

UNIVERSIDADE PAULISTA – UNIP

CIÊNCIA DA COMPUTAÇÃO

Breno Leles Monari - RA: R009HJ4

Diogo Brito Brasil - RA: G81EED0

Deysi Karen Ticona - RA: N299444

Gretzel Kattia Laura - RA: N158930

Vinicius Cartaxo - RA: G8286J4

**APS
CRIPTOGRAFIA**

**SÃO PAULO
2023**

APS DE CRIPTOGRAFIA

Trabalho acadêmico apresentado à disciplina de APS
do Curso Ciência Da Computação como requisito de
nota da NP2. Requerido pelo prof. Álvaro Prado.

SÃO PAULO
2023

ÍNDICE

1. Objetivo do trabalho.....	4
2. Introdução.....	5
<hr/>	
3. Criptografia(Conceitos gerais).....	6
4. Criptografia clássica	8
4.1 Scytale.....	8
4.2 Cifra de César.....	9
4.2 Cifra de Vigenere.....	9
<hr/>	
5. Criptografia moderna.....	10
5.1 Máquina enigma.....	10
6. Chave simétrica.....	12
7. Chave assimétrica.....	13
<hr/>	
8. Técnicas criptográficas mais utilizadas e conhecidas.....	14
<hr/>	
9. Dissertação (Técnica criptográfica escolhida).....	17
9.1 Estrutura, conceitos e fundamentação.....	18
9.2 Benefícios em relação às técnicas anteriores.....	18
9.3 Aplicações que fazem/fizeram uso da técnica	19
9.4 Discussão comparativa entre esta técnica e outras conhecidas/utilizadas..	20
9.5 Vulnerabilidades e falhas	21
9.6 melhorias propostas e/ou implementadas.....	21
<hr/>	
10. Projeto.....	22
10.1 Projeto (estrutura) do programa.....	23
10.2 Relatório com as linhas de código do programa.....	25
<hr/>	
11. Bibliografia.....	28
12. Ficha de atividades Práticas Supervisionadas.....	29

1. OBJETIVO DO TRABALHO

O objetivo final do trabalho é recriar um código de criptografia na linguagem de programação Python. Nesse aspecto, tem-se o intuito de assegurar tanto a confidencialidade quanto a integridade para haver a autenticidade de informações presentes no código.

Para atingir esse objetivo, abordaremos anteriormente a evolução da criptografia e as diferentes técnicas utilizadas por cada um dos criadores. Faremos uma jornada desde a criptografia da Idade Antiga até os dias atuais, identificando eventuais vulnerabilidades detectadas e considerando possíveis aprimoramentos, incluindo os conceitos subjacentes às suas aplicações.

Logo em seguida, detalharemos o método escolhido para a execução do projeto proposto. Através do preenchimento de uma ficha, oferecemos uma visão abrangente de todo o desenvolvimento, desde o início até a conclusão do trabalho proposto na Atividade Prática Supervisionada (APS). Dessa forma, apresentaremos o programa, sua estrutura e o relatório contendo as linhas de código, culminando na finalização do projeto.

2.INTRODUÇÃO

A criptografia é um ramo da computação que se desenvolveu e aprimorou ao longo dos anos, utilizando técnicas e algoritmos que só podem ser acessados pela pessoa que possui a “chave”. Em outras palavras, a criptografia é a técnica responsável por codificar e criptografar dados de forma a torná-los inteligíveis apenas para o destinatário pretendido. Essa técnica é amplamente utilizada em arte, tecnologia e ciência para garantir que as mensagens sejam confidenciais e não possam ser acessadas por terceiros.

Antes do surgimento da computação, a criptografia era realizada por meio de um sistema de cifras e códigos conhecido como tipografia clássica. Esse sistema consistia em ocultar o algoritmo e a chave criptográfica. Com o surgimento da computação e do ambiente 2.0, a criptografia evoluiu para projetar sistemas e códigos de criptografia que permitam criar maior segurança na era das comunicações digitais. Para se adaptar a essas mudanças, a criptografia se dedica a pesquisar, desenvolver e aplicar técnicas matemáticas para atingir esse objetivo.

Também, pode-se ressaltar a importância que tem a relação que existe entre a criptografia e a matemática. Já que o relacionamento entre ambos é notório, já que grande parte do avanço da criptografia se parte da matemática, tudo isso torna as codificações muito mais complexas de serem descobertas por pessoas que queiram possuir esse tipo de informação valiosa. A maioria dos sistemas de criptografia utilizados por empresas, bancos, governos e entidades poderosas utilizam cálculos muito complexos para proteção e aquisição de informações, que são quase indecifráveis, mas nada é garantido sempre existe brechas mesmo a defesa mais poderosa tem uma fraqueza, e claro para cada tipo de criptografia existe uma e elas serão abordadas nos próximos tópicos.

3. CRIPTOGRAFIA (CONCEITOS GERAIS)

A origem da palavra “criptografia” vem da junção de duas palavras gregas, “Kryptós” e “Gráphein”, que significam “oculto” e “escrever” respectivamente. Logo, a palavra “criptografia” se refere a uma maneira de ocultar aquilo que está escrito. Em uma definição menos semântica, a criptografia se refere a um conjunto de ações e regras que tem como objetivo garantir que uma informação não possa ser recebida por ninguém exceto o destinatário. Dessa forma, a criptografia não impede que alguém intercepte uma mensagem, mas sim que esse alguém não consiga compreender o conteúdo da mensagem, com o objetivo principal de garantir a confidencialidade, integridade e privacidade dos dados.

