**UNIVERSIDADE PAULISTA**

**CIÊNCIA DA COMPUTAÇÃO**

**AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES**

**Brasília - DF 2020**

**UNIVERSIDADE PAULISTA**

**Igor Assis De Oliveira**

**RA: F2349C8**

**Jennifer Santos Oliveira**

**RA: F21EFB0**

**João Carlos Pereira Alves**

**RA: F251993**

**João Lucas De Souza Soares**

**RA: N622DH8**

**Thalison Hertel Mortagua**

**RA: N622HH7**

**Brasília - DF 2020**

**SUMÁRIO**

**OBJETIVO GERAL DO TRABALHO**..................................................................5

**OBJETIVO ESPECÍFICO**.........................................................................5

**INTRODUÇÃO**.....................................................................................................6

**CRIPTOGRAFIA (CONCEITOS GERAIS)**..........................................................7

**O QUE É CRIPTOGRAFIA?**......................................................................7

**QUAL SERIA A FUNÇÃO DA CRIPTOGRAFIA?**...................................8

**COMO UMA CRIPTOGRAFIA PROTEGE OS USUÁRIOS?**....................8

**BENEFÍCIOS EM RELAÇÃO ÀS TÉCNICAS ANTERIORES**.................8

**VULNERABILIDADE E FALHAS**..............................................................9

**CIFRA DE CÉSAR**.............................................................................................10

**ESTRUTURAÇÃO, FUNDAMENTOS E CONCEITOS**..........................10

**APLICAÇÃO UTILIXANDO DA CIFRA DE CÉSAR**..............................11

**Quadro de Trithemius**................................................................11

**CRIPTOGRAMA**.....................................................................................12

**Cifra de Vigenère**........................................................................13

**DISCUSSÃO COMPARATIVA**...............................................................14

**PROBLEMAS DA CIFRA DE CÉSAR**.....................................................14

**FORMAS DE APRIMORAR A CIFRA DE CÉSAR**................................14

**Permutação**.................................................................................14

**Índice**...........................................................................................14

**Criptografia**.................................................................................15

**Descriptografia**...........................................................................15

**APRESENTAÇÃO DO PROGRAMA**.................................................................16

**Intuito / Contexto**...................................................................................16

**Funcionalidades**....................................................................................16

**Entrada de dados**..................................................................................17

**Criptografando**......................................................................................17

**Descriptografando**......................................................................18

**BIBLIOGRAFIA**......................................................................................19

**OBJETIVO GERAL DO TRABALHO**

Pesquisar, analisar e dissertar sobre diversos aspectos das técnicas de criptografia, juntamente com a apresentação de um programa funcional de criptografia.

**OBJETIVO ESPECÍFICO**

Explorar diferentes formas de criptografias através de pesquisas pontuadas, desenvolver com maior veemência a Cifra de César demonstrando usos, aplicações, problemáticas e contextualização. Além disso, conciliar todos os conhecimentos adquiridos elaborando um programa.

**INTRODUÇÃO**

As cifras são mensagens com substituições de letras ou símbolos, elas são escritas de forma que fujam do padrão de entendimento comum. Muitos acham que a criptografia só passou a ser usada com a chegada dos computadores, mas a criptografia já é bastante antiga. Se tem registros que indicam que o início das mensagens cifradas se deu por volta dos anos 1000 a.C.

A primeira evidência do uso das cifras ou da criptografia foi encontrada na tumba do Knhumhotep II quefoi um grande chefe egípcio. Os egípcios usaram hieróglifos fora da ordem normal de utilização, na tumba.

A criptografia é bastante usada e as vezes o uso dela até se passa despercebido, como uma carta de amor com algumas palavras trocadas para que ninguém além do casal consiga entender o real significado ou irmãos que conversam por códigos para poderem armar alguma brincadeira ou pegadinha sem que sejam descobertos

Os hebreus usaram uma técnica de substituição monoalfabética e monogâmica, ou seja, eles podiam trocar cada letra da palavra por outra letra qualquer existente em seu alfabeto para proteger a mensagem.

O imperador romano Júlio César, criou uma técnica de criptografia para proteger as mensagens que circulavam no império. A técnica de criptografia de Júlio César passou a ser conhecida como “cifras de césar”. Essa técnica é bem simples, sua criptografia consiste em trocar uma letra pela letra seguinte.

