UNIVERSIDADE PAULISTA - UNIP

Ciências da Computação

Augusto Schirrmeister Gatti - N607AC6

Erick Muniz - N6900H8

Felipe Viana Reis - F287041

Guilherme de Souza Gomes - F298990

Ismael Soares - N6249E6

Marcela Amorim - N621338

Murillo Mariano - N608722

Pedro Henrique Brito Alves - N577410

Rafael Lopes de Melo - N584BJ0

Thaís da Silva Cabral - N655CE1

ATIVIDADE PRÁTICA SUPERVISIONADA - APS

As técnicas criptográficas: conceitos, usos e aplicações

SÃO PAULO

2020

UNIVERSIDADE PAULISTA - UNIP

Ciências da Computação

ATIVIDADE PRÁTICA SUPERVISIONADA - APS

Impactos sócio-ambientais do 'Fast Fashion'

Trabalho apresentado no curso de Ciências da Computação da Universidade Paulista - UNIP, como parte das exigências para conclusão do semestre e obtenção de nota.

SÃO PAULO

2020

A necessidade é a mãe da inovação.

- Platão

SUMÁRIO

1. Objetivo do trabalho

Desde os primórdios da escrita, a criptografia vem se mostrando necessária. A partir do momento que a sociedade começou a escrever, o desejo de ocultar e mascarar seus textos surgiu, para que assim nem todos fossem capazes de compreender o conteúdo escrito.

Com o progressivo crescimento do uso da internet nos últimos anos, a criptografia tem se mostrado ainda mais fundamental e primordial nos meios de comunicação e informação, já que existe uma constante troca de dados entre servidores e usuários, dados estes que incluem informações pessoais e sigilosas.

Assim surge a criptografia, com o objetivo de transformar uma mensagem em um texto totalmente codificado, impedindo a fácil leitura e garantindo a troca segura de informações confidenciais.

Neste trabalho, iremos pesquisar e dissertar sobre os conceitos desta área da criptologia, a fim de entender seus conceitos, usos e aplicações, além de elaborar um programa desenvolvido na linguagem Python, que deverá criptografar frases completas (até 128 caracteres) e também realizar a sua respectiva descriptografia.

Para a realização da pesquisa bibliográfica, fomos inspirados por exímios estudiosos e peritos especialistas que já expuseram as maiores vantagens e desvantagens deste grandioso tipo de codificação, bem como suas instabilidades e aplicabilidades.

2. Introdução

Estudos apontam que a origem da palavra “criptografia” é grega, sendo o resultado da união de duas palavras: “Kryptós”, que significa “oculto” ou “secreto”, e “Gráphein”, que significa “escrever”. Sendo assim, o significado literal da palavra torna-se “escrita oculta” ou também “escrita secreta”.

A séculos atrás surgia a criptografia, com o exclusivo propósito de esconder e preservar textos, os quais autores gostariam de ocultar de leitores indesejados. Porém atualmente a criptografia vai muito além disso.

Na criptografia moderna, o propósito de confidencializar o conteúdo de textos ainda permanece, mas com o acréscimo de preservar e assegurar a autenticidade, integridade e disponibilidade destes, se tornando assim um dos principais tópicos abordados em estudos sobre a segurança da informação.

Basicamente, é um sistema de privacidade e segurança que torna textos, imagens ou vídeos incompreensíveis para quem não tem os códigos de tradução à sua disponibilidade.

A criptografia é executada pelos intitulados “algoritmos criptográficos”, que especificam quais serão as ações que irão provocar a alteração dos bits originais. Para isso ser possível, além de ser preciso escolher o uso de uma determinada técnica criptográfica (serão comentadas mais adiante), também é fundamental o uso das denominadas “chaves criptográficas”, pois sem elas é impossível criptografar ou descriptografar o texto/imagem/vídeo em questão.

Daí vem o nome “chave”, que faz alusão às que usamos cotidianamente para trancar e destrancar fechaduras, sendo estas as únicas ferramentas capazes de concluir esta ação.

Veja bem: para cada fechadura existe uma chave exclusivamente correta. Ao tentar destrancar uma porta com a chave incorreta, a fechadura não será preenchida, impossibilitando concluir a ação de “girar a chave” e ter acesso ao que está por

detrás da porta. O mesmo se aplica à criptografia. Sem a chave correta, ninguém terá acesso à “tradução” dos textos criptografados.

Em resumo, as chaves criptográficas são uma cadeia de bits de valor fixo usados para “preencher” o algoritmo, com a finalidade de conduzi-lo no desenvolvimento do processo de encriptação e decriptação.

São dois os principais tipos de chaves criptográficas estudados: simétricas e assimétricas.