Apesar do termo “criptografia” ter sido mais desenvolvido nos anos atuais, ele já existia desde séculos passados. Isto é, os povos antigos, como os espartanos e romanos, fizeram uso de cifras criptográficas quando precisavam trocar mensagens. Assim, percebe-se a importância da privacidade das informações, principalmente na era digital que o mundo se encontra presente no século XXI, ao qual os cidadãos “digita” seus dados em empresas de grande porte, que para manter a sua reputação (sem sofrer nenhum crime cibernético de dados) necessitam investir cada dia mais em software de criptografia cada vez mais complexa, para manter a segurança dos dados pessoais dos internautas.

A **esteganografia**, que vem do grego “*steganos*” (secreto) e “*grafia*” (escrito). Este procedimento tenta ocultar a própria existência da mensagem, opondo-se à criptografia que não esconde a presença de uma mensagem que pode ser perfeitamente percebida, mas está distorcida de tal forma que é incompreensível.

Sob esse viés, a esteganografia foi desenvolvida desde os tempos imemoriais e tem sido tradicionalmente utilizada por agências militares e de inteligência, criminosos e policiais, bem como por civis que desejam comunicar-se secretamente.

Ademais, os livros de história já fornecem essa informação, sendo usada na civilização antiga grega, os primeiros a aplicar essas técnicas engenhosas para esconder as mensagens, sem que sejam descobertos.



O antecedente mais conhecido da estenografia foi o Heródoto de Halicarnasso, o qual narra em sua obra: “As *Histórias*”, escrita entre os anos 484 e 430. Neste livro, o autor descreveu como o general ateniense Hestieu tentou encorajar seu genro Aristágoras de Mileto a se rebelar contra o pai de Xerxes, o famoso Rei persa, e para evitar que sua mensagem fosse interceptada, Hystieus teve a ideia inovadora de raspar a cabeça de um de seus servos e escrever a mensagem comprometedora em sua pele. Depois esperou que o cabelo voltasse a crescer e mandou o mensageiro que apareceu diante de Aristágoras e, após raspar a cabeça, mostrou a careca com a mensagem privada.

4.Criptografia Clássica

Denomina-se criptografia clássica o período que vai desde os povos antigos, passando pela Idade Média e chegando até as máquinas eletro-mecânicas (Conjunções de dispositivos mecânicos entrelaçados com circuitos elétricos e eletrônicos aptos a controlá-los), principalmente utilizadas durante a Segunda Guerra Mundial. Dentre as cifras clássicas mais conhecidas, destacam-se a scytale espartana, a de César e a de Vigenère.

4.1 SCYTALE

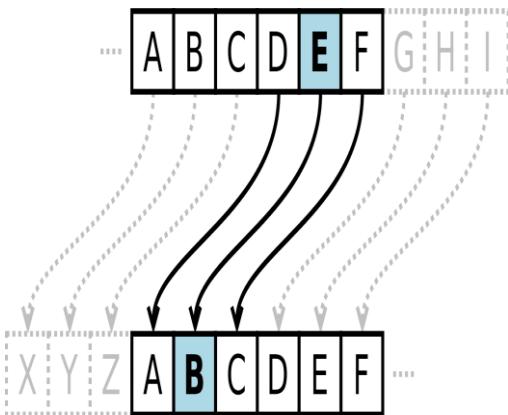


A segurança das comunicações é de extrema importância para o nosso mundo moderno: quando a segurança é violada, as consequências são muitas vezes de importância global. No entanto, estes problemas não são invenção da era da informática: desde a antiguidade, indivíduos de todas as civilizações têm tentado utilizar a tecnologia para cifrar correspondência confidencial, enquanto outros têm tentado desesperadamente decifrá-la.

O Scytale é uma cifra que se baseia em um método de transposição, em que o diâmetro desempenha um

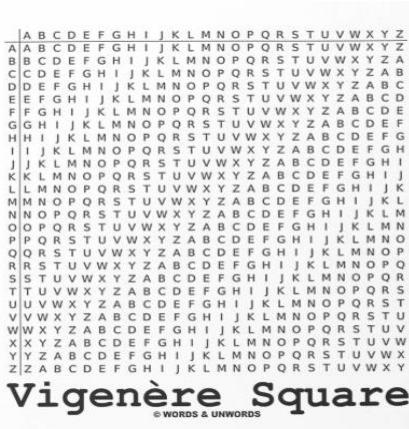
papel crucial como a chave da cifra. Na Grécia Antiga, o cinto do mensageiro era constituído por uma faixa de couro que ostentava caracteres na parte traseira. Aparentava ser uma sequência desconexa, contudo, ao enrolar o pedaço de couro em uma peça de madeira com o diâmetro apropriado, uma mensagem codificada revelava-se. Essa cifra compartilha funcionalidades semelhantes com a Cifra de César.

4.2 CIFRA DE CÉSAR



A Cifra de César é uma cifra de substituição na qual cada letra do alfabeto é deslocada para um certo número de lugares abaixo do alfabeto. Essa cifra foi empregada por Júlio César para se comunicar com suas tropas durante conflitos militares. Apesar do seu uso ter tido notável importância na guerra, ela é notavelmente simples, envolvendo a substituição de cada letra do alfabeto pela letra que se encontra três posições adiante, significando que a letra A seria substituída por D, a letra B por E, e assim por diante. Nesse contexto, o algoritmo da cifra opera pela troca de letras em posições específicas, e a chave, na figura abaixo, é o número 3.

