RECAM
Revista Camalotes

ANALISANDO A FRAGILIDADE DE CÓDIGOS CIFRADOS POR CRIPTOANÁLISE: ESTUDO DE CASO COM O CÓDIGO DE CÉSAR

ANALYZING THE FRAGILITY OF CODES ENCRYPTED BY CRYPTOANALYSIS: A CASE STUDY WITH THE CAESAR CODE

ANALIZANDO LA FRAGILIDAD DE LOS CÓDIGOS CIFRADOS MEDIANTE CRIPTOANÁLISIS: ESTUDIO DE CASO CON EL CÓDIGO DE CÉSAR

Lucas Almeida Tiburtino da Silva[1]

Ederson Roberto da Costa[2]

Gabriela Espinoza de Souza[3]

Bárbara Marcheti Fiorin[4]

RESUMO: A criptoanálise, a arte de descobrir mensagens em textos cifrados, amplamente utilizada em cibersegurança. Portanto, o estudo da quebra de cifra simples é importante para o desenvolvimento pedagógico. O não-estudo da quebra de cifras poderá causar brechas de segurança e falta de proteção, facilitando no acesso indevido das informações. Esta obra foi elaborada em Campo Grande, Mato Grosso do Sul, na graduação do curso de Análise e Desenvolvimento de Sistemas. O objetivo deste artigo é alertar sobre os possíveis riscos do uso de cifras simples, auxiliar o leitor a entender sobre as estratégias atuais que dificultam a descriptografia e propor o desenvolvimento de um algoritmo básico capaz de realizar o processo de criptoanálise desvendando de forma parcial ou completa um texto cifrado. A metodologia foi elaborada com pesquisas na base de dados científicos oficial do Google Acadêmico, buscando por bibliografias e demais artigos, fazendo o uso de leitura objetiva aos temas referentes a criptografia e descriptografia de cifras simples, estudo do código de César, análise de digramas e trigramas cifrados. Os resultados apontam que é possível descriptografar um texto de

[1] Lucas Almeida Tiburtino da Silva é estudante do curso de Análise e Desenvolvimento de Sistemas do Instituto Avançado de Ensino Superior e Desenvolvimento Humano – INSTED. E-mail: lucas.almida.da.silva@gmail.com. ORCID iD: https://orcid.org/0000-0001-7347-810X.

[2] Ederson Roberto da Costa é professor do Instituto Avançado de Ensino Superior e Desenvolvimento Humano – INSTED. E-mail: edersondacosta@hotmail.com. ORCID iD: https://orcid.org/0009-0009-5617-4644

[3] Gabriela Espinoza de Souza é estudante do curso de Análise e Desenvolvimento de Sistemas do Instituto Avançado de Ensino Superior e Desenvolvimento Humano – INSTED. E-mail: ge7384005@gmail.com. ORCID iD: https://orcid.org/0009-0004-8653-6363

[4] Bárbara Marcheti Fiorin é estudante do curso de Análise e Desenvolvimento de Sistemas do Instituto Avançado de Ensino Superior e Desenvolvimento Humano – INSTED. E-mail: bmarchetifiorin@gmail.com. ORCID iD: https://orcid.org/0000-0002-5916-9375

cifra simples no código de César, revelando a fragilidade que o uso do código de César poderá trazer na atualidade.

PALAVRAS-CHAVE: Cibersegurança. Análise. Criptoanálise. Código de César, Descriptografia.

ABSTRACT: Cryptanalysis is the art of discovering messages in ciphertexts, widely used in cybersecurity. Therefore, the study of simple cipher breaking is important for pedagogical development. Failure to study cipher breaking may cause security breaches and lack of protection, facilitating improper access to information. This work was elaborated in Campo Grande, Mato Grosso do Sul, in the graduation of Systems Analysis and Development. The purpose of this article is to warn about the possible risks of using simple ciphers, help the reader to understand current strategies that make decryption difficult, and propose the development of a basic algorithm capable of carrying out the cryptanalysis process, partially revealing or completes a ciphertext. The methodology was elaborated with searches in the official scientific database of Google Scholar, searching for bibliographies and other articles, making use of objective reading of themes related to encryption and decryption of simple ciphers, study of César's code, frequency analysis of simple figures. The results indicate that it is possible to decrypt a simple cipher text in César's code, revealing the fragility that the use of César's code can bring nowadays.

