UNIVERSIDADE SÃO JUDAS TADEU

CIÊNCIA DA COMPUTAÇÃO

GIOVANNI RIBEIRO IANNACE - 82421986

GIOVANNA FONTES DA SILVA - 823148980

GABRIEL FABRÍCIO SILVA MACIEL - 823154960

GABRIELA ALVES RODRIGUES - 82311687

LUCAS GASPARETTO NARCIZO DE MORAIS - 82426494

Votação Eletrônica em Criptografia RSA

São Paulo

2024

1. RESUMO

O presente projeto teve como objetivo desenvolver um sistema de votação eletrônica seguro e eficiente, garantindo a confidencialidade, integridade e anonimato dos votos por meio da aplicação de técnicas de criptografia. Os principais resultados apresentados são que o sistema desenvolvido atende aos requisitos de segurança esperados, com a criptografia RSA garantindo que os votos sejam transmitidos e armazenados de forma segura, preservando o anonimato dos participantes.

2. INTRODUÇÃO

Em um mundo cada vez mais digital, a segurança nos processos eleitorais se tornou uma preocupação central, especialmente com a crescente adoção de sistemas de votação eletrônica. A confiabilidade e a integridade do voto são princípios fundamentais em qualquer eleição, sendo necessário garantir que o sistema utilizado seja capaz de proteger o anonimato das reuniões e prevenir qualquer tipo de fraude ou manipulação de dados.

O presente projeto foi desenvolvido com o objetivo de criar um sistema de votação eletrônica que atenda a esses requisitos de segurança, utilizando técnicas de criptografia. A escolha da criptografia RSA, exclusivamente reconhecida pela sua robustez em garantir a segurança de dados, foi crucial para garantir que os votos fossem transmitidos e armazenados de forma confidencial, além de garantir a integridade e a integridade do processo eleitoral.

Além disso, o projeto buscou fornecer uma interface acessível aos participantes, garantindo uma experiência de uso simples e intuitiva. A gestão e organização das tarefas foram realizadas por meio da ferramenta Trello, permitindo um fluxo eficiente de trabalho entre os membros do grupo. Apesar dos desafios enfrentados durante o desenvolvimento, o resultado final foi um sistema funcional que atende às exigências de segurança e desempenho esperados em um sistema de votação eletrônica moderna.

Este relatório apresentará em detalhes a metodologia utilizada, as tecnologias empregadas, os testes de validação realizados e os principais resultados de exercícios, oferecendo uma visão abrangente sobre o desenvolvimento do sistema.

2.1 Objetivo

Este projeto teve o objetivo de contar os votos em criptografia rsa garantindo segurança, integridade e precisão no resultado final.

3. DESENVOLVIMENTO E METODOLOGIA

A seguir, a pesquisa realizada a fundo pelo grupo para realizar o projeto com êxito.

3.1 O que é criptografia

Criptografia nada mais é do que a prática de proteger informações por meio do uso de algoritmos codificados, hashes e assinaturas. Essas informações podem estar em repouso (como um arquivo em um disco rígido), em trânsito (como comunicação eletrônica trocada entre duas ou mais partes) ou em uso (durante a computação de dados). A criptografia tem quatro objetivos principais:

- Confidencialidade: disponibiliza as informações somente para usuários autorizados.
- Integridade: garante que as informações não tenham sido manipuladas.
- Autenticação: confirma a autenticidade das informações ou a identidade de um usuário.
- Não repúdio: impede que um usuário negue compromissos ou ações anteriores.

A criptografia usa vários algoritmos criptográficos de baixo nível para atingir um ou mais desses objetivos de segurança das informações. Essas ferramentas incluem algoritmos de encriptação, algoritmos de assinatura digital, algoritmos de hash e outras funções. [1]

3.1 Para que serve a criptografia

A criptografia tem origem no envio de informações confidenciais entre figuras militares e políticas. As mensagens deveriam ser criptografadas para parecerem textos aleatórios para qualquer pessoa, exceto para o destinatário pretendido.