A chave simétrica também é popularmente chamada de “criptografia de chave única”. Esta categoria da criptografia lida com apenas uma cadeia de bits - ou conjunto de algoritmos - que são encarregados tanto por encriptar, quanto por decriptar os dados em questão. Resumindo, este método se baseia em dois elementos: um único algoritmo e uma única chave de segurança, que trabalham em conjunto.

Neste modelo de criptografia, a confiança entre locutor e destinatário deve ser mútua e total, tendo em vista que ambos compartilham da mesma chave. Mas é sempre bom lembrar que caso a chave esteja comprometida, é só trocá-la por uma nova, preservando o algoritmo original.

A chave assimétrica já é o total oposto. Esta também é conhecida como “criptografia de chave pública”. Este método é composto por duas chaves: uma pública, que tem o objetivo de codificar, e outra privada, que tem o objetivo de descodificar.

Neste método, qualquer pessoa que precisar enviar algo à alguém precisa apenas ter acesso à chave pública, mas somente quem tem acesso à chave privada pode descriptografar/decifrar o algoritmo. Sendo assim, na criptografia de chave pública, é não apenas essencial, mas primordial manter em segredo o código da chave privada.

Ao contrário da criptografia de chave única, no sistema de criptografia de chave pública, as chances da chave ser comprometida reduzem significativamente, já que o número de pessoas com acesso à chave privada é restrito.

3. Criptografia - Conceitos Gerais

A criptografia é uma ciência de escrever códigos e cifras tendo o objetivo de proporcionar uma comunicação segura, sendo ela um dos elementos mais importantes para a criação das criptomoedas e das blockchains modernas.

Na maioria das civilizações antigas parece ter sido usado algum nível de criptografia. A substituição de símbolos é a forma mais básica de criptografia e ela apareceu em antigos escritos egípcios e mesopotâmicos. Sendo o mais antigo exemplo conhecido desse tipo de criptografia usado no túmulo de um nobre egípcio chamado Khnumhotep II, que viveu há aproximadamente 3.900 anos.

O objetivo desse tipo de criptografia na inscrição de Khnumhotep não era ocultar informações, mas sim aperfeiçoar seu apelo linguístico. O exemplo mais antigo conhecido usado para proteger informações ocorreu por volta de 3.500 anos atrás, quando um escriba da Mesopotâmia usou a criptografia para esconder uma fórmula de esmalte de cerâmica, usado em tabuletas de argila.

Depois da antiguidade, a criptografia foi muito usada para proteger informações militares importantes, servindo até hoje para isto. Na cidade-estado grega de Esparta, as mensagens eram encriptadas, sendo escritas em pergaminhos colocados sobre um cilindro de tamanho específico. Ela só era decifrada quando colocada dentro de um cilindro de tamanho semelhante pelo destinatário. De forma semelhante, espiões da antiga Índia usaram mensagens codificadas no século II a.C.

Muito provavelmente, a criptografia mais avançada do mundo antigo tenha sido feita pelos romanos. Um exemplo que se destaca seria a cifra de César que envolvia a substituição das letras de uma mensagem por outras letras que se encontravam algumas posições abaixo na sequência do alfabeto latino.

Durante a Idade Média, a criptografia tornou-se cada vez mais importante, mas a cifras de substituição permaneceram como padrão. A criptoanálise começou a

alcançar a ainda relativamente recente ciência da criptografia. Sendo Al-Kindi, um matemático árabe que desenvolveu por volta de 800 d.C, uma técnica conhecida como análise de frequência, tornando as cifras de substituição vulneráveis à decodificação.

Em 1465, Leone Alberti desenvolveu a cifra polialfabética, que é considerada a solução contra a técnica de análise de frequência de Al-Kindi. Na cifra polialfabética, uma mensagem é codificada usando dois alfabetos diferentes. Sendo m o alfabeto na qual a mensagem original é escrita, enquanto o segundo, é um alfabeto totalmente diferente, no qual a mensagem aparece depois de ser codificada. Fazendo a combinação com as cifras de substituição tradicionais, as cifras polialfabéticas aumentaram muito a segurança de informações codificadas.

Novos métodos de codificação da informação também foram desenvolvidos no período da Renascença, incluindo um popular método antigo de codificação binária, desenvolvido pelo filósofo e cientista Sir Francis Bacon, em 1623.

Um grande avanço na criptografia foi descrito, embora talvez nunca construído, por Thomas Jefferson na década de 1790. Sua invenção, chamada de roda cifrada, consistia de 36 anéis de letras em rodas móveis que podiam ser usados para obter uma codificação complexa. Esse conceito serviu como base para a criptografia militar americana até a Segunda Guerra Mundial.

A Segunda Guerra Mundial também viu o exemplo perfeito da criptografia analógica, conhecido como a máquina Enigma. De maneira semelhante a roda cifrada, esse dispositivo, empregado pelas Potências do Eixo, usava anéis rotativos para codificar uma mensagem, tornando praticamente impossível ler a mensagem sem outra máquina Enigma. A tecnologia da computação foi eventualmente usada para ajudar a quebrar a cifra Enigma, e a decodificação bem sucedida de mensagens Enigma ainda é considerada um elemento crítico da eventual vitória dos Aliados.