KEYWORDS: Cybersecurity. Analysis. Cryptanalysis. Caesar's Code, Decryption.

RESUMEN: El criptoanálisis es el arte de descubrir mensajes en textos cifrados, muy utilizado en ciberseguridad. Por tanto, el estudio de la descifración de cifrados simples es importante para el desarrollo pedagógico. No estudiar la descifración de cifrados puede provocar violaciones de seguridad y falta de protección, lo que facilita el acceso inadecuado a la información. Este trabajo fue elaborado en Campo Grande, Mato Grosso do Sul, en la graduación de Análisis y Desarrollo de Sistemas. El objetivo de este artículo es advertir sobre los posibles riesgos del uso de cifrados simples, ayudar al lector a comprender las estrategias actuales que dificultan el descifrado y proponer el desarrollo de un algoritmo básico capaz de llevar a cabo el proceso de criptoanálisis descifrando parcialmente o completamente un texto cifrado. La metodología se desarrolló con investigación en la base de datos científica oficial Google Scholar, búsqueda de bibliografías y otros artículos, utilizando lectura objetiva sobre temas relacionados con cifrado y descifrado de cifras simples, estudio del código de César, análisis de frecuencia de cifras simples. Los resultados indican que es posible descifrar un texto cifrado simple en el código de César, revelando la fragilidad que puede traer el uso del código de César hoy en día.

PALABRAS CLAVE: La seguridad cibernética. Análisis. Criptoanálisis. Código de César, descifrado.

1 INTRODUÇÃO

Com o surgimento de uma das maiores tecnologias do mundo, a escrita, deu-se início a um novo modelo de transmissão de mensagens, histórias, artes, dentre outras formas de expor pensamentos no modelo textual.

> A escrita, com o passar do tempo, deixou de ser "protegida" apenas pela barreira linguística, e desde o surgimento, houve a necessidade da transmissão apenas para um seleto grupo de pessoas, motivando o estabelecimento de formas de proteção ao texto, baralhando as informações de forma coordenada ou utilizando outras técnicas que transformem a mensagem uma cifra, e se caso interceptada, tenha uma dificuldade no entendimento da informação por parte do interceptador (BAPTISTA, 2010).

A utilidade da criptografia, se estende aos dias atuais, sendo aplicado aos sistemas *WEBs*, comunicação entre computadores, transações financeiras, dados sensíveis, entre outras modalidades incríveis que necessitam de proteção, e, é de suma importância aplicar as técnicas de cifras nas informações.

Nesta obra, focaremos na técnica da cifra de César, um modelo simples que foi amplamente utilizado durante o Império Romano, com a finalidade de proteção de informações estratégicas militares. Embora a técnica não seja efetiva aos dias atuais, para a época, podia servir como uma boa forma de troca de mensagens. E para os dias atuais, servirá como uma boa didática por ser de fácil entendimento.

A importância de estudar a criptografia consiste no desenvolvimento matemático e do entendimento de como as técnicas são aplicadas e sobretudo, trabalhar a matemática de forma mais articulada com a realidade (PEREIRA et al., 2017). Além de estimular a adoção de métodos mais seguros de comunicação, armazenamento de informações, criação e o aprimoramento constante de aplicações que se baseiam nas técnicas mais recentes. E assim, construir soluções inovadoras e protegidas, contribuindo para um mundo digital mais seguro e confiável.

Portanto, a importância de estudar criptografia transcende a simples aquisição de conhecimento, impactando diretamente a maneira com a interação da tecnologia e a proteção de dados.