Atualmente, as técnicas originais de encriptação foram completamente rompidas. Elas foram rompidas a ponto de serem encontradas apenas nas seções de enigmas de alguns jornais. Felizmente, o campo fez grandes avanços em segurança, e os algoritmos usados hoje dependem de análises e matemática rigorosas para sua segurança. [3]

À medida que a segurança avançou, o campo da criptografia se expandiu para incluir uma gama mais ampla de objetivos de segurança. Isso inclui autenticação de mensagens, integridade de dados, computação segura e muito mais.

A criptografia compõe a base da sociedade moderna. É a base de inúmeras aplicações de Internet através do Secure Hypertext Transfer Protocol (HTTPS), da comunicação segura de texto e voz e até de moedas digitais. [1]

3.2 Criptografia RSA e como ela se compara a outros métodos de criptografia

O mundo funciona com comunicação. Todos precisam enviar e receber informações. Infelizmente, a digitalização e o fácil acesso à internet tornaram necessário o envio de comunicações privadas, uma vez que nem todos on-line são confiáveis.

A humanidade sempre encontrou maneiras de enviar mensagens ocultas que somente o destinatário pretendido poderia interpretar. Essa forma de comunicação é chamada de criptografia, referindo-se à capacidade de criptografar informações que exigem cifras específicas ou métodos para decodificar.

A criptografia é fundamental para uma sociedade digital funcional e segura. Ele impede o fácil acesso de informações pessoais e confidenciais por agentes mal-intencionados com conexão à internet. Também é uma preocupação

significativa, dado que o custo total médio para violações de dados de 50 milhões a 60 milhões de registros atingiu US$ 387 milhões em 2022.

A criptografia RSA é um desses sistemas criptográficos para a descriptografia de mensagens privadas que utiliza um algoritmo de chave pública. Para entender melhor o que é, vamos responder à pergunta: "Qual é a criptografia de dados e o algoritmo de criptografia de chave pública?" [2]

3.3 Criptografia de dados explicada

A criptografia de dados ou a decifração envolve disfarçar informações como texto cifrado. O texto cifrado não é inteligente para pessoas não autorizadas. Por outro lado, decifrar ou descriptografar envolve converter o texto cifrado de volta no formato original. A criptografia manual remonta ao Império Romano. No entanto, hoje em dia, a criptografia é um processo fundamental da criptologia e é sinônimo de ocultar informações por meio de métodos eletrônicos.

Os computadores aplicam um algoritmo para criptografar dados. Um algoritmo é um conjunto de instruções ou procedimentos para executar tarefas específicas em blocos de dados. Uma chave é um nome de criptografia pessoal que somente o usuário ou transmissor da mensagem e o receptor pretendido conhecem. Atualmente, existem dois tipos principais de criptografia:

- A criptografia simétrica usa a mesma chave para criptografar e descriptografar dados, como o padrão de criptografia avançada (AES, Advanced Encryption Standard)
- A criptografia assimétrica que também é chamada de criptografia de chave pública, pois exige um par de chaves, uma pública para criptografia e outra privada para descriptografia. O algoritmo Rivest Shamir Adleman é um exemplo comum. [2]

O RSA funciona porque chaves de criptografia selecionadas aleatoriamente com comprimento suficiente são praticamente intransponíveis. Algoritmo de criptografia de chave pública. Também é chamado de algoritmo assimétrico, no qual o remetente e o destinatário usam chaves diferentes para criptografar e

descriptografar dados. O algoritmo assimétrico atribui a cada remetente um par de chaves:

- Uma chave pública para criptografia
- Uma chave privada para descriptografar dados

Embora as duas chaves estejam vinculadas, é impossível derivar a chave privada da chave pública ou descriptografar dados usando uma chave pública. Como o nome sugere, a chave pública é bem conhecida, mas as chaves privadas são secretas e estão disponíveis apenas para os usuários que as possuem. Resumidamente, qualquer pessoa pode enviar mensagens ao usuário usando suas chaves públicas, mas somente o destinatário desejado pode decifrar as mensagens usando sua chave privada. [2]

3.4 Criptografia RSA

O RSA é o algoritmo de chave pública mais usado no mundo. As iniciais RSA significam Rivest Shamir Adleman, em homenagem ao matemático e dois cientistas da computação que descreveram publicamente o algoritmo em 1977. [3]

Muitos protocolos, como Secure Shell (SSH), SSL-TLS, S/MIME e OpenPGP, contam com criptografia RSA e funções de assinatura digital seguras.