Com a ascensão dos computadores, a criptografia tornou-se muito mais avançada do que na era analógica. A criptografia matemática de 128 bits é muito mais forte

que qualquer cifra antiga ou medieval, sendo agora é o padrão para muitos dispositivos sensíveis e sistemas de computação. Começando em 1990, uma forma inteiramente nova de criptografia, chamada de criptografia quântica, estava em desenvolvimento por cientistas da computação, que procuravam, mais uma vez, elevar o nível de proteção oferecido pela criptografia moderna.

Recentemente, técnicas criptográficas também foram usadas para tornar as criptomoedas possíveis. As criptomoedas aproveitam várias técnicas criptográficas avançadas, incluindo funções hash, criptografia de chave pública e assinaturas digitais. Uma forma especializada de criptografia, conhecida como Algoritmo de Assinatura Digital de Curva Elíptica, sustenta o Bitcoin e os sistemas de outras criptomoedas como um meio de fornecer segurança a mais e garantir que os fundos só possam ser usados por seus legítimos proprietários.

3.1 Fundamentos

Todas as técnicas criptográficas procuram resolver um ou mais dos problemas clássicos da comunicação segura que são confidencialidade, autenticidade e Identificação.

Confidencialidade é o problema que estuda o controle do conhecimento da informação.

Autenticidade, estuda as circunstâncias em que itens de informação (documentos electrónicos, ordens de pagamento, registos numa base de dados, etc.) são autênticos no sentido em que existem garantias de integridade e têm perfeitamente identificado perfeitamente os seus titulares.

Identificação, estuda as relações de entidades (pessoas, organizações e sistemas de informação) entre si. O reconhecimento da identidade de um utilizador num sistema operativo é, provavelmente, a versão mais conhecida deste problema. No entanto, hoje em dia, com a crescente divulgação dos mais variados serviços através de meios electrónicos, a identificação de utilizadores legítimos desses serviços é um problema extremamente urgente. As técnicas de identificação podem

ter várias naturezas: podem ser baseadas em cifras ou em assinaturas digitais, mas podem também ser baseadas em funções de hash.

3.2 Conceitos

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los, desta forma ele não ficam nem o formato original. Os dados só podem ser decodificados ao formato original usando uma chave de descriptografia específica. As técnicas de codificação constituem uma parte importante da segurança dos dados.

3.3 Aplicações

As principais aplicações da criptografia no mundo moderno são as criptomoedas que usa a criptografia para proteção das negociações realizadas pela rede.

Outro dos principais usos são os pessoais e empresariais que podem ser utilizados para proteção de dados empresariais ou pessoais que estejam armazenados em computadores pessoais ou servidores.

Mais um seria a troca de informações, pois navegar e enviar informações pela rede, onde existe ataques constantes para interceptar dados que estão trafegando por ela. Então se estiverem criptografados o atacante não conseguirá decifrar. A VPN é muito utilizada para este objetivo.

Além desses, existe as áreas de segurança que pode ser determinada para criptografar automaticamente áreas específicas dentro do computador do usuário.

E também tem a assinatura digital de documentos, pois muitas empresas preferem utilizar documentos digitais e para isso a criptografia de dados pode ser utilizada para garantir a autenticidade dos documentos.

4. Técnicas criptográficas mais utilizadas e conhecidas

Usada desde a Segunda Guerra Mundial, a criptografia tem um papel muito importante para segurança e autenticidade de dados. Com o passar dos anos a tecnologia foi ganhando força e originou diversos tipos de criptografias. Veremos algumas técnicas mais utilizadas nos dias atuais.

4.1 DES (Data Encryption Standard) e 3EDES

Criado e implementado pelo IBM em 1977, o DES (*Data Encryption Standard)* é conhecido por ser uma proteção básica devido a seus poucos 65 bits que apenas possibilitam cerca de 16 ciclos de codificação o que torna essa técnica de nível básico por não oferecer uma segurança mais forte.

O DES somente realiza duas operações em sua entrada, essas são deslocamento de bits e substituição de bits. A chave controla todo o processo. Quanto feitas essas operações repetidamente de uma forma não contínua desencadeia um resultado que não pode ser revertido a forma original sem o uso da chave.

Ele pode ser decodificado pela técnica da força bruta, na qual o programa testa todas as possibilidades de chaves automaticamente causando um “loop” quase infinito que dura por várias horas. Em 1993 o NIST recertificou o DES pela última vez e passou a recomendar o 3DES, que é uma variação simples do DES que o utiliza em três ciframentos contínuos, podendo utilizar uma versão com duas ou com três chaves diferentes. Apesar de seguro, é um algoritmo que trabalha bem lentamente para se tornar padrão.