4.3 VIGENÈRE



A cifra de Vigenère foi originalmente descrita por Giovan Battista Bellaso, um italiano, em 1553, em sua obra “La cifra del Sig. Giovan Battista Bellaso”. Durante muito tempo, essa cifra foi considerada como “le chiffre indéchiffrable” (a cifra indecifrável), até meados do século XIX, quando Charles Babbage e Friedrich Kasiki desenvolveram um método para decifrá-la. O processo de cifragem da cifra de Vigenère consiste no seguinte: o usuário cifra a mensagem com uma chave alfabética; se o

número de caracteres na chave for inferior ao tamanho da mensagem, a chave é repetida até ambas terem o mesmo número de caracteres. Ao relacionar a mensagem com a chave, cada letra da mensagem é cifrada com um alfabeto determinado pelo caractere correspondente na chave.

5.CRIPTOGRAFIA MODERNA

A criptografia moderna é uma técnica que utiliza conceitos matemáticos avançados, bem como alguns mais básicos, como números binários e hexadecimais, para transformar dados legíveis e conhecidos em dados cifrados que carecem de um padrão reconhecível e decodificável. Isso garante que apenas os autorizados tenham capacidade de compreender as informações. A criptografia moderna teve origem durante a Segunda Guerra Mundial, quando a necessidade de proteger informações sensíveis dos inimigos era crucial. Um exemplo notável é a máquina “ENIGMA” desenvolvida pelos alemães.

Inicialmente empregada principalmente para fins militares, a criptografia viu uma mudança significativa quando perceberam seu potencial comercial na proteção de dados contra concorrentes. Esse reconhecimento ampliou o escopo da criptografia, expandindo sua aplicação para além do cenário de guerra para a esfera empresarial.

5.1MÁQUINA ENIGMA



A máquina Enigma, utilizada pelos alemães durante a Segunda Guerra Mundial, destaca-se entre esses equipamentos. Ela se assemelha a uma máquina de escrever, mas, em vez de imprimir no papel, exibe os resultados em um painel luminoso com caracteres do alfabeto. A chave usada para cifrar/decifrar uma mensagem era configurada por meio de rotores eletromecânicos (3 ou mais), que podiam ser alterados conforme a necessidade para formar a chave. Inicialmente considerada impossível de decifrar, a quebra da cifragem da Enigma foi alcançada graças aos esforços de poloneses e ingleses, com Alan Turing sendo especialmente lembrado por seu trabalho neste feito.

A máquina Enigma desempenhou um papel crucial ao permitir a transmissão de mensagens em códigos cifrados, tornando-se um dispositivo tecnológico vital durante a Segunda Guerra Mundial. Nesse cenário, a Segunda Guerra Mundial foi fundamental para o desenvolvimento das tecnologias, principalmente para fins militares, abrangendo armamentos avançados, aeronaves, submarinos, dispositivos de comunicação e interceptação, como rádios transmissores e radares. Esses avanços, combinados com

máquinas cifrantes como a Enigma, contribuíram significativamente para a dinâmica da guerra e culminaram na criação do primeiro computador do mundo.

O uso da máquina Enigma demandava cuidados minuciosos, desde a configuração diária da chave até a consulta do manual de códigos. A troca diária da chave era essencial para evitar rastreamento por tecnologia similar e a possível decifragem das mensagens transmitidas.

Já durante a Segunda Guerra Mundial, enquanto as máquinas Enigma eram amplamente empregadas pela inteligência militar alemã, um grupo de matemáticos e engenheiros poloneses, em colaboração com a inteligência militar britânica, desenvolveu um modelo ainda mais avançado do que o utilizado pelos alemães. Este modelo foi pioneiro ao conseguir decifrar os códigos da Enigma pela primeira vez.

6.CHAVE SIMÉTRICA

A cifra simétrica é um método de criptografia que utiliza uma única chave para tanto cifragem quanto decifragem, garantindo a confidencialidade e integridade das mensagens trocadas. Ao contrário da cifra assimétrica, que utiliza um par de chaves distintas, a cifra simétrica opera de maneira mais direta, simplificando o processo de criptografia.

O AES (*Advanced Encryption Standard*) é um dos algoritmos mais conhecidos e amplamente utilizados na cifra simétrica.

Além deste, tem-se o AES destaca-se por sua eficácia e segurança, sendo adotado como padrão pelo governo dos Estados Unidos e utilizado globalmente em uma variedade de contextos. Outro algoritmo relevante é o DES (*Data Encryption Standard*), que, embora tenha sido um padrão amplamente aceito, foi posteriormente substituído pelo AES devido a vulnerabilidades identificadas.

A cifra simétrica é aplicada em diversas áreas, incluindo segurança de redes, transações financeiras online e comunicações sensíveis. Sua simplicidade e eficácia a tornam uma escolha valiosa em muitos cenários.

7.CHAVE ASSIMÉTRICA

A cifra assimétrica, também conhecida como criptografia de chave pública, é uma técnica de criptografia que desempenha um papel crucial na garantia da segurança da informação, possibilitando a comunicação segura através de canais considerados inseguros.

Em contraste com as cifras simétricas, que compartilham uma única chave para cifragem e decifragem, a cifra assimétrica utiliza um par de chaves: uma pública e outra privada. A chave pública é divulgada amplamente e pode ser empregada por qualquer indivíduo para cifrar mensagens destinadas ao detentor da chave privada correspondente. No entanto, somente o titular da chave privada possui a capacidade de decifrar as mensagens cifradas com sua chave pública.

