UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA - DCT
CURSO DE BACHARELADO EM CIÊNCIA E TECNOLOGIA

ANDERSON PICASSO LINHARES DA SILVA

A MATEMÁTICA COMO FERRAMENTA DE ESTUDO PARA A CRIPTOGRAFIA

CARAÚBAS
2019

ANDERSON PICASSO LINHARES DA SILVA

A MATEMÁTICA COMO FERRAMENTA DE ESTUDO PARA A CRIPTOGRAFIA

Monografia apresentada a Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Ciência e Tecnologia.

Orientador: Profa. Dra. Mariana de Brito Maia

Co-orientador: Prof. Me. Antônio Alisson Alencar Freitas

CARAÚBAS

2019

S586m Silva, Anderson Picasso Linhares da.
A matemática como ferramenta de estudo para a criptografia / Anderson Picasso Linhares da Silva. - 2019.
50 f. : il.

Orientadora: Mariana de Brito Maia.
Coorientador: Antônio Alisson Alencar Freitas.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de , 2019.

1. criptografia. 2. matemática. 3. cifras. I. Maia, Mariana de Brito, orient. II. Freitas, Antônio Alisson Alencar , co-orient. III. Título.

ANDERSON PICASSO LINHARES DA SILVA

A MATEMÁTICA COMO FERRAMENTA DE ESTUDO PARA A CRIPTOGRAFIA

Monografia apresentada a Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Ciência e Tecnologia.

Defendida em: 14 / 08 / 2019.

BANCA EXAMINADORA

Mariana de Brito Maia
Prof. Dra. Mariana de Brito Maia
Presidente

Antônio Alisson Alencar Freitas
Prof. Me. Antônio Alisson Alencar Freitas
Membro Examinador

Tony Kleverson Nogueira
Prof. Dr. Tony Kleverson Nogueira
Membro Examinador

Rosilda Sousa Santos
Prof. Dra. Rosilda Sousa Santos
Membro Examinador

Dedico este trabalho aos meus familiares

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, por toda força e disposição que este me proporcionou durante todo o curso.

Agradeço a minha família e amigos que sempre acreditaram em mim e me motivaram mesmo nos momentos mais difíceis. Agradeço ao meu pai Antônio Jorgivan da Silva, e em especial a minha mãe, Antônia Onézima Linhares, e a minha avó Maria Petronila Filha que sempre me forneceram os recursos necessários para que eu continuasse estudando, além de serem grandes exemplo para mim. Bem como a minha tia Maria Docarmo Cavalcante Costa pela hospitalidade, sendo esta quem me acolheu desde o momento em que decidi fazer o curso até os dias de hoje.

Agradeço aos meus colegas de curso por toda ajuda e aos meus amigos mais próximos por me auxiliarem nos desafios enfrentados até aqui, deixo aqui um agradecimento especial a minha melhor amiga Naila Nayane de Lima, por todo incentivo e por sempre acreditar em meu potencial, bem como pelo apoio mútuo e por todo o carinho que tem por mim.

Agradeço ao meu co-orientador Me. Antônio Alisson Alencar Freitas, que esteve presente desde a escolha do tema deste trabalho. Agradeço também a minha orientadora Dra. Mariana de Brito Maia, por toda paciência e disponibilidade.

“Não há empecilho que mate um talento, a não ser a preguiça”

Rashide

RESUMO

Tendo em vista a necessidade da segurança de dados, um conceito bastante presente nos dias atuais, faz-se necessário um estudo acerca desta área. Desta forma, para se entender algumas das formas como esta segurança é feita, é preciso entender sobre criptografia, que é o conjunto de técnicas que tem como objetivo garantir a segurança das informações enviadas e recebidas. O presente trabalho trata da criptografia de maneira prática buscando analisar algumas de suas formas e técnicas fazendo uso não apenas da teoria, mas dos cálculos que permeiam estes métodos para cifrar mensagens. Por meio de testes e estudos, este texto buscou entender o funcionamento da criptografia, expondo as formas como esta pode ser divida e trazendo junto a isso os conceitos básicos a respeito deste tema, para que só então, através de cálculos, pudéssemos encontrar formas para se romper as defesas dos métodos vistos e analisar de maneira qualitativa cada cifra. Por fim sugerimos as formas como cada método pode ser usado, unido os seus pontos fortes e fracos.

Palavras-chave: Criptografia. Cifra. Métodos. Segurança.

ABSTRACT

Considering the need for data security, being this concept very present nowadays, it is necessary a study about this area. Thus, to understand some of the ways this security is done, it is necessary to understand encryption, which is the set of techniques that aims to ensure the security of information sent and received. This research deals with cryptography in a practical way trying to analyze some of its forms and techniques using not only the theory but the calculations that permeate these methods to encrypt messages. Through tests and studies, this work aimed to understand the operation of cryptography, exposing the ways in which it can be divided and bringing together the basic concepts on this topic so that through calculations, we could find ways to break the defences of the methods seen and thus qualitatively analyze each cypher. Finally, we suggest ways in which each method can be used, together with its strengths and weaknesses.

Keywords: Encryption. Cypher. Methods. Security.

LISTA DE GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Desde a antiguidade o homem vive em sociedade, que com o passar do tempo foi se tornando mais complexa, a comunicação dentro de seu próprio grupo, ou entre grupos próximos foi sendo amplificada. Porém, nem toda informação tinha como intuito ser compartilhada, e essa necessidade de se comunicar sem que se revelasse o que estava sendo enviado é, talvez, o problema mais antigo da criptografia[1], sendo este problema relacionado com a necessidade de se ter uma comunicação segura, quando se comunica por vias inseguras. Para solucionar este problema, surgiu a criptografia, que apresentou-se de grande importância desde sua criação e se mantém como um dos pilares da segurança de dados até hoje.

Falar sobre a criptografia é falar sobre grande parte dos conflitos humanos, sendo estes, parte fundamental da história da humanidade, apresentando pontos de virada para as civilizações. Segurança exige proteger suas informações, informação é conhecimento, e conhecimento é poder. Em um conflito aquele que possui em mãos o maior número de informações acerca de seu adversário, possuirá vantagem sobre ele, sendo assim, possuir o conhecimento para proteger suas próprias informações, assim como possuir o entendimento sobre as defesas de seu inimigo, são pontos fundamentais. Estes são conceitos que a criptografia adota, seja na criação de um novo método, ou em testes e análise de um método já existente.

As técnicas podem ser variadas, sendo algumas mais simples, e outras mais complexas. Mas o objetivo principal é o mesmo, manter a confidencialidade do texto secreto. Esta ciência possui uma vasta quantidade de técnicas que variaram com o passar dos séculos. O caso mais antigo que se tem conhecimento é de 4000 anos atrás, no Egito, onde o uso de alguns hieróglifos fora do convencional impossibilitou a compreensão do texto escrito.

Um outro exemplo antigo é a cítala espartana, que consistia em um bastão de madeira e uma tira de couro ou papiro, e seu uso se limitava a escrever a mensagem na tira de couro, enquanto estava enrolada no bastão. A mensagem era então enviada a seu devido destinatário onde se enrolava a tira em um bastão de igual diâmetro ao que a mensagem foi originalmente escrita, e assim, se conseguindo ler a mensagem. Evidentemente, estes são apenas alguns dos vários exemplos do uso da criptografia encontrados ao longo da história antiga.

[1] Palavra que deriva dos termos grego kryptós que significa oculto, e graphien entendido como escrever

Um dos casos mais conhecidos sobre a criptografia é provavelmente o confronto entre a máquina alemã, enigma e as forças aliadas. Durante a segunda guerra mundial os alemães faziam uso de um dispositivo para criptografar mensagens. Esta máquina criada por Arthur Scherbius foi chamada de Enigma. E graças a sua invenção, os alemães tiveram durante muito tempo uma grande vantagem sobre as forças aliadas, pois estes, ainda que conseguissem obter informações, não conseguiriam entendê-las.

Graças a isso os aliados tiveram que montar uma equipe para analisar e quebrar a criptografia da Enigma, sendo um dos membros mais notáveis desta equipe o matemático Alan Turing. O fato da Enigma ter sido vencida contribuiu para que os alemães fossem vencidos, reforçando ainda a importância do estudo da criptografia, destacando que sempre que uma técnica de criptografia é quebrada, os resultados são catastróficos, além de deixar evidente que esta área precisa estar em crescente evolução, pois sempre que uma cifra é vencida, uma nova é criada com intuito de resolver as falhas da anterior.

A necessidade de aperfeiçoar as técnicas usadas e buscar técnicas mais complexas decorre de acordo com a necessidade de seu uso, já que com o avanço tecnológico, a necessidade da segurança de dados passou a ser cada vez mais evidente. A criptografia vem alterando a forma como é feita a ocultação da mensagem, pois à medida que o tempo passa, algumas técnicas tornam-se mais eficientes que outras, seja em decorrência da forma como a mensagem é “escondida”, ou pelos métodos que podem ser usados pelo invasor para reverter o processo e revelar a mensagem, de modo que a criptografia é uma constante batalha entre o algoritmo que garante a integridade da mensagem, e o invasor que tenta romper sua segurança buscando falhas em seu funcionamento.

Desta forma, sempre que a tecnologia avança, a criptografia precisa acompanhar esse avanço, para que, assim, a segurança das mensagens seja feita da forma mais eficiente possível. À medida que a computação evolua, a criptografia torna-se ainda mais presente no cotidiano das pessoas, fazendo-se necessário buscar técnicas ainda mais complexas para garantir que os dados dos usuários estejam seguros, tornando a criptografia imprescindível em uma época em que o fluxo de dados aumenta a cada dia, e suas formas de armazenamento e transferência são feitas, em sua maioria, de maneira online.

Visto que, atualmente, o ambiente virtual é responsável pela maior parte dos armazenamentos das informações, seria muito fácil romper a privacidade de uma pessoa caso não se tivesse uma defesa segura, por isso o estudo da criptografia vem evoluindo a cada dia,

buscando ser cada vez mais imprevisível, pois ainda que não se tenha um sistema criptográfico perfeito, deve-se ter em mente que é possível minimizar falhas, tornando-os cada vez mais impenetrável.

Disto isto, o presente trabalho tem por objetivo buscar promover um estudo a cerca dos métodos escolhidos, bem como mostrar a fundamentação matemática que regem o funcionamento dos mesmos. E ainda, entender o funcionamento, para que possamos executar um comparativo entre as cifras escolhidas.

2. REFERENCIAL TEÓRICO

De maneira simples define-se criptografia como um conjunto de técnicas que permitem aos seus usuários trocar informações de modo que a mensagem se mantenha oculta para terceiros. Ou ainda, como visto em Andrade; Silva (2009) "A criptografia trata de métodos e técnicas para transformar a mensagem em outra, de difícil compreensão, em que somente o seu destinatário legítimo possa decifrá-la, tendo assim acesso à mensagem inicial".

Colocando em termos mais formais, tem-se que a mensagem que se deseja cifrar é chamada de texto simples (ou plaintext), como visto em (TANENBAUM; WETHERALL, 2011), para que o texto simples seja transformado em um texto cifrado é preciso que a mensagem passe por uma função que variará de acordo com o tipo de cifra, como também é explicado. Os textos simples passam por uma função parametrizada por uma chave, o resultado deste processo é o texto cifrado (TANENBAUM; WETHERALL, 2011).

Para que se consiga criptografar a mensagem é preciso fazer uso de cifras, sendo essas as funções que transformam o texto simples em texto crifrado, ou texto cifrado em mensagem, "uma **cifra** é uma transformação de caractere por caractere ou bit por bit, sem levar em conta a estrutura linguística da mensagem." (TANENBAUM; WETHERALL, 2011, grifo do autor).

Outro ponto que merece destaque quando se estuda a criptografia é o principio de Kerckhoffs, que como é dito em Easttom (2016) a segurança de uma cifra depende apenas do segredo da chave e não do sigilo do algoritmo, isto é, um bom criptossistema se manterá seguro, ainda que um invasor conheça os princípios que regem o seu funcionamento, desde que este não tenha posse da chave.

Existe uma outra forma de se analisar o sentido do principio de Kerckhoffs, pode-se entender através deste que tornar pública uma determinada cifra é de extrema importância para garantir que a mesma seja segura. Tal conceito pode parecer contraditório, porém como visto em Easttom (2016), publicar um algoritmo tem como propósito fazer com que o algoritmo seja analisado, revisado e examinado por especialista da área, para que, só depois que sua segurança seja testada, o mesmo possa ser cogitado para uso.

Este conceito é complementado por Ferguson; Schneier; Kohno (2010), que diz que se o algoritmo se manter em segredo o atacante pode ser o primeiro a encontrar as falhas comprometendo assim a segurança.

A análise de criptossistemas é parte fundamental para ampliar a segurança das cifras e garantir seu funcionamento da forma devida, o que contribuí para a evolução da criptografia. Na antiguidade utilizavam-se processos empíricos para considerar uma cifra segura ou não, porém, com o passar do tempo, a criptografia passou a ser uma ciência, e faz uso de técnicas matemáticas para desenvolver criptossistemas, com objetivo de garantir a segurança das informações.

Como visto em Anjos (2016) “A criptografia estuda do ponto de vista matemático os métodos utilizados na proteção de uma informação digital. É considerada uma ciência com objetivo de escrever um texto de modo imperceptível pelo leitor (adversário)”.

2.1. TIPOS DE CIFRAS

Cifras são partes fundamentais da criptografia, sendo responsáveis pelo processo de “esconder” a informação. É através delas que os textos simples são convertidos em textos cifrados fazendo uso de uma ou mais chaves para executar esta conversão.

Para Guimarães (2001) cifra

> é o ato de transformar dados em alguma forma ilegível. A intenção é de garantir a privacidade, conservando a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados.

Como forma de facilitar o entendimento acerca do estudo da criptografia, pode-se dividir os criptossistemas de três formas, ou como dito por Stalings (2014), os sistemas criptográficos podem ser divididos de três formas, sendo estas: a forma como se altera o texto, o modo como o texto é processado e número de chaves usadas no processado.

Para o primeiro, que diz respeito a forma como se altera o texto, pode-se dividir as técnicas em dois grupos distintos, sendo estes de substituição ou de transposição. As técnicas ou cifras de substituição são aquelas em que se altera as letras da mensagem. Para Stalings (2014) na técnica de substituição as letras do texto são substituídas por outras letras, números ou símbolos.

As cifras de substituição podem ainda ser divididas entre as cifras de substituição monoalfabéticas, que usa uma substituição fixa, isto é, a letra do texto simples será sempre substituída da mesma forma, ou seja, utiliza-se um único alfabeto de cifra (PACHECO, 2014) e polialfabéticas, onde cifras utilizam diversos alfabetos de cifra; fazendo com que cada uma das letras possa ser substituída por diversas letras ou símbolos (FIARRESGA, 2010).

Já a de transposição, muda-se apenas a posição das letras, em Pacheco (2014) temos as cifras de substituição que baseia-se na troca dos caracteres, onde utiliza-se os mesmos em uma ordem diferente.

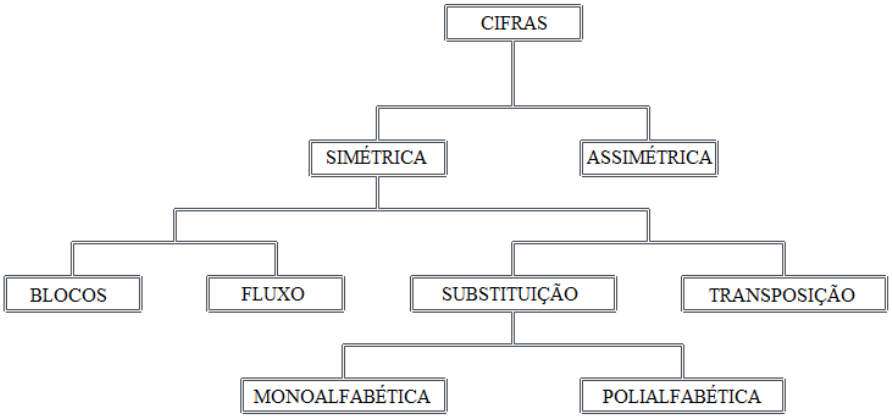
Quando divide-se as cifras com base na forma como o texto é processado, tem-se que as mesmas podem ser divididas em, cifra de fluxo ou de blocos, onde para o primeiro caso analisa-se cada caractere (ou bit) da mensagem unitariamente, retornado saídas respectivas para cada um, tratando este conceito computacionalmente pode-se tomar que cada bit recebido da mensagem é criptografado um a um, retornando um texto criptografado. Em Pellegrini (2018) tem-se que a cifra de fluxo "[...] transformam cada bit da mensagem em um bit do texto cifrado ao misturá-lo com um bit de outra fonte de bits [...]".

As cifras de blocos, como o próprio nome sugere, processa os dados da mensagem em bloco, que passarão por uma função para que sejam criptografados, que retornará blocos com a mensagem criptografada, ainda em Pellegrini (2018) é dito que as cifras de blocos "transformam sequências de bits de tamanho fixo, realizando nelas transformações difíceis de inverter", uma outra definição para as cifras de blocos é dada em Stalings (2014), onde é dito que este tipo de cifra processa a entrada como um bloco de elementos, e produz uma saída para cada entrada.

Por fim, se analisarmos as cifras com base em seu número de chaves, vemos então que as mesmas podem ser divididas entre cifras simétricas e assimétricas, sendo esta a definição adotada no presente trabalho, assim, tem-se que a cifra simétrica é tida como as cifras em que uma única chave é responsável por cifrar e decifrar a mensagem, já as assimétricas possuem conjunto de chaves publicas e privadas, que são responsáveis pelo processo de cifrar e decifrar, estes conceitos serão aprofundados ao longo de todo texto. De agora em diante vai-se focar na última classificação dada.

As divisões das cifras podem ser melhor entendidas no organograma abaixo:

Figura 1: Organograma das divisões de cifras



Fonte: Própria (2019)

2.1.1. Cifras simétricas

Os criptossistemas simétricos possuem apenas uma chave, como afirma Anjos (2016); "Nessa primeira técnica de criptografia, usa-se um sistema com chave secreta, e essa chave usada para fechar a informação, é a mesma para abri-la", devido a isso, tanto o emissor quanto o receptor da mensagem devem possuir a chave para que se comuniquem.

Esta é a forma mais simples de cifras, o principal problema deste tipo é a necessidade de que tanto o emissor quanto o receptor da mensagem devem possuir a chave e, se existir uma grande distância entre eles, a integridade da mensagem torna-se questionável.

2.1.1.1. Cifra de César

Como já mencionado neste texto, a criptografia é uma ferramenta bastante antiga que vem sendo empregada desde a antiguidade, como visto em Cozzens; Miller (2013) a mais de 2000 anos atrás os segredos militares do império romano se mantinham seguros através do uso da criptografia.

A cifra usada nesse processo é conhecida como cifra de César e foi de grande importância para o império romano, como visto em Oliveira (2005, p. 4)

> As cifras de substituição também foi o método criptográfico preferido de Júlio César. Em seu livro intitulado “Guerras Gaulesas”, ele conta como enviava mensagens substituindo as letras romanas por letras gregas, tornando a mensagem inteligível aos inimigos. (apud ANDRADE; SILVA, 2012)

Para que se tivesse essa segurança os romanos faziam uso de um cifra de substituição simples, onde cada letra do texto cifrado era trocada por outra localizada três posições à frente.

É preciso observar que a cifra de César é apenas um caso da cifra de deslocamento onde a chave escolhida neste caso é 3, partindo do pressuposto de que a cifra não será igual a mensagem original, a cifra de deslocamento pode possui até 25 chaves, sendo assim bastante limitada Cozzens; Miller (2013) afirmam que devido a isso um invasor só precisaria de máximo 25 tentativas para decifrar a mensagem.

2.1.1.2. Cifra afim

Como visto anteriormente a limitação de chaves da cifra de deslocamento, faz com que a cifra tenha uma segurança frágil, podendo ser quebrada em pouco tempo, fazendo uso de métodos simples, como o da força bruta (tentativa e erro), ou métodos um pouco mais específicos, como a análise de frequência. Assim é natural buscar sistemas mais complexos (COZZENS; MILLER, 2013).

Para chegar a funções mais complexas, parte-se da análise de que a função presente na cifra de César pode ser tomada como uma função afim $f(x) = ax + b$, onde **a** = 1, **b** = 3, e x é o valor correspondente as letras da mensagem.

Como visto em Cozzens; Miller (2013), isso é possível, pois a cifra de César é apenas um caso particular de uma cifra afim, deste modo tem-se uma nova forma de se obter a mensagem criptografada, aplicando os valores correspondeste as letras da mensagem na função afim. Partindo deste conceito e generalizando essa analise para caso em que **a** e **b** podem assumir valores quaisquer, obtém-se a cifra afim.

Contudo os valores de **a** devem ser escolhidos de modo que se atenda a seguinte condição, m.d.c.(a, 26) = 1. Como dito por Fiarresga (2010), está condição deve ser cumprida para que a função seja injetiva, sendo essa proposição de grande importância para o funcionamento da cifra, por dois motivos principais, o primeiro é que, se a função é injetiva isto garante que cada letra terá apenas um valor, evitado assim confusão no momento da leitura da mensagem. O segundo pelo mesmo motivo, garante-se que a função possui inversa, e através disso, é possível descriptografar a mensagem, pois sabendo que f(x) = ax + b = y, onde y é o texto cifrado, para reverter o processo e obter-se o valor da mensagem original, é bem simples, só é preciso por x em evidência na função vista anteriormente, e assim faz-se que x = (1/a)(y - b).

Visto que o valor para **a** possuem restrições devido a condição já mencionada, tem-se então que **a** pode assumir 12 valores todos cumprindo a condição dentro do intervalo de 1 a 26 sendo eles: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. Usado a informação sobre os possíveis valores para **a** é possível, então, calcular-se a quantidade de chaves para a cifra afim, como afirma Fiarresga (2010) está cifra possui 312 possíveis chaves, pois 12*26 = 312.

Sendo assim, ainda que apresente uma segurança mais estável que a de deslocamento, a cifra afim ainda poderia ser quebrada fazendo uso do método da força bruta devido a sua pequena quantidade de chaves, e como citado por Easttom (2016), assim como as demais cifras de substituição, a cifra afim também possuí o mesmo problema de preservar a frequência das letras, ainda que se altere o texto, preserva-se a frequência de letras, deste modo tornando-se vulnerável a análise de frequência.

2.1.1.3. Cifras de Vigenère

Tanto a cifra de deslocamento quanto a cifra afim por serem cifras monoalfabéticas e possuem problemas de segurança devido a sua limitada quantidade de chaves, bem como devido a análise de frequência. Buscando técnicas mais complexas que possam ampliar as possibilidades de chaves e reduzir a suscetibilidade de ataques por análise de frequência, inicia-se então a analise de uma cifra polialfabética, dentre elas a escolhida foi a cifra de Vigenère.

Criada pelo criptólogo francês Blaise de Vigenère, essa cifra baseia-se no mesmo principio da cifra de César, mas com deslocamento relacionado ao número de um caractere da chave escrito de maneira cíclica em baixo da mensagem (PACHECO, 2014), ainda que dito isto, é preciso ressaltar que nem todos atribuem a criação desta cifra a Vigenère, como pode-se observar ainda em Pacheco (2014) alguns afirmam que o verdadeiro criador deste método é o criptólogo italiano Giovan Battista Bellaso, no ano de 1553.

Pode-se ver essa segunda opinião a respeito da criação desta cifra em Easttom (2016) que é dito que a mesma foi descrita a primeira vez por Bellaso em 1553, ainda que seja mal atribuída a Vigenère no século XIX.

Este tipo de cifra é um grande avanço se comparado com as vista anteriormente, pois como explicado em Cozzens; Miller (2013) não se tem um único valor para a chave como a cifra de César, ou um par de valores como na cifra afim, para a cifra de Vigenère a chave pode ser uma palavr ou uma frase.

Sendo assim, dentro de uma chave têm-se um grupo de valores, para encriptar a mensagem, a forma de uso da mesma se dá da seguinte forma; primeiro escreve-se a chave escolhida embaixo da mensagem repetidamente (para o caso da chave ter um tamanho inferior a mensagem), em seguida soma-se os valores de ambos, usa-se o mod 26 no resultado para que se tenha valores que se possa converter em letras novamente. Este processo é explicado da seguinte forma em Stalings (2015); a primeira letra da chave é somada a primeira letra da mensagem, aplicando o mod 26, em seguida, a segunda letra de ambas são somadas, depois a terceira, e assim por diante, repete-se o processo até que toda a mensagem tenha sido criptografada.

Dito isto, pode-se analisar a cifra de Vigenère como uma cifra de César, em Easttom (2016) é dito que ambas as cifras podem ser vistas de forma semelhante diferindo em um ponto de extrema importância, a chave. Usando essa informação pode-se então chegar a conclusão de que para de retornar a mensagem original tendo em mãos a chave e o texto cifrado é simple. O que precisa ser feito é apenas escrever a chave embaixo do texto e subtrair os valores da chave do mesmo.

É notável a vantagem que esta cifra tem sobre as cifras de substituição monoalfabéticas, pois a quantidade de possíveis chaves que possui é muito superior, e estas podem variar de acordo com o tamanho da chave escolhida. Em Fiarresga (2010) é

apresentada a seguinte equação pra se obter o número de possíveis chaves $|K_m| = 26^m$, onde m é o número de letras da chave escolhida, sendo assim, pode-se ter valores muito superiores aos da cifra afim.

Devido ao fato de se ter valores diferentes para uma mesma letra, a análise de frequência de letras costuma falhar quando aplicada na cifra de Vegenère, em Stalings (2015) é dito que "A força dessa cifra é que existem múltiplas letras de texto cifrado para cada uma do texto claro, uma para cada letra exclusiva da palavra-chave. Assim, informações referentes à frequência de letra são ocultadas.".

2.1.2. Cifras assimétricas

Como mencionado acima cifras simétricas possuem problema quanto a distribuição da chave, pois para estas a chave é responsável por criptografar e descriptografar as mensagens. Se um invasor tiver acesso a chave, o conteúdo estará ameaçado, sendo assim, a distribuição de chaves é um ponto bastante problemático, pois "independentemente de quanto um sistema de criptografia fosse sólido, se um intruso conseguisse roubar a chave, o sistema acabava sendo inútil." (TANENBAUM; WETHERALL, 2011).

Tendo em vista isto, para solucionar o problema das chaves fez-se necessário formular um novo sistema. "Em 1976, dois pesquisadores da Universidade de Stanford, Diffie; Hellman (1976), propuseram um sistema de criptografia radicalmente novo no qual as chaves de criptografia e de descriptografia eram diferentes, e a chave de descriptografia não podia ser derivada da chave de criptografia." (TANENBAUM; WETHERALL, 2011).

Para este novo sistema a comunicação não é feita usando apenas uma chave, mas sim um par de chaves, em Easttom (2016) é dito que a chave que é usada para cifrar é diferente daquela que se usa para decifrar, mas ainda assim elas se relacionam entre si. Essas chaves são chamadas de chaves públicas e privadas, onde a chave pública é de conhecimento de todos, enquanto a privada é mantida por quem recebe a mensagem (GUIMARÃES, 2001).

A troca de informação se mantem em sigilo utilizando esse sistema de chaves múltiplas, onde o emissor da mensagem usa a chave pública do receptor para criptografar a

mensagem que será enviada, enquanto o receptor recebe a mensagem criptografada com sua chave publica, e em seguida utiliza sua chave privada para decifrar a mensagem recebida. Como complementado por Easttom (2016), para este tipo de sistema não importa se todas as pessoas possuem a chave pública, a segurança deste será mantida desde que a chave privada se mantenha secreta.

2.1.2.1. Criptossistema RSA

Um dos mais notáveis sistemas de chave pública é o RSA, sendo bastante consistente, como dito por Tanenbaum; Wetherall (2011) "Ele sobreviveu a todas as tentativas de rompimento por mais de um quarto de século e é considerado um algoritmo muito forte." Sendo ainda hoje bastante aplicável, como visto em Andrade; Silva (2012) "São diversas aplicações, como por exemplo, no software *Skype*". Pode ver a força deste algoritmo levando em conta o tempo que o mesmo vem sendo testado, sendo sua criação da década de 70. "O RSA foi desenvolvido no *Massachussets Institute of Technology* (MIT) em 1978 por Rom Rivest, Adi Shamir e Leonard Adleman, e batizado com as iniciais de seus nomes." (ANDRADE; SILVA, 2012, grifo do autor).

Já foi mencionado neste texto que as cifras assimétricas possuem chaves públicas e privadas, isto é, as funções responsáveis pelo processo de criptografar e descriptografar possuem chaves distintas, mas relacionadas. Esta relação pode ser vista nos equacionamentos que regem o funcionamento deste criptossistema, em Fiarresga (2010) é dito que "Esta cifra baseia-se na escolha de dois números primos e na aritmética modular." Sendo este um dos motivos que tornam o RSA tão forte, os conceitos matemáticos serão vistos mais a fundo posteriormente, contudo, apresenta-se neste tópico as funções usadas.

Matematicamente a função que criptografa o texto simples para o criptossistema RSA é a seguinte, $e = x^b$ (mod n), onde **b** e **n** são valores públicos, e x é o valor correspondente da mensagem. Para que se reverta o processo faz-se que $d = y^a$ (mod n), onde **a** é um valor privado, desta forma tem-se que, para enviar uma mensagem qualquer, aplicamos na primeira função os valores do texto simples, onde **b** e **n** serão fornecidos pelo destinatário, quando o mesmo a recebe, este usa a segunda função e reverte o processo de cifra da mensagem.

Nota-se que não é necessário que o emissor da mensagem possua o valor de **a**, assim como o fato dos valores de **b** e **n** serem conhecidos não torna possível que **a** seja descoberto de maneira simples.

Algumas condições devem ser cumpridas para que se tenha um funcionamento correto. A primeira delas é que **n** é resultado do produto de dois primos **p** e **q**, assim tem-se que n = pq, **p** e **q** são valores privados, ainda que **n** seja publico é extremamente difícil se calcular **p** e **q** partindo do valore de **n**, em Andrade; Silva (2012) é dito que "A segurança desse sistema se baseia na dificuldade de fatorar um número inteiro muito grande, pois muitas operações são envolvidas no processo".

É evidente que se o valor de **n** é pequeno essa dificuldade é reduzida, contudo, na prática os valores de **p** e **q** são extremamente grandes, fazendo do desafio de se encontrar **p** e **q** partindo de **n**, uma tarefa quase impossível, mesmo para os computadores. Como visto em Fiarresga (2010) não existem, atualmente, algoritmos que decomponha em fatores primos um número enorme, e que o faça de maneira rápida. Um exemplo desta dificuldade é dada em Tanenbaum; Wetherall (2011) onde tem-se que "De acordo com Rivest e seus Colegas, a fatoração de um número 500 dígitos requer 10^{25} anos, usando-se a força bruta. Neste caso, eles pressupõem o melhor algoritmo conhecido e um computador com um tempo por instrução de 1μs."

Outras condições devem ser abordadas, tem-se ainda que m.d.c.(**b**, φ(n)) = 1, onde o valor de φ é dado pela seguinte função, φ (n) = (p-1)(q-1), por fim resta determinar o valor de **a**, para isto é preciso que **ab** = 1 (mod φ (n)). Assim analisa-se que a chave publica consiste no par de valore **b** e **n**, enquanto a chave privada é dada por **a** e **n** (TANENBAUM; WETHERALL, 2011).

2.2. MÉTODOS DE ATAQUE

Partindo dos conceitos adquiridos ao longo deste texto, sabemos que para se obter uma cifra consistente, é preciso que se leve em conta os possíveis ataques que esta será submetida, e para isto é preciso conhecer as formas destes possíveis ataques. "A arte de solucionar mensagens cifradas, conhecida como **criptoanálise**, e a arte de criar mensagens

cifradas (criptografia) é chamada coletivamente de **criptologia**." (TANENBAUM; WETHERALL, 2011, grifo do autor). Desta forma, é visto que tanto quem cria os métodos para manter segura as mensagens, quanto quem põem à prova esta segurança, fazem parte de um mesmo ramo de estudo, a criptologia.

Tem-se então que, compreender as maneiras como um intruso pode ameaçar a integridade do funcionamento seguro de uma determinada cifra, é tão importante para se manter seguro, quanto entender a forma de funcionamento da própria cifra. Vale ressaltar que nem todo ataque é feito com intuito de se causar prejuízos ao sistema, a criptoanálise pode ser usada como forma a se testar a eficiência de uma nova cifra, antes que seja submetida a uso.

2.2.1. Força bruta

É talvez o método mais intuitivo, consiste basicamente em tentativa e erro, em Stallings (2015) é dito que um invasor pode testar todas as chaves, até obter uma tradução inteligível para a mensagem.

A eficiência de seu uso depende da complexidade da cifra a qual se pretende aplicá-lo. Por exemplo, para sistemas com um número pequeno de chaves o método pode funcionar, contudo "Em média, metade de todas as chaves possíveis precisa ser experimentada para se obter sucesso. Ou seja, se houver X chaves diferentes, um intruso descobriria a verdadeira após X/2 tentativas, em média." (STALLINGS, 2015), isto apenas reforça que para cifras que possuem um número muito grande de chaves o método torna-se inviável.

2.2.2. Análise de frequência

Para o caso em que o método da força bruta não possa ser aplicado, faz-se necessário então buscar um método que permita a decifragem da mensagem. Um método simples e que permite a quebra de cifras de substituição de maneira consideravelmente rápida, é através da análise de frequência. A força deste método firma-se na frequência com que as letras são

utilizadas dentro de uma determinada língua, dado que a repetição de letras é algo que se pode destacar em idiomas distintos (PACHECO, 2014).

Evidentemente que este método é bastante efetivo para cifras monoalfabéticas, onde cada letra é substituída por outra e se tem apenas um alfabeto de cifra. Stalling (2015) reforça este conceito dizendo que "As cifras monoalfabéticas são fáceis de se quebrar porque refletem os dados de frequência do alfabeto original". Tem-se então, que através da frequência que uma determinada letra aparece no texto cifrado, é possível supor que esta é a letra que aparece com maior frequência dentro da língua na qual a mensagem foi escrita.

2.2.3. Teste de Kasiski

Sabe-se agora que para cifras em que usa-se apenas um alfabeto de cifra, a análise de frequência consegue romper as defesas impostas, contudo para as cifras polialfabéticas como a de Vigenère, por exemplo, a análise de frequência pode ser um trabalho demorado, e se feita da maneira convencional o resultado obtido da mensagem será um texto quase inelegível. A forma como usar-se a análise de frequência para a cifra de Vigenère será explicada mais a fundo posteriormente, por ora, desconsidera-se este método para o caso.

Sendo assim, uma opção para este caso é o teste de Kasiski, que permite descobrir o tamanho da palavra chave através de análise do texto cifrado. Sendo esta a solução para cifras polialfabéticas, revelada por Friedrich W. Kasiski (MARTINS, 2005), pode-se ainda ressaltar que apesar de ser creditado a Kasiski, em Cozzens; Miller (2013) é dito que Babbage havia descoberto este método de maneira independente a mais de uma década antes.

O método é aplicado através da observação das repetições de frases dentro do texto cifrado. Fazendo uso disto, supõe-se que se a mesma frase se repete, esta representa os mesmos caracteres no texto simples. A grande observação de Kasiski é que as repetições ocorriam da mesma maneira quando a distância entre as primeiras letras da sequência repetida é um múltiplo do comprimento da palavra-chave (COZZENS; MILLER, 2013).

Uma outra forma de se explicar Almeida (2012) é que este teste é baseado no fato de dois segmentos idênticos do texto serem cifrados da mesma forma, sendo que a sua ocorrência está com x posições de separação, com $x \equiv 0 \bmod n$, onde n é o comprimento da palavra-

chave. Obtido o comprimento da palavra-chave através de análise de frequência é possível obter-se a mensagem.

3. METODOLOGIA

Com intuito de entender os diferentes tipos de cifras, bem como avaliar quais dessas seriam de maior interesse para o presente texto, desenvolveu-se uma pesquisa bibliográfica, usando como fonte livros, artigos e páginas onlines, que contribuíram na decisão da escolhas das cifras vistas até então. Este tipo de método é de grande valor para desenvolvimento de pesquisas de um modo geral, como visto em Gil (2008, p.50 apud Lima, 2018)

> A principal vantagem de pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômeno muito mais amplo do que aquela que poderia pesquisar diretamente. Esta vantagem torna particularmente importante quando o problema de pesquisa requer dados muitos dispersos pelo espaço. Por exemplo, seria impossível um pesquisador percorrer todo o território brasileiro em busca de dados sobre a população ou renda per capita; todavia, se tem a sua disposição uma bibliografia adequada, não terá os maiores obstáculos para contar com as informações requeridas.

Tendo ao alcance um vasto leque de referências, podemos escolher as cifras, para em seguida testá-las, não só o seu uso, mas também sua segurança, assim deseja-se obter um parecer acerca de cada uma delas, e, por fim, avaliar tais resultados de maneira qualitativa, bem como propor formas de aumentar o nível de seguranças dos métodos avaliados.

3.1. TESTES CIFRAS SIMÉTRICAS

No intuito de exemplificar a forma de uso de cada cifra, para que posteriormente as mesmas sejam submetidas à invasão, escolheu-se um trecho de um texto, sendo este a mensagem a ser criptografada, é importante salientar que para fins comparativos a mensagem é a mesma para todas as cifras.

A mensagem escolhida foi:

“Muitas das promessas não passam de janeiro, as que não se afogam pulando as sete ondas, são esquecidas perdidas no carnaval.”

Uma observação que deve ser feita é que para os cálculos os valores de “a” e “ã”, ou “e” e “é” são os mesmo, bem como as pontuações e os espaços não entram nos cálculos executados neste trabalho. Sendo assim, pode-se reescrever a mensagem como sendo:

Muitasdaspromessasnaopassamdejaneiroasquenaoseafogampulandoasseteondassaoesquecidasperdidasnocarnaval

Para que a mensagem possa ser tratada de maneira numérica é preciso que se converta cada letra para números, essa conversão será feita usando a tabela 1.

Tabela 1: Equivalência entre letras e número

A	B	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Própria (2019)

Desta forma tem-se que a mensagem pode ser representada de maneira numérica como descrito abaixo:

12 20 8 19 0 18 3 0 18 15 17 14 12 4 18 18 0 18 13 0 14 15 0 18 18 0 12 3 4 9 0 13 4 8 17 14 0 18 16 20 4 13 0 14 18 4 0 5 14 6 0 12 15 20 11 0 13 3 14 0 18 18 4 19 4 14 13 3 0 18 18 0 14 4 18 16 20 4 2 8 3 0 18 15 4 17 3 8 3 0 18 13 14 2 0 17 13 0 21 0 11

Feito isto, é possível aplicar a diferentes cifras. Evidentemente, os procedimentos de cálculos possuem embasamentos em conceitos matemáticos. Tais teoremas e definições que garantem o funcionamento destes métodos serão apresentados mais a frente neste trabalho.

Sendo assim, a aplicação e análise das cifras simétricas foram feitas considerando um conjunto finito dentro dos naturais, que vai de 0 a 25, denotado ao longo deste texto como $\mathbb{Z}_{26}$. Este conjunto é um sistema de números inteiro mod 26.

3.1.1. Cifra de César

Tomando a mensagem descrita anteriormente, pode-se utilizar a seguinte função para criptografar a mensagem:

Inicialmente considera-se a seguinte definição:

Seja **a** e **b** inteiros e **n** um inteiro positivo. Se n | (a - b), dizemos que **a** é congruente com **b** e escrevemos: a ≡ b mod n.

$$C(x) = x + k \bmod 26,$$

onde para a cifra de César o valor é k = 3. Como já mencionado, considera-se o conjunto finito $\mathbb{Z}_{26}$. Obtém-se assim todos os possíveis valores que podem estar presente na mensagem.

É importante observar, que apesar de ser denotado desta maneira ao longo do texto e em algumas das bibliografias utilizadas, expressar a função mod da maneira como é feita no presente trabalho, é um abuso de notação, visto que o mod diz respeito a congruência, sendo assim relacionado a grupos de equivalência e não a igualde como visto.

C(0) = 0 + 3 mod 26 = 3

C(1) = 1 + 3 mod 26 = 4

C(2) = 2 + 3 mod 26 = 5

C(3) = 3 + 3 mod 26 = 6

C(4) = 4 + 3 mod 26 = 7

C(5) = 5 + 3 mod 26 = 8

C(6) = 6 + 3 mod 26 = 9

C(7) = 7 + 3 mod 26 = 10

C(8) = 8 + 3 mod 26 = 11

C(9) = 9 + 3 mod 26 = 12

C(10) = 10 + 3 mod 26 = 13

C(11) = 11 + 3 mod 26 = 14

C(12) = 12 + 3 mod 26 = 15

C(13) = 13 + 3 mod 26 = 16

C(14) = 14 + 3 mod 26 = 17

C(15) = 15 + 3 mod 26 = 18

C(16) = 16 + 3 mod 26 = 19

C(17) = 17 + 3 mod 26 = 20

C(18) = 18 + 3 mod 26 = 21

C(19) = 19 + 3 mod 26 = 22

C(20) = 20 + 3 mod 26 = 23

C(21) = 21 + 3 mod 26 = 24

C(22) = 22 + 3 mod 26 = 25

C(23) = 23 + 3 mod 26 = 0

C(24) = 24 + 3 mod 26 = 1

C(25) = 25 + 3 mod 26 = 2

Os resultados foram:

Tabela 2: Equivalência de letras e números para a cifra de César

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
3	4	5	6	7	8	9	10	11	12	13	14	15
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
16	17	18	19	20	21	22	23	24	25	0	1	2

Fonte: Própria (2019)

Sendo assim, para a cifra de César o A passa de 0 para 3, o B de 1 para 4, e assim por diante, utilizando os valores calculados e substituindo os valores da mensagem por este, segue que:

15 23 11 22 3 21 6 3 21 18 20 17 15 7 21 21 3 21 16 3 17 18 3 21 21 3 15 6 7 12 3 16 7 11 20 17 3 21 19 23 7 16 3 17 21 7 3 8 17 9 3 15 18 23 14 3 16 6 17 3 21 21 7 22 7 17 16 6 3 21 21 3 17 7 21 19 23 7 5 11 6 3 21 18 7 20 6 11 6 3 21 16 17 5 3 20 16 3 24 3 14

Com os valores já calculados usa-se a tabela 1, e converte-se a mensagem para sua forma alfabética, sendo a nova mensagem:

PXLWDVGDVSURPHVVDVQDRSDVVDPGHMDQHLURDVTXHQDRV HDIRJDPSXODQGRDVVHWHRQGDVVDR HVTX HFLGDVSHUGLGD VQRFDUQDY DO

Para que o destinatário obtenha a mensagem original, o mesmo só precisa converter o texto cifrado para sua forma numérica e em seguida aplicar os valores na seguinte função:

$$D(y) = y - k \bmod 26,$$

onde como já visto k = 3, e para esta função y representa o valor do texto cifrado. Feito isto, a mensagem original pode ser obtida.

3.1.2. Cifra afim

Como o próprio nome sugere, a cifra afim faz uso de uma função afim para criptografar a mensagem, sendo esta função:

$$y \equiv ax + b \bmod 26,$$

onde y é o valor do texto cifrado e x é o valor da mensagem.

Pelo teorema abaixo tem-se que:

ax ≡ b mod n, tem soluções, se e só se d | b, onde d = m.d.c. (a, n). Se d | b então a solução é única $mod\ \frac{n}{d}$.

Em seguida é preciso garantir que a função possui inversa, desta forma pela definição, tem-se que

Sejam a e n inteiros tais que m.d.c.(a, n) = 1. Ao único inteiro, que é solução da equação

$$ax \equiv 1 \bmod n$$

chamamos de inverso de a mod n e denotamos por a^{-1} mod n.

Desta forma temos que satisfazer a seguinte condição para que a cifra seja válida:

m.d.c.(a, 26) = 1, para todo b $\in \mathbb{Z}_{26}$.

Esta consideração fornece também a quantidade de chaves da cifra, pois os únicos valores válidos pertencentes a $\mathbb{Z}_{26}$ seriam: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 e 25. Assim, os possíveis valores de K seriam K = (12)(26) = 312.

Tomando a = 3 e b = 5, tem-se que m.d.c.(3, 26) = 1, deste modo garante-se que a função possui inversa, sendo assim possível aplicá-la no exemplo a seguir.

Considerando a mensagem anterior, busca-se criptografá-la usando agora a cifra afim, fazendo da mesma forma como feita para a cifra de César, pode-se calcular os valores possíveis para x, de modo que se obtenha todos os possíveis valores para a mensagem, sendo assim, aplicando os valores de 0 a 25 na função C(x) = 3x + 5 mod 26, onde a = 3 e b = 5, nota-se que estes são valores simples, pois o foco é a analise, sendo assim tem-se os seguintes resultado:

C(0) = 3(0) + 5 mod 26 = 5

C(1) = 3(1) + 5 mod 26 = 8

C(2) = 3(2) + 5 mod 26 = 11

C(3) = 3(3) + 5 mod 26 = 14

C(4) = 3(4) + 5 mod 26 = 17

C(5) = 3(5) + 5 mod 26 = 20

C(6) = 3(6) + 5 mod 26 = 23

C(7) = 3(7) + 5 mod 26 = 0

C(8) = 3(8) + 5 mod 26 = 3

C(9) = 3(9) + 5 mod 26 = 6

C(10) = 3(10) + 5 mod 26 = 9

C(11) = 3(11) + 5 mod 26 = 12

C(12) = 3(12) + 5 mod 26 = 15

C(13) = 3(13) + 5 mod 26 = 18

C(14) = 3(14) + 5 mod 26 = 21

C(15) = 3(15) + 5 mod 26 = 24

C(16) = 3(16) + 5 mod 26 = 1

C(17) = 3(17) + 5 mod 26 = 4

C(18) = 3(18) + 5 mod 26 = 7

C(19) = 3(19) + 5 mod 26 = 10

C(20) = 3(20) + 5 mod 26 = 13

C(21) = 3(21) + 5 mod 26 = 16

C(22) = 3(22) + 5 mod 26 = 19

C(23) = 3(23) + 5 mod 26 = 22

C(24) = 3(24) + 5 mod 26 = 25

C(25) = 3(25) + 5 mod 26 = 2

Tem-se então que para a cifra afim o alfabeto seria:

Tabela 3: Equivalência de letras e números para a cifra de afim

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
5	8	11	14	17	20	23	0	3	6	9	12	15
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
18	21	24	1	4	7	10	13	16	19	22	25	2

Fonte: Própria (2019)

Tendo isto, substituindo as letras da mensagem pelos valores obtidos é simples criptografar o texto escolhido, onde numericamente obteve-se os seguintes valores:

15 13 3 10 5 7 14 5 7 24 4 21 15 17 7 7 5 7 18 5 21 24 5 7 7 5 15 14 17 6 5 18 17 3 4 21 5 7 1 13 17 18 5 21 7 17 5 20 21 23 5 15 24 13 12 5 18 14 21 5 7 7 17 10 17 21 18 14 5 7 7 5 21 17 7 1 13 17 11 3 14 5 7 24 17 4 14 3 14 5 7 18 21 11 5 4 18 5 16 5 12

Esses valores são convertidos na seguinte mensagem antes desta ser enviada ao devido destinatário:

PNDKFHOFHYEVPRHHFHSFVYFHHFPORGFSRDEVFHBNRSFVHRFU VXFPYNMFSOVFHHRKRVSOFHHFVRHBNRLDOFHYREODOFHSVLF ESFQFM

Tendo o texto cifrado, é possível retornar o texto cifrado à mensagem fazendo uso da função inversa de C(x), sendo está D(y) = a^{-1}(y - b), está função é obtida através da consequência da condição anterior, onde se m.d.c.(a, 26) = 1, sabe-se que y ≡ ax + b mod 26 sendo está equivalente a x ≡ a^{-1}(y – b) mod 26. Usando os valores calculados para o texto e aplicando-os na função D(y) = a^{-1} (y - b), obtém-se os valores da mensagem.

É preciso ressaltar que os valores usados para decifrar não são os da mensagem, mas sim os obtidos quando aplicado na função, por exemplo, quando aplicado 13(N) na função tem-se como resultado na mensagem 18(S), esse valor é obtido após executar-se o mod 26, porém para descriptografar a mensagem o valor usado é 44, que seria 44 = 3(13) + 5, ou seja, o valor obtido antes da aplicação do mod 26.

3.1.3. Cifra de Vígenère

O último caso analisado foi o da Cifra de Vegenere, para este a chave não é um valor apenas, a chave pode ser uma frase, ou palavra, apesar de parecer mais complexo seu uso é bastante simples, para o caso analisado considera-se uma chave simples como a palavra "GOL", o tamanho da chave é 3, desta forma, tem-se que o corpo finito será $\mathbb{Z}_{26}^{3}$.

O procedimento para cifrar a mensagem é semelhante a de César, a função será:

C(X) = X + K, o X é a mensagem e K é a chave, ampliado a análise, tem-se

$C(X_1, X_2, X_3, ...,X_n) = (X_1 + K_1, X_2 + K_2, X_3 + K_3, ...,X_n + K_n)$

Assim, organiza-se a mensagem em bloco de acordo com o tamanho da chave e em seguida somam-se os valores da mensagem com os da chave. Se a palavra escolhida como chave é GOL, numericamente dada por 6 14 11, segue que

	1ª soma			2ª soma			3ª soma			4ª soma		
Texto claro	12	20	8	19	0	18	3	0	18	15	17	14
Chave	6	14	11	6	14	11	6	14	11	6	14	11
Texto cifrado	18	8	19	25	14	3	9	14	3	21	5	25

Repete-se o processo até que se tenha criptografado toda a mensagem, os valores obtidos com esse processo podem ser vistos abaixo:

> 18 8 19 25 14 3 9 14 3 21 5 25 18 18 3 24 14 3 19 14 25 21 14 3 24 14 23 9 18 20 6 1 15 14 5 25 6 6 1 0 18 24 6 2 3 10 14 16 20 20 11 18 3 5 17 14 24 9 2 11 24 6 15 25 18 25 19 17 11 24 6 11 20 18 3 22 8 15 8 22 14 6 6 0 10 5 14 14 17 11 24 1 25 8 14 2 19 14 6 6 25

A mensagem recebida pelo destinatário para este caso seria:

> SITZODJODVFZSSDYODTOZVODYOXJSUGBPOFZGGBASYGCDKOQ UULSDFROYJCLYGPZSZTRLYGLUSDWIPIWOGGAKFOORLYBZIOCT OGGZ

Como já mencionado este método é semelhante a cifra de César, porém para cada letra do texto claro tem-se um chave especifica, sendo assim, para descriptografar a mensagem a função seria D(Y) = Y – K, Y são os valores obtidos no processo de criptografar, ampliandoa função obtém-se:

$$D(Y_1, Y_2, Y_3, ...,Y_n) = (Y_1 - K_1, Y_2 - K_2, Y_3 - K_3, ...,Y_n - K_n)$$

3.2. TESTE CRIPTOSSISTEMA RSA

Utilizando o mesmo texto claro, busca-se criptografá-los usando a RSA que possui funções D(Y) = Y^a mod n e C(X) =X^b mod n, para isso é preciso analisar as seguintes

condições: n = pq, onde p e q são primos; φ(n) = (p-1)(q-1); m.d.c. (b, φ(n)) = 1, onde 1 < b < φ(n) e ab=1 mod(φ(n)), onde 1 < a < φ(n).

Aplicando o alfabeto na função anterior, criptografa-se assim seus valores, tomando p = 3 e q = 11, resultando em um n = 33, além de φ(n) = 20, por fim tem-se que a =3 e b =7.

Sendo assim a chave pública é (33, 7) enquanto a privada é (33, 3)

C(0) = 0^7 mod 33 = 0

C(1) = 1^7 mod 33 = 1

C(2) = 2^7 mod 33 = 29

C(3) = 3^7 mod 33 = 9

C(4) = 4^7 mod 33 = 16

C(5) = 5^7 mod 33 = 14

C(6) = 6^7 mod 33 = 30

C(7) = 7^7 mod 33 = 28

C(8) = 8^7 mod 33 = 2

C(9) = 9^7 mod 33 = 15

C(10) = 10^7 mod 33 = 10

C(11) = 11^7 mod 33 = 11

C(12) = 12^7 mod 33 = 12

C(13) = 13^7 mod 33 = 7

C(14) = 14^7 mod 33 = 20

C(15) = 15^7 mod 33 = 27

C(16) = 16^7 mod 33 = 25

C(17) = 17^7 mod 33 = 8

C(18) = 18^7 mod 33 = 6

C(19) = 19^7 mod 33 = 13

C(20) = 20^7 mod 33 = 26

C(21) = 21^7 mod 33 = 21

C(22) = 22^7 mod 33 = 22

C(23) = 23^7 mod 33 = 23

C(24) = 24^7 mod 33 = 18

C(25) = 25^7 mod 33 = 31

Sendo assim, os valores que devem substituir cada letra do texto claro são

Tabela 4: Equivalência de letras e números com valores definidos em RSA

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	29	9	16	14	30	28	2	15	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
7	20	27	25	8	6	13	26	21	22	23	18	31

Fonte: Própria (2019)

Notamos que os valores acima de 25, isto se dá devido ao fato do mod ser referente a n e não mais 26, isto é, o corpo finito é $\mathbb{Z}$n.

A mensagem obtida com esta operação é:

12 26 2 13 0 6 9 0 6 27 8 20 12 16 6 6 0 6 7 0 20 27 0 6 6 0 12 9 16 15 0 7 16 2 8 20 0 6 25 26 16 7 0 20 6 16 0 14 20 30 0 12 27 26 11 0 7 9 20 0 6 16 13 16 20 7 9 0 6 6 0 20 16 6 25 26 16 29 2 0 6 27 16 8 9 2 9 0 6 7 20 29 0 8 7 0 21 0 11

Para se obter o texto claro o destinatário aplica os valores recebidos pelo emissor na seguinte função D(Y) = Y^3 mod 33, onde como já dito (33,3) é a chave privada, mantendo desta forma a segurança de sua mensagem.

3.3. CRIPTOANÁLISE

Sabendo a forma como funcionam as cifras, é possível então buscar formas de se obter a mensagem partindo do texto cifrado, logicamente que considera-se o caso em que não se tenha conhecimento da chave, ou seja, a análise será feita do ponto de vista do invasor.

Como sugere o principio de Kerckhoff, considera-se que o invasor possui informações sobre a cifra, sendo assim, é possível que este tenha alguma noção sobre a língua em que a cifra foi escrita, bem como algum conhecimento sobre seu funcionamento. Partindo disto, é possível testar maneiras de se encontrar o texto claro usando apenas o texto cifrado.

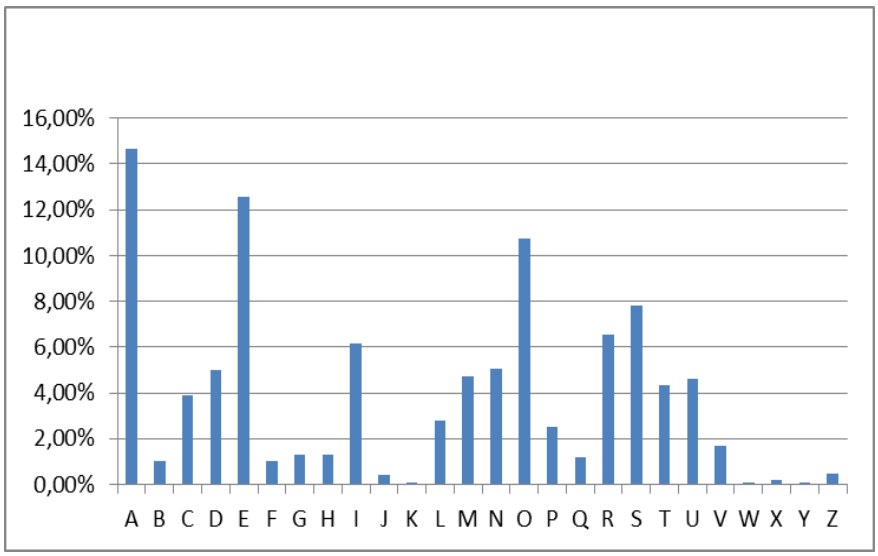
Um dos conceitos de maior importância para que se consiga quebrar cifras simétricas de substituição, é entender a frequência com que determinadas letras aparecem dentro de uma língua, pois independente da língua sempre haverá alguns letras que serão mais usadas do que outras, para a língua portuguesa a frequência com que as letras do alfabeto aparecem é dada por:

Tabela 5: Frequência de aparecimento de letras para o português

A	B	C	D	E	F	G	H	I	J	K	L	M
14,63%	1,04%	3,88%	4,99%	12,57%	1,02%	1,30%	1,28%	6,18%	0,40%	0,02%	2,78%	4,74%
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
5,05%	10,73%	2,52%	1,20%	6,53%	7,81%	4,34%	4,63%	1,67%	0,01%	0,21%	0,01%	0,47%

Fonte: Aldeia numaboa (2019)

Gráfico 1: Frequência de aparecimento de letras para o português



Fonte: Própria (2019)

Através disto é possível supor que letras que aparecem mais no texto cifrado serão as de maior frequência de aparecimento, por isso, conhecer a língua em que a mensagem foi escrita auxilia no método para quebrar a cifra.

3.3.1. Cifra de César

Para que se possa quebrar a cifra de César, primeiro analisa-se a mensagem cifrada, sendo esta:

PXLWDVGDVSURPHVVDVQDRSDVVDPGHMDQHLURDVTXHQDRVHDIR JDPSXODQGRDVVHWHRQGDVVDR HVTX HFLGDVSHUGLGDVQRFDUQDYDO

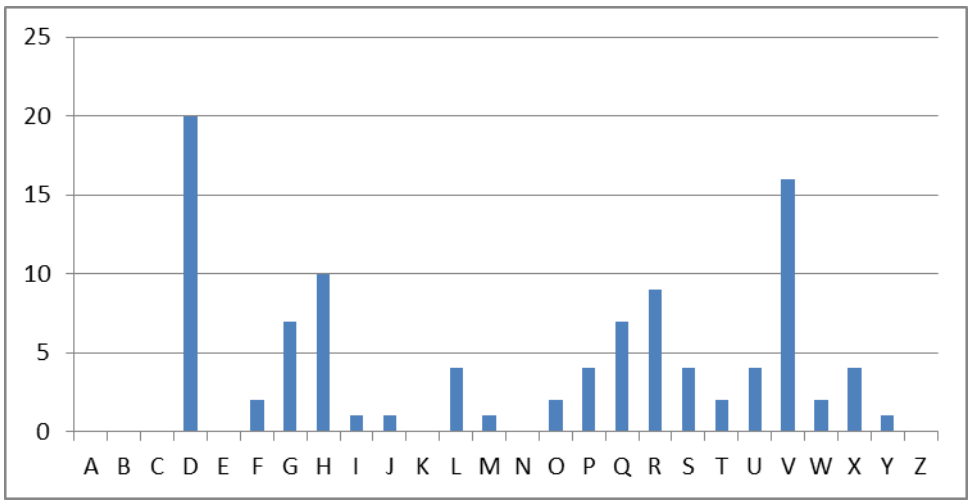
Para esta mensagem as letras que mais se repetem são D e V como visto abaixo

Tabela 6: Ocorrência de letras para o texto cifrado com a cifra de César

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	0	0	20	0	2	7	10	1	1	0	4	1
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	2	4	7	9	4	2	4	16	2	4	1	0

Fonte: Própria (2019)

Gráfico 2: Ocorrência de letras para o texto cifrado com a cifra de César



Fonte: Própria (2019)

Deste modo, pode-se supor que para o texto cifrado, D corresponde a A, pois esta é a letra que mais aparece, uma outra consideração é a de que VV aparece algumas vezes no texto, para a língua portuguesa pode-se supor que este termo corresponde a RR ou SS, como S é uma letra de maior frequência que R, não é difícil supor que esta seria a corresponde a V.

Substituindo então D por A e V por S, ficaria:

PXLW**AS**G**AS**SURPH**SSAS**Q**A**RS**ASSA**PGHM**A**QHLUR**AS**TXHQ**A**R**S**H**A**IRJ**A**P SXO**A**QGR**ASS**HWHRQG**ASSA**R H**S**TX HFLG**AS**SHUGLG**AS**QRF**A**UQ**A**Y**A**O

As próximas letras de maior frequência são E e O respectivamente, assim, substitui-se H por E e R por O.

PXLW**AS**G**AS**SU**O**P**ESSAS**Q**AO**S**ASSA**PG**E**M**A**Q**E**LU**OAS**TX**E**Q**AOSEA**I**O**J**A** PSXO**A**QG**OASSE**W**EO**QG**ASSAOES**TX**E**FLG**AS**S**E**UGLG**AS**Q**O**F**A**UQ**A**Y**A**O

Já é possível notar-se alguns trechos de palavras, utilizando os gráficos tem-se que as próximas letras de maior frequência seriam I e R, no texto cifrado as próximas de maior frequência seriam Q e G, porém suponha-se que R seja Q e I seja G.

PXLW**ASIAS**SU**O**P**ESSASRAO**S**ASSA**P**IE**M**ARE**LU**OAS**TX**ERAOSEA**I**O**J**A**P SXO**ARIOASSE**W**EORIASSAOES**TX**E**FL**IAS**S**E**U**I**L**IASRO**F**A**U**RA**Y**A**O

O que pode ser visto é que o sentido do texto é perdido, o mesmo ocorre quando se substitui G por R e Q por I, sendo assim, é mais provável que estes não sejam os valores correspondentes para Q e G, sendo assim é necessário observar novamente o gráfico de frequência, onde ver-se que as próximas letras seriam N e D, aplicando N em Q e D em G.

PXLW**ASDAS**SU**O**P**ESSASNAO**S**ASSA**P**DE**M**ANE**LU**OAS**TX**ENAOSEAIOJA**
PSXO**ANDOASSE**W**EONDASSAOES**TX**E**FL**DAS**S**E**U**D**L**DASNO**F**A**U**NA**Y**A**O

Partindo deste ponto é preciso fazer suposições e análise sobre trechos encontrados no texto, por exemplo, no trecho S**ASSA**P**DE**, como DE é comumente usando entre palavras, pode-se supor que S**ASSA**P é um termo isolado de DE, onde P é a letra final, tomando P como M, sendo esta uma letra comum em finais de palavras, além de ser a próxima letra de maior frequência. Assim toma-se P como sendo M, evidentemente que P poderia ser R já que está também é comum em fins de palavras, porém após substituir ver-se que M é mais provável, assim tem-se que:

MXLW**ASDAS**SU**OMESSASNAO**S**ASSAMDE**M**ANE**LU**OAS**TX**ENAOSEAIO**
J**AM**SXO**ANDOASSE**W**EONDASSAOES**TX**E**FL**DAS**S**E**U**D**L**DASNO**F**A**U**NA**Y**A**O

Com o resultado anterior tem-se S**ASSAMDE**, podem S pode ser P, visto que formaria um palavras conhecida, além disso no trecho **SE**W**EONDAS**, suponhe-se que W seja T, resultando em:

MXL**TASDASP**U**OMESSASNAOPASSAMDE**M**ANE**LU**OAS**TX**ENAOSEAIOJ**
AMPXO**ANDOASSETEONDASSAOES**TX**E**FL**DASPE**U**D**L**DASNO**F**A**U**NA**Y**A**O

Alguns outros trechos fornecem informações pertinentes como **P**U**OMESSAS**, onde permite supor que U é R, **PE**U**D**L**DAS** sendo assim tem-se que L é I, e posterior a isso ainda encontra-se que **M**XL**TAS** X é U.

MUITASDASPROMESSASNAOPASSAMDEM**ANEIROAS**T**UENAOSEAIOJ**
AMPUO**ANDOASSETEONDASSAOES**T**UE**F**IDASPERDIDASNO**F**ARNA**Y**A**O

Os demais termos podem ser facilmente encontrados através de suposições, desta forma a mensagem foi descriptografada sem que tivéssemos acesso a chave, lógico que não seria necessário aplicar um método tão demorado, sendo que este tipo de cifra possui apenas 25 chaves (desconsiderando que 0 seja uma chave aplicável), seria possível encontrar a mensagem através de tentativa e erro.

Uma outra forma seria encontrar o valor da chave através do termo mais comum, por exemplo, se D é a letra mais comum, então provavelmente esta será A, se para uma cifra qualquer de deslocamento o valor cifrado é dado por Y = X + K, onde Y = 3 (D) e X = 0 (A), tem-se então que K = Y- X, assim K = 3 – 0, K = 3, obtido a chave encontrar a mensagem seria simples, sendo necessário apenas diminuir o valor da chave do valor cifrado.

3.3.2. Cifra afim

Para que se obtenha o texto claro cifrado pela cifra afim faz-se um procedimento semelhante ao visto anteriormente, por esta ser uma cifra monoalfabética. As frequências das letras são mantidas no texto cifrado, sendo assim se analisar-se a mensagem é possível identificar padrões, se a mensagem é

PNDKFHOFHYEVPRHHFHSFVYFHHFPORGFSRDEVFHBNRSFVHRFUVXFP YNMFSOVFHHRKRVSOFHHFVRHBNRLDOFHYREODOFHSVLFESFQFM

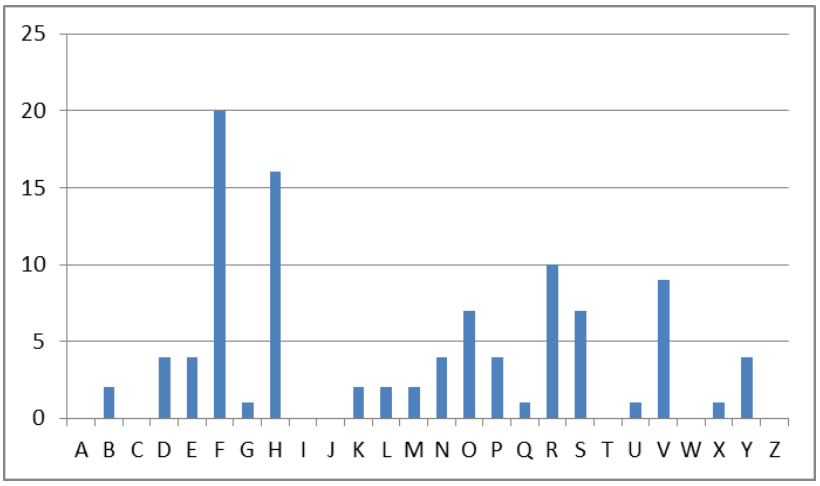
Onde tem-se as seguintes quantidades de letras:

Tabela 7: Ocorrência de letras para o texto cifrado com a cifra afim

A	B	C	D	E	F	G	H	I	J	K	L	M
0	2	0	4	4	20	1	16	0	0	2	2	2
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
4	7	4	1	10	7	0	1	9	0	1	4	0

Fonte: Própria (2019)

Gráfico 3: Ocorrência de letras para o texto cifrado com a cifra afim



Fonte: Própria (2019)

Como já era esperado, o gráfico de frequências de letras no texto cifrado pela cifra afim é semelhante ao visto na cifra de César, isso ocorre devido ao fato de que ainda que

cifras monoalfabéticas alterem as letras da mensagem por métodos diferentes, a frequência com que uma determinada letra aparece no texto claro é refletida no texto cifrado.

Sendo assim, considera-se que F seja A e H seja S, devido aos mesmos motivos visto na cifra de César, e ainda pode-se supor que R equivale a E, bem como V equivalente a O, tem-se então que

PNDK**AS**O**AS**YE**O**P**ESSAS**S**AO**Y**ASSA**PO**E**G**A**S**E**DE**OAS**BN**E**S**AOSEA**U**O**X**A**
PYNM**A**SO**OASSE**K**EO**SO**ASSAOES**BN**E**LDO**AS**Y**E**EODO**AS**S**O**L**A**ES**A**Q**A**M

Mantendo as considerações faz-se que S vale N, O vale D

PNDK**ASDAS**YE**O**P**ESSASNAO**Y**ASSA**P**DE**G**ANE**DE**OAS**BN**ENAOSEA**U**O**X
APYNM**ANDOASSE**K**EONDASSAOES**BN**E**LD**DAS**Y**E**E**D**DD**DASNO**L**A**E**NA**Q**A**M

Se P equivale M, fazendo análise de trechos do texto, também encontramos que Y é P e K é T, assim

MND**TASDASP**E**OMESSASNAOPASSAMDE**G**ANE**DE**OAS**BN**ENAOSEA**U**O**
X**AMP**NM**ANDOASSETEONDASSAOES**BN**E**LD**DASPE**E**D**DD**DASNO**L**A**E**NA**Q**A**M

Visto que podemos supor que E vale R, D seria I e N seria U

MUITASDASPROMESSASNAOPASSAMDEG**ANEIROAS**B**UENAOSEA**U**O**
X**AMPU**M**ANDOASSETEONDASSAOES**B**UE**L**IDASPERDIDASNO**L**ARNA**Q**A**M

Por fim tomando M como L chega-se a um ponto onde as próximas letras são facilmente encontradas por suposição

MUITASDASPROMESSASNAOPASSAMDEG**ANEIROAS**B**UENAOSEA**U**O**
X**AMPULANDOASSETEONDASSAOES**B**UE**L**IDASPERDIDASNO**L**ARNA**Q**AL**

Para este caso a análise de frequência ainda é um método demorado, contudo caso não se tenha em mãos formas computacionais para executar o método da força bruta, esta é um opção viável, pois diferente da cifra de César esta possui uma quantidade maior de chaves, como visto esta cifra conta 312 valores possíveis para sua chave, inviabilizando o método da força bruta (se feito sem auxilio computacional).

Análogo a cifra de César, se conhecido o valor de A, onde neste caso A = 5, e aplicando este conceito em $y = ax + b \bmod 26$, tem-se que $5 = a(0) + b$, logo b = 5, para se obter o valor de **a**, aplica-se o valor obtido de **b** na mesma equação para um outro valor

conhecido, como por exemplo, E = 17, portanto, 17 = a(4) + 5, com isso tem-se que a = 3, sendo possível desta forma quebrar a cifra de uma maneira mais rápida.

3.3.3. Cifra de Vigenère

A cifra de Vigenère é uma cifra polialfabética o que impossibilita a análise de frequência convencional, pois dois valores iguais podem representar duas letras diferentes, para que se aplique a análise de frequência em um texto cifrado por esta método é necessário que se conheça o comprimento da chave. Além de não ser viável utilizar-se o método da força bruta, tendo em vista que este possui um comprimento de chave dado por 26^n, onde n é o comprimento da palavra-chave, por exemplo, se n = 3, tem-se então 17576 possíveis valores para a chave.

Utilizando o teste de Kasiski é possível obter-se o comprimento da palavra-chave para a cifra de Vigenère. O teste de Kasiski faz uso da análise de repetições de trechos do texto, ou seja, se uma certa quantidade de letras se repete no texto em uma mesma sequência, isto indica que provavelmente o motivo é que tais letras foram cifradas da mesma maneira pelo mesmo valor da mensagem, isto é, a mensagem se alinhou que a chave da mesma forma em pontos diferente do texto cifrado, resultando assim na repetição de grupos de caracteres.

Tomando o texto cifrado como sendo o seguinte:

SITZ**OD**J**OD**VFZSSDY**OD**TOZV**OD**YOXJSUGBPOFZGGBASYGCDKOQUUL SDFROYJCLYGPZSZTRLYGLUSDWIPIWOGGAKFOORLYBZIOCTOGGZ

Nota-se que a sequência OD aparece quatro vezes dentro do texto cifrado, sendo assim o próximo passo para encontrar o tamanho da chave seria contar as quantidade de caracteres entre o inicio da primeira parição até as demais, feito isto tem-se que, do inicio da primeira aparição de OD até a segunda tem-se 3 caracteres, da primeira pra segunda tem-se 12 e da primeira para a terceira tem-se 18, sendo assim o valores obtidos são: 3,12,18.

A suposição do teste de Kasiski para se determinar o comprimento da palavra-chave é que as distâncias obtidas são múltiplas da palavra-chava, logo, o comprimento da chave é o

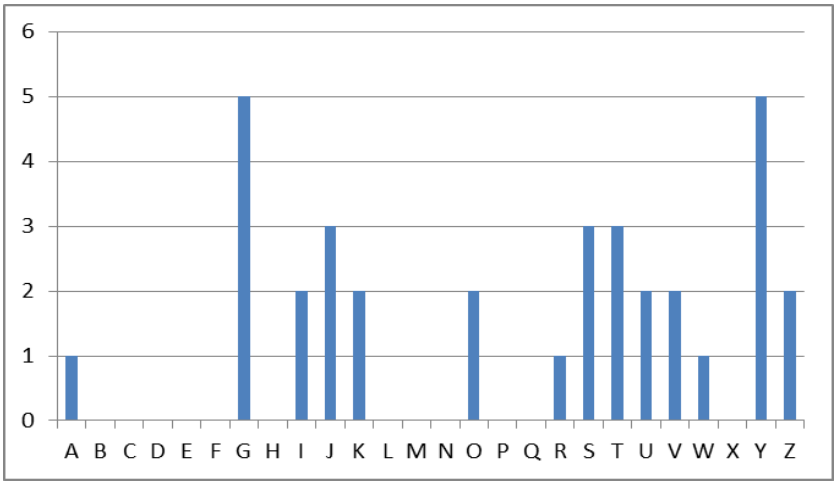
máximo divisor comum destas distâncias, sendo assim m.d.c (3,12,18) = 3, obtém-se assim o comprimento da palavra-chave.

Em seguida, é preciso analisar a frequência com que as letras se repetem, porém não no texto como um todo, a análise é feita usando a informação que se obteve sobre o comprimento da chave. Considerando que a chave tem comprimento 3, isto significa que S,Z,J,..., foram cifradas usando o mesmo valores da mesma forma I,O,O,..., ou seja, obtém-se grupos em que o valor usado para cifrar a mensagem é o mesmo, dividindo o texto em grupos de três caracteres segue que:

Grupo 1	S	Z	J	V	S	Y	T	V	Y	J	G	O	G	A	G	K	U
	S	R	J	Y	Z	T	Y	U	W	I	G	K	O	Y	I	T	G
Grupo 2	I	O	O	F	S	O	O	O	O	S	B	F	G	S	C	O	U
	D	O	C	G	S	R	G	S	I	W	G	F	R	B	O	O	Z
Grupo 3	T	D	D	Z	D	D	Z	D	X	U	P	Z	B	Y	D	Q	L
	F	Y	L	P	Z	L	L	D	P	O	A	O	L	Z	C	G	

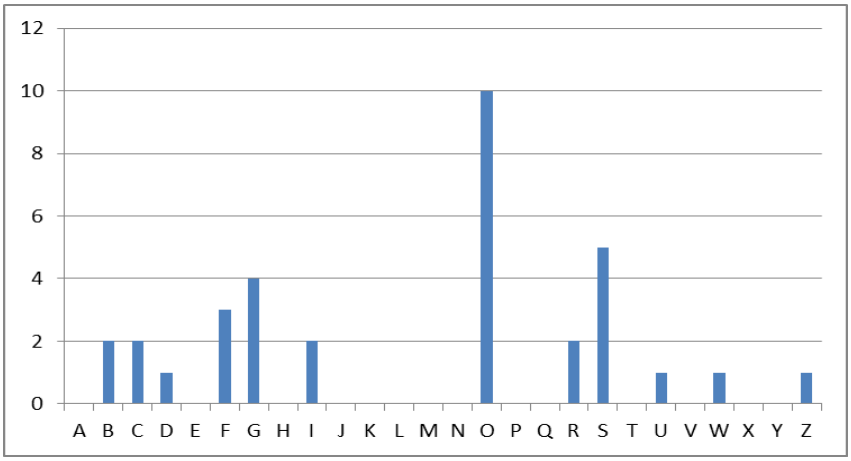
Feito a divisão por grupos, em seguida aplica-se a analise de frequência para cada grupo, sendo assim os seguintes gráficos são obtidos:

Gráfico 4: Ocorrência de letras para o grupo 1



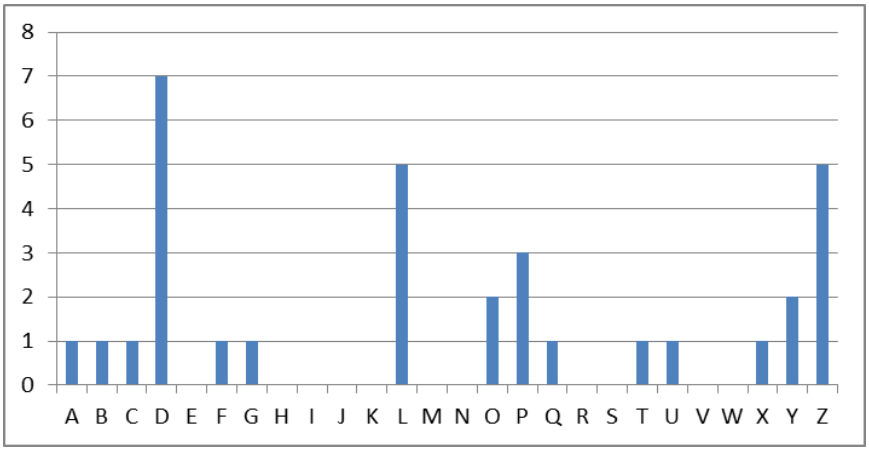
Fonte: Própria (2019)

Gráfico 5: Ocorrência de letras para o grupo 2



Fonte: Própria (2019)

Gráfico 6: Ocorrência de letras para o grupo 3



Fonte: Própria (2019)

Visto que para o grupo 2 o valor que mais se repete é O, usa-se o conhecimento adquirido anteriormente para supor que O para o grupo 2 provavelmente é a, tendo essa relação é possível obter o valor desta parte da chave fazendo 14(O) = 14(O) + 0(A), assim obtém-se o valor da chave para o grupo 2. Chegando assim no seguinte texto

S**U**TZ**A**DJ**A**DV**R**ZS**E**DY**A**DT**A**ZV**A**DY**A**XJ**E**UG**N**PO**R**ZG**S**BA**E**YG**O**DK**A**QU**G**
LS**P**FR**A**YJ**O**LY**S**PZ**E**ZT**D**LY**S**LU**E**DW**U**PI**I**OG**S**AK**R**OO**D**LY**N**ZI**A**CT**A**GG**L**

Para o grupo 1, tem-se dois valores possíveis para A, onde A pode ser G ou Y, aplicando A em Y chega-se ao valor de chave para o grupo dois como sendo 24, porém se aplicado o resultado visto no texto revela que Y não é equivalente a A, sendo assim considera-

se A como sendo G, e obtém-se que a chave do grupo 2 é 6 (G). usando o resultando o texto fica

MUT**TA**D**DA**D**PR**Z**ME**D**SA**D**NA**Z**PA**D**SA**X**DE**U**AN**P**IR**Z**AS**B**UE**Y**AO**D**EA**Q**O** **G**L**MP**F**LA**Y**DO**L**SS**P**TE**Z**ND**L**SS**L**OE**D**QU**P**CI**O**AS**A**ER**O**ID**L**SN**Z **CA**C**NA**G**AL**

Partindo do texto acima, o texto claro pode-se obter apenas por suposição de valores, sendo assim possível quebrar a cifra de Vegenère. É preciso salientar que para o caso escolhido a chave era pequena e muitas suposições foram feitas para se chegar ao valor, bem como aplicação de valores que não eram corretos, até que se chegasse a um resultado satisfatório.

3.3.4. Criptossistema RSA

Para que se obtenha a mensagem através do processo de cifrar, é preciso que se tenha os valores da chave privada, de maneira prática é difícil supor os valores que **p** e **q** partindo do valor de **n**, como se sabe **n** é um valor público, para o exemplo dado acima este é 33, assim como **b** também é público, onde **b** foi definido anteriormente como 7.

Para se encontrar o valor de **a**, e, posteriormente,, romper as defesas deste método é preciso que se tenha o valor de φ(n), que como visto anteriormente é dado por φ(n) = (p - 1)(q - 1). Para o caso visto, não é difícil supor valor para **n** e **q**, visto que se n = 33, e sabendo que p e q são primos, tem-se então que p = 3 e q = 11 ou p = 11 e q = 3. Note que não importa qual das suposições se escolha, em ambos os casos tem-se φ(n) =20, sendo assim pode-se verificar a condição que m.d.c.(b, φ(n)) = 1.

Conhecendo **b**, φ(n) e **n**, é possível então determinar o valor de a, usando a condição ab ≡ 1 mod(φ(n)), aplicando os valores já obtidos segue que a(7) ≡ 1 mod 20, desta forma não é difícil supor que um valor válido para a é 3, pois (3)(7) ≡ 1 mod 20. Ainda que não pareça devido aos valores baixos escolhidos, encontrar os valores de **p** e **q** na prática é extremamente difícil, pois estes são valores muito grandes, sendo assim ainda que se tenha o valor de **n** (que evidentemente também será um valor grande), torna-se quase impossível encontrar **p** e **q**, visto que não se tenha um algoritmo que fatore um grande valor em um produto de primos.

4. RESULTADOS E DISCUSSÕES

Neste capitulo serão discutidas as vantagens de cada métodos, além de propor um comparativo entre as cifras simétricas escolhidas, e um segundo comparativo entre as cifras simétricas e assimétricas.

No tópico anterior fez-se testes com cada um das cifras, mostrando suas fraquezas para o caso analisado, todavia este é apenas um caso dos infinitos que podem ser analisados. Por exemplo, se o texto em questão tivesse uma frequência maior de E do que de A, ou aparece mais R do que S, seriam necessário fazer-se avaliações mais demoradas e um número maior de testes até que se avaliar-se que a frequência da mensagem é diferente do que se esperava.

Voltando as análises vistas, tem-se que a cifra de César e a afim possuem vulnerabilidade devido ao seu limitado número de chave, quanto a isso não pode-se fazer nada, já que estas são limitadas por motivo matemáticos como já foi visto, contudo uma forma para se obter mais segurança no uso destas cifras seria acrescentar caracteres aleatórios que não fazem parte do texto, de modo a dificultar a análise de frequência.

Para a cifra de Vegenère, só seria necessário fazer uso de uma chave muito grande, fazendo assim com que a dificuldade de quebra-la aumentasse, uma chave que tivesse o tamanho da mensagem evitaria que as repetições da chave se alinhassem com o texto, e como a chave não precisa fazer sentido pode-se gerar caracteres aleatórios e usá-los como chave, desde que se tenha uma forma segura de se compartilhar esta chave.

Assim temos que, de maneira evidente, a superioridade entre as cifras polialfabéticas, se comparadas com as monoalfabéticas. É preciso ressaltar que esta afirmação leva em consideração os casos em que se usa os métodos de maior eficiência para a segurança, pois como visto se escolhida uma chave pequena para a de Vegenère quebra-la é tão fácil quanto quebrar a cifra monoalfabética, ou seja, conhecer o método apenas, não garante a segurança, é preciso que se tenhamos conhecimento sobre os métodos para quebrar tais cifras, para que assim, antecipemos as ações dos invasores e usemos métodos que não os permitam vencer.

Por fim, tem-se o criptossistema RSA, ainda que o exemplo visto neste trabalho seja simples, devido ao fato de se buscar apenas exemplificar o método e não usá-lo para garantir a segurança de uma informação especificamente, este é o de maior eficiência. Suas condições

tornam seu uso um pouco difícil se feito sem auxilio computacional devido a escolha de valores que garantam tais condições, assim como os valores grande que este retorna, contudo o trabalho “extra” vale a pena, visto que entre os métodos analisados este é o único que mesmo que se conheça um forma de romper sua defesa, fazê-lo não é fácil, mesmo com a ajuda de aparelhos computacionais.

Esta consideração fornece outro ponto importante, as cifras simétricas são mais inseguras, porém são mais rápidas, o processo para cifrar e decifrar uma mensagem com estas são feitos de maneira mais simples, enquanto as assimétricas possuem um processo mais demorado, mesmo ao analisar-se de maneira computacional, deste modo pode-se supor que ainda que as cifras simétricas possuam um fragilidade alta, dependendo do fim para que se quer usá-las estas podem ser úteis, pois são rápidas e praticas para serem usadas, já quando se busca maior segurança usa-se as cifras assimétricas.

5. CONCLUSÃO

Ao observar os objetivos desta pesquisa e avaliando os dados obtidos percebe-se que este trabalho contribuiu a princípio para fornecer uma outra forma de se estudar alguns conceitos matemáticos que podem parecer abstratos. Quando apresenta-se uma metodologia de estudo acerca de um conteúdo que incialmente parece complexo, como criptografia, é de grande interesse fornecer formas de aplicar de maneira prática, para que assim possibilite-se a associação do que vem sendo visto com os conceitos que já são conhecidos.

Uma vez que a diversidade dos métodos vistos amplia a forma como se observa alguns destes conceitos, o estudo fornece uma visão matemática, buscado fazê-la de forma simples e clara, sem que se deixe de lado os conceitos e teoremas necessários, sendo assim, é através da aplicação pratica que se associa tais conceitos. Ainda que seja através da matemática que se entende o funcionamento destes sistemas, ambos os conhecimentos (teoria e prática) devem sempre estarem associados, pois ainda que se entenda o funcionamento de um método usando noções matemáticas, saber quais situações pode-se aplicá-los, bem como as formas como estes podem ser comprometidos são obtidos através do conhecimento prático.

Sendo assim, continuar análise de cifras e buscar entender outros métodos podem ser de grande valor acadêmico, analisar cifras que usem métodos que diferem dos visto até

então agregarão ainda mais conhecimento, permitindo estudar outros conceitos matemáticos e entender uma diversidade de teoremas, existe um leque grande de opções de cifras que podem ser entendidas e avaliadas, podendo ser esse texto um ponto de partida para um estudo ainda maior acerca deste assunto.

REFERÊNCIAS BIBLIOGRÁFICAS

ALDEIA NUMABOA. **Frequência de ocorrência de letras no português**. Disponível em:< http://www.numaboa.com.br/criptografia/criptoanalise/310-Frequencia-no-Portugues>. Acesso em: 28/07/2019.

ALMEIDA, Paulo J. **Criptografia e Segurança**. Disponível em<http://arquivoescolar.org/bitstream/arquivo-e/195/1/CS11_12.pdf>.Acesso em: 28/07/2019.

ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **Algoritmo de criptografia RSA:** análise entre a segurança e velocidade. Disponível em:< http://sinop.unemat.br/projetos/revista/index.php/eventos/article/download/967/681>. Acesso em: 21/07/2019.

ANJOS, Leandro Terra Versiani dos. **Segurança da Informação na Programação com uso de Criptografia e Certificação Digital**. Disponível em:<https://app.uff.br/riuff/bitstream/1/5696/1/TCC_LEANDRO_TERRA_VERSIANI_DOS_ANJOS.pdf >. Acesso em: 12/05/2019.

COZZENS, Margaret; MILLER, Steven J. **The mathematics of encryption : an elementary introduction**. Providence: American Mathematical Society, 2013.

EASTTOM, Chuck. **Modern Cryptography: Applied Mathematics for Encryption and Information Security**. New York: McGraw-Hill Education, 2016.

FERGUSON, Niels; SCHNEIER, Bruce; KOHNO, Tadayoshi. Cryptography Engineering: Design Principles and Practical Applications. Indianapolis: Wiley Publishing, Inc., 2010.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**. Disponível em:< https://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf>. Acesso em: 21/07/2019.

GUIMARÃES, Carla Rocha. **Criptografia para Segurança de Dados**. Disponível: <http://www.computacao.unitri.edu.br/downloads/monografia/79431146079328.pdf>. Acesso em: 12/05/2019.

LIMA, Naila Nayane de. **Impacto de mudanças de gestão no ambiente de trabalho:** estudo de caso numa instituição de ensino situada nazona rural da cidade de Caraúbas/RN [mensagem pessoal]. Mensagem recebida por <andersonpicass19@gmail.com>.em 24 jul. 2019.

MARTINS, Ana Margarida da Gama Correia. **Elementos de Criptologia:** uma aplicação da Álgebra. Disponível em:< http://repositorium.sdum.uminho.pt/handle/1822/4684 >. Acesso em: 28/07/2019.

PACHECO, Federico. **Criptografía**. 1 ed. Buenos Aires: Fox Andina, 2014.

PELLEGRINI, Jerônimo C. **Introdução à Criptografia e seus Fundamentos**. Disponível em:<http://aleph0.info/cursos/ic/notas/cripto.pdf>. Acesso em: 12/05/2019.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. Tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi Messeder Barreto, Rafael Misoczki. 6 ed. São Paulo: Pearson Education do Brasil, 2015.

TANENBAUM, Andrew S. ; WETHERALL, David. **Redes de computadores**. Tradução de Daniel Vieira; revisão técnica: Isaías Lima. 5 ed. São Paulo: Pearson Prentice Hall, 2011.

MINISTÉRIO DA EDUCAÇÃO
Universidade Federal Rural do Semi-Árido - UFERSA
CAMPUS DE CARAÚBAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Às 17:00 horas do dia 14 de agosto do ano de 2019, na Sala 8 do Bloco de Aulas II da Universidade Federal Rural do Semi-árido – UFERSA (Campus Caraúbas), sob a presidência da professora Profª. Dra. Mariana de Brito Maia, reuniu-se a Banca Examinadora de defesa de monografia de autoria do aluno **Anderson Picasso Linhares da Silva,** aluno do curso de Bacharelado em Ciência e Tecnologia desta Universidade, com o título ***"A matemática como ferramenta de estudo para a criptografia".*** A Banca Examinadora ficou assim constituída: Profª. Dra. Mariana de Brito Maia, presidente da banca e orientadora da monografia; Prof. Me. Antônio Alisson Alencar Freitas, co-orientador; Prof. Dr. Tony Kleverson Nogueira e Profª. Dra. Rosilda Sousa Santos. Foram registradas as seguintes ocorrências: _____. Concluída a defesa, procedeu-se o julgamento pelos membros da banca examinadora, em reunião fechada, tendo o aluno obtido as seguintes notas: 9,5; 9,5; 9,5; 9,5. Apuradas as notas verificou-se que o aluno foi aprovado com *média geral* 9,5, fazendo jus, portanto, ao título de Bacharel em Ciência e Tecnologia. E para constar, eu, Profª. Dra. Mariana de Brito Maia, lavrei a presente ata que, após lida e aprovada pelos membros da banca examinadora, será assinada por todos. Caraúbas, 14 de agosto de 2019.

Assinatura dos membros da Banca Examinadora.

Mariana de Brito Maia
Profª. Dra. Mariana de Brito Maia – Presidente

Antônio Alisson Alencar Freitas
Prof. Me. Antônio Alisson Alencar Freitas - Membro

Tony Kleverson Nogueira
Prof. Dr. Tony Kleverson Nogueira - Membro

Rosilda Sousa Santos
Profª. Dra. Rosilda Sousa Santos - Membro