4.2 DESX

Consiste em uma outra variante do algoritmo DES e propõe uma solução e melhoria para o mesmo que aumenta de forma excepcionalmente a sua resistência contra ataques de força bruta sem abrir mão do seu método e não aumenta a complexidade do programa.

Antes de criptografar os dados, são adicionados mais 64 bits, aumentando a proteção para 120 bits contra força bruta.

4.3 AES

AES conhecida como Advanced Encryption Standard (Padrão Avançado de Criptografia) é o principal método de criptografia bastante utilizada no mundo pelas principais organizações mundiais como a Apple, Microsoft, NSA, dentre outras. A AES utiliza a chave simétrica, ou seja, usa a mesma chave para criptografar e descriptografar a mensagem.

Esse método, utiliza o algoritmo Cifra de bloco. É constituído por três cifras de blocos: AES-128, AES-192 e AES-256. Cada cifra criptografa e descriptografa os dados em blocos de 128 bits utilizando-se as chaves de 128, 192 e 256 bits. Em seu processo criptográfico, as chaves de 128 bits possuem 10 rodadas, as chaves de 192 bits têm 12 e para a as chaves de 256 bits são 14 rodadas. As rodadas correspondem às etapas de processamento, que incluem permutação e substituição do texto criptografado, que o transforma na sua forma criptografada.

Os recursos do AES são o que os coloca como principal método de criptografia avançada. Possui uma ótima segurança, pois pode resistir melhor aos ataques. O AES foi projetado para ser usado sem nenhum custo, royalties ou lucro. Por fim, o algoritmo possui facilidade em seu uso e uma boa flexibilidade quando implantados nos softwares e hardwares.

4.4 RSA

O RSA possui o método de criptografia assimétrica e utiliza duas chaves: uma pública e uma privada. É a técnica de chave pública mais utilizada e uma das mais poderosas formas de criptografia utilizadas no mundo contemporâneo. O RSA foi construído através de combinações matemáticas e se baseia nos números primos. O segredo por trás do RSA consiste na facilidade de multiplicar números primos a fim de encontrar um terceiro número.

A segurança desse método é baseada na dificuldade de fatorar números grandes e esse é um problema que leva muito tempo para ser descoberto. As chaves públicas e privadas são baseadas na multiplicação de dois números primos. O resultado desta operação é público, e se o número foi muito grande, fatora-lo para saber os primos poderia levar anos.

4.5 BLOWFISH

O blowfish foi desenvolvido como uma alternativa para mais rápida para os algoritmos existentes, possui sua licença gratuita e não é patenteado. Este algoritmo utiliza uma cifra simétrica e chaves de tamanho variável, ideais para aplicações domésticas ou comerciais.

A cifragem do texto é feita em blocos de 64 ou 128 bits, que são tratados separadamente em grupos de 32 bits. O blowfish consiste de duas partes: A expansão da chave e a criptografia dos dados.

4.6 IDEA

O International Data Encryption (IDEA) utiliza a chave simétrica que é utilizado por diversos governos internacionais visando proteger seus dados sigilosos. O IDEA opera com blocos de informações de 64 bits e usa chaves de 128 bits e é considerado um algoritmo de criptografia complexo. O seu funcionamento consiste no uso de funções matemáticas que manipulam a sequência dos caracteres. Ele usa grupos algébricos com operações embaralhadas e incluem multiplicações simples e álgebra avançada. Dessa forma, a IDEA consegue proteger os seus dados que trafega pela rede, visto a complexidade do código e a dificuldade para decifrá-lo.

4.7 SAFER (Secure and Faster Ecryption Routine)

Mais seguro (traduzindo para o portguês), o *SAFER*faz criptografias em blocos de 64 bits e por isso ficou mais conhecido como SAFER SK-64. Muitos especialistas encontram falhas nessa técnica o que resultou na criação de técnicas derivadas com o uso de chaves diferentes como SK- 40 e SK-128.

4.8 CAMELLIA

Desenvolvido em 2005, a técnica *Camellia* decifra blocos de informações. Pode ser processado em 128, 192 e 256 bits, muito semelhante ao AES.

Pode ser implementada tanto em softwares quanto hardwares. Também é compatível com tecnologias mais econômicas de 8 bits (smartcards, sistemas de operação em tempo real etc.) até com processadores mais potentes de 32 bits (desktop)

4.9 AES

Advanced Encryption Standard (AES) — ou Padrão de Criptografia Avançada, em português . É o algoritmo padrão utilizado nos Estados Unidos e por muitas outras organizações mundiais. Um algoritmo confiável seguro e funcional em seus 128 bits(mas também é acessivel para usar chaves maiores como 192 e 256 bits nos casos de processar informações maiores).