O (*Rivest-Shamir-Adleman*) é um dos algoritmos mais notáveis de cifra assimétrica, proposto por Ron Rivest. O RSA fundamenta-se na complexidade computacional associada à fatoração de números primos grandes, tornando a quebra da cifra uma tarefa impraticável em tempo razoável, mesmo para computadores modernos.

Outro algoritmo relevante é o ElGamal, que adota uma abordagem distinta baseada no problema do logaritmo discreto. Além destes, destaca-se a ECC (*Elliptic Curve Cryptography*), que utiliza propriedades matemáticas de curvas elípticas para garantir a segurança na comunicação. Esses algoritmos são amplamente empregados na segurança de transações online, assinaturas digitais e em protocolos de segurança como o TLS/SSL para garantir comunicações seguras na web.

Esses algoritmos são amplamente empregados na segurança de transações online, assinaturas digitais e em protocolos de segurança como o TLS/SSL para garantir comunicações seguras na web

8.TÉCNICAS CRIPTOGRÁFICAS MAIS UTILIZADAS E CONHECIDAS

Criptografia DES

Criado na IBM, o Data Encryption Standard (DES) foi um dos primeiros algoritmos criptográficos desenvolvidos. Ele é um algoritmo de tipo chave simétrica e era considerado o padrão federal de criptografia de dados dos Estados Unidos até 1999.

Devido a algumas preocupações com a segurança do método, novos algoritmos criptográficos modernos substituíram o já ultrapassado Data Encryption Standard. Isso porque suas chaves de 56 bits são muito curtas e, portanto, fáceis de serem decifradas por um computador moderno.

Antes de se tornar obsoleto, o DES era tipicamente utilizado para proteger transações financeiras eletrônicas. Seu uso na atualidade inclui treinamentos em criptografia e projetos de pesquisa.

Criptografia 3DES

O algoritmo criptográfico 3DES (Triple Data Encryption Standard) é o sucessor do algoritmo DES original. Seu propósito inicial era resolver os principais problemas do DES. Mais especificamente, a questão do tamanho pequeno da chave secreta (56 bits). Assim como seu antecessor, o 3DES é um algoritmo criptográfico simétrico, e o tamanho das suas chaves é de 64 bits. Ele também foi desenvolvido a partir da mesma estrutura de códigos da Cifra de Feistel. O algoritmo simétrico 3DES utiliza um método de criptografia triplo, aplicando três vezes o algoritmo DES em cada bloco de dados. É assim que a chave do 3DES se torna mais longa e, portanto, significativamente mais difícil de decifrar.

Criptografia AES

O padrão de criptografia avançado — Advanced Encryption Standard (AES) — é um algoritmo simétrico mais recente. Ele substituiu o DES como o padrão criptográfico nacional dos EUA a partir da aprovação feita pelo Instituto Nacional de Padrões e Tecnologia, o NIST. A principal vantagem do AES sobre o DES é o tamanho das chaves geradas, cujo comprimento pode ser de até 256 bits, tornando-as mais difíceis de decifrar por usuários não autorizados. Além disso, o algoritmo de criptografia AES é mais rápido, já que é matematicamente mais eficiente. Entre os algoritmos criptográficos simétricos, o AES é atualmente o mais popular. Seus principais usos incluem a segurança de redes Wi-Fi e a proteção de informações em plataformas de armazenamento de dados e em aplicativos móveis.

Criptografia RSA

O Rivest-Shamir-Adleman (RSA) é um dos primeiros algoritmos criptográficos assimétricos. Apesar de ser antigo, ele se mantém como uma opção popular, já que oferece um alto nível de segurança. O RSA utiliza o método matemático de Fatoração Primária — uma espécie de decomposição em fatores primos — para gerar uma longa sequência de números a partir de combinações menores. Assim, a partir de longas strings, os cibercriminosos precisam determinar quais são as pequenas strings de números primos para então descobrir a chave secreta.

O algoritmo criptográfico RSA utiliza tamanhos de chave significativamente maiores do que outras soluções de algoritmos de criptografia de chave pública. O RSA suporta chaves assimétricas de até 4096 bits, que são quase impossíveis de decifrar, mesmo com um computador moderno

Esse algoritmo de chave pública costuma ser utilizado para proteger aplicações web, mensagens de email e blockchains de criptomoedas. Os certificados SSL e TLS também fazem uso do algoritmo RSA para executar seus processos de criptografia assimétrica.

Criptografia Twofish

O Twofish é um algoritmo de criptografia simétrica que suporta chaves de comprimento de até 256 bits. Ele foi inicialmente desenvolvido para substituir o DES, mas seu desempenho com chaves de 128 bits ficou aquém do algoritmo de criptografia AES.

Apesar de um pouco mais lento, este algoritmo oferece um nível de segurança similar ao do AES. A principal vantagem do Twofish, entretanto, está na sua flexibilidade, já que esse algoritmo adequado pode ser utilizado numa ampla gama de casos e aplicativos.

O Twofish possibilita a compensação de desempenho de acordo com a relevância de diversos parâmetros, como velocidade de encriptação e capacidades de hardware. Sendo assim, isso faz com que o algoritmo criptográfico Twofish seja a solução ideal para aplicações com recursos limitados de armazenamento e memória RAM.

Hoje, a criptografia é usada para proteger bilhões de transações online, dados confidenciais e mensagens privadas que transmitimos. Uma maneira de garantir a segurança é por meio de TLS/SSL.

