UNIVERSIDADE CATÓLICA DE SANTOS

CIÊNCIA DA COMPUTAÇÃO

TRABALHO DISCENTE EFETIVO

Criptografia Militar e Segurança de Dados

Análise e Estudo das implicações do Padrão de Criptografia Avançada (AES)

Felipe Barbosa dos Santos - 4324223
Gustavo da Silva Silvestre - 7354473
Lucas Carmona Neto - 8342055
Lucas Cerqueira Galvão - 4477944
Pedro Henrique Bonifacio Martins - 2502334

Santos
2023

Sumário

1. Resumo

Este trabalho aborda a evolução histórica da criptografia, desde sua origem na antiguidade até sua importância atual na sociedade digital. Exploramos a definição de criptografia como a arte e ciência de tornar informações ininteligíveis para qualquer pessoa sem as chaves ou métodos adequados. Inicialmente utilizada para propósitos militares e diplomáticos na antiguidade, a criptografia tornou-se fundamental para a segurança de dados em uma era digital.

Nossa análise começa com uma investigação das técnicas utilizadas por civilizações antigas, como os egípcios e gregos, para proteger informações confidenciais. Além disso, destacamos o papel crucial da criptografia na Segunda Guerra Mundial, incluindo a quebra da máquina de cifragem Enigma por Alan Turing.

Ao longo deste estudo, dedicamos especial atenção ao estudo do algoritmo de criptografia AES (Advanced Encryption Standard), que é amplamente reconhecido como um dos padrões mais seguros em criptografia de simetria. Nossa análise abrange não apenas os princípios teóricos por trás do AES, mas também sua implementação prática.

Para demonstrar a aplicação prática dos princípios da criptografia avançada do AES, desenvolvemos um sistema de criptografia completo. Este sistema compreende um site interativo, uma API de comunicação e um algoritmo de criptografia em linguagem C. O destaque deste projeto é a implementação eficaz do algoritmo AES, que permite aos usuários proteger suas informações confidenciais e comunicações com segurança. O algoritmo incorpora etapas como a expansão das chaves, substituições baseadas em tabela e operações XOR, garantindo segurança e eficiência no processo de criptografia.

Este projeto tem como foco o estudo, desenvolvimento e aplicação prática do algoritmo de criptografia AES (Advanced Encryption Standard). Nosso objetivo central é aprofundar o entendimento do AES e demonstrar sua relevância e eficácia em aplicações reais de segurança de dados.

2. Introdução

A criptografia é uma disciplina de importância histórica que tem evoluído ao longo dos séculos, passando de uma prática rudimentar e misteriosa na antiguidade para se tornar uma ciência é uma tecnologia fundamental nos dias atuais. Em termos técnicos, a criptografia pode ser definida como a arte e a ciência de tornar informações ininteligíveis para qualquer pessoa que não possua as chaves ou os métodos apropriados para decifrá-las. Essa definição amplamente aceita foi estabelecida por Claude Shannon, um pioneiro na teoria da informação e criptografia, em meados do século XX.

Na antiguidade, a criptografia era frequentemente utilizada com propósitos militares e diplomáticos, visando proteger segredos de Estado e comunicações sensíveis. Através do estudo das técnicas utilizadas por civilizações antigas, como os egípcios, gregos e romanos, é possível compreender como a criptografia era uma ferramenta crucial para manter a confidencialidade das informações em um mundo onde as comunicações estavam sujeitas a espionagem constante.

Nos dias atuais, a criptografia desempenha um papel essencial em nossa sociedade digital. Com a proliferação da internet e a crescente dependência de sistemas de informação, a segurança de dados tornou-se uma prioridade incontestável. A criptografia moderna, representada por algoritmos robustos como o AES (Advanced Encryption Standard), é a espinha dorsal da proteção de dados em trânsito e em repouso, garantindo que informações pessoais, financeiras e empresariais permaneçam confidenciais e seguras.

Além de explorar a evolução histórica da criptografia, este trabalho também lança um olhar para o futuro, onde será desenvolvido um algoritmo próprio baseado nos princípios da criptografia avançada do AES. Isso demonstra como a criptografia não é apenas um campo de estudo acadêmico, mas também uma área em constante evolução, onde a inovação e a criatividade desempenham papeis cruciais na busca por soluções cada vez mais seguras e eficazes para proteger informações sensíveis.

3. Revisão Bibliográfica

3.1. Criptografia Antiga

No Egito Antigo, por volta de 1900 a.C., os hieróglifos eram usados tanto como forma de escrita artística quanto como base para técnicas de criptografia. Como afirmou Jean-François Champollion, decifrador dos hieróglifos egípcios, as tumbas dos faraós frequentemente escondiam mensagens cifradas, evidenciando o conhecimento avançado dos antigos egípcios na proteção de informações sensíveis.

> O livro de Jeremias, por exemplo, foi escrito usando a técnica de criptografia. Os hebreus utilizavam a cifra de substituição simples, monoalfabética e monogâmica, e assim trocavam caracteres um pelo outro. (Keevo, 2020)

Os gregos antigos também contribuíram para a história da criptografia com dispositivos como as escítalas. Estas eram tiras de pergaminho enroladas ao redor de um bastão de madeira, com a mensagem escrita de forma linear. Quando desenrolada em torno de um bastão idêntico, a mensagem se tornava ilegível, a menos que o destinatário possuísse o bastão certo, um exemplo precoce de criptografia baseada em chave.

A Idade Média testemunhou a criptografia desempenhando um papel vital, especialmente nos mosteiros, onde manuscritos religiosos eram copiados e protegidos. Bruce Schneier, especialista em segurança da informação, destaca que "os monges medievais foram os primeiros 'criptógrafos', usando técnicas de cifragem para proteger seus manuscritos sagrados".

3.2. Criptografia na Era da Computação

Com a rápida evolução da capacidade computacional e o crescimento exponencial do volume de dados online, a criptografia teve que se adaptar. Autores como Whitfield Diffie e Martin Hellman desempenharam um papel fundamental na criação da criptografia de chave pública nos anos 70, mas após 2000, vimos uma expansão significativa no uso de algoritmos de criptografia assimétrica para proteger transações online e comunicações seguras.

Com a proliferação de serviços online e redes sociais, a proteção de dados pessoais tornou-se uma prioridade crítica. A implementação do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia em 2018 foi um marco importante na legislação de privacidade. "A criptografia desempenha um papel crucial na proteção da privacidade online, permitindo que indivíduos controlem suas informações pessoais" (SCHNEIER, 2012).

A era pós-2000 testemunhou um aumento dramático nas ameaças cibernéticas. A criptografia desempenha um papel central na proteção de sistemas e redes contra ataques.

Autores como Dan Boneh contribuíram para o desenvolvimento de criptografia pós-quântica, que visa resistir a ameaças futuras de computadores quânticos.

Na era contemporânea da computação, a criptografia desempenha um papel vital na proteção de informações sensíveis em uma ampla gama de aplicações, desde comunicações online até transações financeiras e armazenamento de dados pessoais. Com a rápida evolução da capacidade computacional e o crescimento exponencial do volume de dados online, a criptografia teve que se adaptar. Autores como Whitfield Diffie e Martin Hellman desempenharam um papel fundamental na criação da criptografia de chave pública nos anos 70, mas após 2000, vimos uma expansão significativa no uso de algoritmos de criptografia assimétrica para proteger transações online e comunicações seguras.

Além disso, com a proliferação de serviços online e redes sociais, a proteção de dados pessoais tornou-se uma prioridade crítica. A implementação do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia em 2018 foi um marco importante na legislação de privacidade. Bruce Schneier, especialista em segurança da informação, observa que "a criptografia desempenha um papel crucial na proteção da privacidade online, permitindo que indivíduos controlem suas informações pessoais".

No entanto, a era pós-2000 também testemunhou um aumento dramático nas ameaças cibernéticas. A criptografia desempenha um papel central na proteção de sistemas e redes contra ataques. Autores como Dan Boneh contribuíram para o desenvolvimento de criptografia pós-quântica, que visa resistir a ameaças futuras de computadores quânticos. Nesse cenário em constante evolução, a criptografia continua a ser a âncora da segurança e privacidade na era digital, protegendo nossas comunicações, transações e informações pessoais em um mundo cada vez mais conectado.

3.3. Criptografia na Segunda Guerra Mundial

Durante a Segunda Guerra Mundial, a criptografia desempenhou um papel fundamental na proteção das comunicações militares e na quebra dos códigos inimigos. A máquina de cifragem alemã Enigma, considerada quase indecifrável, foi decifrada graças ao trabalho de Turing e sua equipe em Bletchley Park, no Reino Unido. Isso teve um impacto decisivo no resultado da guerra,

> Este foi Alan Turing, o pai intelectual do computador e o homem que desenvolveu uma maneira melhor de resolver as mensagens Enigma. Turing modificou o mecanismo da bomba polonesa para obter um efeito muito mais poderoso, método criptoanalítico. (Kahn, 2018)

A criptografia foi tão importante durante a Segunda Guerra mundial que os Aliados muitas vezes mantiveram em segredo o fato de terem quebrado a Enigma e lido mensagens alemãs. Isto permitiu continuar a obter informações sigilosas sem que os alemães soubessem que as suas comunicações tinham sido comprometidas.

Além da Enigma, outros países desenvolveram sistemas avançados de criptografia durante a Segunda Guerra Mundial. Por exemplo, os Estados Unidos usaram o código Navajo, que usava a língua Navajo para transmitir mensagens com segurança porque era improvável que os inimigos na Alemanha e no Japão entendessem a língua.

Após a guerra, Alan Turing continuou a influenciar a criptografia e a ciência da computação. Sua pesquisa pioneira sobre máquinas universais de Turing e a ideia de que os computadores poderiam ser programados para realizar uma variedade de tarefas moldaram a forma como encaramos a computação e a criptografia moderna. Bruce Schneier, especialista em segurança da informação, observa que "o trabalho de Turing na Segunda Guerra Mundial e suas contribuições posteriores revolucionaram a criptografia e a computação".

Após a Segunda Guerra Mundial, a criptografia continuou a evoluir com base nos avanços tecnológicos e nas ideias de Turing. O desenvolvimento de algoritmos de criptografia de chave pública, como o RSA, e o crescimento da computação quântica trouxeram novos desafios e oportunidades para a ciência da criptografia na era pós-guerra.

3.4. Criptografia e a Privacidade Digital

No início do século XXI, testemunhamos uma transformação radical na forma como as pessoas se comunicam e compartilham informações. A Internet trouxe inúmeras conveniências, mas também desafios à privacidade. Whitfield Diffie, pioneiro em criptografia de chave pública, observou que "a criptografia se tornou uma ferramenta essencial para proteger a privacidade em um mundo digital".

Com a proliferação de serviços online, redes sociais e vigilância governamental, a privacidade digital enfrenta desafios significativos. A criptografia se tornou um escudo vital contra a interceptação não autorizada de comunicações e o acesso a dados pessoais. Autoridades como Edward Snowden alertaram sobre a importância de medidas de segurança e privacidade na era digital.

A criptografia de chave pública, um dos avanços mais marcantes em criptografia, permite comunicações seguras pela Internet. A tecnologia de assinatura digital, baseada em conceitos de Diffie, garante a autenticidade e integridade de mensagens. Essas técnicas fortalecem a proteção da privacidade nas transações online.

A relação entre a criptografia e a privacidade digital tem sido muito debatido sobre a necessidade de equilibrar a segurança cibernética com a capacidade das autoridades de investigar atividades suspeitas. Algumas propostas de backdoors de criptografia têm sido amplamente debatidas devido aos riscos que representam para a privacidade do usuário .

3.5. Figuras Notáveis na Criptografia

- **Julius César** (100 a.C. - 44 a.C.) - O imperador romano é creditado com a criação do "Cifra de César", uma das primeiras técnicas de criptografia conhecidas, que envolve a substituição de letras em uma mensagem por outras letras do alfabeto.

- **Blaise de Vigenère** (1523 - 1596) - Matemático francês que desenvolveu a Cifra de Vigenère, um método polialfabético de criptografia que desafiou a quebra de códigos por séculos.

- **Auguste and Louis Lumière** (1862 - 1954, 1864 - 1948) - Os irmãos franceses inventaram o "Chaveiro Autônomo" durante a Primeira Guerra Mundial, um dispositivo mecânico usado para cifrar e decifrar mensagens.

- **Alan Turing** (1912 - 1954) - Matemático e criptoanalista britânico que desempenhou um papel vital na quebra dos códigos da máquina de cifragem alemã Enigma durante a Segunda Guerra Mundial, contribuindo significativamente para a vitória dos Aliados.

- **Claude Shannon** (1916 - 2001) - Pai da teoria da informação e pioneiro na criptografia matemática. Seus trabalhos influenciaram o desenvolvimento de sistemas criptográficos modernos.

- **Whitfield Diffie** (1944 -) e Martin Hellman (1945 -) - Juntos, eles desenvolveram a criptografia de chave pública nos anos 70, revolucionando a segurança digital ao permitir a troca segura de chaves pela Internet.

- **Rivest, Shamir e Adleman** (1947 - , 1952 - , 1956 -) - Os três matemáticos são os criadores do algoritmo RSA, um dos mais amplamente utilizados em sistemas de criptografia de chave pública.

- **Bruce Schneier** (1963 -) - Notável autor e especialista em segurança da informação, cujos escritos e contribuições na criptografia moderna desempenharam um papel importante na proteção de dados digitais.

- **Joan Daemen e Vincent Rijmen** (1965 - , 1970 -) - Desenvolveram o algoritmo de criptografia avançada (AES), considerado um dos padrões mais seguros em criptografia de simetria.

4. Problematização

A criptografia AES (Advanced Encryption Standard), também conhecida como Rijndael, é um dos algoritmos de criptografia mais amplamente usados em todo o mundo. Embora seja altamente eficaz em proteger informações sensíveis, também é alvo de várias problemáticas e discussões. Vamos explorar algumas das questões mais importantes relacionadas à criptografia AES. Ao considerar a crescente ameaça dos ciberataques, reconhecemos a necessidade de analisar seu papel atual na defesa contra essas ameaças em constante evolução.

A AES é altamente eficaz e considerada segura contra a maioria dos ataques criptográficos conhecidos. No entanto, com o aumento da capacidade computacional e o desenvolvimento de técnicas avançadas, como a computação quântica, há preocupações sobre sua resistência a ameaças futuras. Pesquisadores estão trabalhando em variantes da AES que são mais resistentes a esses avanços tecnológicos. A AES suporta tamanhos de chave de 128, 192 e 256 bits. O tamanho da chave é diretamente proporcional à segurança, com tamanhos maiores sendo mais seguros, mas também mais lentos. A escolha do tamanho da chave é uma consideração importante, e decisões erradas podem comprometer a segurança dos dados.

Com o tempo, técnicas de criptoanálise continuam a evoluir, e vulnerabilidades anteriormente desconhecidas podem ser descobertas. Isso enfatiza a importância da pesquisa contínua e da adaptação da criptografia. A AES fornece confidencialidade dos dados, mas não garante integridade. Para garantir a integridade dos dados, é necessário usar funções adicionais, como códigos de autenticação de mensagem (MAC) ou assinaturas digitais.

4.1. Problema da Pesquisa

Um dos principais problemas de pesquisa relacionados à criptografia AES, envolve sua segurança contínua no contexto de avanços tecnológicos, computacionais e criptográficos. Os pesquisadores estão constantemente explorando novas abordagens e desafios relacionados à AES para garantir que ela continue sendo uma técnica segura de proteção de dados. Uma parte crítica do uso da AES é o gerenciamento adequado das chaves. Se as chaves forem fracas, compartilhadas inadequadamente ou armazenadas sem proteção, a segurança da criptografia é comprometida. Além disso, embora a AES seja resistente a ataques de força bruta, com a tecnologia atual, é teoricamente possível realizar ataques bem-sucedidos usando força bruta se a chave for fraca. Portanto, a escolha de senhas fortes ou chaves seguras é fundamental.

Ademais, mesmo com uma criptografia sólida como a AES, a implementação incorreta ou falhas de segurança em sistemas que a utilizam podem comprometer a proteção dos dados. A segurança depende não apenas do algoritmo em si, mas de sua aplicação, e à medida que a criptografia desempenha um papel fundamental na proteção da privacidade, os

pesquisadores exploram as implicações éticas e legais do uso da AES em diferentes contextos, especialmente em relação à privacidade dos dados dos usuários.

4.2. Justificativa da pesquisa

A seleção do algoritmo de criptografia AES (Advanced Encryption Standard) como foco deste projeto se baseia em sua significativa importância histórica e relevância contemporânea, mas principalmente na motivação intrínseca ao aprendizado. A criptografia desempenha um papel vital na sociedade digital atual, à medida que a dependência de tecnologia e a transferência de informações sensíveis pela internet continuam a crescer. O AES é um dos algoritmos de criptografia mais amplamente adotados em todo o mundo, sendo crucial para entender a evolução da criptografia e sua capacidade de proteger informações confidenciais no passado e no presente. O interesse nesse campo de estudo está profundamente enraizado na busca pelo conhecimento sobre como a criptografia funciona e como podemos aplicá-la eficazmente, o que servirá não apenas para a pesquisa em si, mas também para a promoção do aprendizado contínuo e do avanço pessoal na área da segurança digital.

5. Objetivos

5.1. Objetivo Geral

O objetivo geral deste trabalho é estudar e compreender a importância da criptografia militar ao longo da história, desde suas origens até os métodos modernos, e sua aplicação na segurança de comunicações e proteção de informações confidenciais, além de analisar seu papel atual em um cenário de grandes ameaças cibernéticas crescentes, destacando a relevância da tecnologia AES (Advanced Encryption Standard) como uma das principais ferramentas nesse contexto.

5.2. Objetivos específicos

- **Explorar fundamentos teóricos da criptografia**: Compreender os princípios matemáticos e teóricos da criptografia militar, com foco na tecnologia AES.
- **Estudar a aplicação da tecnologia AES em operações reais**: Analisar estudos de caso que demonstram a implementação bem-sucedida da tecnologia AES em operações militares e cenários governamentais.
- **Avaliar a importância da criptografia na segurança nacional e internacional**: Investigar como a criptografia militar desempenha um papel vital na proteção de comunicações estratégicas e informações críticas para a segurança nacional e internacional.
- **Analisar os desafios atuais em segurança cibernética**: Examinar o cenário atual de ameaças cibernéticas crescentes e identificar como a criptografia militar se adapta para enfrentar estes desafios.
- **Desenvolver um programa de criptografia com AES**: Criar um programa que utilize a tecnologia AES para realizar criptografia de dados, demonstrando sua aplicação prática e relevância em situações do mundo real.

6. Metodologia

Para alcançar com sucesso os objetivos deste projeto, estabelecemos uma metodologia que abrange quatro tarefas distintas, cada uma desempenhando um papel crucial na implementação do nosso sistema de criptografia. Essas tarefas, trabalhando em conjunto, visam garantir a segurança e eficiência do processo de criptografia e descriptografia.

A primeira tarefa concentra-se no desenvolvimento de um site, proporcionando aos usuários a capacidade de inserir o texto a ser criptografado, juntamente com a chave de criptografia. Na segunda tarefa, é realizada a criação de uma API para facilitar a comunicação entre o site e o algoritmo de criptografia. Esse algoritmo, desenvolvido em linguagem C, interage harmoniosamente com o site, construído com HTML, CSS e JavaScript.

A terceira tarefa é dedicada à expansão das chaves de criptografia, um passo crítico para garantir a segurança do processo. Isso torna o trabalho virtualmente dificílimo de descriptografar para computadores convencionais. Por fim, a quarta tarefa lida diretamente com o processo de criptografia e descriptografia. Ela envolve o embaralhamento do texto inserido e faz chamadas às funções de chave quando necessário para executar operações XOR, resultando na entrega da mensagem criptografada ou descriptografada ao solicitante da API.

Cada uma dessas tarefas desempenha um papel vital na implementação de nosso sistema de criptografia. Nas seções a seguir, exploraremos detalhadamente cada uma delas, destacando sua importância e contribuição para o sucesso deste projeto.

6.1. Site

Nesta seção, discutiremos em detalhes o desenvolvimento do site como parte do projeto de criptografia. O site desempenha papel fundamental na interação dos usuários com o sistema de criptografia. Abaixo, falaremos sobre os principais aspectos do desenvolvimento do site, incluindo linguagens de programação, layout e funcionalidades.

6.1.1. Linguagem de Programação e Tecnologias Utilizadas

- **HTML (Hypertext Markup Language):** O HTML foi a base para a estrutura do site, que permitiu a criação dos elementos para entrada de texto e botões.
- **CSS (Cascading Style Sheets):** O CSS foi utilizado para estilizar o site, garantindo uma interface intuitiva.
- **JavaScript:** Foi utilizado para melhorar a interatividade do site, e permitir a comunicação com a API de criptografia.

6.1.2. Layout e Design

- **Layout Responsivo:** O site foi projetado para se adaptar a diferentes dispositivos, como tablets, celulares e computadores.
- **Simplicidade:** A interface foi desenvolvida para ser simples e interativa com o usuário, então pode ser entendida e usada facilmente.

6.1.3. Funcionalidades

- **Entrada de Texto:** Os usuários podem escolher e inserir o texto que desejam criptografar ou descriptografar.
- **Entrada da Chave de Criptografia:** Além do texto, os usuários podem escolher e inserir uma chave de criptografia qualquer, com limite de 16 caracteres.
- **Comunicação com a API:** O site interage com a API de criptografia, permitindo que os dados sejam exibidos na tela para o usuário.

6.2. API

A API desempenha um papel essencial na comunicação entre o site e o programa de criptografia em C. Discutiremos detalhadamente como essa API foi projetada, sua função e sua integração com o sistema de criptografia. Em resumo, a API desenvolvida é o elo de comunicação vital entre o nosso site e o programa em C responsável por criptografar e descriptografar os dados.

6.2.1. Descrição

A API foi desenvolvida utilizando a linguagem de programação PHP e foi projetada com o objetivo de atuar como uma interface de comunicação entre o site e o programa de criptografia em C. Isso permitiu que o site solicitasse operações de criptografia e descriptografia, bem como a passagem de dados relevantes ao sistema de criptografia em C.

6.2.2. Uso da Função exec

Uma das características distintivas da nossa API é a utilização da função exec em PHP. Essa função é responsável por permitir a execução de comandos diretamente no servidor. No contexto do nosso projeto, ela é fundamental para acionar a execução do código em C que realiza as operações de criptografia e descriptografia. A função exec recebe os parâmetros necessários, como o texto a ser criptografado, a chave de criptografia e a ação a ser realizada (criptografar ou descriptografar), e os repassa ao programa em C para processamento.

6.2.3. Resposta em formato JSON

A API é projetada para fornecer respostas bem estruturadas em formato JSON. Isso facilita a integração com o site, pois os dados podem ser facilmente consumidos e exibidos de forma organizada. A resposta inclui informações relevantes, como o resultado da operação de criptografia, o texto de entrada, a chave de criptografia e a ação realizada.

6.3 A algoritmo de criptografia Rijndae

Em janeiro de 1997 o Instituto Nacional de Padrões e Tecnologia (US NIST) anunciava a competição para especificar um Padrão de Criptografia Avançada (AES) para subistituir o então vigente Padrão de criptografia de dados (DES). O objetivo da competição, de acordo com o NIST, era "an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century", o que pode ser traduzido como "Um algoritmo de criptografia não classificado e publicamente divulgado capaz de proteger informações governamentais por um longo período, até o próximo século".

"A chamada AES solicita um cifrador de bloco de 128 bits com um comprimento de chave variável. (Pelo menos comprimentos de chave de 128, 192 e 256 bits devem ser suportados.) O cifrador deve ser eficiente em uma plataforma Pentium, processadores de 8 bits e em hardware" (DAEMEN; RIJMEN,1998, 1, tradução nossa).

Os cinco finalistas da comeptição foram, em ordem de colocação: Rijndael (Vincent Rijmen, Joan Daemin), MARS (Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas, Luke O'Connor, Mohammad Peyravian, David Safford, Nevenko Zunic), RC6 (
Ron Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa Yin), Serpent (Ross Anderson, Eli Biham, Lars Knudsen), Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson).

Em 1998, no artigo "The Block Cipher Rijndael", foi apresentado o algoritmo vencedor da comeptiçao pelos autores Joan Daemen - criptográfo belga que já além de contribuir com a criaçao do algortimo em questão tambem foi responsável pela criaçao de outros projetos relacionados a criptografia, dentre eles o mais significativo foi o SHA-3, algoritmo de hash selecionado pelo NIST para fazer parte do "Secure Hash Algorithm family standards" - e Vincent Rijment - também belga, conhecido também pela co-autoria no algoritmo de hash WHIRLPOOL. Quando apresentado era um dos quinze candidatos para o Padrão de Criptografia Avançada (AES).

O algortimo Rujndael se tornou o vencedor da competição para o Padrão de Criptografia Avançada (AES) depois de uma extensa avaliação de diversos especialistas. Este algoritmo oferece segurança sólida e eficiência notável, com tamanhos de chave de 128, 192 e 256 bits.

O AES é um algoritmo de criptografia simétrica que opera em blocos de 128 bits de dados. Utiliza um processo de substituição, permutação e mistura de dados para proteger as informações. A chave de criptografia é aplicada iterativamente em várias rodadas, onde os dados são transformados de maneira complexa. Essa abordagem oferece uma camada sólida de segurança, tornando o AES amplamente utilizado em aplicações que exigem a proteção de dados sensíveis.

6.3.1 Termos e Definições

Bit: Digito binário podendo ter o valor 0 ou 1;

Block: É um bloco de 16 bytes, repesentará parte do dado a ser criptografado ou descriptografado;

Byte: Um grupo de oito bits que é tratado como uma entidade única ou como um matriz de 8 bits individuais;

Hex: Hex nestá explicação está se referindo a numeros hexadecimais de 1 byte. Cada digito em hexadecimal pode ser representado por 4 bits, exemplo:

D4 = 1101 0100
D = 1101
4 = 0100

Char: É um caracter que pode ser representado por 1 byte, exemplo:

$A = 0100\ 0001_2 = 65_{10} = 41_{16}$

Key: Senha de entrada de tamanho váriavel, no minimo 1 caracter e no máximo 32 (256 bits);

Plaintext: Dado sem sem criptografia;

Cyphertext: Dado criptografado;

Round Key: Senha da rodada;

State: Estado atual de um bloco que está sendo processado;

S-box: Tabela de substituição não linear, usada em funções de substituições de bytes;

COLOQUE A SBOX E SBOX INVERTIDA AQUI

XOR: (OU exclusivo) é uma operação lógica. o xor é aplicado bit a bit entre bytes da seguinte forma:

0 XOR 0 = 0
1 XOR 0 = 1
1 XOR 1 = 0
0 XOR 1 = 1

Por exemplo, $D4_{16}$ XOR FF_{16}

$1101\ 0100_2$
XOR $1111\ 1111_2$
==========
$0010\ 1011_2 = 2B_{16}$

6.3.2 O Algortimo

O AES é uma cifra de bloco iterado. Uma cifra de bloco é aqual que criptografa utilizando um bloco pré definido de dado, no AES utilizamos blocos de 16 bytes tanto o conteúdo a ser criptografado quanto a chave de rodada. Já a parte "iterado" signifa que o bloco é cifrado fazendo várias rodadas das mesmas funções, além disos outra caracteristica deste tipo de algortimo é que para desfazer o cyphertext utilizamos quase que as mesmas funçoes, com alguns ajustes - cada algortmo tem a sua particulariedade. Algumas máximas do AES especificadas no paper "AES (Advanced Encryption Standard) Simplified" de Adam Berent:

- AES funciona repetindo os mesmos passos definidos várias vezes.
- AES é um algoritmo de criptografia de chave secreta.
- AES opera em um número fixo de bytes.
  (tradução nossa)

Logo abaixo listamos os nome das etapas do AES (funçoes). Em nossa implementação utilizamos os mesmos nomes de funçoes usados no paper dos authores do algortimo, em "The Rijndael Block Cipher":

SubBytes
ShiftRows
MixColumns
AddRoundKey

Além dessas etapas também temos a etapa de expançao de key, que geralmente se tem uma funçao que retorna todas as chaves, mas em nossa implementacao é retornada a chave da rodada especificica solicitada, explicaremos mais adiante.

6.3.3 SubBytes

6.3. Key Expansion

A função que faz a expansão das Keys recebe como parâmetros a matriz com os 16 valores hexadecimais já convertidos da digitada pelo usuário e o valor do Round, que pode ir de 1 a 10.

Em seguida, a matriz passa por uma série de etapas, incluindo 'RotWord', que realiza uma rotação nos elementos da matriz, seguida de 'SBox', que substitui valores com base em uma tabela SBox predefinida. O resultado dessas etapas é crucial para a segurança da criptografia.

O algoritmo também envolve a geração de uma constante de rodada ('Rcon') que é utilizada em operações posteriores. Essa constante varia de acordo com a rodada do processo.

Finalmente, a matriz é submetida a uma operação 'fim' (Finalização) que envolve operações XOR entre elementos da matriz. Essa etapa é repetida várias vezes, resultando na expansão da chave.

6.4. Encryption and Decryption

A Criptografia e Descriptografia desempenham um papel central neste projeto e foram implementadas usando a linguagem de programação C. Para aprimorar a compreensão abrangente do problema, nossa estrutura principal de execução foi subdividida em vários módulos, os quais são invocados na função principal (main) durante o processo. Cada um desses módulos possui funcionalidades específicas, conforme descrito a seguir. Em seguida, apresentamos uma descrição detalhada de como o programa opera durante os processos de criptografia e descriptografia.

6.4.1. Main

A função main é o ponto de entrada do programa e desempenha um papel essencial na coordenação da execução da criptografia e descriptografia AES de 16 bytes. Ela é responsável por realizar as seguintes ações:

I. Inicialização de Variáveis:

A função main inicia definindo uma string de texto de 16 bytes chamada texto e uma chave de criptografia key.

A string texto contém o texto que será criptografado e descriptografado, enquanto a key armazena a chave de criptografia.

II. Apresentação do Texto de Entrada:

Antes de executar a criptografia, a função main exibe o texto de entrada em formato de bytes. Isso ajuda a visualizar a representação em bytes dos caracteres do texto.

III. Chamada da Função aes para Criptografia:

Em seguida, a função aes é chamada com o texto de entrada, a chave e a ação de criptografia (indicada pelo valor 1).

A função aes realiza a criptografia do texto usando a chave fornecida e atualiza o texto original com o texto cifrado.

IV. Apresentação do Texto Cifrado:

Após a criptografia, a função main exibe o texto cifrado em formato de bytes. Isso permite a visualização do resultado da criptografia.

V. Chamada da Função aes para Descriptografia:

A função aes é chamada novamente, desta vez com a ação de descriptografia (indicada pelo valor -1).

Isso reverte o processo de criptografia, restaurando o texto original a partir do texto cifrado usando a mesma chave.

VI. Apresentação do Texto Descriptografado:

Por fim, a função main exibe o texto descriptografado em formato de bytes. Isso permite verificar se o processo de descriptografia foi bem-sucedido e se o texto original foi recuperado com êxito.

A função main atua como um ponto de partida para a execução do programa e demonstra a funcionalidade da criptografia e descriptografia AES de 16 bytes com um exemplo de entrada e chave. Ela facilita a visualização dos resultados e a validação do processo de criptografia e descriptografia.

6.4.2. Core

A função core desempenha um papel central na implementação das operações de criptografia AES de 16 bytes. Dentro desta função, estão contidas várias subfunções que executam tarefas essenciais para a criptografia, como adição de chave, substituição de bytes, permutação de linhas e mistura de colunas.

A subfunção addRoundKey é responsável por realizar a operação XOR entre o estado atual e a chave da rodada. Essa operação é vital para garantir a segurança, uma vez que cada rodada da criptografia é única e depende da chave fornecida.

A subfunção byteSub executa a substituição dos bytes no estado com base em tabelas de substituição, usando a S-box. Ela é usada tanto na criptografia quanto na descriptografia, dependendo da ação fornecida (1 para substituição normal e -1 para substituição invertida).

A subfunção shiftRow desempenha a permutação das linhas do estado, embaralhando os bytes. A ação determina se as linhas são permutadas ou revertidas, contribuindo para a confusão e difusão dos dados.

A subfunção mixColumn implementa a operação de mistura de colunas, que é aplicada às colunas do estado. Essa operação aumenta a segurança do algoritmo AES, contribuindo para a difusão dos dados. A ação (1 para mistura, -1 para desmistura) determina se a operação é realizada ou desfeita.

A função core coordena a execução dessas subfunções, permitindo que elas operem em conjunto para criptografar e descriptografar o texto de entrada com base na chave fornecida. Cada subfunção tem um papel específico e é essencial para o funcionamento bem-sucedido do algoritmo AES de 16 bytes.

6.4.3. Derive Key

A função deriveKey é responsável por gerar uma chave derivada com base em uma chave de entrada e um valor de "sal" (salt). Essa chave derivada é usada como parte do processo de criptografia e descriptografia do algoritmo AES de 16 bytes.

A função recebe vários parâmetros, incluindo a chave de entrada original (key), um ponteiro onde a chave derivada será armazenada (derivedKey), o comprimento da chave de entrada em bytes (keyLength), um valor de "sal" (salt) que aumenta a segurança da derivação e uma ação indicando se a função está sendo usada para criptografia (1) ou descriptografia (-1).

No início do processo de derivação, a função cria uma cópia do valor de "sal" (saltCopy). Se a função estiver sendo usada para criptografia, ela gera um novo valor aleatório para saltCopy. Caso contrário, ela copia o valor do salt fornecido como entrada para saltCopy.

A função define o número de iterações de derivação (geralmente 10.000) e calcula o tamanho da chave derivada (keySize) com base no comprimento da chave de entrada.

Em seguida, a função inicializa o OpenSSL, preparando-o para as operações de derivação de chave.

A derivação da chave é realizada usando o algoritmo PBKDF2-HMAC-SHA256. A função PKCS5_PBKDF2_HMAC do OpenSSL é utilizada para este fim, com a chave de entrada, o "sal" (saltCopy), o número de iterações, o algoritmo de hash SHA-256 e o tamanho da chave derivada.

Após a derivação da chave, o valor final da chave derivada é armazenado no ponteiro derivedKey.

A função também assegura que o "sal" (salt) seja atualizado com o valor de saltCopy, garantindo que corresponda ao "sal" usado na derivação da chave.

Por fim, a função limpa o OpenSSL, finalizando qualquer recurso alocado durante o processo. A função deriveKey desempenha um papel crucial na geração da chave usada para criptografar e descriptografar dados, garantindo que a chave derivada seja única para cada conjunto de dados e aumentando a segurança do processo de criptografia.

6.4.4. Utilits

O arquivo de cabeçalho "utils.h" contém várias definições e funções auxiliares usadas em um contexto de criptografia e descriptografia de dados, geralmente relacionado ao algoritmo AES (Advanced Encryption Standard).

Ele começa definindo duas tabelas chamadas sBox e invSBox, que são matrizes 16x16. Essas tabelas são usadas no processo de substituição de bytes no AES.

Em seguida, há a definição de uma função extractXY, que é usada para extrair os valores de x e y a partir de um número hexadecimal de 8 bits.

O arquivo também inclui matrizes chamadas multiplicationMatrixEncrypt e multiplicationMatrixDecrypt, que contêm valores usados para a multiplicação de colunas durante o processo de mixColumns na criptografia e descriptografia.

Há ainda as matrizes eTable e lTable, que são usadas no processo de substituição de bytes para a expansão da chave (key expansion). Essas tabelas permitem realizar operações de substituição eficientes.

A função getEorLValue é definida para obter valores a partir das tabelas eTable ou lTable, dependendo do contexto.

O arquivo também inclui funções como removeBytes para remover bytes de uma sequência de caracteres, getKeyLength para obter o tamanho da chave e nearestKeySize para determinar o tamanho da chave mais próximo com base em um valor x.

No geral, o arquivo "utils.h" fornece uma série de utilitários e estruturas de dados necessárias para realizar operações de criptografia e descriptografia com o algoritmo AES. É uma parte fundamental de um sistema de segurança que implementa o AES para proteger dados sensíveis.

6.4.5. Blocks

O código inclui várias bibliotecas padrão, como <stdio.h>, <string.h>, <math.h>, e a biblioteca OpenSSL <openssl/rand.h>. Estas bibliotecas são usadas para funções relacionadas a strings, matemática e criptografia.

É definida uma constante BLOCK_SIZE com valor 16. Isso representa o tamanho de cada bloco de dados. É um valor comum em algoritmos de criptografia de bloco, como o AES.

A função blocksCount(char *text) calcula o número de blocos necessários para armazenar um texto fornecido. Ele faz isso dividindo o tamanho do texto pelo tamanho do bloco (16) e arredondando o resultado para cima usando a função ceil da biblioteca matemática. O resultado é retornado como um número inteiro.

A função toBlocks(char *text, unsigned char (*textBlocks)[BLOCK_SIZE]) divide o texto em blocos de 16 bytes (ou o tamanho especificado em BLOCK_SIZE) e armazena cada bloco como uma matriz de bytes. A função realiza as seguintes etapas: Converte o texto de entrada em uma matriz de bytes chamada textInBytes. Calcula o número total de blocos necessários usando blocksCount. Preenche cada bloco com dados do textInBytes e, se necessário, preenche com caracteres nulos para o último bloco.

A função toVector(unsigned char (*textBlocks)[BLOCK_SIZE], char *textVector, int blocks, unsigned char *salt, short action) é responsável por criar um vetor de bytes a partir dos blocos de dados. Ela leva em consideração o número de blocos, o tamanho do bloco e um parâmetro de ação que, se for igual a 1, envolve a inserção de um "sal" (salt) no início do

vetor (essa parte está comentada no código). A função, então, copia os bytes de cada bloco para o vetor resultante textVector.

No geral, esse código fornece funcionalidades para dividir um texto em blocos e montar um vetor contínuo de bytes desses blocos. Isso é útil em contextos de criptografia e descriptografia, onde a manipulação de dados em blocos é comum. Além disso, ele inclui a capacidade de incorporar um "sal" no início do vetor, o que é útil em certos cenários de criptografia para tornar os dados mais seguros.

6.4.6. Key

No código AES, a chave é utilizada da seguinte maneira: no início do processo de criptografia, a chave é configurada. Essa configuração ocorre apenas uma vez no início do processo. Conforme o algoritmo AES progride por suas várias rodadas, a chave relevante para cada rodada é acessada a partir de uma matriz de chaves derivadas. Essa matriz contém todas as chaves derivadas, organizadas em uma ordem específica. Portanto, a chave apropriada para a rodada atual é obtida através do índice correto na matriz. Essa abordagem é fundamental para garantir que uma chave diferente seja usada em cada rodada do algoritmo, o que contribui para aumentar a segurança do processo de criptografia. A organização e a chamada das chaves derivadas dependem da estrutura específica do código do AES, mas geralmente, a matriz de chaves derivadas é referenciada no código para obter a chave apropriada a ser utilizada em cada rodada subsequente.

7. Resultado e Discussão

7.1. Resultados da Implementação

A implementação bem-sucedida do sistema de criptografia, composta por um site interativo, uma API e um algoritmo de criptografia em linguagem C, resultou em um sistema funcional e eficaz. Os usuários têm a capacidade de inserir texto para criptografia, junto com uma chave, através da interface do site. A API desempenha um papel fundamental na comunicação entre o site e o algoritmo de criptografia em C. Com esses componentes trabalhando harmoniosamente, conseguimos alcançar a principal meta do projeto.

7.2. Segurança e Eficiência

Uma análise aprofundada revela que o sistema é eficaz na criptografia e descriptografia de mensagens. A expansão das chaves, que envolve rotações e substituições, desempenha um papel significativo na segurança do sistema. A função Rcon gera constantes de rodada que tornam o processo virtualmente impossível de descriptografar para computadores convencionais. Isso garante a segurança dos dados criptografados.

Além disso, a função SBox, que realiza substituições baseadas em uma tabela predefinida, contribui para a confusão dos dados, tornando a análise de padrões uma tarefa árdua. Isso é fundamental para a resistência a ataques de força bruta e criptoanálise.

7.3. Desempenho e Aplicabilidade

Em termos de desempenho, o sistema opera de maneira eficiente, oferecendo respostas rápidas e precisas aos usuários. A API permite uma comunicação suave entre o site e o algoritmo de criptografia, garantindo tempos de resposta mínimos.

Além disso, o sistema demonstra uma ampla gama de aplicabilidade. O site interativo com a API é um exemplo prático de como o sistema pode ser facilmente utilizado. A sua implementação eficaz permite que os usuários protejam suas informações e comunicações com facilidade, sem a necessidade de conhecimento técnico avançado. Isso torna o sistema acessível e valioso em uma variedade de contextos.

8. Conclusão

Com base nos resultados obtidos, é possível concluir que o sistema de criptografia desenvolvido é eficaz, seguro e eficiente. Este projeto proporcionou uma visão abrangente da criptografia, suas raízes históricas e sua importância contínua na sociedade atual. O sistema demonstrou aplicações práticas em diversos cenários, tornando-se uma solução versátil para a proteção de informações confidenciais.

Neste trabalho, desenvolvemos um algoritmo de criptografia em linguagem C e o integramos a um site, utilizando JavaScript e uma API que permite ao site ler e executar o código em C. Essa abordagem inovadora nos permitiu explorar a trajetória histórica da criptografia, destacando sua relevância essencial para os futuros profissionais de Ciência da Computação.

Além disso, compreendemos a necessidade de um entendimento profundo sobre o que é criptografia, como ela se originou e qual é o seu propósito, uma vez que seremos responsáveis por empregar esse conhecimento em nosso futuro no mercado de trabalho. Nosso objetivo geral de estudar a criptografia militar ao longo da história e sua aplicação na segurança de comunicações e proteção de informações confidenciais nos permitiu compreender a evolução e a importância dessa disciplina.

Ao delinear nossos objetivos específicos, destacamos a importância de investigar e compreender a criptografia avançada representada pelo algoritmo AES, que desempenha um papel fundamental na proteção de dados em todo o mundo. Com a criação de um algoritmo de criptografia em C e a integração com JavaScript em um site, demonstramos nossa determinação em aplicar o conhecimento adquirido de forma prática e contribuir para a contínua inovação no campo da segurança digital.

Portanto, o projeto alcançou com êxito seus objetivos, fornecendo uma ferramenta robusta para a criptografia de dados em um mundo cada vez mais digital e interconectado. Esta abordagem não apenas nos proporcionou uma visão abrangente da criptografia, suas raízes históricas e seu papel vital na sociedade atual, mas também nos permitiu aplicar esse conhecimento de maneira concreta, criando uma solução que envolve a execução de código em C através de uma API no contexto de um site. Compreendemos a importância de sua aplicação em nossa futura carreira em Ciência da Computação e estamos comprometidos em contribuir para a evolução e segurança contínua das comunicações e proteção de informações em um mundo digital em constante transformação.

9. Referências

Bruno, Odemir M. Criptografia: de arma de guerra a pilar da sociedade moderna, Jornal da USP, 2017. Disponível em: https://jornal.usp.br/artigos/criptografia-de-arma-de-guerra-a-pilar-da-sociedade-moderna/. Acesso em: 16 set. 2023.

COMER, Douglas E. Redes de computadores e Internet. 6. Ed. Porto Alegre: Bookman, 2016.

DAEMEN, Joan, Rijmen, Vicent. The Design of Rijndael: AES – The Advanced Encryption Standard. Springer, 2002.

FOROUZAN, Behrouz A. Comunicação de dados e redes de computadores. 4. Ed. Porto Alegre: AMGH, 2010.

KAHN, David. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Washington, D.C.: Editora DEF, 2018.

LEVY, Steven. Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. San Francisco: Editora GHI, 2020.

NAKAMURA, E. T.; GEUS, P. PL. Segurança de redes em ambientes cooperativos. São Paulo: Novatec, 2007.

NIST. FIPS PUB 197: Advanced Encryption Standard (AES). Ed. 1. Gaithersburg, 2001.

STALLINGS, William. Cryptography and Network Security: Principles and Practice. Nova York: Editora ABC, 2019.

STALLINGS, William. Cryptography and Network Security: Principles and Practice. 8. ed. Pearson, 2021.

SINGH, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Londes: Editora XYZ, 2020.

Instituto Nacional de Padrões e Tecnologia (NIST) (ed.). Processing Standards Publication: advanced encryption standard (aes). 197. ed. Estados Unidos: Nist, 2001. 51 p. Tradução nossa. Disponível em: https://csrc.nist.gov/files/pubs/fips/197/final/docs/fips-197.pdf. Acesso em: 10 out. 2023