O AES resiste a todo tipo de ataque, mas seu ponto fraco é a força bruta que faz com que se crie um loop infinito ao tentar decifrar o código com a grande quantidade de bits que esta técnica tem o que é extremamente difícil nos dias de hoje.

4.10 RC2 (8 a 1024 bits)

Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor dos algoritmos RC4, RC5 e RC6.

4.11 CAST (128 bits)

É um algoritmo de cifra de bloco, sendo criado em 1996 por Carlisle Adams e Stafford Tavares. O CAST-128 é um algoritmo de Feistel, com 12 a 16 iterações da etapa principal, tamanho de bloco de 64 bits e chave de tamanho variável (40 a 128

bits, com acréscimos de 8 bits). Os 16 rounds de iteração são usados quando a chave tem comprimento maior que 80 bits.

5. Técnica criptográfica escolhida (ROT-13)

A técnica criptográfica escolhida é a ROT-13, a qual se trata de um procedimento simples e eficaz usado basicamente para garantir que textos eletrônicos não sejam lidos por distração ou acidente. Seu nome significa “ROTate by 13 places”, ou seja, “Rotacionar 13 posições”.

Seu nome é bastante descritivo, já que explica de forma geral o funcionamento desta técnica de criptografia. Ela se baseia em rotacionar cada caracter de uma mensagem 13 letras acima, seguindo a ordem do alfabeto latino básico (letras de A-Z, incluindo K, Y e W). Como há 26 letras no alfabeto, o ROT-13 é sua própria inversão, assim, para desfazer a codificação basta repetir a técnica em cima da mensagem criptografada. Em suma, o processo de codificação e decodificação é exatamente o mesmo, simplesmente aplicamos o mesmo procedimento uma segunda vez.

Em se tratando de termos técnicos, ROT-13 constitui uma cifra de César que utiliza apenas caracteres alfabéticos (da língua inglesa) e com passo 13. Comparando com um outro algoritmo menos popular, o ROT-47 gira todos os caracteres ASCII de códigos entre 33 (“!”) e 126 (“~”) e usa o passo 47.

Esclarecendo de forma geral do que se trata uma Cifra de César, é uma técnica de criptografia bastante simples e a mais conhecida de todas. É basicamente um tipo de cifra de substituição na qual as letras do texto a ser criptografado são substituídas por outra letra, também presente no alfabeto porém deslocada um certo número de posições à esquerda ou à direita.

O ROT-13 fornece nenhuma segurança criptográfica e é citado frequente e acertadamente como um exemplo de criptografia fraca, ou seja, não é seguro em

relação às informações codificadas, pois com apenas uma tabela simples de letras com posições invertidas, qualquer pessoa é capaz de codificar e decodificar o texto original.

Por ser um método bem simples de criptografia, o ROT-13 é aplicável em situações simples que não exigem grande codificação de dados. É mais utilizado para impedir que uma pessoa leia algo ofensivo em fóruns e grupos de discussão, ou ainda para impedir que por descuido alguém acabe lendo informações privadas. Também é útil para proteger endereços de correio eletrônico (evitando SPAM). Além disso, o método é aplicável apenas para quem deseja decodificar a informação de forma rápida e fácil.

Sendo assim, se há necessidade de manter arquivos seguros e informações autênticas, é recomendado utilizar criptografias fortes, como o SHA-256, ou até mesmo outras modalidades de SHA que são mais fracas, porém mais fortes que o ROT-13. No caso de informações que não podem ser lidas automaticamente, mas que não exigem tanta segurança, as criptografias simples como o ROT-13 são mais indicadas.

A grande vantagem da criptografia ROT-13 sobre as outras é seu fácil processo de reversão. Sendo assim, ao utilizar deste método, não devemos pensar em segurança, mas sim em uma forma de evitar uma leitura acidental indesejada. Esta técnica já foi aprimorada para a ROT-47, a qual inclui caracteres especiais como pontuação e acentuação.

Apesar da versão mais complexa, o ROT-13 é capaz de realizar seu papel de forma eficiente sem exigir muito do hardware, além de ser de fácil implementação tanto no processo de criptografia como no reverso em qualquer linguagem de programação.

6. Estrutura do programa

6.1 Descrição de funcionamento

O código que foi feito tem duas utilidades: tanto criptografar quanto descriptografar algo que o usuário deseja. Para isso se utiliza a biblioteca OS que é importada na primeira linha do código para que alguns processos possam ser realizados.

As primeiras linhas dão ao usuário a escolha de criptografar ou descriptografar o texto que será inserido pelo mesmo, e este bloco é formado por “print” e “input” para que o usuário possa informar a sua escolha.

Já no segundo bloco são criadas duas variáveis: a primeira para listar todo o alfabeto e a segunda é variável ROT com valor de 13 atribuído a ela, que vai servir na rotação de letras.