“TLS permite que informações confidenciais inseridas sejam transmitidas com segurança. Os exemplos incluem um servidor e navegador da web e um servidor de e-mail e cliente de e-mail.

Para estabelecer essa conexão segura, o navegador e o servidor precisam de um certificado TLS. Se um site começar com https, o site é protegido com um certificado TLS”, conclui Dean.

Tudo isso é possível por causa da criptografia por trás da criptografia TLS. O uso de criptografia assimétrica (ou criptografia de chave pública) e criptografia simétrica e os muitos algoritmos usados para criar as chaves assimétricas e simétricas por trás dessa criptografia permitem a criptografia de dados tão segura que os maiores supercomputadores do mundo não conseguem quebrá-la.

9.DISSERTAÇÃO (TÉCNICA CRIPTOGRÁFICA ESCOLHIDA)

A criptografia é uma prática antiga que consiste em transformar dados importantes em um formato ilegível como um enigma, a fim de salvar ou guardar as informações contra acesso não autorizado. A origem da criptografia vem das civilizações antigas, como egípcios, babilônios e gregos que utilizavam métodos rudimentares para ocultar informações cruciais, esses métodos envolviam alterar a ordem das letras em uma mensagem ou usar símbolos para representar letras, sendo que somente aqueles com conhecimento do sistema poderiam decifrar.

Uma delas é a Cifra de César, a técnica principal desse trabalho, e uma das mais simples técnicas de criptografia, sendo muito utilizada por Júlio César durante o período romano. Ela exemplifica a substituição de letras, onde cada letra do texto original é substituída por outra que se encontra um número fixo de posições adiante no alfabeto. Sendo assim a cifra de césar é uma cifra de substituição monoalfabética, um tipo de criptografia simples de entender e executar, e por essa razão, é uma das cifras mais populares entre iniciantes na área.

Apesar de ser uma técnica antiga, a Cifra de César continua sendo utilizada atualmente como uma forma simples de introduzir o conceito de criptografia em sala de aula e em cursos introdutórios, além de ser um exemplo interessante para mostrar a importância do uso de técnicas mais sofisticadas e seguras na proteção de informações sensíveis. É um dos melhores exemplos de criptografia para cursos de programação iniciais, tornando-se uma técnica bem simples e fácil de executar por alunos que não possuem amplo conhecimento, e também muito menos experiência prática com o assunto abordado.

9.1 Estrutura, conceitos e fundamentação

A criptografia é o processo de codificação de texto legível em um código seguro, é uma tecnologia fundamental para proteger informações contra acesso externo.

Historicamente, é usada em espionagem e em tempos de guerra para comunicações confidenciais, Júlio César, imperador romano de 100 a.C. a 44 a.C., utilizava um código para proteger as mensagens enviadas a seus generais. Assim, se a mensagem caísse em mãos inimigas, a informação não poderia ser compreendida.

A criptografia usa uma fórmula chamada “cifra” ou algoritmo de criptografia, que garante que qualquer pessoa que tente interceptar informações comunicadas não consiga ler seu conteúdo verdadeiro.

A criptografia impede que suas informações sejam adulteradas. Em uma era digital que carece de confiança, a criptografia pode fazer com que você se sinta mais seguro de que as informações que envia e recebe são autênticas. Melhorar a integridade e a autenticidade dos dados é outro dos principais benefícios da criptografia.

Saber estes conceitos fundamentais sobre criptografia é fundamental para os profissionais da área de segurança e também para os profissionais da área de desenvolvimento de software.

9.2 Benefícios em relação às técnicas anteriores

Simplicidade e Facilidade de Implementação: A cifra de César é notável por sua simplicidade. É uma técnica de criptografia de substituição simples em que cada letra do texto é deslocada por uma quantidade fixa, determinada pela chave. Essa simplicidade torna a cifra de César fácil de entender e implementar, sendo uma opção acessível para usuários comuns.

Eficiência na Encriptação Rápida: A cifra de César é eficiente em termos de velocidade de encriptação, pois a única operação realizada é o deslocamento dos caracteres no alfabeto. Isso a torna uma escolha prática em situações em que é necessário um processo rápido de criptografia e descriptografia.

Facilidade de Compreensão e Ensino: A simplicidade da cifra de César também a torna uma ferramenta eficaz para fins educacionais. Ao ensinar princípios básicos de criptografia, é comum começar com a cifra de César para ajudar os estudantes a compreenderem os fundamentos antes de abordar técnicas mais avançadas.

Flexibilidade e Adaptabilidade: A cifra de César pode ser adaptada para diferentes línguas e alfabetos. Mesmo quando aplicada a idiomas não latinos, como o hebraico ou o cirílico, o conceito subjacente de deslocamento de caracteres pode ser mantido, demonstrando sua flexibilidade.

Compreensão Intuitiva da Chave: O uso de uma chave numérica para determinar o deslocamento facilita a compreensão da cifra de César. A chave é diretamente relacionada à quantidade de deslocamento, o que simplifica a comunicação entre usuários autorizados e facilita o entendimento da técnica.

Comparação com outras técnicas: pode-se comparar a Cifra de César em com técnicas mais complexas, por exemplo, a cifra de Vigenère. Assim, a cifra de César se destaca pela sua simplicidade. Embora seja menos segura contra métodos de análise mais avançados, ela continua sendo uma opção valiosa em cenários específicos, especialmente quando a segurança adicional não é uma prioridade e a simplicidade é vantajosa.