**CRIPTOGRAFIA (CONCEITOS GERAIS)**

A história da criptografia começa há milhares de anos. Até décadas recentes, ela havia sido a história do que poderia ser chamado de criptografia clássica — isto é, de métodos de criptografia que usam caneta e papel, ou talvez auxílios mecânicos simples. No começo do século XX, a invenção de complexas máquinas mecânicas e eletromecânicas, tais como a máquina com rotores Enigma, providenciou meios mais sofisticados e eficientes de encriptação; e a posterior introdução da eletrônica e computação permitiu elaborar esquemas de ainda maior complexidade, muitos completamente inadequáveis ao papel e caneta.

**O QUE É CRIPTOGRAFIA?**

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

Na computação. A técnica usada são a de chaves as “chaves criptográficas”, trata-se de um conjunto de bit’s baseado em um algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave diferente e incompatível com a do emissor ela não conseguirá ter a informação.

A primeira técnica de criptografia usava apenas um algoritmo de decodificação, assim bastava o receptor de o algoritmo para decifrá-la, porém se um intruso conhecesse esse algoritmo poderia decifrar a informações caso capturasse os dados criptografados. Ainda existe outro problema imagine:

Se a pessoa “X” tivesse que enviar uma informação para a pessoa “Y”, e a pessoa “Z” tivesse que receber uma informação da pessoa “X”, mas a pessoa “Z” não pode saber a informação passada a pessoa “Y”, mas para a pessoa “Y” e a pessoa “Z” obterem a informação precisaria ter o algoritmo, assim teríamos que ter mais que um algoritmo.



**QUAL SERIA A FUNÇÃO DA CRIPTOGRAFIA?**

Trata de um conjunto de regras que mostra codificar a informação de forma que só o emissor e o receptor consigam decifrá-la. Para isso são feitas várias técnicas são usadas, e ao passar do tempo modificada e o surgimento de novas outras de maneira que fiquem mais seguras.

**COMO UMA CRIPTOGRAFIA PROTEGE OS USUÁRIOS?**

Em geral, você geralmente tem contato com a criptografia de dados quando precisa inserir informações de identificação pessoal em um formulário da Web. Sites financeiros, do governo, de escolas e de compras costumam criptografar seus dados para ajudar na proteção contra roubo e fraude.

O princípio geral de funcionamento da criptografia é o embaralhamento do conteúdo de uma mensagem ou de um arquivo. Esse desarranjo oculta os dados por meio da reorganização de informações a partir de um código. Nesse processo, o emissor e o receptor da informação criptografada dispõem de uma determinada chave, ou seja, a linguagem correta para decifrar o código usado na ocultação do dado.

Assim, a criptografia protege os dados dos usuários tornando essas informações ilegíveis a aqueles que não possuem o código correto para lê-las, além de evitarem a exploração por malware, ações que impedem que aconteçam roubos de arquivos e fraudes.

**BENEFÍCIOS EM RELAÇÃO ÀS TÉCNICAS ANTERIORES**

As técnicas anteriores utilizavam o mesmo método substituição, que é o método usado pelos hebreus, mas substituíam a primeira letra do alfabeto pela última, a segunda pela penúltima e assim sucessivamente invertendo o alfabeto por completo. E que a técnica de César era razoavelmente segura e melhor.

Uma das técnicas anteriores seria a cifra de Vigenère que se trata de uma versão simplificada de uma mais geral cifra de substituição poli alfabética. Para cifrar, é usada uma tabela de alfabetos que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição. As 26 linhas correspondem às 26 possíveis cifras de César. Uma palavra é escolhida como “palavra-chave”, e cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem.

**VULNERABILIDADE E FALHAS**

A principal vulnerabilidade desse método de criptografia consiste na possibilidade de desincriptação ao se analisar o padrão de frequência dos símbolos. Essa questão já havia sido avaliada antes mesmo da existência do primeiro computador.