Caso criptografar seja a decisão feita, o programa irá pedir para que o texto a ser criptografado seja inserido. E com isso é criada uma variável “t” que a princípio é vazia. Logo após isso cada letra do texto que foi emitido pelo usuário é analisado pelo programa, letra por letra. Depois da análise feita é criada uma variável que armazena a posição no alfabeto de cada letra utilizada.

Agora a variável “t” que antes era vazia, recebe a nova posição da letra analisada, ou seja, ela será o resto da divisão da posição da letra, somada a variável ROT que tem 13 como valor atribuído. Lembrando que caso o que for escrito não estiver no alfabeto listado, ela será ignorada.

Depois desse processo o programa cria um arquivo no desktop chamado “criptografado” que será usado para armazenar o texto que usuário inseriu após ser criptografado, sendo assim, tudo que está na variável “t” - que é o resultado do programa - é escrito no .txt que foi criado.

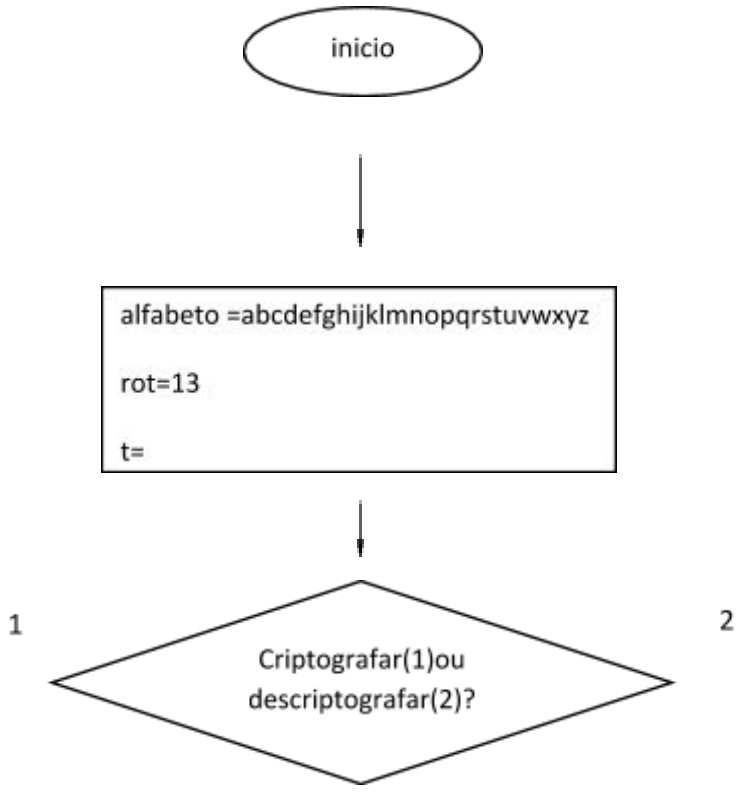
Se a opção for descriptografar o texto, o usuário terá mais duas opções: descriptografar o arquivo que foi criado ou escrever um texto para fazer tal ação.

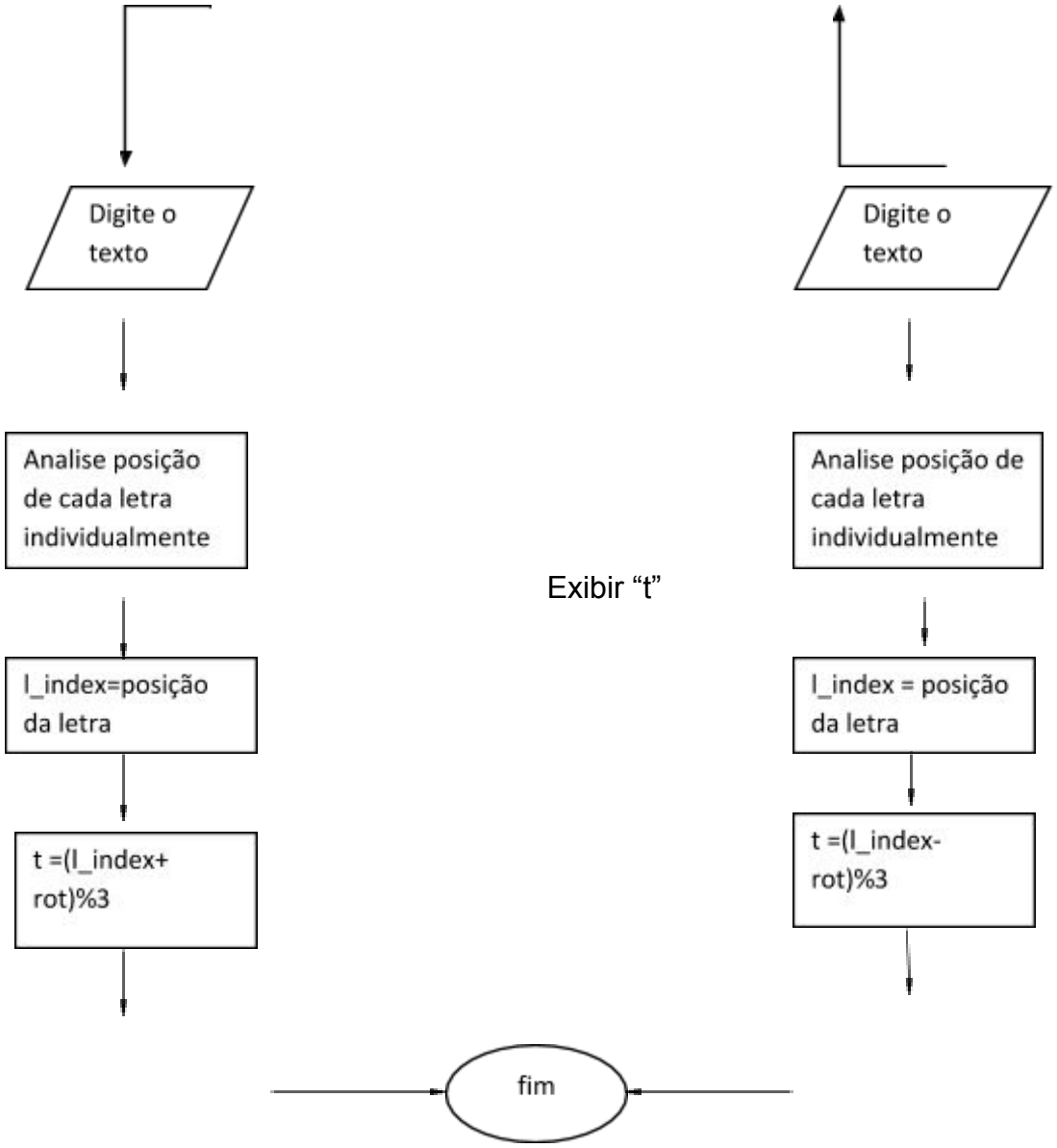
Caso a função escolhida tenha sido a do arquivo criado, o programa basicamente vai fazer o processo inverso da criptografia. No caso, o valor da variável “t” será a posição do alfabeto, subtraída a variável ROT.

Se o usuário optar por inserir um texto para ser descriptografado, assim como no primeiro processo, o programa vai pedir para que o usuário insira o texto, que vai ser analisado letra por letra, e mais uma vez se o texto possuir algo que não for nenhuma das letras que foram listadas, será ignorado, então será realizado o mesmo processo do arquivo do desktop e o texto descriptografado será exibido no terminal.

Como podemos ver, mesmo que o resultado do código apresentado seja bem interessante e útil, ele é bem simples e bastante funcional.

6.2 Fluxograma do código





O código, como já dito antes, é bem simples e pode ter algumas saídas, porém em alguns casos pode exibir algumas saídas padrão para determinadas situações.

Se o usuário inserir alguma opção inválida uma mensagem será exibida pois o programa pode não estar suportando aqueles dados, já não foram pedidos. Mas além dessas situações, o programa será executado normalmente fazendo assim o resultado esperado pelo usuário ser exibido.

7. Conclusões

A criptografia nos tempos atuais é uma ferramenta crucial da segurança da informação, existem diversas técnicas de criptografia, algumas de altíssima defesa e outras de baixa. A criptografia consiste basicamente em impedir que caso terceiros consigam interceptar as informações que estão sendo transmitidas, que dificulte sua interpretação de forma que apenas o destinatário e o remetente consigam interpretá-las.

Como vimos, a técnica de criptografia escolhida pelo grupo foi ROT-13, uma técnica de criptografia simples que não oferece um nível de segurança muito elevado que se baseia em substituir os caracteres do texto inserido por outro dentro do alfabeto, além de ser um sistema criptografia leve que não exige tanto do seu hardware.

Também existe o conceito das chaves criptográficas, que são uma série de bits de valor fixo usados para “preencher” o algoritmo, com a finalidade de conduzi-lo no desenvolvimento do processo de encriptação e decriptação. Existem dois principais tipos de chaves criptográficas: Chave simétrica e assimétrica.

A chave simétrica basicamente utiliza a série de bits para criptografar e descriptografar o conteúdo e a assimétrica utiliza uma série de bits para criptografar e outra para descriptografar.

Com os conceitos e técnicas abordadas foi elaborado então um programa simples de se usar, e ainda eficaz para os propósitos da criptografia ROT-13, permitindo uma rápida conversão entre os dados criptografados e os sem formatação, e vice-versa.

8. Bibliografia

https://academy.binance.com/pt/articles/history-of-cryptography

https://blog.rebel.com.br/criptografia-de-dados-saiba-quais-sao-suas-principais-aplicacoes-e-onde-usa-la/

http://www4.di.uminho.pt/~mac/9900/fc/Html/

https://www.kaspersky.com.br/resource-center/definitions/encryption

https://inova.globalweb.com.br/post/tipos-de-criptografia-descubra-as-mais-importantes-para-a-sua-empresa

https://blog.validcertificadora.com.br/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/

https://www.netinbag.com/pt/internet/what-is-idea-encryption.html

https://medium.com/@tarcisioma/algoritmo-de-criptografia-assim%C3%A9trica-rsa-c6254a3c7042

https://kryptazia.wordpress.com/criptografia/blowfish/

https://pt.wikipedia.org/wiki/ROT13

https://calculareconverter.com.br/rot13-decoder/

http://www.bosontreinamentos.com.br/seguranca/criptografia-cifra-de-cesar/#:~:text=A%20Cifra%20de%20C%C3%A9sar%20%C3%A9%20uma%20t%C3%A9cnica%20de,n%C3%BAmero%20de%20posi%C3%A7%C3%B5es%20%C3%A0%20esquerda%20ou%20%C3%A0%20direita

Fichas das Atividades Práticas Supervisionadas - APS

UNIP UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: MARCELA AMORIM TURMA: CC2P04 RA: N621338

CURSO: Ciência da Computação CAMPUS: Paulista SEMESTRE: 2º TURNO: Noturno

CÓDIGO DA ATIVIDADE: SEMESTRE: 2º ANO GRADE: 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:

Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Pedro Henrique Brito Alves TURMA: CC2Q04 RA: N57741-0

CURSO: Ciência da Computação CAMPUS: Paulista SEMESTRE: 2º TURNO: Noturno

CÓDIGO DA ATIVIDADE: SEMESTRE: 2º ANO GRADE: 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:
Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Felipe Viana Reis TURMA: CC2Q04 RA: F287041

CURSO: Ciência da Computação CAMPUS: Paulista SEMESTRE: 2º TURNO: Noturno

CÓDIGO DA ATIVIDADE: SEMESTRE: 2º ANO GRADE: 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:
Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIP
UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Guilherme de Souza Gomes **TURMA:** CC2Q04 **RA:** F29899-0

CURSO: Ciência da Computação **CAMPUS:** Paulista **SEMESTRE:** 2º **TURNO:** Noturno

CÓDIGO DA ATIVIDADE: **SEMESTRE:** 2º **ANO GRADE:** 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:
Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIP
UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Thaís da Silva Cabral **TURMA:** CC2P04 **RA:** N655CE1

CURSO: Ciência da Computação **CAMPUS:** Paulista **SEMESTRE:** 2º **TURNO:** Noturno

CÓDIGO DA ATIVIDADE: **SEMESTRE:** 2º **ANO GRADE:** 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:
Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIP
UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Ismael Soares Vilaça TURMA: CC2Q04 RA: N6249E6

CURSO: Ciência da Computação CAMPUS: Paulista SEMESTRE: 2º TURNO: Noturno

CÓDIGO DA ATIVIDADE: SEMESTRE: 2º ANO GRADE: 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:
Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIP
UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Murillo Giovanni Ferreira Mariano TURMA: RA:

CURSO: Ciência da Computação CAMPUS: Paulista SEMESTRE: 2º TURNO: Noturno

CÓDIGO DA ATIVIDADE: SEMESTRE: 2º ANO GRADE: 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:

AVALIAÇÃO:
Aprovado ou Reprovado

NOTA:

DATA:____/_____/_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

UNIP
UNIVERSIDADE PAULISTA

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Rafael Lopes de Melo TURMA: CC2P04 RA: N584BJ0

CURSO: Ciência da Computação CAMPUS: Paulista SEMESTRE: 2º TURNO: Noturno

CÓDIGO DA ATIVIDADE: SEMESTRE: 2º ANO GRADE: 2020

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
20/10/2020	Objetivo do trabalho		Marcela Amorim		
20/10/2020	Introdução		Marcela Amorim		
09/11/2020	Criptografia (conceitos gerais)		Pedro Henrique Brito Alves		
09/11/2020	Técnicas criptográficas mais utilizadas		Thais e Ismael		
07/11/2020	Técnica que utilizamos		Rafael Lopes de Melo		
10/11/2020	Estrutura do programa		Erick Muniz		
16/11/2020	Conclusões		Augusto, Felipe e guilherme		
01/09/2020	Criação do código		Murillo Mariano		

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

TOTAL DE HORAS ATRIBUÍDAS:_____

AVALIAÇÃO:_____
Aprovado ou Reprovado

NOTA:_____

DATA:____/_____/_____

_____
CARIMBO E ASSINATURA DO COORDENADOR DO CURSO