9.3 Aplicações que fazem/fizeram uso da técnica

O primeiro uso da cifra de substituição com propósito militar que se tem conhecimento aconteceu nas Guerras da Gália de Júlio César. O imperador romano Júlio César descreveu como enviou uma mensagem a Cícero, que estava cercado e à beira da rendição. A substituição foi feita de forma a substituir as letras romanas por letras gregas, tornando a mensagem ininteligível para o inimigo, a forma de substituição empregada por Júlio César ficou conhecida como cifra de César. A cifra de César funciona tomando cada letra da mensagem de texto aberto e substituindo-a pela késima letra sucessiva do alfabeto, permitindo a rotatividade do alfabeto, isto é, a letra Z seria seguida novamente da letra A. Por exemplo, se $k = 4$, então a letra A do texto claro fica sendo E no texto cifrado; B no texto claro se transforma em F no texto cifrado, e assim por diante.

9.4 Discussão comparativa entre esta técnica e outras conhecidas/utilizadas

Cifra de César vs. Cifra de Vigenère: Tanto a cifra de César quanto a cifra de Vigenère compartilham a ideia básica de substituição de caracteres, mas diferem na implementação. A cifra de César usa um deslocamento fixo para criptografar cada caractere, enquanto a cifra de Vigenère utiliza uma palavra-chave para determinar o deslocamento, tornando-a mais segura. No entanto, a cifra de Vigenère pode ser mais complexa de entender e implementar, enquanto a cifra de César destaca-se pela sua simplicidade.

Cifra de César vs. Cifra de Substituição Simples: Ambas as cifras de César e de substituição simples são técnicas de criptografia de substituição, mas a cifra de César é uma forma específica de cifra de substituição. A cifra de substituição simples substitui cada caractere por outro pré-determinado, enquanto a cifra de César envolve um deslocamento fixo. A cifra de César é mais fácil de implementar e compreender, mas é menos segura do que a cifra de substituição simples.

Cifra de César vs. Métodos Criptográficos Modernos: Comparado com métodos modernos de criptografia, como AES (Advanced Encryption Standard) ou RSA (Rivest-Shamir-Adleman), a cifra de César é considerada muito insegura. Métodos modernos oferecem segurança muito mais robusta, usando algoritmos avançados e chaves mais longas. No entanto, a cifra de César pode ser útil em situações simples, onde a segurança não é a principal preocupação.

Cifra de César vs. Cifras de Transposição: Cifras de transposição, como a cifra de coluna, alteram a ordem dos caracteres, enquanto a cifra de César os substitui. Ambas são técnicas de criptografia clássicas, mas as cifras de transposição tendem a ser mais seguras, especialmente quando combinadas com outras técnicas. No entanto, as cifras de transposição podem ser mais complexas e exigir mais recursos computacionais.

Escolha na Implementação do Código: A escolha entre a cifra de César e outras técnicas no código depende dos requisitos de segurança e complexidade do projeto. Se a segurança é uma preocupação primordial, é recomendável usar métodos modernos de criptografia, como AES e RSA. No entanto, se a simplicidade é mais importante do que a segurança, a cifra de César pode ser uma opção viável. As cifras de transposição também podem ser uma boa escolha, especialmente quando combinadas com outras técnicas de criptografia.

9.5 Vulnerabilidades e falhas

Cifra de César possui suas desvantagens bem visíveis e sua desvantagem está na segurança relativamente baixa, uma vez que torna-se fácil desvendá-la por meio de análise estatística, especialmente em idiomas como o português, os quais apresentam tendências específicas nas frequências das letras. No entanto, a Cifra de César também é fácil de ser quebrada por meio do método de força bruta, no qual todas as chaves possíveis são testadas até que a mensagem original seja descoberta. Com a computação moderna, é possível realizar a quebra da cifra com uma certa facilidade, o que faz com que a segurança da mesma seja questionada para certos objetivos específicos como proteção de dados de empresas.

Nesse aspecto, a criptografia é uma ferramenta essencial para garantir a proteção e a privacidade das informações de uma empresa. Independentemente do tamanho ou do setor de atuação da empresa, é fundamental adotar medidas de segurança adequadas, como a criptografia, para evitar possíveis perdas financeiras e danos à reputação da empresa.

9.6 melhorias propostas e/ou implementadas

A Cifra de César usa um método de criptografia simples e obsoleta, elaborado pelo líder militar romano Júlio César. Ela funciona deslocando as letras do alfabeto por um número fixo de posições, apesar de simples precisam de melhorias.

Considere o uso de um alfabeto amplo que inclui letras, números, caracteres especiais e espaços. Isso aumentará a segurança de uma mensagem.

Embaralhar o alfabeto antes de poder enviar uma mensagem usando esse método seria mais difícil de poder decifrar. Seria mais complicado a quebra da cifra, mesmo que alguém descubra o padrão, ele precisaria primeiro decifrar o alfabeto embaralhado.

Em vez de depender de métodos históricos como a Cifra de César, é aconselhável utilizar algoritmos de criptografia modernos, como AES (Advanced Encryption Standard) ou RSA (Rivest–Shamir–Adleman), que são considerados mais seguros.

Mesmo com as melhorias ainda não seria possível usá-las para a segurança de algo importante, por isso só é possível usar este método para uso acadêmico somente, sem ser designada a proteção de dados.