O sistema de criptografia RSA resolveu o que já foi um problema significativo na criptografia: como enviar uma mensagem codificada para alguém sem compartilhar previamente o código com eles. [2]

Digamos que você queira dizer a alguém um segredo. Se eles estiverem bem perto de você, você pode sussurrar. No entanto, se eles estiverem a quilômetros de distância de você, você não poderá. Você precisaria usar o telefone ou anotá-lo e enviá-lo por e-mail. Infelizmente, esses canais de comunicação não são seguros, e qualquer pessoa com motivação suficiente pode interceptar ou bisbilhotar a mensagem.

Uma solução para evitar espionagem é criptografar a mensagem. Isso significa adicionar um código a ele que o transforma em uma bagunça. Se você usar um

código suficientemente complexo, somente aqueles com acesso ao código poderão acessar a mensagem original. Caso contrário, ele permanecerá ilegível.

Se você compartilhou o código com seu amigo antecipadamente, você pode enviar mensagens criptografadas a qualquer momento, pois apenas vocês dois têm o código para ler o conteúdo original.

Mas e se você não compartilhou o código de antemão? Como você se comunica com segurança? Esse é um problema fundamental que a criptografia aborda usando esquemas de criptografia de chave pública ou criptografia assimétrica, como o RSA. [2]

A criptografia de RSA permite que os usuários criptografem mensagens com um código chamado chave pública que podem ser compartilhadas abertamente. Devido às propriedades matemáticas específicas do algoritmo RSA, uma vez que um usuário criptografa uma mensagem com uma chave pública, somente uma chave privada pode descriptografá-la. Os usuários têm um par de chaves públicas e privadas e este último são mantidos em segredo. Os sistemas de criptografia de chave pública diferem das criptografias de chave simétrica, que utilizam a mesma chave tanto para a criptografia quanto para a descriptografia. Portanto, o RSA é útil para se comunicar nos casos em que os usuários não tenham distribuído chaves com segurança antecipadamente. [2]

3.5 O uso da criptografia RSA

A criptografia de RSA não é adequada para criptografar arquivos inteiros ou mensagens porque é mais forte em recursos e menos eficiente do que a criptografia de chave simétrica. Portanto, é prática comum usar a criptografia RSA em conjunto com outros sistemas de criptografia ou para criptografar assinaturas digitais, a fim de comprovar a integridade e autenticidade das mensagens. [2]

