XYZ deve gerenciar todos os processos de uma livraria virtual, desde a aquisição até a venda dos livros para o consumidor final. O acesso dos compradores e gerentes deve ser feito por meio de um site WEB, incluindo a possibilidade de acesso por outras tecnologias (ex. celular, tablet). Os clientes poderão fazem as compras pagando com cartão de crédito ou depósito bancário. Existem promoções eventuais pelas quais os livros podem ser comprados com desconto.

De início, a livraria vai trabalhar apenas com livros novos a serem adquiridos de editoras que tenham sistema automatizado de aquisição. Desta forma, o sistema a ser desenvolvido deve conectar-se aos sistemas das editoras para efetuar as compras.

O sistema deve calcular o custo de entrega baseado no peso dos livros e na distância do ponto de entrega. Eventualmente podem haver promoções do tipo “entrega gratuita” para determinadas localidades.

O sistema deve permitir a um gerente emitir relatórios de livros mais vendidos, e compradores mais assíduos, bem como sugerir compras para compradores baseadas em seus interesses anteriores.

6.2 Modelagem do sistema

A modelagem do sistema inclui os diagramas e as descrições textuais para representar o problema e a solução.

Sendo assim, primeiramente esse item deve apresentar diagramas utilizados para a modelagem de negócios (ex. diagramas de atividade e estado), se esses tenham sido necessários. Em seguida esse item deve conter a descrição dos requisitos obtidos do usuário, contendo sua respectiva classificação (funcionais e não funcionais). Sugere-se o uso de um modelo formal sugerido por autores (ex. Wazlawick, Bezerra) para a apresentação dessa classificação.

Se utilizada orientação a objetos e a UML, nesta seção ainda são apresentados, por exemplo, os diagramas de casos de uso, com suas descrições suplementares, os diagramas de classe de análise (ou modelo conceitual), de sequência e/ou comunicação, diagrama de classes de projeto.

Nesta seção também estão os diagramas da modelagem de banco de dados, como entidade-relacionamento. Nesse item pode ser apresentada a descrição de cada uma das classes do modelo de classes apresentado acima, assim como a descrição das tabelas do banco de dados. Também podem estar documentados modelos e padronizações utilizados para a interface, diagramas de navegação, a representação da arquitetura do sistema e dos padrões de projeto utilizados.

6.3 Apresentação do sistema

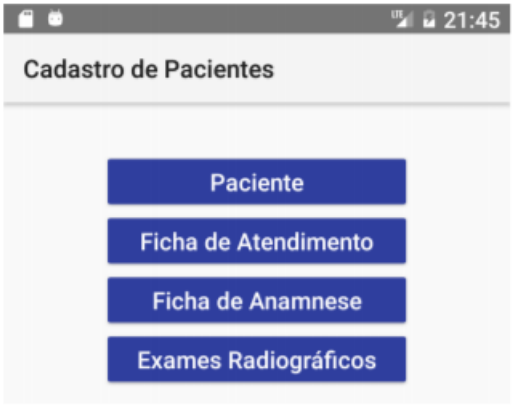
Apresenta as funcionalidades e o uso de recursos tecnológicos do sistema por meio de suas telas, enfatizando a interação com o sistema. A apresentação do sistema é feita sob a forma de texto, com telas e definição de padrões que forem relevantes ao contexto do trabalho. As telas são tratadas como figuras, cópias (print screen) de relatórios ou consultas também são figuras.

A Figura 1 exibe a tela de acesso ao Cadastro de Pacientes.

6.4 Implementação do sistema

Nesta seção é documentada a implementação do sistema com partes relevantes ou exemplos de código, rotinas, funções. Inclui, ainda, a descrição técnica do uso de recursos (componentes, bibliotecas, etc.) da linguagem. Ressalta-se que cada orientador avaliará juntamente com seu orientado o que poderá ser descrito nesta seção. Isso sem que sejam revelados detalhes do sistema que possam comprometer seu uso comercial ou científico ou que a descrição fique muito sucinta ou superficial.

Figura 1 – Tela de acesso ao Cadastro de Pacientes.



Fonte: Autoria própria (2024).

Em materiais e método estão quais os recursos utilizados, neste capítulo é reportado como esses recursos foram utilizados para resolver o problema.

Sugere-se colocar listagens curtas de código, enfatizando aspectos específicos das tecnologias utilizadas ou da implementação. Sugere-se, ainda, que o código não seja apresentado sob a forma de print screen, e sim copiado e colado no texto, mantendo, se possível, a formatação. Todas as listagens de código devem ser devidamente explicadas. A explicação deve ser técnica, fundamentada em aspectos conceituais e boas práticas de programação.

Enfatizar os diferenciais do sistema: procedimentos armazenados, consultas SQL, uso de componentes, uso de padrões de projeto, a forma de uso dos recursos da linguagem. Esses diferenciais são no sentido de explicitar as vantagens, desvantagens, dificuldades e facilidades que esses recursos impetraram no desenvolvimento do sistema em termos técnicos. Esses diferenciais servirão para avaliar pela utilização ou não desses recursos, pelo menos para sistemas iguais ou semelhantes ao reportado no trabalho.

Reportar a forma como o sistema foi verificado e validado. No sentido de verificar se os requisitos definidos para o mesmo foram atendidos. Os testes podem ser realizados pelo professor orientador, pelos professores que compõem a banca, por pessoas que serviram de base para as informações para o sistema e etc. Os testes podem ser realizados com base em um plano de testes elaborado juntamente com a análise e projeto do sistema. Para validar a implementação podem ser desenvolvidas rotinas de teste unitário.

Se houver implantação do sistema, mesmo que seja para teste, reportar a forma como isso foi feito, a geração de instaladores, os problemas com ambiente e sistema operacional, incluindo banco de dados e outros. Deixar explícito o procedimento para instalar e usar o sistema.

Quando for necessário, citar no texto do trabalho nomes de campos, tabelas ou rotinas específicas utilizadas na implementação de um software, utilizar a fonte courier new para destacar esses nomes.

Um exemplo de listagem de código fonte pode ser observado na Listagem 1, que representa a classe Aluno.

Listagem 1 – Classe Aluno

```
1  @Entity
2  public class Foo {
3
4      @Id
5      @GeneratedValue(strategy = GenerationType.IDENTITY)
6      private Long id;
7
8      private String nome;
9
10     private Integer ra;
11
12     // constructor, getters and setters
13 }
```

Fonte: Autoria própria (2024).

6.5 Discussões (opcional)

O trabalho contém esta seção quando considerado que há resultados (em termos de dados) e discussões relevantes ou suficientes para justificar uma seção. Se existentes e não justificarem uma seção, eles podem estar na seção que relata a implementação do sistema.

Nesta seção estão os resultados obtidos da realização de testes quantitativos e qualitativos, independentemente da quantidade, tipo e volume de testes realizados. Os resultados dos testes são discutidos tendo como base o referencial teórico e os objetivos pretendidos com o trabalho. Esses testes podem resultar de implantação e testes de uso do sistema.

7 CONCLUSÃO

Inicia com um resumo do trabalho, retomando o(s) objetivo(s), o referencial teórico e o uso das ferramentas e das tecnologias utilizadas no trabalho.

A conclusão contém a opinião do autor em relação às vantagens, desvantagens, facilidades e limitações das tecnologias e/ou do método utilizados, as dificuldades encontradas e como foram superadas.

Também devem ser apresentadas as vantagens, desvantagens e limitações do trabalho desenvolvido, sempre tendo em vista a sua contribuição para a comunidade acadêmica e profissional e para a sociedade como um todo.

É a opinião técnica do autor do trabalho em relação ao assunto sob a forma de uma espécie de avaliação em relação ao trabalho desenvolvido e as tecnologias utilizadas.

Finaliza verificando se o objetivo foi alcançado e com a opinião do autor sobre o assunto, de acordo com o referencial teórico e com os resultados obtidos.

As perspectivas futuras são opcionais, devem ser apresentadas somente caso o acadêmico pretenda dar continuidade ao trabalho, ou mesmo se ele julgar relevante que outras pessoas dêem continuidade ao seu trabalho.