10. PROJETO

Para a elaboração do nosso projeto, foi necessário questionar para o professor Álvaro algumas sugestões de qual tipo de Criptografia utilizar para o trabalho da APS, sendo sugerido a Cifra de Vigenère ou a cifra de César. Após o encontro, uma breve discussão foi realizada para decidir qual deles o grupo iria se focar mais, sendo optado (de forma unânime) a cifra de césar, pois a sua estrutura era mais simples e prática para o grupo se empenhar junto, já que estávamos iniciando o aprendizado com a linguagem de programação Python. Logo, após algumas tentativas individuais, com o intuito de juntar as melhores ideias de cada um dos membros, foi apresentado a nova proposta, o que agradou o professor Álvaro, sugerindo adicionar o arquivo .txt no programa. Assim, foi remontado o código com as ideias mais destacadas de cada um, e adicionando o arquivo texto como uma chave variável (contendo nele o nome dos usuários do programa, para a continuidade do programa (chave assimétrica) , ou somente escolhendo uma única chave (chave simétrica). No fim, com o último encontro com o professor (que nos orientou durante todo o desenvolvimento do programa de criptografia) foi proposta que o .txt só conteria a chave que deveria ser criptografada pelo programa, após adicionar a palavra-chave para obter a informação contida nela

10.1 PROJETO (ESTRUTURA) DO PROGRAMA

Após a escolha da Cifra de César, que percorre cada letra da palavra original, verifica-se se é uma letra do alfabeto e realiza-se o deslocamento da cifra de César. O deslocamento é feito considerando se a letra é maiúscula ou minúscula.

Foi designado um dia para cada membro pensar em diferentes ideias e apresentá-las no grupo, incluindo o código que continha parte da ideia ou total. Como a primeira linguagem de programação que tínhamos conhecimento era o Python, que se assemelha mais à linguagem natural, facilitando a compreensão, foi a forma escolhida para iniciar a criação do código. Logo após essas tentativas individuais, com o intuito de juntar as melhores ideias de cada um, foi apresentada a nova proposta, que continha não somente a cifra de César, mas também opções para criptografar e descriptografar a mensagem, designando até uma saída para o programa parar.

Fomos novamente em busca do professor Álvaro que gostou do resultado, mas sugeriu adicionar o arquivo .txt no programa. Assim, foi remontado o código, adicionando o arquivo texto como uma chave variável, contendo nela o nome dos usuários do programa, para o programa prosseguir (chave assimétrica), ou somente escolhendo uma única chave (chave simétrica).

Finalmente, no último encontro com o professor, que nos orientou durante todo o desenvolvimento do programa de criptografia, foi proposto que o .txt só conteria a mensagem que deveria ser criptografada/descriptografada pelo programa, após adicionar a palavra-chave para obter a informação contida nela. Assim, foram feitas as seguintes alterações no código.

A função “criptografar” recebe um texto e uma chave como entrada e retorna o texto criptografado usando a cifra de César. Ela itera em cada caractere no texto e verifica se é uma letra do alfabeto, mantendo a caixa (maiúscula ou minúscula) do caractere original. Em seguida, aplicar a criptografia de César, deslocando cada letra pela quantidade especificada pela chave, utilizando a tabela ASCII.

A função “descriptografar” chama a função “criptografar”, mas com uma chave negativa, invertendo o deslocamento para realizar a descriptografia. Ela recebe um texto criptografado que o usuário preferir e uma chave como entrada, retornando o texto original descriptografado.

A função “main” é a principal do programa. Utilizando um loop while, ou seja, efetuando loop infinito para permitir múltiplas operações, ela permite que o usuário escolha entre criptografar, descriptografar ou sair do programa. Para isso, solicita o modo de operação,

lê o nome do arquivo de texto, realiza a operação escolhida e exibe o resultado, garantindo exceções se por acaso o arquivo não exista, exibindo uma mensagem ao console.

A abertura do arquivo texto é realizada na função “main” usando a declaração “with open (nome_arquivo, ‘r’, encoding=‘utf-8’) as arquivo”. Isso garante que o arquivo seja fechado automaticamente após o bloco “with” ser concluído, garantindo a correta gestão de recursos, como também usar a codificação UTF-8 para lidar com caracteres especiais. O conteúdo do arquivo é lido usando “arquivo.read()”, e o texto resultante é utilizado nas operações de criptografia ou descriptografia. O código também utiliza o bloco “try” e “except” para lidar com a abertura do arquivo “XXXX.txt”. Caso o arquivo não seja encontrado, uma mensagem de erro é exibida.

Na função main, a chave de criptografia é definida ao gosto do usuário, ao selecionar a opção de criptografar e descriptografar o texto contido no arquivo. Em seguida, ao escolher uma opção de criptografia, o programa solicita uma chave de criptografia e exibe o texto criptografado. Ao escolher a opção de descriptografar, o usuário fornece uma chave de descrição, e o programa exibe o texto descritivo dentro do arquivo.txt.

O programa permanece em um loop enquanto o usuário não escolhe a opção de sair (‘s’). Dessa forma, cria-se uma experiência interativa que permite ao usuário realizar diversas transações sem reiniciar o programa. Somente quando o usuário escolhe sair, o programa exibe uma mensagem de encerramento e sai do loop, finalizando a execução.