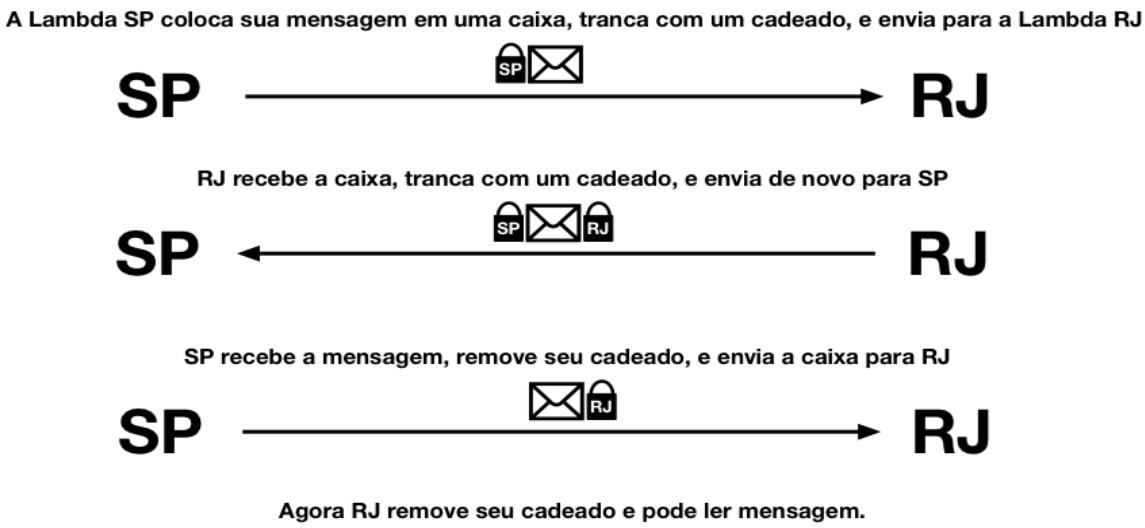

Figura 1: Entendendo (de verdade) a criptografia RSA

Fonte: Entendendo (de verdade) a criptografia RSA | Lambda3

As assinaturas digitais ajudam a autenticar e verificar arquivos e documentos. Eles evitam adulteração durante a transmissão de documentos oficiais e outros documentos confidenciais e evitam falsificação ou manipulação. No entanto, as assinaturas digitais usam chaves privadas para criptografia e chaves públicas para descriptografia para autenticar a origem da assinatura.

Geralmente, os usuários criptografam um arquivo com um algoritmo de chave assimétrica e utilizam a criptografia RSA para criptografar a chave simétrica. Assim, apenas uma chave privada RSA pode descriptografar a chave simétrica usada e sem ela, não é possível descriptografar a mensagem.

Além disso, a RSA garante conexões seguras entre servidores e clientes VPN. Em protocolos como o OpenVPN, os usuários podem usar o algoritmo RSA para realizar as negociações TLS e trocar chaves, estabelecendo assim canais de comunicação seguros.

3.6 Como funciona a criptografia RSA

A matemática que oferece suporte à criptografia RSA é bastante complicada de explicar detalhadamente. Existem vários conceitos a serem discutidos antes de mergulhar no algoritmo RSA na criptografia. Por exemplo:

- Funções de porta de armadilha
- Gerando números primos
- Função tociente de Carmichael
- Gerando chaves públicas e privadas

As equações que são simples de calcular em uma direção e extremamente difíceis na direção inversa são chamadas de funções de porta de armadilha. A premissa subjacente da criptografia RSA é que o algoritmo é relativamente fácil de computar em uma direção e quase impossível de reverter. Por exemplo, se você recebeu 543.111 como um produto de dois números primos, poderia descobrir os dois primos?

Mesmo com uma calculadora, é difícil saber por onde começar, mas inverter as coisas torna as coisas muito mais fáceis porque:

- 807*673 = 543.111

Ainda assim, dado 543.111 e um número primo, é fácil descobrir o outro da seguinte forma:

- 543.111/807 = 673

A criptografia RSA usa números significativamente maiores. Por exemplo, no RSA de 2048 bits, as chaves teriam 617 dígitos.

As funções de porta de armadilha são a base para o funcionamento dos esquemas de criptografia de chave pública e privada. Suas propriedades permitem o compartilhamento de chaves públicas sem revelar a chave privada ou ameaçar a mensagem. [2]

Gerar as chaves é o primeiro passo para criptografar dados e o processo utiliza dois números primos (p e q) selecionados com um teste de primalidade. Estes são algoritmos que encontram eficientemente números primos para criptografia,

como o teste de primalidade de Ranbin-Miller. Os números primos devem ser grandes e relativamente distantes para que seja mais difícil quebrar as chaves.

Gerando chaves públicas e privadas

As chaves públicas do RSA são números primos e módulo n. Módulo (mod) é uma operação de módulo que significa o restante deixado após dividir um lado ou número pelo outro, como:

- 10 mod 3 = 1 (3 entra em 10 três vezes com um restante de 1)

A seguinte é a fórmula para gerar a chave pública:

- C = me mod n

Depois de fazer toda a matemática e aplicar a chave pública (C=me mod n), os dados finais criptografados são o texto cifrado (c). [2]

As chaves privadas são as únicas chaves que os usuários podem usar para decifrar textos cifrados com uma chave pública, e elas devem ser de um par de chaves semelhante. Chaves privadas são feitas de d e n e como já sabemos n, é fácil calcular d usando a fórmula:

- d = 1/e mod λ (n)

O exemplo do algoritmo RSA acima demonstra que a matemática envolvida na criptografia é complexa e, quando feita corretamente, resulta em uma solução segura. [2]

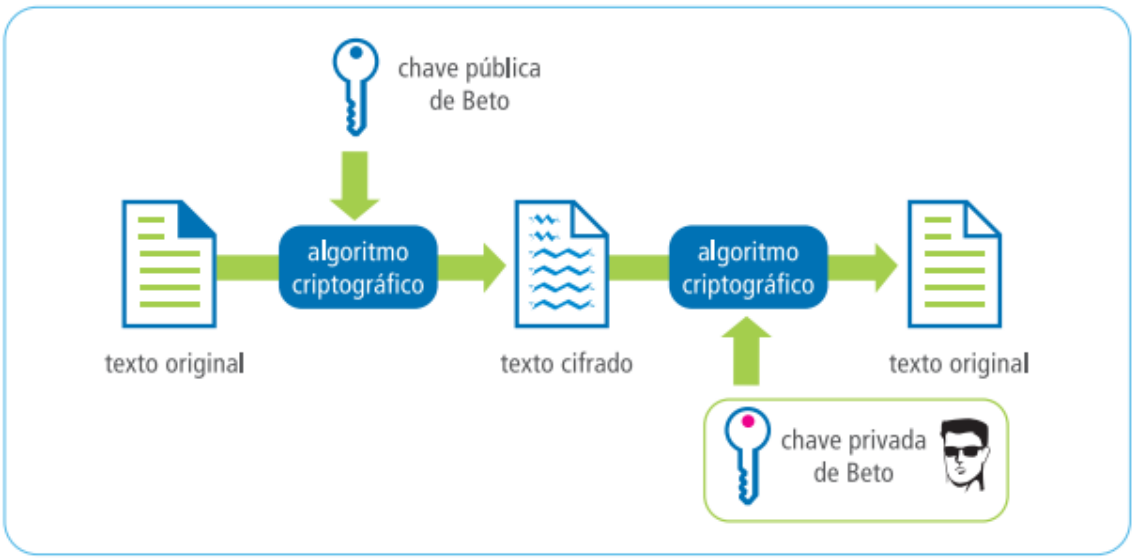

Figura 2: Chaves Simétricas e Assimétricas

Fonte: Chaves Simétricas e Assimétricas - Diego Macêdo

3.7 Benefícios da criptografia RSA

Existem muitas vantagens de usar criptografia RSA, incluindo:

- **Segurança:** a criptografia RSA tem um algoritmo seguro que protege a transmissão de dados
- **Criptografia de chave pública:** o RSA usa um algoritmo de criptografia de chave pública para segurança. Isso significa que usa duas chaves diferentes para criptografar e descriptografar dados.
- **Troca de chaves:** como o algoritmo RSA utiliza duas chaves para criptografia e descriptografia, é possível trocar chaves secretas sem realmente enviar a chave privada pela rede.Ele permite a criptografia e transmissão segura de dados sem enviar chaves de descriptografia com antecedência.
- **Assinaturas digitais:** o algoritmo RSA é ideal para assinaturas digitais, pois o remetente pode assinar um documento ou mensagem usando uma chave privada, enquanto o destinatário verifica a assinatura usando uma chave pública. [2]

3.8 Desafios da criptografia RSA

O RSA enfrenta alguns desafios que limitam seu uso em alguns casos devido à capacidade dos invasores explorá-los. Por exemplo, ele implementa uma chave longa em seu algoritmo de criptografia. Algoritmos AES são incontestáveis, mas assimétricos como RSA dependem do tamanho de suas chaves para torná-los difíceis de quebrar.

Portanto, as chaves RSA mais longas são mais seguras e difíceis de quebrar do que as mais curtas. Por exemplo, pesquisadores usaram fator prime para quebrar uma chave de criptografia RSA de 768 bits em dois anos.

Isso exigiu recursos significativos, mas o fato de ser possível deve sempre ser considerado em conversas sobre a segurança do sistema criptográfico RSA. Embora os indivíduos possam não ter a capacidade de quebrar essas criptografias, os governos podem fazê-lo porque têm mais recursos à sua disposição. [2]

O NIST recomenda um comprimento mínimo de chave de 2048 bits, mas organizações estão adotando comprimentos de chave de 4096 bits para uma segurança ampliada.

Outras desvantagens do RSA incluem:

- **Velocidade de processamento lenta:** o algoritmo RSA tem uma velocidade de processamento lenta em comparação com outros algoritmos de criptografia ao lidar com grandes quantidades de dados. Não é sempre adequado para aplicações que exigem criptografia e descriptografia regulares de grandes volumes de dados.
- **Tamanho de chave grande:** a criptografia RSA exige o uso de chaves de tamanho grande para garantir a segurança. Portanto, ele exige mais potência computacional, recursos e armazenamento.
- **Vulnerabilidade a ataques de canal lateral:** o algoritmo é vulnerável quando um invasor usa informações vazadas através de canais laterais para extrair informações de chave privada. Esses canais incluem consumo de energia, análise de tempo e radiação eletromagnética.

- **Geração fraca de chaves:** por exemplo, se os dois números primos selecionados estiverem muito próximos ou se um dos números que compõem um dos pares de chaves for muito pequeno, o algoritmo se torna mais fácil de resolver. [2]

3.9 Qual é a segurança da criptografia RSA

Apesar das vulnerabilidades mencionadas, o RSA é atualmente relativamente seguro de ser usado, desde que os usuários o implementem corretamente e utilizem chaves longas e difíceis de serem quebradas. Implementações que não usam números primos de tamanho adequado ou que tenham outras vulnerabilidades não são seguras.

Desde que os usuários estejam cientes das fraquezas e potenciais vulnerabilidades do algoritmo de criptografia RSA, eles podem usá-lo com segurança para compartilhamento de chaves e outras tarefas, como assinaturas digitais que exigem criptografia de chave pública. [6]

3.10 Como a computação quântica afetará o algoritmo RSA na criptografia

A criptografia RSA on-line é segura no momento, mas o advento da computação quântica pode representar desafios no futuro. Os computadores quânticos podem resolver facilmente certos problemas que atualmente consideramos extremamente difíceis. Visto que essa dificuldade é o que torna os sistemas criptográficos seguros, é seguro afirmar que o tamanho atual das chaves RSA se tornará mais vulnerável.

Computadores quânticos resolverão facilmente o problema de fatoração de inteiros. No entanto, esse futuro ainda está longe porque os computadores quânticos ainda estão em desenvolvimento e são usados principalmente em ambientes de pesquisa. Os players do setor de segurança cibernética também estão constantemente procurando melhorar os algoritmos de chave pública para garantir sua segurança em um mundo pós tecnologia quântica.

O OAEP (Optimal Asymmetric Encryption Padding - preenchimento de criptografia assimétrica) agora é o principal preenchimento padrão para criptografia de chave pública RSA. O acréscimo permite a formatação de

mensagens antes que sua criptografia atinja níveis mais altos de segurança, excluindo ataques básicos. [2]

4. RESULTADOS E CONCLUSÕES

Agora, explicando um pouco como chegamos nos resultados do nosso sistema, e o que concluímos disso.

4.1 Resumo do código

Como dito anteriormente, o código do nosso projeto foi feito para gerar um sistema de urna eletrônica, sistema esse que foi desenvolvido pelo grupo em Python. Ele também usa o framework Flask para criar uma interface web simples e um banco de dados para armazenar os votos dos eleitores, parte importante para garantir a segurança das informações. Nomeamos o banco com “a3_criptografia”, além de informações padrão, como o usuário root e a senha 1234. A biblioteca “flask_mysqldb” é usada para integrar o Flask ao MySQL, permitindo que o código envie e receba dados do banco, e essa troca de informações é fundamental para armazenar as informações dos votos e torná-las acessíveis ao sistema.

A criptografia RSA é uma das partes principais do nosso sistema e garante a segurança e a integridade dos votos. O código gera dois números primos grandes e aleatórios e com base nisso, o sistema define uma chave pública e uma chave privada. A chave pública é usada para codificar os votos, transformando o texto legível em números codificados, e a chave privada é justamente o oposto disso, visto que é necessária para descriptografar esses números, retornando o assim para o conteúdo original.

A página inicial do nosso sistema é acessada por uma rota onde os usuários podem registrar seus votos, e quando o voto é enviado, ele é cifrado usando a função “encrypt_message” do código, que converte cada caractere do texto em um número criptografado com base na chave pública. Esses números são armazenados no banco de dados junto com o nome do usuário que enviou o voto, e a funcionalidade de inserir votos no banco é realizada pela rota insert,

que também mostra uma mensagem de confirmação para o usuário, informando assim que o voto foi registrado com sucesso.

O sistema também tem a função de listar os votos registrados, que pode ser acessada pela rota voteslist. Normalmente os votos aparecem de forma criptografada, mas há uma opção para visualizá-los descriptografados, usando a função decrypt_message, que aplica a chave privada para transformar os números criptografados de volta em texto legível. Essa funcionalidade é útil para verificar a integridade dos votos e/ou exibir os resultados de forma clara, caso uma verificação manual seja necessária. O banco de dados usado tem uma tabela chamada votes, que possui as colunas para armazenar o voto criptografado e o nome do usuário que votou. Isso garante que cada voto seja associado a um usuário específico, mas sem expor o conteúdo do voto diretamente. Como os votos estão armazenados de forma cifrada, mesmo que alguém consiga acessar o banco de dados, não será possível entender os dados sem a chave privada do sistema.

Nosso sistema é um modelo básico, porém eficaz, para obter uma votação segura. Ele garante a privacidade dos votos com a criptografia RSA e utiliza o banco de dados para gerenciar e armazenar as informações. Apesar de simples, o sistema é funcional e pode ser expandido com novos recursos e atualizações. [7]

4.2 Conclusões gerais

O desenvolvimento deste sistema de votação eletrônica utilizando criptografia RSA demonstrou ser uma solução eficaz para garantir a segurança, integridade e anonimato em processos eleitorais digitais. Ao longo do projeto, enfrentamos desafios técnicos relacionados à melhoria dos algoritmos de criptografia e à gestão de dados, mas conseguimos superá-los através de uma boa organização e trabalho em equipe. O uso do Trello foi fundamental para o controle das tarefas e a divisão clara de responsabilidades entre os membros do grupo.

Os testes realizados confirmaram que o sistema é capaz de proteger os votos de forma segura, desde o momento em que são inseridos até a sua contagem

final, preservando o anonimato das reuniões e prevenindo fraudes. A criptografia RSA desempenhou um papel central no sucesso do projeto, garantindo que as informações trafegadas entre os componentes do sistema fossem indecifráveis por terceiros.

Embora o projeto tenha alcançado seus objetivos, há espaço para melhorias e trabalhos futuros. A adoção de outros algoritmos criptográficos, ou a expansão da plataforma para suportar um número maior de participações, são algumas das possibilidades de aprimoramento. Além disso, a inclusão de recursos de acessibilidade e uma interface ainda mais intuitiva poderia ampliar o alcance e a usabilidade do sistema.

Em conclusão, o sistema desenvolvido oferece uma base sólida para futuras implementações de votações eletrônicas, atendendo aos requisitos essenciais de segurança e desempenho, e mostrando que soluções tecnológicas podem ser aplicadas com sucesso no cenário eleitoral.

Referências bibliográficas

[1] https://aws.amazon.com/pt/what-is/cryptography/

[2] https://www.veritas.com/pt/br/information-center/rsa-encryption

[3] https://www.ibm.com/br-pt/topics/cryptography

[4] https://www.ssldragon.com/pt/blog/algoritmos-de-criptografia/#types-of-encryption

[5] https://www.ibm.com/br-pt/think/topics/cryptography-types

[6]https://www.uesb.br/noticias/ensino-de-matematica-pode-ser-estimulado-pela-criptografia/

[7]https://www.contabeis.com.br/noticias/40188/a-matematica-e-criptografia-na-protecao-de-dados-bancarios/

- **Figura 1:** https://images.app.goo.gl/xMWn714cbYMgiDZVA
- **Figura 2:** https://images.app.goo.gl/eEsxLfGwjM62qrtw5