A metodologia foi elaborada utilizando pesquisas na base de dados científicos oficial do *Google* Acadêmico e demais artigos, utilizando leitura objetivada e pesquisas aos temas referentes à criptoanálise, criptografia e descriptografia de cifras simples, tipos e modelos de descriptografia de cifras simples, estudo do código de César, análise de digramas e trigramas cifrados

A linguagem de programação utilizada foi o *Python*, por ser simples de codificar e famosa pela estrutura matemática. Foram utilizados conceitos simples da linguagem, sendo assim, necessário apenas ter conhecimentos básicos de programação.

De tal modo, com a breve introdução, segue uma abordagem completa do referencial teórico onde serão abordados o objetivo e os questionamentos que serviram para a fundação desta obra.

2 REFERENCIAL TEÓRICO

O objetivo deste artigo é alertar sobre os possíveis riscos da utilização de cifras simples, como a utilização de códigos de César para desenvolvimento de sistemas, além de ajudar o leitor a compreender o processo de criptoanálise em códigos de César e recomendar o desenvolvimento de um algoritmo básico capaz de realizar o processo de criptoanálise, obtendo o resultado parcial ou totalmente descriptografado.

Para o desenvolvimento do objetivo, e de forma posterior, o desenvolvimento do algoritmo criptoanálise, necessitou-se encontrar respostas diante de dois questionamentos:

- Quais causas podem o ocorrer com a falta do estudo da quebra de cifras?
- Quais as possíveis soluções para as causas da falta de estudo?

Para esclarecer as dúvidas e melhorar a compreensão, foi elaborado um diagrama com as principais premissas obtidas por meio de pesquisas e conversas durante o planejamento.

2.1 Esclarecimento do objetivo

Foi elaborado um Diagrama de Objetivo Geral, buscando detalhar o processo de segurança de um sistema com base nos questionamentos, o diagrama é exibido na Figura 1.

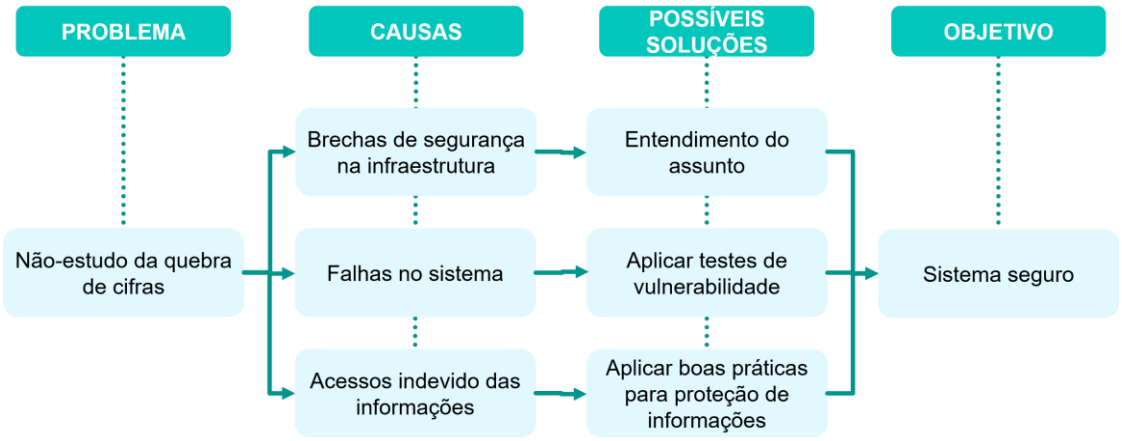

Figura 1 – Diagrama de Objetivo Geral (Figura do autor).

Conforme demonstrado na Figura 1 (Diagrama de Objetivo Geral), a coluna "objetivo" revela o esperado, porém, o foco serão as demais colunas. A coluna "problema" condiz com a problemática do artigo. A coluna "possíveis soluções" serve como explicação do segundo questionamento, com o detalhamento das possíveis soluções para cada causa.

A coluna "causas" aponta algumas das situações que poderiam ocorrer em uma implementação real desenvolvida usando baixo ou nenhum meio de segurança de criptografias, e, embora as situações sejam semelhantes, existe uma sutil diferença que devem ser levadas em consideração. Essa coluna serve como uma possível resposta à primeira pergunta.