Portanto, esse programa possui um código bem simples, já que a Cifra de Cesar não é o método mais eficaz atualmente, e com certeza não seria usado como método de segurança para nenhuma empresa, já a segurança poderia ser quebrada muito facilmente usando a maioria dos métodos, inclusive o de força bruta. Então foi necessário desenvolver mais conceitos, com a base da sendo esse tipo de criptografia para fins educativos, pois é um método de fácil compreensão, teste e prática. Assim, o código é estruturado de forma modular, com funções separadas para diferentes tarefas, promovendo a legibilidade e manutenção. A interação com o usuário é feita de maneira amigável, fornecendo instruções claras e tratando erros de entrada. O uso do “with” foi essencial para o resultado deste trabalho, responsável por abrir o arquivo e certificar de forma correta a manipulação do recurso, isso contribuindo para a robustez do programa.

10.2 Relatório com as linhas de código

```
print("=====")  
print(" Olá programador(a), você foi selecionado para este evento secreto ")  
print("=====")  
  
def descriptografar(texto, chave):  
    return criptografar(texto,-chave)  
  
def main():  
    while True:  
        modo = input("Você deseja: 'c' para criptografar, 'd' para descriptografar, ou 's' para sair: ").lower()  
  
        if modo == 'c':  
            # Leitura do arquivo de entrada  
            nome_arquivo = input("Digite o nome do arquivo.txt (Tenha certeza de estar na mesma pasta): ")  
  
            try:  
                with open(nome_arquivo, 'r', encoding='utf-8') as arquivo:  
                    texto_original = arquivo.read()  
            except FileNotFoundError:  
                print(f"Erro: Arquivo '{nome_arquivo}' não encontrado.")  
                continue  
            except Exception as e:  
                print(f"Erro ao ler o arquivo: {e}")  
                continue  
  
        # Solicitação da chave de criptografia
```

```

chave = int(input("Digite a chave de criptografia (um número inteiro): "))

### Criptografia
texto_criptografado = criptografar(texto_original, chave)
print(f"\nTexto Criptografado:\n{texto_criptografado}\n")

elif modo == 'd':
    # Leitura do arquivo de entrada
    nome_arquivo = input("Digite o nome do arquivo.txt (Tenha certeza de estar na
mesma pasta): ")

try:
    with open(nome_arquivo, 'r', encoding='utf-8') as arquivo:
        texto_criptografado = arquivo.read()
except FileNotFoundError:
    print(f"Erro: Arquivo '{nome_arquivo}' não encontrado.")
    continue
except Exception as e:
    print(f"Erro ao ler o arquivo: {e}")
    continue

# Solicitação da chave de descriptografia
chave = int(input("Digite a chave de descriptografia (um número inteiro negativo):
"))

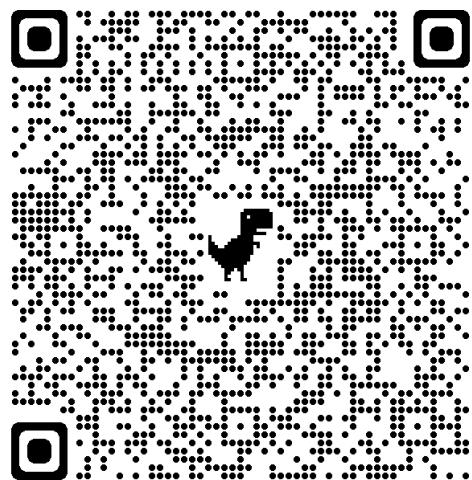
### Descriptografia
texto_descriptografado = criptografar(texto_criptografado, chave) # Usar a mesma
chave para descriptografia
print(f"Texto Descriptografado:\n{texto_descriptografado}")

###saída
elif modo == 's':
    print("Programa encerrado.")
    break

```

LINK DO CÓDIGO:

https://unipead-my.sharepoint.com/:f/g/personal/gretzel_penaloza_aluno_unip_br/EgietFfEokZEuMKODfBwucBQUpJTxvIZrpL9kydIRWlnw?e=rWb13N



11.BIBLIOGRAFIA

Aumasson, J.-P. (2017). *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press.

Criptoide. (2023). História da Criptografia. Disponível em:
<https://cryptoid.com.br/identidade-digital-destaques/a-historia-da-criptografia-2/>. Acesso em: 02 nov. 2023.

Da Silva, J. (2022). Criptografia e Segurança. E-Locução São Paulo, 11.

Destejiendo. (2018). Esteganografia. Disponível em:
<https://dEstejiendo.blogspot.com/2018/02/breve-historia-de-la-esteganografia-1.html>. Acesso em: 02 nov. 2023.

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.

Fiarresga, V. (2010). Criptografia e Matemática. Repositório da Universidade de Lisboa. Disponível em: <https://repositorio.ul.pt/handle/10451/3647>. Acesso em: 02 nov. 2023.

Hosting. (2023). O que é Criptografia. Disponível em:
<https://www.hostinger.com.br/tutoriais/o-que-e-criptografia>. Acesso em: 02 nov. 2023.

Machado, F. N. R. (2014). *Segurança da Informação: Princípios e Controle de Ameaças*. Saraiva.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.

Trappe, W., & Washington, L. C. (2006). *Introduction to Cryptography with Coding Theory*. Pearson Prentice Hall.



FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Gretzel Kattia Laura Brozozza

TURMA: CCL A33 RA N158930

CURSO: Ciéncia da Computacão

CAMPUS: Tatuapé

SEMESTRE: 2º TURNO: Matutino

CÓDIGO DA ATIVIDADE: 36 B.S.

SEMESTRE: 2^e semestre

AND GRADE: 2023

(1) Horas atribuídas de acordo com o regulamento das Atividades Práticas Supervisionadas do curso.

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:

Aprobado o Reprobado

NOTA:

DATA: / /

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO