COLÉGIO ÍTACA

MICHEL MISKULIN CARNEIRO

Criptografia e Crise Criptográfica

São Paulo

2022

MICHEL MISKULIN CARNEIRO

Criptografia e Crise Criptográfica

Trabalho monográfico apresentado no segundo ano do ensino médio do Colégio Ítaca

Orientadora: Professora Marilia Prado

São Paulo

2022

AGRADECIMENTOS

À professora Marilia Prado, que me orientou, ajudou e permitiu a construção desse trabalho.

À professora Cecília Jorquera, pelas aulas de iniciação científica, coordenação do projeto e auxílio na monografia.

Aos meus pais, que me ajudaram na construção desse trabalho, me apoiaram nos momentos difíceis e sempre suportam minhas decisões e desejos.

RESUMO

Criptografia é um conjunto de técnicas utilizadas para ocultar informações, que podem ser recuperadas posteriormente. O objetivo dessa pesquisa é explicar a história da criptografia, evidenciando o algoritmo criptográfico moderno RSA. Outro ponto focado é esclarecer o futuro desse algoritmo perante as evoluções tecnológicas e computacionais que estamos vivendo. Este trabalho foi realizado de forma bibliográfica, utilizaram-se artigos científicos, trabalhos acadêmicos, livros e documentos. A partir da pesquisa, verificou-se que a criptografia teve uma grande relevância em diversas culturas ao longo da história e que seu papel é crucial para o mundo atual, pois ela compões os alicerces do funcionamento da internet. Além disso, observou-se que, devido ao avanço de tecnologias como computação quântica, o algoritmo RSA não será seguro no futuro. Apesar da segurança do RSA não ser suficiente para um futuro com computação quântica desenvolvida, diversos países, empresas e ONGs estão tomando ações para fazer uma transição para um algoritmo seguro. Essas ações são importantes, pois impedem uma crise criptográfica, em que o algoritmo RSA consegue ser descriptografado por pessoas não autorizadas, o que criaria um grande impacto negativo no mundo.

Palavras-chave: Criptografia; RSA; Crise Criptográfica

ABSTRACT

Encryption is a set of techniques used to hide information, which can be retrieved later. The objective of this work is to explain the history of cryptography, highlighting the modern cryptographic algorithm RSA. Another focused point is to clarify the future of this algorithm in the face of the technological and computational developments that we are experiencing. This work was carried out in a bibliographic way, using scientific articles, academic works, books, and documents. From the research, it was found that cryptography has had great relevance in different cultures throughout history and that its role is crucial for the current world, as it forms the foundations of the internet. Furthermore, it was observed that due to the advancement of technologies such as quantum computing, the RSA algorithm will not be secure in the future. Although the security of RSA is not enough for a future with advanced quantum computing, several countries, companies, and NGOs are taking action to make a transition to a secure algorithm. These actions are important as they prevent a cryptographic crisis where the RSA algorithm manages to be decrypted by unauthorized people, which would create a big negative impact on the world.

Keywords: Encryption; RSA; Cryptographic Crisis

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A criptografia emprega um enorme papel no mundo atual. Sua importância é gigante e ela é crucial para o funcionamento de nossa sociedade. Este conjunto de técnicas para ocultar e recuperar informações vem sendo utilizado por diversas sociedades e culturas diferentes há muito tempo, seu uso era evidenciado em guerras e batalhas, em que a informação passava a ter um valor importante para a vitória.

Hoje em dia, a criptografia é fundamental no funcionamento da internet. Qualquer ação realizada nessa rede utiliza algum tipo de criptografia para garantir a segurança dos dados ao transitarem de um computador para outro. Sem criptografia não há internet como conhecemos.

Um dos algoritmos mais importantes da criptografia moderna é o RSA. Devido a sua segurança e importância, ele é utilizado em diversas aplicações e sistemas. Este algoritmo é seguro no mundo em condições atuais, porém o avanço tecnológico está ameaçando essa segurança. Tecnologias como a computação quântica mostram-se como um problema para o RSA, pois essa tecnologia, se consolidada, multiplicaria a capacidade computacional atual, o que permitiria ataques ao algoritmo.

Este trabalho procura analisar a história da criptografia, ressaltando a importância dessa técnica ao mostrar sua coexistência em diferentes sociedades. O surgimento e funcionamento do RSA serão explicados, para isso os conceitos-chave presentes na criptografia serão esclarecidos.

Além disso, tem-se como objetivo mostrar os aspectos de uma crise criptográfica, causada pela quebra da criptografia do RSA, decorrente da evolução da tecnologia. Também serão apresentadas as ações que estão sendo tomadas por países, empresas e ONGs para evitar tal crise.

Esta pesquisa foi feita de forma bibliográfica, fontes como livros, trabalhos acadêmicos, documentos e artigos científicos serão analisados e estudados. Com isso, o trabalho ensinará o leitor sobre criptografia, para lhe apresentar a problemática que a humanidade enfrenta: a mudança para a criptografia pós-quântica.

2 DEFINIÇÃO E HISTÓRIA DA CRIPTOGRAFIA

Neste capítulo veremos a definição de criptografia, seu surgimento na história e duas criptografias clássicas muito usadas na história da humanidade. Explicaremos o conceito de criptografia de substituição monoalfabética e substituição polialfabética. Também explicaremos a distinção entre criptografia simétrica e assimétrica com uma breve menção no algoritmo RSA, que será estudado no capítulo seguinte.

2.1 SURGIMENTO DA CRIPTOGRAFIA

A capacidade de se comunicar de forma complexa é uma das maiores habilidades do ser humano. Com a presença de uma comunicação tão rica e relações sócias complexas, é natural a presença de informações confidenciais a certos indivíduos. De forma a resguardar esses segredos foi necessária a criação de técnicas para mascarar as informações, isto é, técnicas de criptografia.

Segundo Darci Dala Costa (2014, p. 1) criptografia é um “termo cuja origem vem do grego, kryptós (escondido), gráphein (escrita)”. Essa palavra é usada para caracterizar as técnicas utilizadas para transformar uma mensagem em um texto ilegível, que pode ser transformado de volta na mensagem pelo uso de certo método característico da técnica.

A origem da criptografia é incerta, segundo Costa (2014), um dos primeiros exércitos ocidentais a utilizar a técnica foram os espartanos, há mais de 2500 anos. A explicação de Costa não é aceita por todos os autores, existem outras explicações sobre a origem da técnica:

> Segundo Kahn (1967)[1], o primeiro exemplo documentado da escrita cifrada aconteceu aproximadamente no ano de 1900 a.C, quando o escriba de Khnumhotep II[2] teve a ideia de substituir algumas palavras ou trechos de texto. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro e morreria de fome perdido nas catacumbas da pirâmide (ORDONEZ; CHIARAMONTE; PEREIRA; 2005, p. 12).

O livro *RSA and public-key cryptography*, de Richard A Mollin explica outra versão do surgimento da criptografia, também vinda dos egípcios:

1 KAHN, David., The Codebreakers. Macmillan, 1967.

2 Khnumhotep II foi governador de uma província do Egito no século XX a.C

> O primeiro registro de uma técnica criptográfica está escrito em uma pedra de quase quatro milênios atrás, escrita por um escriba egípcio que usou a substituição de símbolos hierográficos na escritura de uma parede de pedra na tumba de um nobre de seu tempo, Khnumhotep (MOLLIN, 2003, p. 2, tradução nossa).[3]

O surgimento da criptografia é incerto e tem várias versões, isso acontece, pois informações confidências estão presentes em diversas culturas diferentes, e junto destas, estão presentes técnicas de criptografia para ocultá-las, conforme discorremos a seguir.

2.2 CRIPTOGRAFIA MONOALFABÉTICA

As técnicas criptográficas são importantes para manter a confidencialidade de segredos, porém é nas guerras que sua real importância é mostrada. Antigamente, a comunicação do exército era feita usando de mensageiros, se estes fossem capturados as informações cairiam nas mãos dos inimigos, portanto mascará-las era fundamental para a vitória. O imperador romano Júlio César estava ciente disso e criou uma técnica simples, porém efetiva para criptografar suas informações.

Para nos explicar a técnica criada pelo imperador, Mollin cita a biografia de Júlio César, escrita por Suetonius Tranquillus[4]:

> No livro *The Lives of the Twelve Caesars*, Suetonius escreve sobre Júlio Caesar: … se houvesse ocasião para segredo, ele escrevia com cifras; isto é, ele usava o alfabeto de uma maneira, que nem uma única palavra conseguia ser entendida. O método para decifrar era substituindo a quarta pela primeira letra, ‘d’ virava ‘a’, fazendo isso para as outras letras respectivamente (TRANQUILLUS, 1978, p.45 apud MOLLIN, 2003, p. 1, tradução nossa).[5]

A técnica criada por Júlio César consistia em trocar cada letra da mensagem, pela terceira letra depois dessa no alfabeto. Se uma palavra como ‘GUERRA’ fosse

3 No original: “The first recorded instance of a cryptographic technique was literally written in stone almost four millennia ago by an Egyptian scribe who used hieroglyphic symbol substitution in his writing on a rock wall in the tomb of a nobleman of the time, *Khnumhotep*.”

4 Suetonius Tranquillus foi um historiador e escritor que viveu durante o Império Romano, sua obra mais importante é a biografia de Júlio César.

5 No original: “In *The Lives of the Twelve Caesars*, Suetonius writes of Julius Caesar: “... if there was occasion for secrecy, he wrote in cyphers; that is, he used the alphabet in such a manner, that not a single word could be made out. The way to decipher those epistles was to substitute the fourth for the first letter, as d for a, and so for the other letters respectively.””

criptografada usando a cifra de César ela ficaria escrita como ‘JXHUUD’. A figura 1 mostra como cada letra fica após a criptografia ser aplicada.

Figura 1 – Cifra de César

Antes	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
Depois	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

Fonte: Autor

Ao ser empregada na guerra, essa técnica se mostrou muito útil. Quando usada em uma mensagem, se o inimigo não tivesse conhecimento da técnica, não entenderia palavra nenhuma, porém se a mensagem chegasse ao real destinatário, este conseguiria descriptografar a mensagem fazendo a ação reversa, trocando as letras por suas antecedentes.

A cifra de César não é limitada pela mudança da letra pela terceira posterior do alfabeto. O número do deslocamento das letras não precisa ser 3, este número é arbitrário e a única exigência é que o remetente e o destinatário da mensagem precisam estar em consenso sobre o valor. Como o alfabeto tem somente 26 letras, existe 25 variantes da cifra.

Essa técnica foi útil por certo tempo, porém ao ser popularizada, ela perdeu sua eficácia. Se o inimigo conhecesse o método de criptografia, ele poderia descriptografar a mensagem, pois como existem 25 possíveis variantes, existia a possibilidade de testá-las todas, isso demoraria, porém seria um método viável.

Segundo Costa (2014) esses tipos de criptografia denominados códigos de substituição monoalfabéticos eram muito utilizados até o século IX, quando o cientista árabe Al-Kindi descobriu uma maneira de descriptografá-los usando da frequência em que as letras são usadas na língua.

Como foi visto na cifra de César[6], a criptografia de substituição monoalfabética é caracterizada pela troca de símbolos na frase, cada letra ganha um novo símbolo ou outra letra para representá-la. Esse método contém uma grave falha que foi explorado por Al-Kindi.

6 A cifra de César também foi base para uma série de outras criptografias de substituição monoalfabéticas, e outras versões mais complexas.

Nas línguas que utilizam de alfabetos, certas letras são usadas muito mais que outras. Analisando um texto, pode-se observar que a letra ‘A’ e a letra ‘E’ são as duas mais usadas na língua portuguesa, portanto ao analisar a mensagem criptografada, pode-se assumir com bastante confiança que o símbolo mais usado será um ‘A’ ou um ‘E’, utilizando dessa análise pode-se quebrar com facilidade qualquer técnica de substituição monoalfabética.

2.3 CRIPTOGRAFIA POLIALFABÉTICA

Após a descoberta do cientista Al-Kindi, as criptografias de substituição monoalfabéticas não poderiam mais ser usadas, pois havia um método sólido para descriptografar qualquer técnica. O próximo marco da história da criptografia foi feito por Blaise de Vigenère, Costa (2014) nos explica que no final do século XVI Vigenère escreveu um livro chamado *Traité des chiffres ou secrètes manières d’écrire*, onde descrevia as técnicas criptográficas mais utilizadas de sua época. Em seu livro, estava presente a técnica proposta por Giovan Batista Belaso que levou o nome de cifra de Vigenère[7].

Ao contrário do método de Júlio César, a cifra de Vigenère foi utilizada por muito tempo sem ser descriptografada, esse novo método era uma criptografia do tipo polialfabética[8], pois cada letra é substituída de forma diferente conforme sua posição na palavra. A cifra de Vigenère era considerada como indecifrável, Costa (2014) nos diz que somente 300 anos após sua invenção foi descoberto um método para descriptografá-la.

A cifra de Vigenère durou muito mais tempo que as anteriores, isso aconteceu devido a forma que as letras eram criptografadas. A técnica utiliza como base uma figura (Figura 2) chamada quadrado de Trithemius, que foi proposta pelo abade João Trithemius para a realização de outros métodos criptográficos.

Figura 2 – Quadrado de Trithemius

7 Apesar de ter sido criada por Giovan Batista Belaso, a criptografia levou o nome de Vigenère pois foi este o responsável por sua popularização.

8 Classificação de Darci Dala Costa (2014, p. 3)

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Fonte: ResearchGate[9]

Na Figura 2 vemos o quadrado de Trithemius que serviu de base para a cifra de Vigenère. Para começar a criptografar uma mensagem, devera ser decidida previamente uma chave, isto é, uma palavra que será usada para realizar a criptografia e descriptografia. A chave é o que garantirá a descriptografia da mensagem quando esta chegar ao seu destino, portanto deve estar sob conhecimento tanto do remetente quanto do destinatário.

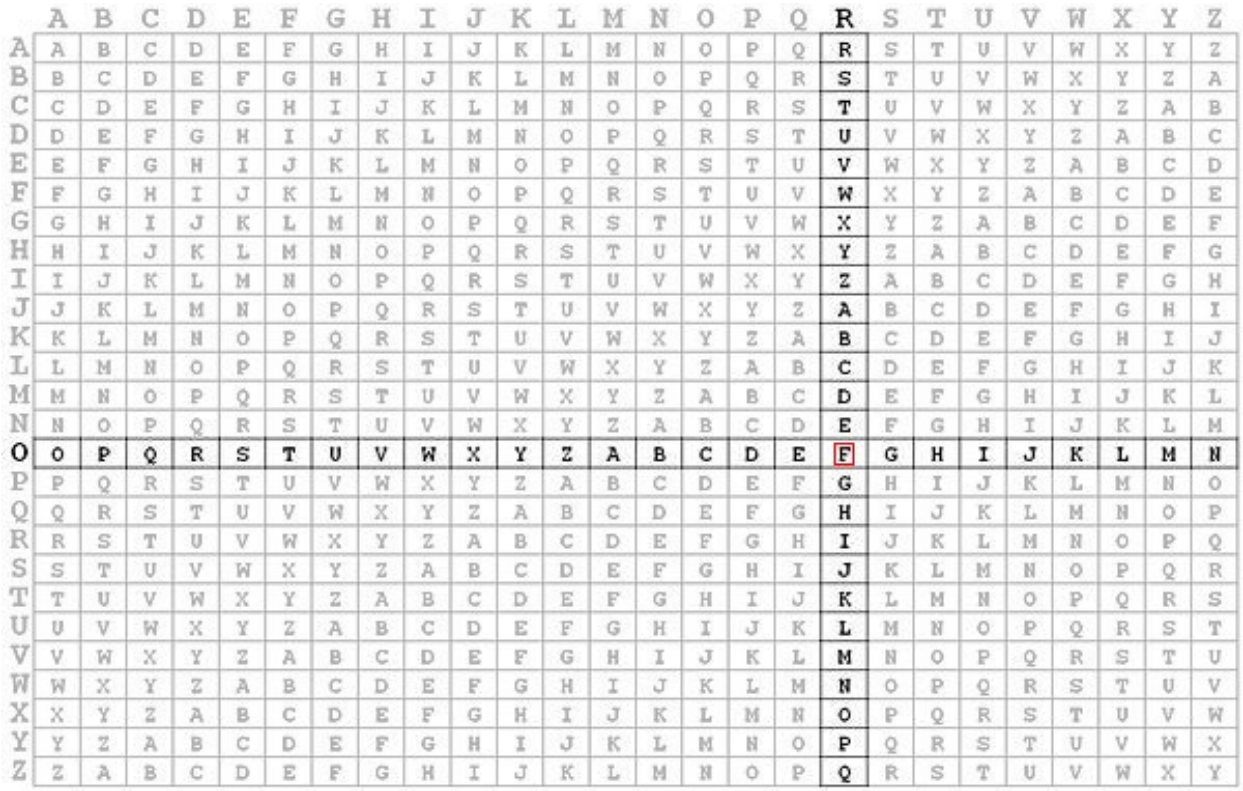
Para realizar a criptografia, a palavra-chave escolhida será ‘OBJETO’, e a palavra a ser criptografa será ‘RECUAR’. Criptografaremos letra por letra da palavra ‘RECUAR’, para isso, olhamos a coluna que tem a primeira letra da palavra, isto é, a coluna que começa com a letra ‘R’, após isso, olhamos a linha que tem a primeira letra da chave, isto é, a linha que começa com a letra ‘O’. A letra em que a linha e a coluna se encontrarem será a primeira letra da mensagem criptografada.

A figura 3 mostra o processo feito para a primeira letra, em que encontramos a letra ‘F’. Para continuar o método devemos fazer o mesmo processo com a letra seguinte. Encontramos a coluna que começa com a letra ‘E’ (segunda letra da palavra ‘RECUAR’),

9 Disponível em: https://www.researchgate.net/figure/The-Original-26-26-Vigenere-table-13-The-encryption-equation-E-for-a-Vigenere_fig1_342474014 Acesso em: 5 jun. 2022.

e encontramos a linha que começa com a letra ‘B’ (segunda letra da palavra ‘OBJETO’), a letra onde essa linha e coluna se encontrar será a segunda letra da mensagem criptografada. Fazendo isso para todas as letras da palavra ‘RECUAR’, conseguimos realizar a criptografia.

Figura 3 – Exemplo de criptografia usando o quadrado de Trithemius



	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Fonte: Autor

Com a mensagem criptografada ‘FFLYTF’ e chave ‘OBJETO’ em mãos, o destinatário localizará no quadrado de Trithemius a linha que contem a primeira letra da chave, isto é, a linha que começa com a letra ‘O’. Ele procurará nesta linha a letra ‘F’, a primeira letra da mensagem criptografada, e anotará em que coluna esta letra se encontra, fazendo isso, ele achará a coluna com a letra ‘R’, conforme a Figura 3. Fazendo isso para todas as letras da mensagem criptografada, ele consegue reverter a criptografia, chegando na palavra RECUAR.

Figura 4 – Cifra de Vigenère

Mensagem	R	E	C	U	A	R
Chave	O	B	J	E	T	O
Mensagem Criptografada	F	F	L	Y	T	F

Fonte: Autor

A figura 4 mostra a mensagem, após todas as letras terem sido individualmente criptografadas. Nossa mensagem criptografada é ‘FFLYTF’ e se alguém mal-intencionado interceptar a mensagem, mesmo tendo amplo conhecimento sobre o funcionamento da cifra de Vigenère, se não tiver conhecimento da chave, não conseguirá realizar a descriptografia. Se a mensagem criptografada chegar em seu destinatário, este utilizara a chave para fazer o processo reverso e recuperar o texto original.

A cifra de Vigenère era uma criptografia muito sólida, um de seus únicos defeitos era que a chave precisava ser do mesmo tamanho da mensagem. Para corrigir esse defeito, quando a criptografia de uma frase ou texto eram necessários, era definida a palavra-chave, que era então repetida até conseguir o tamanho ideal. Se a frase ‘ATACAR AO AMANHECER’ fosse ser criptografada e a chave fosse a palavra ‘OBJETO’, na hora de realizar a criptografia e descriptografia, se usaria a frase ‘OBJETOOBJETOOBJET’, composta pela palavra objeto repetida de forma que as duas frases tenham o mesmo número de letras.

2.4 CRIPTOGRAFIA ASSIMÉTRICA

Tanto na criptografia de Júlio César, como na de Vigenère fomos apresentados com o conceito de chave. Na cifra de César a chave é o número correspondente ao deslocamento das letras no alfabeto, já na cifra de Vigenère a chave é uma palavra qualquer.

O conceito de criptografia é intrínseco ao de chave criptográfica. Segundo Ordonez, Chiaramonte e Pereira (2005, p. 17) “A chave protege a informação cifrada. Para decifrar o texto cifrado o algoritmo deve ser alimentado com a chave correta, que é única” A chave criptográfica é o que garante a proteção da mensagem, portanto é vital mantê-la em segredo.

Nos dois métodos criptográficos vistos, existe apenas uma chave que funciona tanto para criptografar, como para descriptografar. Os métodos que utilizam somente uma

chave fazem parte do conjunto de criptografias simétricas. Como essas técnicas utilizam da chave para realizar a descriptografia, o remetente e o destinatário precisam estar em consenso sobre a chave para que a criptografia funcione.

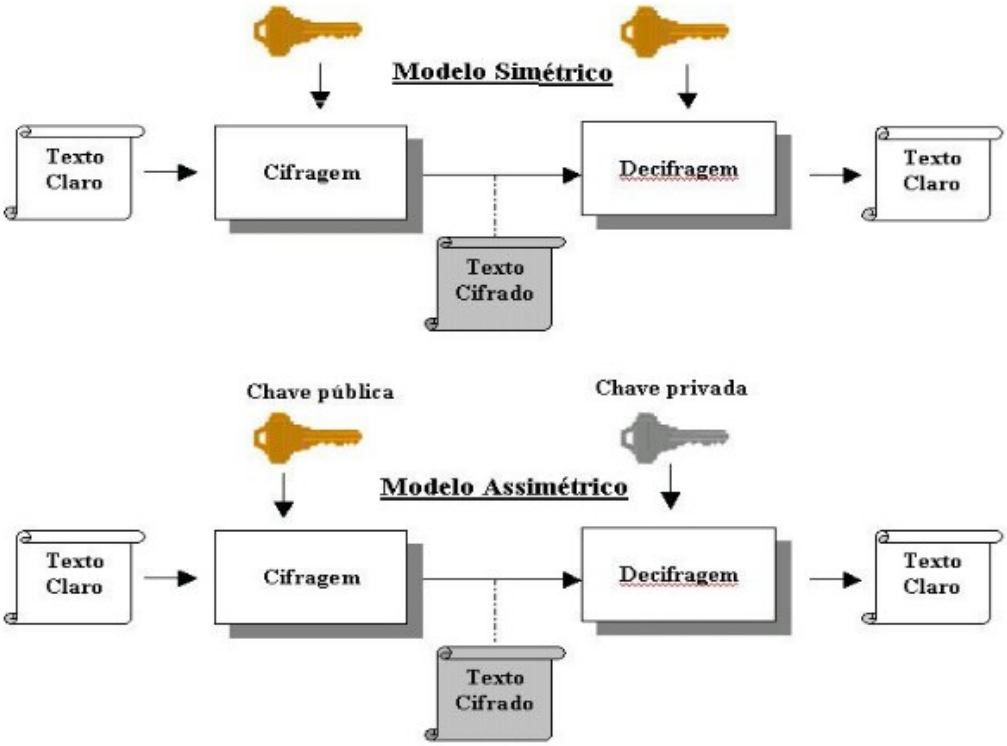
A criptografia existe para que caso haja interceptação da mensagem, seu conteúdo seja ininteligível, porém se a chave for decidida por um meio de comunicação suscetível a interceptação, o uso da criptografia com essa chave será sem propósito, pois não se poderia ter certeza de sua confiabilidade. A decisão da chave precisa ser feita em um local seguro sem interceptação de mensagens, isto é, o mundo real. Em todos os meios de comunicação à distância, não se pode ter absoluta certeza sobre o que acontece com a mensagem no meio do trajeto, porém no mundo real, existe total conhecimento sobre o que está acontecendo enquanto ocorre a troca de informações. O mundo real é o único método seguro para a troca de informação sem criptografia.

As criptografias simétricas funcionavam muito bem para seus propósitos enquanto a comunicação era mais restrita, porém com o advento das técnicas de comunicação à distância, elas foram ficando cada vez mais inconvenientes. Ter que se encontrar pessoalmente com o destinatário para combinar a chave era um empecilho muito grande, e para solucionar esse problema, surgiram as criptografias assimétricas.

A criptografia assimétrica foi inventada em 1976 por Whitfield Diffie e Martin Hellmané. Nesse tipo de criptografia existem dois tipos distintos de chave, uma chave responsável por criptografar a mensagem e outra responsável por descriptografar. A chave usada para criptografar é chamada de chave pública, pois ela é transmitida publicamente para qualquer um. Já a chave responsável pela descriptografia é chamada de chave privada, pois é mantida em segredo.

Se alguém quiser mandar uma mensagem para certo indivíduo usando de chaves públicas e privadas, ele usará a chave pública para criptografar a mensagem. Esta mensagem poderá ser enviada usando qualquer meio de transmissão, pois se alguém interceptá-la, não conseguirá ler o conteúdo. Quando a mensagem chegar no destinatário este usará sua chave privada para descriptografar a mensagem. A chave pública criptografa e a privada descriptografa. A figura 5 exemplifica esse processo.

Figura 5 – Modelo simétrico e assimétrico de criptografia



Fonte: ORDONEZ, CHIARAMONTE, PEREIRA (2005, p. 29)

A chave pública e a chave privada são duas chaves diferentes, porém são ligadas de forma matemática, permitindo que uma seja usada somente para criptografar e a outra somente para descriptografar. Um indivíduo que quer utilizar da criptografia assimétrica utiliza de um algoritmo[10] para gerar estas duas chaves, as chaves geradas são únicas e pertencem somente a este indivíduo, após isso ele guarda sua chave privada em local seguro, e informa a chave pública para a pessoa se comunicará com ele.

Essa ideia inovadora de criptografia assimétrica foi incorporada por professores do MIT no algorítimo chamado RSA. Nas palavras de Costa (2014, p. 46), o RSA é “um dos métodos de criptografia mais seguro de todos os tempos, utilizado por governos e empresas do mundo inteiro.” O funcionamento desse algoritmo será explicado em detalhes no próximo capítulo.

10 Algoritmos são uma sequência de comandos e instruções que o computador realiza. Neste caso os comandos são uma série de operações matemáticas que geram as chaves públicas e privadas.

3 FUNCIONAMENTO DO RSA E CRISE CRIPTOGRÁFICA

Neste capítulo veremos a história e surgimento do RSA, o funcionamento e principais conceitos matemáticos que tornam esse algoritmo possível, a influência da computação quântica na criptografia moderna, o futuro da criptografia perante os avanços tecnológicos e as ações que estão sendo tomadas para mitigar uma possível crise criptográfica.

3.1 SURGIMENTO DO RSA

Como foi dito no capítulo anterior, o RSA é um algoritmo que incorpora a ideia de chave pública e privada, um algoritmo desse tipo resolveria diversos problemas causados pela longa distância de comunicação, portanto estava sendo campo de pesquisas na época. Os professores Ronald Rivest e Adi Shamir, do MIT e o professor Leonard Adleman, da USC triunfaram na criação de um algoritmo desse tipo em 1977, surgindo assim o RSA. O nome do algoritmo vem da primeira letra do sobrenome de cada um deles. Apesar de ter sido criado 45 anos atrás, ele vem sendo usado até hoje e é um dos pilares da criptografia.

O conceito de criptografia pública e privada que havia sido criado em 1976 por Whitfield Diffie e Martin Hellmané se mostrou revolucionador, porém ainda não existia um algoritmo capaz de utilizar esses conceitos de forma funcional. O RSA surgiu com esse objetivo. Os criadores buscavam criar um algoritmo funcional, eficiente e seguro que utilizava-se do conceito criado. De acordo com Calderbant (2007), a criação do algoritmo teve um avanço repentino em uma noite em que Rivest não conseguia dormir. Ele estava com insônia, quando pensou no algoritmo e teve uma intuição de como finalizá-lo, com isso ele passou o resto da noite formalizando e provando sua ideia. No amanhecer ele tinha um artigo científico quase completo.

Segundo Robinson (2003), Adleman foi outro professor que trabalhou na criação do algoritmo do RSA ajudando Rivest, após a publicação do artigo sobre o RSA, ele não estava confiante sobre o trabalho. Ele achou que o algoritmo havia sido a coisa menos importante que havia publicado e que ninguém leria a publicação. Ele estava errado sobre isso, pois o RSA foi publicado em um jornal importante e o interesse gerado pela criação foi extremamente grande.

A história do RSA é anormal, sua criação é consequência do surto de inspiração um de seus criadores, não era esperado que esse algoritmo se tornasse um dos mais importantes para a criptografia, porém ele vem funcionando por décadas, isso só é possível graças a matemática por trás da programação do algoritmo.

3.2 NÚMEROS PRIMOS E ARITMÉTICA MODULAR

Antes do funcionamento do RSA ser explicado, alguns conceitos matemáticos precisam ser esclarecidos. Números primos são um conceito central da teoria dos números, eles têm vital importância para a criptografia e o RSA utiliza-os para criar as chaves. Números primos são números naturais maiores que 1 e que não são produto de outros números naturais maiores que 1. Por exemplo, o número 6 não é primo, pois ele pode ser obtido pelo produto de 2 e 3. Já o número 11 é um número primo, pois não há produto de número natural maior que 1, que forme o número 11. Foi provado pelo matemático grego Euclides que existem infinitos números primos, no RSA são utilizados números primos com centenas de algarismos de forma a aumentar sua segurança.

Outro conceito matemático utilizado no RSA é a aritmética modular, apesar do nome parecer complexo, essa aritmética se baseia no que chamamos “resto” em uma divisão convencional. Quando se divide 7 por 3, obtemos o resultado 2, com resto de 1, esse resto é o que procuramos na aritmética modular. Com isso foi criado o operador modular “mod”, que é uma forma de indicarmos que faremos uma divisão, porém o resultado será o resto. Do exemplo descrito, podemos escrever, 7 mod 3 = 1.

A aritmética modular é útil para criptografia pois dado o resultado de uma função, não conseguimos descobrir seus parâmetros iniciais. Da mesma forma que 7 mod 3 = 1, 10 mod 3 = 1. As duas equações têm o mesmo valor, entretanto os números que as compõem são diferentes. Com isso, se alguém disser que obteve o valor 1, de uma função f(x) = x mod 3, não saberemos qual o valor de x. Esse princípio é usado para garantir o funcionamento do RSA.

3.3 FUNCIONAMENTO DO RSA

Como já foi dito, o RSA é um algoritmo de criptografia assimétrica, pois utiliza uma chave para criptografar a mensagem e outra para descriptografar. Esse conceito de

chaves criptográficas aparenta ser abstrato, porém existe um exemplo cotidiano que se utiliza disso. Em uma caixa de correspondências qualquer pessoa pode deixar uma carta, porém só o dono da caixa tem sua chave e pode abri-la para coletar as correspondências. Dessa forma, quando deixamos uma carta na caixa de alguém, sabemos que só aquela pessoa tem acesso à mensagem. O mesmo acontece com as chaves públicas e privadas: deixar uma carta dentro da caixa equivale a criptografar uma mensagem com a chave pública, e abrir essa caixa para ler a carta equivale a descriptografar a mensagem com a chave privada.

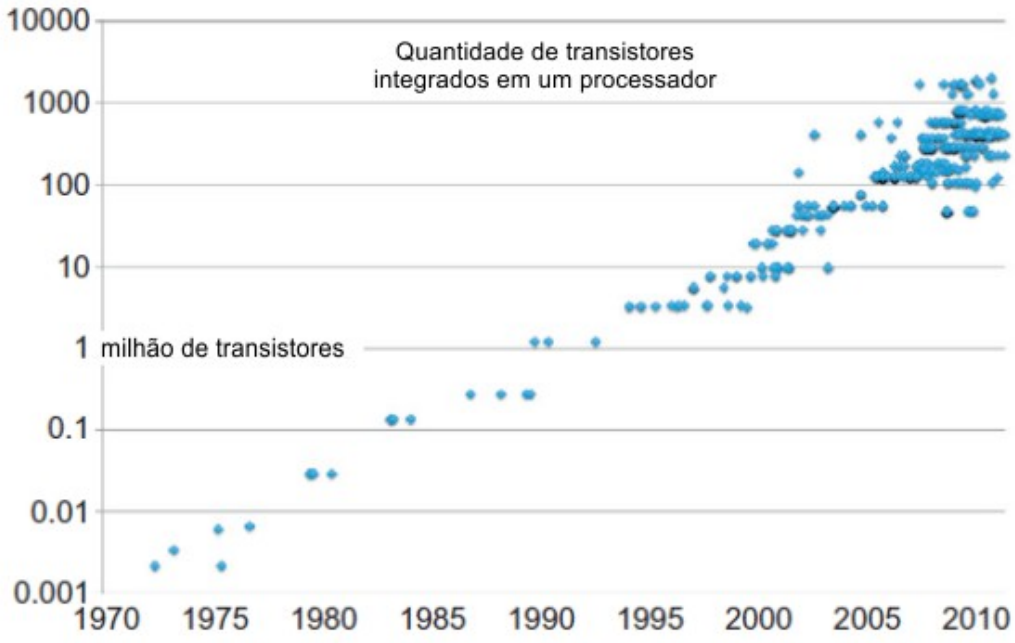
No mundo físico existem chaveiros que conseguem abrir uma fechadura sem utilizar a chave original, porém isso não pode acontecer no RSA. Para garantir a segurança das chaves são utilizados números primos. Ao gerar as chaves, são escolhidos dois números primos extremamente grandes, esses números são então multiplicados e se forma um novo número “n”. Esse número “n” faz parte da chave pública, e os dois números primos originais fazem parte da chave privada. Dessa maneira, quando alguém obtém acesso ao número “n”, esta pessoa não sabe quais são os números originais que fizeram o número “n” - quem tem acesso à chave pública não tem acesso à chave privada. As duas chaves estarem ligadas matematicamente pela multiplicação dos dois números primos faz com que, a partir do uso de equações da aritmética modular, a criptografia e descriptografia da mensagem sejam possíveis.

3.4 CRIPTOGRAFIA PÓS RSA

Quando usado de forma ideal, o RSA nunca apresentou falhas. Esse algoritmo permite a troca de mensagens totalmente criptografadas e não pode ser quebrado, entretanto essa segurança está sendo ameaçada. Como a figura 6 mostra, a capacidade computacional – diretamente ligada com a quantidade de transistores[11] em um processador – aumentou imensamente desde a criação do RSA.

Figura 6 – Quantidade de transistores integrados em um processador

11 Transistor é um microcomponente do processador responsável por seu funcionamento. Cada processador tem bilhões de transistores, que ao serem ligados entre si formam circuitos complexos.



Fonte: ResearchGate[12]

O aumento da capacidade computacional está aumentando de forma linear. Para acompanhar esse aumento, ocorreu uma ampliação no tamanho dos números que compõem o algoritmo, de forma a continuar mantendo-o seguro, porém isso pode não ser suficiente para o futuro. A computação quântica é um novo conceito que promete aumentar imensamente a capacidade computacional.

Utilizando da física quântica, cientistas estão desenvolvendo esse novo tipo de computação. Ela se baseia em um novo tipo de bit[13], o qubit, que utiliza estados de sobreposição quântica e outras propriedades da física quântica. Com isso o qubit não é limitado aos valores binários do bit convencional.

Esse novo tipo de arquitetura computacional está criando processadores muito mais velozes que os convencionais. Em 2019, os cientistas do Google, Arute *et al*. (2019) publicaram na revista “Nature” que seu computador quântico realizou, em 200 segundos, um cálculo que demoraria, em um computador convencional, 10000 anos. Essa afirmação foi cercada de controvérsia, porém é inegável que a computação quântica ameaça os algoritmos atuais.

---

12 Disponível em: https://www.researchgate.net/figure/Figura-1-Grafico-da-evolucao-da-quantidade-de-transistores-integrados-em-um_fig3_267393184 Acesso em: 10 set. 2022.

13 Bit é a menor unidade de informação de um computador, o bit representa um estado binário de verdadeiro ou falso, ligado ou desligado.

Se a pesquisa em computadores quânticos continuar a avançar e os novos computadores quânticos se consolidarem, devido à capacidade computacional muito maior, não será suficiente aumentar os números do RSA para torná-lo seguro. Será necessário criar um outro algoritmo, seguro para computadores quânticos, se isso não for feito, haverá uma crise na internet.

Hoje em dia a internet é vital para o funcionamento da sociedade, trilhões de dólares são movimentados com sua ajuda e seu funcionamento é crucial para a economia global. Se o RSA fosse quebrado o mundo entraria numa nova recessão, pois mesmo se outro algoritmo fosse feito, tal acontecimento teria um enorme impacto. No mercado financeiro, grandes empresas de tecnologia perderiam bilhões em valor de mercado, pois seus sistemas entrariam em colapso. Bancos online seriam seriamente comprometidos, e diversos clientes perderiam seus patrimônios. Diversas empresas seriam hackeadas devido a falhas na criptografia. Até o ato banal de se conectar a um site seria dificultado, pois o RSA faz parte da criptografia responsável pela autenticação da conexão entre o computador e o servidor.

Para impedir essa crise, diversas medidas estão sendo tomadas. No dia 4 de maio de 2022, o presidente americano Joe Biden assinou um memorando de segurança nacional promovendo a liderança dos Estados Unidos na computação quântica, enquanto mitigam-se os riscos nos sistemas de criptografia vulneráveis. A secção 3 do memorando diz:

> Qualquer sistema digital que utilize os padrões públicos de criptografia assimétrica, ou que esteja planejando a transição para esta criptografia, estaria vulnerável a um ataque com computadores quânticos. Para mitigar esse risco, os Estados Unidos deve priorizar a transição efetiva dos sistemas criptográficos para a criptografia *quantum-resistant*, com o objetivo de diminuir os riscos o máximo possível até 2035 (BIDEN, 2022, tradução nossa)[14].

Conforme o memorando, os Estados Unidos têm a meta de substituir algoritmos vulneráveis por algoritmos que sejam *quantum-resistant* até 2035. Nas palavras da Agência de Segurança Nacional (NSA) a *quantum-resistant cryptography* que os Estados Unidos almeja, são algoritmos criptográficos reconhecidos por especialistas que são

14 No original: “Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC. To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035”

resistentes a ataques vindos tanto computadores normais, como de computadores quânticos (NSA, 2021).

Apesar da pesquisa em computadores quânticos ainda ter muito a evoluir, a criação de algoritmos pós quânticos já começou. No dia 5 de julho de 2022, o Instituto Nacional de Padrões e Tecnologia (NIST) escolheu quatro algoritmos resistentes a criptografia pós quântica para seu programa que tem como objetivo criar um padrão internacional de algoritmos pós quânticos. Esse programa tem a meta de ser finalizado em dois anos, definindo um padrão de algoritmos que serão usados no futuro (NIST, 2022).

A União Europeia também está preocupada com a possível crise criptográfica e também está tomando medidas para impedi-la. No dia 22 de outubro de 2022, a Agência Espacial Europeia (ESA) anunciou que a Europa planeja lançar em 2024, um satélite para comunicação utilizando um novo tipo de criptografia, que promete ser muito mais segura que a atual. O satélite chamado de ‘Eagle-1’ será lançado em 2024 e planeja ficar três anos em órbita (ESA, 2022).

Atualmente a humanidade vive em segurança criptográfica, já que os algoritmos usados são bem estabelecidos e não têm falhas conhecidas. Essa segurança está sendo ameaçada por inovações tecnológicas. Diversos países, empresas e organizações já reconheceram o perigo de uma crise criptográfica e estão se preparando para mudar seus padrões de criptografia, de forma a evitar uma crise global.

4 CONCLUSÃO

A necessidade de ocultar informações está presente em diversas sociedades distintas. Para suprir tal necessidade, existe criptografia, técnicas para ocultar e recuperar informações. Essas técnicas são utilizadas desde a antiguidade e empregam um papel extremamente importante na sociedade atual. A criptografia está presente no funcionamento primordial da internet, sem criptografia não há internet como conhecemos.

Um algoritmo moderno de criptografia seguro e consolidado é o RSA. Esse algoritmo é muito utilizado na internet, aplicativos e sistemas. Na realidade atual não existem falhas, nem meios de quebrar esse algoritmo, porém o avanço da tecnologia coloca-se como uma ameaça a essa segurança. O advento de tecnologias como computação quântica colocam em cheque a segurança do RSA e criam a necessidade de uma mudança para a criptografia pôs quântica.

Caso essa mudança não seja feita, haverão consequências para a humanidade. Se fosse descoberta alguma maneira de quebrar o RSA, o impacto negativo aconteceria especialmente na internet, que pararia de funcionar, devido à quantidade massiva de ataques. Isso levaria em colapso diversas empresas e afetaria o mercado financeiro de forma nunca antes vista. As empresas de tecnologia perderiam muito em valor de mercado, o que afetaria a realidade material fora da internet.

Essa crise criptográfica traria péssimas consequências para o mundo, portanto já estão sendo tomadas diversas medidas para evitá-la. Diversas empresas, países e ONGs estão tomando ações para mudar os algoritmos atuais para algoritmos que sejam capazes de suportar a computação quântica; a mudança para a criptografia pós quântica já está acontecendo.

Se a humanidade continuar a transição para criptografia pós quântica na velocidade em que está sendo feito, provavelmente uma crise criptográfica será evitada, porém as descobertas científicas são imprevisíveis. Da mesma forma que o RSA teve grande progresso de forma súbita durante uma noite, nada impede a computação quântica de ter um avanço repentino.

Apesar de ações estarem sendo tomadas, ainda precisamos ficar atentos para uma possível crise criptográfica. Por isso é de vital importância elucidar a população sobre as

descobertas acadêmicas no campo da computação quântica e instrui-los sobre a importância da criptografia na sociedade.

REFERÊNCIAS

ARUTE, Frank *et al*. Quantum supremacy using a programmable superconducting processor. **Nature**. Out. 2019. Disponível em: https://www.nature.com/articles/s41586-019-1666-5 Acessado em: nov. 2022.

BIDEN JR, Joseph R. **National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.** 2022. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ Acessado em: set. 2022.

CALDERBANK, Michael. **The RSA Cryptosystem: History, Algorithm, Primes.** 2007. Disponível em: www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf Acessado em: set. 2022.

COSTA, Darci Dala. **A matemática e os códigos secretos**: uma introdução à criptografia. 2014. Dissertação (Mestrado Profissional em Matemática) – Centro de Ciências Exatas, Universidade Estadual de Maringá, Maringá, 2014.

ESA. **Quantum encryption to boost European autonomy.** 2022. Disponível em: https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Quantum_encryption_to_boost_European_autonomy Acessado em: nov. 2022.

MOLLIN, Richard A. **RSA and public-key cryptography**. Boca Raton: CRC Press LLC, 2003.

NIST. **NIST Announces First Four Quantum-Resistant Cryptographic Algorithms.** 2022. Disponível em: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms Acessado em: set. 2022.

NSA. **Quantum Computing and Post-Quantum Cryptography FAQs.** 2021. Disponível em: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF Acessado em: set. 2022.

ORDONEZ, Edward David Moreno; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. São Paulo: Novatec, 2005.

ROBINSON, Sara. Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. **SIAM News**, Vol. 36, N. 5, jun. 2003, p. 1-4. Disponível em: https://www.msri.org/people/members/sara/articles/rsa.pdf Acessado em: set. 2022.