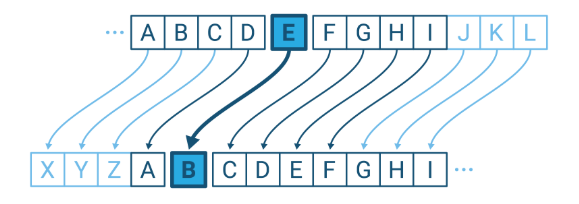
**CIFRA DE CÉSAR**

A Cifra de César é uma das mais fáceis e conhecidas técnicas de criptografia. Tratasse de um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto (26 Letras), porém transportada um certo número de posições à esquerda ou à direita.

O processo de criptografia de uma cifra de César é frequentemente incorporado como parte de esquemas mais complexos tendo aplicações modernas, como no sistema ROT13. Como todas as cifras de substituição monoalfabéticas, a cifra de César é facilmente decifrada e na prática não oferece essencialmente nenhuma segurança na comunicação.

**ESTRUTURAÇÃO, FUNDAMENTOS E CONCEITOS**

A cifra de substituição mais antiga que conhecemos, e o mais simples foi feito por Júlio César. A Cifra de César é a forma de criptografia mais conhecida no mundo, com propósitos militares, surgiu nas Guerras da Gália de Júlio César, e por este motivo ficou conhecida como Cifra de César. Ela basicamente substituía cada letra na mensagem por outra que estivesse três casas à frente. Mesmo com sua facilidade na época obteve muito sucesso, visto ser analfabeta a maioria dos inimigos do Império Romano, e os poucos que sabiam ler imaginavam que o texto estivesse escrito em outra língua.



Exemplificando a lógica deste método:

Em um texto criptografado com chave 3, o que corresponde o tamanho do intervalo de letras que serão puladas: ‘A’ se tornaria ‘D’, ‘B’ se tornaria ‘E’ e assim por diante. Chegando ao final do alfabeto, ele retornaria ao início, por exemplo, ‘Z’ se tornaria ‘C’.

A cifra de César usa o que chamamos de criptografia de chave simétrica, onde a mesma chave usada para criptografar o texto é usada também para descriptografar.

O algoritmo pode ser expresso da forma a seguir. Para cada letra em texto claro p, substitua-a pela letra do texto cifrado C2:

C = E (3, p) = (p + 3) mod 26

Um deslocamento pode ser de qualquer magnitude, de modo que o algoritmo de César é:

C = E (k, p) = (p + k) mod 26 (2.1)

Onde ‘k’ assume um valor no intervalo de 1 a 25. O algoritmo de decriptação é simplesmente:

p = D (k, C) = (C – k) mod 26

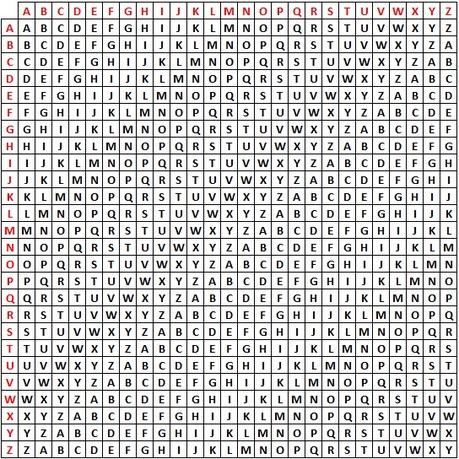
**APLICAÇÃO UTILIXANDO DA CIFRA DE CÉSAR**

**Quadro de Trithemius**

Os textos criptogrados com substituição monoalfabética se tornaram vulneráveis após AI-Kindi (figura proeminente na Casa da Sabedoria). Mesmo assim, perduraram por algum tempo pois a troca de informações era muita mais lenta nessa época. No século XV, Leon Battista Alberti utilizava um quadro composto por 26 linhas e 26 colunas contendo todas as letras do alfabeto, ficando conhecido como Quadro de Trithemius devido ao primeiro livro impresso sobre criptografia “Poligrafia em seis livros por João Trithemius”.

Jonathan Strickland explica que um estudioso chamado Johannes Trithemius, se propôs a colocar o alfabeto em uma matriz. A primeira linha continha o alfabeto normalmente escrito. A próxima linha usava uma cifra de César para mover o alfabeto sobre um espaço. Cada linha alterava o alfabeto em um outro ponto para que a linha final iniciasse com a letra ‘z’ e terminasse com a letra ‘y’. Qualquer pessoa poderia ler o alfabeto normalmente olhando para a primeira linha ou pela primeira coluna. Resultando assim:

**QUADRO DE TRITHEMIUS**



**CRIPTOGRAMA**

Jonathan Strickland explica que cada linha é uma cifra de César e que para criptografar uma letra, o criptógrafo escolhe uma linha e usa a primeira linha como guia do texto simples. Um criptógrafo usando a 10ª linha, por exemplo, codificaria a letra de texto simples ‘a’ como ‘j’. Strickland completa ainda falando que Trithemius sugeriu que os criptógrafos criptografassem suas mensagens usando a primeira linha para a primeira letra, a segunda linha para a segunda letra e assim por diante até o final do quadro. Após chegar ao final, o criptógrafo volta a primeira linha e segue a sequência até criptografar a mensagem toda.

O quadro de Trithemius é um bom exemplo de uma cifra poli alfabética. A maioria das cifras antigas eram monoalfabéticas, o que significa que um alfabeto em cifra substitui um alfabeto de texto simples. Uma cifra poli alfabética usa múltiplos alfabetos para substituir o texto simples. Apesar das mesmas palavras serem usadas em cada linha, as letras dessa linha têm um significado diferente. Um criptógrafo codifica um texto simples ‘a’ na linha três como um ‘c’, porém um ‘a’ na linha 23 é um ‘w’. O sistema de Trithemius, no entanto, usa 26 alfabetos, um para cada letra no alfabeto normal.

**Cifra de Vigenère**

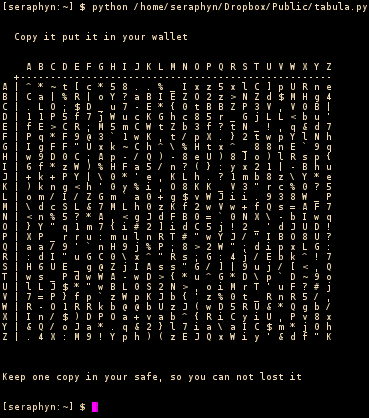
Este tipo de cifra de substituição inventada pelo criptógrafo francês do século XVI Blaise de Vigenère é usada para criptografia de dados em que a estrutura original do texto-planície é um pouco escondida no texto cifrado usando várias diferentes cifras de substituição monoalfabéticas em vez de apenas uma. Está cifra é constituída por 26 cifras de César, com diferentes variações. A diferença é que numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de lugares, enquanto na cifra de Vigenère consiste de várias cifras de César com diferentes valores de deslocamentos.

Esse método de criptografia foi descrito originalmente pelo criptologista italiano Giovan Battista Bellaso em um livro de 1553 de nome “La cifra del. Sig. Giovan Battista Bellaso”. Curiosamente, o método foi atribuído posteriormente – e de forma errônea – a Blaise de Vigenère no século XIX, e por isso é conhecida até os dias de hoje por “Cifra de Vigenère”.

A cifragem é realizada com o uso de uma tabela de alfabetos, denominada tabula recta, ou “quadrado de Vigenère”, que consiste no alfabeto escrito 26 vezes em linhas diferentes, cada um deslocado ciclicamente para a esquerda comparado com o alfabeto anterior, de forma a corresponder às 26 cifras de César possíveis. Durante o processo de criptografia, a cifra usa um alfabeto diferente de uma das linhas, e o alfabeto a ser utilizado em cada ponto depende da palavra-chave, que é repetida caso a mensagem a ser cifrada seja maior do que ela.

**TABULA RECTA**

**Programa em python demonstrando tabula recta**



**DISCUSSÃO COMPARATIVA**

É importante observar o contexto e época de criação da cifra de César para compará-la com outros métodos de criptografia. A cifra de César foi construída de forma extremamente simples comparando com as tecnologias atuais como Advanced Encryption Standard (AES). Entretanto em usos didáticos e para públicos que estão se introduzindo no grandioso mundo dos algoritmos, a cifra de César é um excelente meio para iniciar os estudos.

**PROBLEMAS DA CIFRA DE CÉSAR**

Dentre os problemas da cifra de César podemos listar, número limitado e pequeno de chaves, não permitir a autenticação, alta probabilidade de sofrer diversos tipos de criptoanálise e dificuldade de gerenciamento e transmissão de chaves

A cifra de César, portanto, é evidentemente bastante limitada em termos das capacidades de criptografia que pode oferecer. Na era e nos tempos de capacidades extraordinárias de computação, a cifra de César não vale a pena implementar como um esquema de criptografia, simplesmente não é segura. No entanto, a cifra de César ainda pode encontrar seu uso em algumas aplicações triviais, onde a cifra de César poderia ser empregada como um meio simples apenas para obscurecer o significado das mensagens.

**FORMAS DE APRIMORAR A CIFRA DE CÉSAR**

**Permutação**

Nesta abordagem, em vez de mudar as letras linearmente, eles são deslocados aleatoriamente usando a substituição e técnicas de caixa de permutação que são implementadas em técnicas modernas de criptografia como DES.

Então a caixa de substituição deve ser criada implementando a técnica de cifra affine (ou seja, Texto cifrado = (Texto Simples \* chave1) + chave2. Os caracteres são então substituídos por seus valores equivalentes referentes a caixa de substituição. Adicionando a funcionalidade de embaralhar o texto cifrado para esconder as características da linguagem usando técnicas de permutação. A permutação do texto cifrado é feita usando coluna dupla transposição no texto cifrado. O algoritmo proposto pode criptografar a gama de caracteres que a cifra césar não pode criptografar, ou seja, caracteres ASCII e ASCII estendidos.

**Índice**

Neste método, em primeiro lugar, o índice do alfabeto é verificado se o índice do alfabeto é mesmo, então, aumentar o valor por uma outra forma o índice é ímpar diminuir o valor-chave por um. Além disso, os caracteres do texto criptografado são mexidos de tal forma que se uma tentativa é feita para descriptografar o texto cifrado não seria fácil de decifrar.

Passo 1: Tome o texto simples como entrada.

Passo 2: Em primeiro lugar, o índice do alfabeto é verificado se o índice do alfabeto é mesmo, então aumenta-se o valor por mais um ou diminui-se a chave por menos um.

**Criptografia:**

C=E (P) = (P+1) se P for igual ou zero do que adicionar um

E (P) = (P-1) (mod 26) se p for ímpar do que subtrair um

**Descriptografia:**

P=D(C) =(C-1) se C for estranho que subtrair um

D(C) = (C+1) se P for igual ou zero do que adicionar

**APRESENTAÇÃO DO PROGRAMA**

**Intuito / Contexto:**

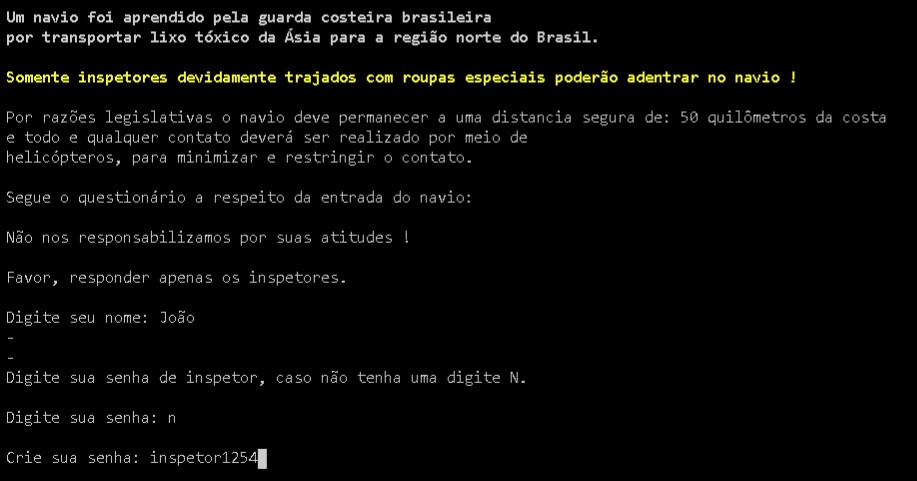
O programa foi desenvolvido no intuito de assegurar uma informação de um indivíduo. Como contexto utilizamos o cenário de um navio que transportava lixo tóxico.

Com base na história só poderia ter acesso ao navio se o tripulante fosse um inspetor, para entrar seria preciso criar uma senha, logo o programa iria guardá-la e em seguida criptografá-la para que o tripulante tivesse a segurança de suas informações.

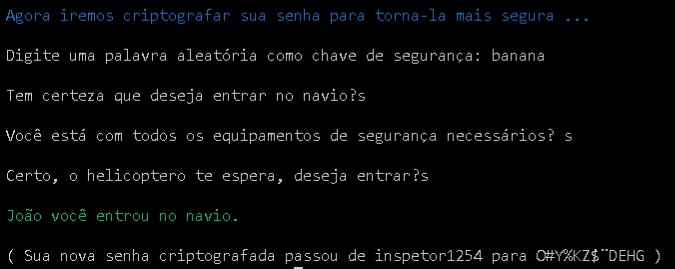
**Funcionalidades:**

Este programa pode ser usado para criptografar mensagens com x carácteres por meio da técnica de criptografia de César, ao executar o programa ele pedirá uma senha onde será feita a entrada de dados, e logo em seguida solicitará uma palavra chave para ser executado a criptografia. Ao final o programa retorna a senha que foi inserida e a mesma na versão criptografada.

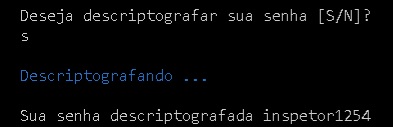
**Entrada de dados:**

****

**Criptografando:**

****

**Descriptografando:**

****

**BIBLIOGRAFIA**

Disponível em: <http://www.dsc.ufcg.edu.br/~pet/jornal/abril2014/materias/historia_da_computacao.html#:~:text=A%20hist%C3%B3ria%20da%20criptografia%20come%C3%A7a,letra%20do%20alfabeto%20pela%20%C3%BAltima>

* Acesso em: 20 de outubro de 2020.

Disponível em: <https://artsandculture.google.com/entity/khnumhotep-ii/m011vm2bg>

* Acesso em: 20 de outubro de 2020.

Disponível em: <https://www.kaspersky.com.br/blog/vigenere-cipher-history/5688/>

* Acesso em: 01 de novembro de 2020.

Disponível em: <https://www.passeidireto.com/arquivo/39716459/aps-2-semestre-ciencia-da-computacao-as-tecnicas-criptograficas-conceitos-usos-e>

* Acesso em: 01 de novembro de 2020.

Disponível em: <https://www.docusign.com.br/blog/criptografia-o-que-e-e-quando-ela-deve-ser-usada>

* Acesso em: 01 de novembro de 2020.

Disponível em: <https://www.passeidireto.com/arquivo/39716459/aps-2-semestre-ciencia-da-computacao-as-tecnicas-criptograficas-conceitos-usos-e>

* Acesso em: 01 de novembro de 2020.

Disponível em: <http://blog.mastermaq.com.br/criptografia-em-aplicativos/#:~:text=Como%20a%20criptografia%20protege%20os%20usu%C3%A1rios%3F,ser%20lidos%20por%20qualquer%20pessoa>

* Acesso em: 01 de novembro de 2020.

Disponível em: <http://visonet.com.br/2019/03/29/criptografia-e-seguranca-de-dados-como-funciona/>

* Acesso em: 01 de novembro de 2020.

Disponível em:

A.F., S., & R.M, M. (2018). *cryptograma.blogspot*. Fonte: cryptograma.

Araújo, E. J. (2018). Criptografia dos rudmentos á atualidade. p. 75.

Certificadora, V. (06 de 02 de 2019). *cryptoid*. Fonte: crypto id: https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/

Khandoker Abdul Rahad, Sayed Mohsin Reza . (01 de 2013). A Study on Network Security Services with Cryptography and an Implementation of Vigenere-Multiplicative Cipher.

Rosiane de Freitas, Karla Pereira, Larissa Pessoa e Ariel Bentes. (21 de 04 de 2018). Cifra de Cesar - Princípios de criptografia. p. 9.

Sant´Ana, A. A. (01 de 12 de 2014). Criptografia RSA.

Sarkar, S. (01 de 06 de 2020). Know about the Caesar Cipher. p. 4.

Simmons, G. J. (s.d.). *Britannica*. Fonte: https://www.britannica.com/topic/Vigenere-cipher

* Acesso em: 28 de Outubro de 2020.