A primeira ocorrência dessa coluna, destaca as brechas de segurança. Como o não uso criptografia, o sistema poderá ter brechas em informações de

suma importância, como senhas de usuários, logs do servidor e mensagens privadas. O não uso de protocolos criptografados também possibilita servir como uma "porta" para o invasor. Portanto, é importante a definição dos protocolos de rede das redes corporativos.

A segunda ressalva, acontecimentos internos, como engenharia social e ataques de força bruta, essas duas não necessitam de criptografia; o ideal seria a utilização massiva de testes de vulnerabilidade, a criptografia, poderá servir como aliada, para o impedimento de ocorrências como o acesso ao banco de senhas.

A terceira ocorrência, é um problema grave relacionado à falta de segurança de criptografia em sistemas. Quando não há criptografia adequada, informações sensíveis e confidenciais podem ser acessadas por pessoas não autorizadas. Isso pode incluir dados pessoais de usuários, informações financeiras e documentos sigilosos.

Conforme (VERNALHA, 2023) para evitar esses problemas, é fundamental implementar medidas de segurança e boas práticas de gestão de tecnologia, como criptografia de dados em repouso e em trânsito, políticas e procedimentos, treinamento de funcionários, autenticação robusta e controle de acesso adequado. Dessa forma, protege-se contra o acesso não autorizado e preservar a privacidade das informações.

2.2 Estudo da Criptografia de César

De acordo com (NASCIMENTO, SERTÃ, 2020) a criptografia de César utiliza como dinâmica o modelo de substituição – basta substituir um valor por outro. Seguindo a estrutura alfabética e tendo um valor n como deslocamento.

Nessa analogia, se tiver uma frase simples sem assentos definida, "hoje o dia esta quente", basta substituir as letras por outras de acordo com a posição do deslocamento. O exemplo "Krmh r gld hvwd txhqwh" obteve o deslocamento de três casas a esquerda do alfabeto, conforme a Figura 2.

Alfabeto	A	B	C	D	E	F	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Deslocamento	D	E	F	G	H	I	J	**K**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Frase													HOJE O DIA ESTA QUENTE													
Cifrado													KRMH R GLD HVWD TXHQWH													

Figura 2 – Exemplo de Código Cifrado de César Para a Esquerda (Figura do autor).

Conforme visto na Figura 2 e de acordo com (HOGER et al., 2022), fica evidente a facilidade na quebra do código, pois se o interceptor descobrir qual o valor de deslocamento, o restante da frase ficará comprometida. Uma forma simples de realizar essa descoberta é utilizando duas réguas com alfabeto, uma ficará estática enquanto a segunda será ajustada com as primeiras letras da frase, e assim por diante até descobrir por hipótese a primeira palavra. Ao deduzir a primeira palavra, obtém-se o valor de deslocamento comprometendo o restante da frase.

De acordo com (DE SOUSA, PIRES, 2018) existem outras formas de se obter o resultado do código cifrado, um modelo mais robusto é utilizar a análise de frequência de digramas e trigramas. Essa análise é utilizada em cifras mais complexas, limitada apenas ao poder computacional e ao desafio da cifra.

Logo, com o fechamento do referencial teórico, segue o desenvolvimento, com uma proposta de desenvolvimento de um algoritmo simples de criptoanálise do código de César.

3 DESENVOLVIMENTO

Com a compreensão do funcionamento da cifra de César, fica simples o desenvolvimento de um algoritmo. Entretanto, essa obra buscou na criptoanálise obter o resultado do deslocamento da cifra, deste modo, inicialmente, será revelado o método que realiza a cifra. A Figura 3, demonstra o fragmento do algoritmo desenvolvido na linguagem de programação *Python* que fará o deslocamento do alfabeto.

```python
alfabeto_original = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def deslocar_alfabeto(alfabeto, deslocamento):
    alfabeto_deslocado = []
    for letra in alfabeto:
        indice = (ord(letra) - ord('A') + deslocamento) % 26
        nova_letra = chr(ord('A') + indice)
        alfabeto_deslocado.append(nova_letra)
    return alfabeto_deslocado
```

Figura 3 – Função de deslocamento do alfabeto (Figura do autor).

O algoritmo da Figura 3 é uma função de deslocamento do alfabeto utilizada no código de César, é importante refletir que não consta letras com acento e caracteres especiais, portanto o código ficará limitado a frases simples ou escritas de modo errôneas. Das linhas três ao nove, contém a função de deslocamento do alfabeto. A função tem como valores de entrada o alfabeto (texto ou lista) e o valor de deslocamento (apenas valor inteiro), em seguida na linha cinco, realiza um laço de repetição *for* do alfabeto em que cada letra será deslocada no valor determinado, e por fim, é registrada na nova lista. Uma função complementar pode ser vista na Figura 4 para a realização da cifra.

```python
def deslocar_letras(frase, deslocamento):
    alfabeto_deslocado = deslocar_alfabeto(list(alfabeto_original), deslocamento)

    resultado = []

    for letra in frase:
        if letra.isalpha(): # Se a letra é realmente for uma letra faça isso...
            is_upper = letra.isupper() # a letra é maiúscula?
            letra = letra.upper()
            indice = alfabeto_original.index(letra)
            letra_deslocada = alfabeto_deslocado[indice]
            if not is_upper: # Se a letra é não é maiúscula, então faça ser minúscula
                letra_deslocada = letra_deslocada.lower()
            resultado.append(letra_deslocada)
        else: # Caso a letra realmente não seja uma letra então faça isso...
            resultado.append(letra)

    cifra = ''.join(resultado)
    return cifra
```

Figura 4 – Função de Deslocamento da Frase (Figura do autor).

A Figura 4 representa a função de deslocamento das letras da frase, essa função é mais complexa que a da Figura 3. Essa função é a responsável por realizar a cifra do código de César. Os valores de entrada são: frase (apenas texto) o e valor de deslocamento (apenas número inteiro). A função chama a função anterior, e em seguida na linha 16 realiza um laço de repetição na frase passando cada letra para a correspondente deslocada. Note que o uso de "*upper*" e "*lower*" servem para manter a originalidade da frase no sentido de letras maiúsculas e minúsculas (respectivamente).

A função revelada na Figura 5 recebe uma entrada "frase" (valor em texto do código cifrado). E em um laço de repetição integra sobre os números de zero até o valor total do comprimento da lista "alfabeto_original".

```
36  def recuperar(frase):
37      resultados = ""
38
39      for i in range(len(list(alfabeto_original))):
40          resultado = deslocar_letras(frase, -i)
41          resultados += (f'{resultado}, {i}\n')
42
43      return resultados
```

Figura 5 – Função de Recuperação da Cifra (Figura do autor).

Dentro do laço, é chamada a função "deslocar_letras" no sentido negativo "-i" pois, se antes o valor foi cifrado com no sentido esquerdo, agora terá o sentido contrário, entretanto, é esperado um resultado similar se aplicado no mesmo sentido de deslocamento.

Por fim, o resultado da função "deslocar_letras" é formatado e armazenado no campo "resultados" juntamente com o valor "i" de descolamento.

O laço de repetição fará com que a função continue testando diferentes deslocamentos. Ao encerrar os testes, será retornado em forma similar à de uma tabela com as colunas de resultado e valor de deslocamento. Note que em nenhum momento a função faz uso do valor de entrada do deslocamento, pois o conceito é descobrir o valor do deslocamento – simulando uma quebra de cifras.

Para poder usufruir dos resultados, há necessidade de chamar as funções e determinar um valor para ser cifrado. Conforme a Figura 6 revela, o valor de descolamento e a frase a ser cifrada foram as mesmas do exemplo anterior.

```
31    deslocamento = 3
32    frase = "Hoje o dia esta quente"
33    frase_deslocada = deslocar_letras(frase, deslocamento)
34    print(frase_deslocada)
```

Figura 6 – Controle para Cifrar Texto (Figura do autor).

Nesse ponto, encerra-se o tópico de desenvolvimento, onde foram implementados os conhecimentos da cifra de César. Passa-se para o tópico de resultados seguido das conclusões, onde serão abordados os valores obtidos, projetos futuros a finalização dessa obra.

RESULTADOS

Os resultados são satisfatórios, o valor cifrado é revelado na Figura 7. O resultado, idêntico ao valor cifrado manualmente.

```
Krmh r gld hvwd txhqwh
```

Figura 7 – Valor cifrado (Figura do autor).

O processo contrário de cifrar é revelado na Figura 8, sendo o sistema isolado do valor de deslocamento. O resultado lista as possíveis frases com os respectivos valores de deslocamento, conforme a formatação imposta na linha 41 da Figura 5.

```
Krmh r gld hvwd txhqwh, 0   Xezu e tyq uijq gkudju, 13
Jqlg q fkc guvc swgpvg, 1   Wdyt d sxp thip fjtcit, 14
Ipkf p ejb ftub rvfouf, 2   Vcxs c rwo sgho eisbhs, 15
Hoje o dia esta quente, 3   Ubwr b qvn rfgn dhragr, 16
Gnid n chz drsz ptdmsd, 4   Tavq a pum qefm cgqzfq, 17
Fmhc m bgy cqry osclrc, 5   Szup z otl pdel bfpyep, 18
Elgb l afx bpqx nrbkqb, 6   Ryto y nsk ocdk aeoxdo, 19
Dkfa k zew aopw mqajpa, 7   Qxsn x mrj nbcj zdnwcn, 20
Cjez j ydv znov lpzioz, 8   Pwrm w lqi mabi ycmvbm, 21
Bidy i xcu ymnu koyhny, 9   Ovql v kph lzah xblual, 22
Ahcx h wbt xlmt jnxgmx, 10  Nupk u jog kyzg waktzk, 23
Zgbw g vas wkls imwflw, 11  Mtoj t inf jxyf vzjsyj, 24
Yfav f uzr vjkr hlvekv, 12  Lsni s hme iwxe uyirxi, 25
```

Figura 8 – Possíveis resultados da cifra (Figura do autor).

Na figura, a frase destacada em azul, mostra que o algoritmo conseguiu encontrar a frase e o valor de deslocamento.

O destaque em azul, foi feito de forma manual, dependente de um usuário-operador para escolher o melhor resultado, portanto, isso será discutido no próximo tópico onde também será o fechamento desta obra. A visão completa do código encontrasse no Apêndice A.

CONCLUSÃO

Como trabalhos futuros, o primeiro passo seria melhorar o isolamento entre a função de criptoanálise e valor do alfabeto. Permitindo que o algoritmo consiga obter um valor aproximado da variável do alfabeto sem o uso da variável original.

Também, seria de grande interesse que o algoritmo conseguisse identificar a frase de forma correta sem haver necessidade do uso do laço de repetição e sem a interação humana.

Para promover a educação e a conscientização em segurança da informação, explorar a criação de recursos pedagógicos interativos ou jogos educacionais baseados na cifra de César pode ser uma abordagem valiosa. Um exemplo disso, seria o uso desse algoritmo para dinâmicas em grupo, onde o principal objetivo é descobrir os textos cifrados dos adversários.

A criptoanálise é uma disciplina importante para compreender e melhorar a segurança da informação. A investigação e o desenvolvimento contínuos nesta área têm potencial para contribuir significativamente para a proteção de dados e de sistemas. Portanto, buscar melhorias nos desafios criptoanalíticos e disseminar o conhecimento adquirido representa uma valiosa contribuição para a academia e para a segurança cibernética em geral.

REFERÊNCIAS BIBLIOGRÁFICAS

BAPTISTA, Gabriel. **Criptoanálise:** Trabalho de Final de Redes II. 2010. In: GTA UFRJ. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/gabriel/index.htm. Acesso em: 21 agosto 2023.

DE SOUSA, Deivison Porto; PIRES, Jandresson Dias. **CRIPTOANÁLISECOMOPROSPOSTA DIDÁTICA PARA O ENSINO DE ESTATÍSTICA**. 2018. In: Revista de Ensino de Ciências e Matemática. Disponível em: https://revistapos.cruzeirodosul.edu.br/index.php/rencima/article/view/1639. Acesso em: 23 agosto 2023.

HOGER, Mayara; AMADOR, Bruna; TURATO, Patricie; SANTOS, Lara; BERARDI, Rita; BIM, Silvia. **Desconstruindo Estereótipos em uma Oficina de Criptografia para Docentes da Educação Básica**. 2022. In: Anais do XVI Women in Information Technology. Disponível em: https://sol.sbc.org.br/index.php/wit/article/view/20872. Acesso em: 23 agosto 2023.

NASCIMENTO, Igor; SERTÃ, Christine. **Criptografia na educação básica**: das escritas ocultas ao código RSA. 2020. In: PMO SBM. Disponível em: https://www.editorarealize.com.br/editora/anais/conedu/2017/TRABALHO_EV073_MD1_SA13_ID6939_11092017150529.pdf. Acesso em: 21 agosto 2023.

PEREIRA, Naiara; FERREIRA, Francisca; PEREIRA, Maria; CORDEIRO, Reginaldo. **CRIPTOGRAFIA:** UMA FERRAMENTA DE ENSINO DAS OPERAÇÕES MATRICIAIS. 2017. In: editora realize. Disponível em: https://www.editorarealize.com.br/editora/anais/conedu/2017/TRABALHO_EV073_MD1_SA13_ID6939_11092017150529.pdf. Acesso em: 21 agosto 2023.

VERNALHA, Fabricio. **Privacidade de Dados e Segurança Cibernética na Gestão de Tecnologia**. 2023. In: Linkedin. Disponível em: https://www.linkedin.com/pulse/privacidade-de-dados-e-segurança-cibernética-na-gestão-vernalha. Acesso em: 21 agosto 2023.

APÊNDICE A – Código desenvolvido pelos autores.

```
'''
CRIPTOANÁLISE DE CÉSAR
DESENVOLVIDO EM 21/08/2023
ULTIMA ATUALIZAÇÃO: 07/09/2023
AUTORES:
    Lucas Almeida Tiburtino da
Silva    https://github.com/LucasATS
    Ederson Roberto da Costa
    Gabriela Espinoza de
Souza          https://github.com/Espinoza9
    Bárbara Marcheti
Fiorin             https://github.com/bamarcheti
'''
alfabeto_original = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def deslocar_alfabeto(alfabeto, deslocamento):
    alfabeto_deslocado = []
    for letra in alfabeto:
        indice = (ord(letra) - ord('A') +
deslocamento) % 26
        nova_letra = chr(ord('A') + indice)
        alfabeto_deslocado.append(nova_letra)
    return alfabeto_deslocado

def deslocar_letras(frase, deslocamento):
    alfabeto_deslocado = deslocar_alfabeto(
        list(alfabeto_original), deslocamento)
    resultado = []
    for letra in frase:
        if letra.isalpha():  # Se a letra é
realmente for uma letra faça isso...
            is_upper = letra.isupper()  # a
letra é maiúscula?
            letra = letra.upper()
            indice =
alfabeto_original.index(letra)
            letra_deslocada =
alfabeto_deslocado[indice]
            if not is_upper:  # Se a letra é não
é maiúscula, então faça ser minúscula
                letra_deslocada =
letra_deslocada.lower()
            resultado.append(letra_deslocada)
        else:  # Caso a letra realmente não
seja uma letra então faça isso...
            resultado.append(letra)
    cifra = ''.join(resultado)
    return cifra

deslocamento = 3
frase = "Hoje o dia esta quente"
frase_deslocada = deslocar_letras(frase,
deslocamento)
# print(frase_deslocada)

def recuperar(frase):
    resultados = ""
    for i in
range(len(list(alfabeto_original))):
        resultado = deslocar_letras(frase,
-i)
        resultados += (f'{resultado},
{i}\n')
    return resultados

frases = recuperar('Krmh r gld hvwd
txhqwh')
print(frases)
```