MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

PRIMEIRO TENENTE (QC-CA) CAIO CARNEIRO SILVA ROCHA

OS EFEITOS DA COMPUTAÇÃO QUÂNTICA PARA A MARINHA DO BRASIL

Rio de Janeiro
2020

PRIMEIRO TENENTE (QC-CA) CAIO CARNEIRO SILVA ROCHA

OS EFEITOS DA COMPUTAÇÃO QUÂNTICA PARA A MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações

Orientadores:
Professor David Ben Svaiter
Capitão de Mar e Guerra (RM-1) Ricardo Ungaretti

CIAW
Rio de Janeiro
2020

Rocha, Caio Carneiro Silva
Os Efeitos da Computação Quântica para a Marinha do Brasil / Caio Carneiro Silva Rocha. - Rio de Janeiro, 2020.
56 f. : il.

Orientador técnico: Professor David Ben Svaiter.
Orientador acadêmico: CMG (RM1) Ricardo Ungaretti.

Monografia (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações). - Centro de Instrução Almirante Wandenkolk, Centro de Pós-Graduação Avançada, Rio de Janeiro, 2020.

1. Criptografia. 2. Quântica. 3. Comunicação. I. Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada. II. Título.

PRIMEIRO TENENTE (QC-CA) CAIO CARNEIRO SILVA ROCHA

OS EFEITOS DA COMPUTAÇÃO QUÂNTICA PARA A MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em ___ de março de 2020

Banca Examinadora:

Gian Karlo Huback Macedo de Almeida, Capitão de Mar e Guerra (RM1-EN), CIAW

Ricardo Ungaretti, Capitão de Mar e Guerra (RM-1), CASNAV

Professor David Ben Svaiter

CIAW
Rio de Janeiro
2020

Dedico esse trabalho à minha família, especialmente à minha esposa, que mesmo longe sempre me deu força para seguir em frente em busca dos meus objetivos.

AGRADECIMENTOS

A minha esposa Leila Monique, por todo amor, paciência e confiança depositada em mim. Mesmo estando distante durante o período do curso sempre esteve na torcida e incentivando para que tudo terminasse com sucesso.

Aos meus pais, Jadson Rocha e Rita Carneiro, por todos os ensinamentos ao longo da minha trajetória e incentivos para me tornar Oficial da Marinha do Brasil.

A meu tio Luiz Paixão e a minha tia Tânia Nunes, por todos os momentos presentes me apoiando nas minhas escolhas.

A minha irmã Bruna Carneiro pela fidelidade incondicional e a minha irmã Tainá Nunes pelo carinho de sempre.

A toda a minha família que foi o grande pilar nessa minha trajetória.

Aos meus orientadores CMG Ungaretti e Professor Svaiter pela atenção, ensinamentos e boa relação que tivemos ao longo do trabalho, contribuindo para um bom resultado.

Ao CMG Huback por sempre ajuda quando precisei, seja por motivos pessoais ou no andamento do curso.

Aos Professores da PUC-RJ que de alguma forma contribuíram para o meu crescimento profissional.

Aos amigos de turma pelo companheirismo nesse ano de curso.

A Marinha do Brasil por me ter dado oportunidade de realizar um curso de grande importância na minha formação profissional.

“Nada deve ser mais estimado do que a informação, mais bem pago do que a informação, e nada deve ser mais confidencial do que o trabalho de coleta de informações.”
(Sun-Tzu)

OS EFEITOS DA COMPUTAÇÃO QUÂNTICA PARA A MARINHA DO BRASIL

Resumo

A segurança da informação em uma comunicação sempre foi um fator de grande importância e objeto de estudos e pesquisas ao redor do mundo. Para isso diversos sistemas de criptografia surgiram e foram sendo substituídos ao longo do tempo à medida que novas necessidades surgiam e os sistemas computacionais foram evoluindo e sendo capazes de processar algoritmos cada vez mais complexos. Porém os estudos na área mostram que está cada vez mais próximo de ocorrer uma quebra de paradigma na criptologia, com o uso dos computadores quânticos. Com o seu alto poder de processamento, eles serão capazes de quebrar chaves criptográficas que ainda hoje se pensa ser impossível de serem quebradas. Este trabalho de conclusão de curso visa apresentar um estudo da criptologia, mostrando um breve histórico, alguns tipos de algoritmos clássicos utilizados, a evolução dos sistemas criptográficos com o advento da computação clássica e enfim chegar ao computador quântico e nos sistemas criptográficos quânticos e pós-quânticos. Tendo discutido a cerca disso, é feita uma análise do impacto para a Marinha do Brasil, quando se pensa em um cenário onde os computadores quânticos estarão em plena operação e como a instituição deve se preparar e precaver para essa nova realidade que se aproxima.

Palavras- chave: Criptografia. Quântica. Comunicação.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE SIGLAS E ABREVIATURAS

MB	Marinha do Brasil
DES	*Data Encryption Standard* (Padrão de Encriptação de Dados)
NIST	*U.S. National Institute of Standards and Technology* (Instituto Nacional (Americano) de padrões e tecnologia)
AES	*Advanced Encryption Standart* (Padrão Avançado de Encriptação)
RSA	Rivest-Shamir-Adleman
ETSI	Instituto Europeu de Padrões de Telecomunicações
PQCS	*Post-Quantum Cryptography Standardization* (Padronização de Criptografia pós-quântica)

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais é cada vez mais importante ter a certeza que se tem segurança nas informações e comunicações. Isso se dá porque alguns dados são muito sensíveis nas mais diversas áreas. A criptografia é utilizada pelos diversos sistemas que necessitam de alguma forma manter o sigilo das informações.

A partir da junção de duas palavras gregas, kryptós (escondido) e grápho (grafia), que significa escrita secreta, originou-se a palavra criptografia. Os primeiros protocolos de criptografia que a utilizam nesse sentido têm registros de milhares de anos e utilizam um procedimento, também conhecido como algoritmo, para cifrar e decifrar a informação. (GOYA, 2006).

Um algoritmo pode ser entendido como uma sequência finita de passos (operações matemáticas) com a finalidade de resolver um problema de interesse. DES, AES e RSA são alguns exemplos de algoritmos criptográficos clássicos, que serão comentados no trabalho. Posteriormente será comentado a respeito de alguns algoritmos quânticos.

A segurança da informação e comunicações possui alguns requisitos básicos, que são listados nas alíneas abaixo. (STALLINGS, 2015)

a) **Confidencialidade**: preservar restrições autorizadas sobre acesso e divulgação de informação, incluindo meios para proteger a privacidade de indivíduos e informações privadas. Uma perda de confidencialidade seria a divulgação não autorizada de informação.
b) **Integridade**: prevenir-se contra a modificação ou destruição imprópria da informação, incluindo a irretratabilidade e autenticidade dela. Uma perda de integridade seria a modificação ou destruição não autorizada da informação.
c) **Disponibilidade**: assegurar acesso e uso rápido e confiável da informação. Uma perda de disponibilidade é a perda de acesso ou de uso da informação ou sistema de informação.
d) **Autenticidade**: a propriedade de ser genuíno e capaz de ser verificado e confiável; confiança na validação de uma transmissão, em uma mensagem ou na origem de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e, além disso, que cada entrada no sistema vem de uma fonte confiável.

e) **Responsabilização (Não-repúdio)**: a meta de segurança que gera o requisito para que ações de uma entidade sejam atribuídas exclusivamente a ela. Isso prevê irretratabilidade, dissuasão, isolamento de falhas, detecção e prevenção de intrusão, além de recuperação pós-ação e ações legais. Como sistemas totalmente seguros não é ainda uma meta alcançável, tem-se que ser capaz de associar uma violação de segurança a uma parte responsável. Os sistemas precisam manter registros de suas atividades a fim de permitir posterior análise forense, de modo a rastrear as violações de segurança ou auxiliar em disputas de uma transação.

De todos os requisitos da segurança da informação e comunicações, “disponibilidade” é o único que não se aplica na área da criptologia.

1.1 Apresentação do problema

Com o avanço dos sistemas de computação e o aumento da capacidade de processamento dos computadores, os algoritmos clássicos de criptografia se mostram cada vez mais vulneráveis.

O presente trabalho estará focado em um estudo teórico a respeito da criptografia clássica até a criptografia pós-quântica, visando apresentar o que ocorrerá de mudanças para a Marinha do Brasil na área de segurança da informação e comunicações com a criptografia quântica. Além disso, deseja-se mostrar o quão vulneráveis estarão as chaves secretas da instituição com o desenvolvimento da criptoanálise quântica.

1.2 Justificativa e relevância

A justificativa para esta pesquisa é mostrar o novo cenário da criptografia com os avanços da computação quântica, que acarretará uma mudança abrupta nas idéias que se tem até então. Com a segurança das informações ameaçadas, deve-se estudar e conhecer os sistemas quânticos, capazes de quebrar as chaves assimétricas atuais, bem como os algoritmos pós-quânticos que são resistentes aos ataques dos computadores quânticos.

A relevância deste trabalho é mostrar para MB o que existe de moderno na área da criptografia, realizando estudo e pesquisa, a fim de aumentar os conhecimentos e capacidades do pessoal envolvido na área de segurança da informação.

1.3 Objetivos

Este trabalho visa aumentar o conhecimento a respeito de criptografia no âmbito da MB e alertar para a evolução dos algoritmos pós-quânticos que são desenvolvidos paralelamente às descobertas do computador quântico.

Para isso será realizado um estudo das técnicas de criptografia clássicas e apresentada a criptografia quântica e pós-quântica. Assim podem-se mostrar as vulnerabilidades das informações e comunicações da MB, com o uso de um computador quântico por um inimigo, bem como melhorar a segurança das chaves criptográficas através das técnicas de criptografia quântica.

2 REFERENCIAL TEÓRICO

O avanço das tecnologias tem causado nas comunicações, cada vez mais, uma dependência dos sistemas computacionais. Ao longo da história a comunicação já sofreu muitas alterações nos seus modos de operação.

Os sinais sonoros e visuais, como berrante, gongo e sinais de fumaça foram os primeiros utilizados pelo homem para se comunicar a certa distância. Essas eram algumas tecnologias utilizadas nos primórdios da comunicação, já que com elas era possível enviar uma mensagem fora do âmbito familiar ou grupal. (PERLES, 2007)

Já no século IV, com a invenção da escrita o homem conseguiu vencer a dificuldade do alcance, já que a mensagem escrita pode ser levada de um local ao outro independente da distância. (PERLES, 2007)

Ao longo dos anos a linguagem escrita foi se desenvolvendo, e com ela os meios de comunicação foram se aperfeiçoando. O papel, que foi criação dos chineses, substituiu as superfícies de pedra, os papiros e os pergaminhos de couro, que até então eram utilizados para escrever. (PERLES, 2007)

Os anos foram se passando e muito se evoluiu quando se fala em comunicação. Muitos estudiosos se empenharam e dedicaram muitos anos de suas vidas em estudos e pesquisas que levaram ao crescimento relativamente rápido da tecnologia de comunicação.

O telégrafo foi criado e com as transmissões eletromagnéticas foi realizada a primeira ligação radiotelegráfica de 300 km entre duas cidades da Inglaterra em 1900. (PERLES, 2007)

A primeira geração de computadores foi marcada pelo invento de Vannevar Bush, no início da década de 1930. Ele foi responsável pela construção do “Analisador Diferencial Mecânico”, que possibilitava a resolução de equações diferenciais. Porém elas eram pesadas, lentas e aqueciam muito. Já entre 1935 e 1938, Konrad Zuse, construiu um equipamento mais parecido com o que se tem hoje como um computador, pois nele já existia unidade de controle, memória e lógica. (CURY, 2011)

Após isso, os computadores foram evoluindo e os avanços tecnológicos nas áreas de eletrônica propiciaram um crescimento de grandes proporções e com uma velocidade muito grande na área da computação. Diante disso, tem-se hoje uma busca diária de melhorias da tecnologia que visa o aprimoramento dos sistemas computacionais.

Paralelo ao crescimento das tecnologias de comunicações nasceu a preocupação com a segurança das informações transmitidas. A segurança dos dados é uma das principais

preocupações dos usuários de sistemas computacionais. Para se obter sigilo dos dados trafegados por tais sistemas são utilizadas técnicas de criptografia. (GOYA, 2006)

2.1 A história da criptografia

A criptografia é feita há muitos anos pelo ser humano em diversas sociedades. Ela é tão antiga quanto à escrita, já que se podem observar técnicas criptográficas nos hieróglifos egípcios, nos códigos secretos utilizados pelos romanos em batalhas e já nas grandes guerras mundiais com o advento dos computadores se observou um grande crescimento com aplicações de algoritmos matemáticos complexos. (MORENO et al, 2005)

O primeiro caso que se tem registro de um texto cifrado data aproximadamente de 1900 a.C. quando o escriba de Khnumhotep II decidiu substituir palavras ou trechos de um texto. Ele fez isso com intuito de atrapalhar algum ladrão que viesse a roubar o documento e com o texto cifrado o caminho não levaria ao tesouro e o ladrão morreria de fome perdido nas catacumbas da pirâmide. (MORENO et al, 2005 e KAHN, 1996)

Já em 50 a.C. Júlio César fez uso de uma técnica de criptografia para cifrar comunicações governamentais. Sua técnica consistia na substituição de letras do alfabeto alterando em três posições, ou seja, o "A" se tornava "D", o "B" se tornava "E" e nessa lógica ele conseguia alterar todas as letras do alfabeto. (MORENO et al, 2005)

O código de César foi utilizado por oficiais sulistas na Guerra de Secessão nos Estados Unidos e pelo exército russo em 1915. Na tabela 1 está mostrado como funciona a substituição de letras no código de César. (MORENO et al, 2005)

Tabela 1: Cifra de César

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
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: (MORENO et al, 2005)

Outros códigos utilizados para criptografar mensagens ao longo da história foram o de Heródoto, o Bastão de Licurgo e a Blaise de Vigenère. O ex-presidente dos Estados Unidos entre 1801 e 1809, Thomas Jefferson, desenvolveu um código próprio de criptografia chamada "Cilindro de Jefferson", que foi utilizado durante a revolução americana, quando ele precisava enviar mensagens. (KAHN, 1996)

Heródoto, em aproximadamente 450 a.C. desenvolveu métodos um tanto quanto rudimentares para ocultar suas mensagens que seriam enviadas. Esses métodos foram chamados de esteganografia, palavra que tem origem no grego, em que “estegano” significa “esconder ou mascarar” e “grafia” quer dizer “escrita”. (PETRI, 2004) Logo esse termo é entendido como a arte de esconder informações, tornando-as ocultas. Um desses métodos era raspar o cabelo do mensageiro, escrever a mensagem e esperar que o cabelo crescesse novamente para assim enviar ao destino e outro era escrever mensagens em tabletes e cobrir com cera. (BONFIM, 2017 e ARTZ, 2001)

Exemplos mais aplicáveis à segurança da informação e comunicações é o caso em que mensagens são escondidas em imagens, onde são utilizadas técnicas específicas. Arquivos de áudio também podem ser utilizados para ocultar mensagens, de maneira que estas não sejam notadas pelo usuário do áudio. Outros métodos usam arquivos de texto, arquivos HTML e pacotes TCP para esconder informações. (ARTZ, 2001)

O Cítala de Licurgo foi o primeiro equipamento criptográfico utilizado para fins militares, datando do século V a.C., pelos espartanos a fim de enviar mensagens secretas. Ele era formado por dois bastões de madeira de mesma espessura e uma fita de couro. Um bastão ficava com o emissor e o outro com o destinatário. Para escrever a mensagem a fita de couro era enrolada de forma espiral no bastão do emissor e então a mensagem era escrita de forma longitudinal, de forma que cada letra aparecia em cada parte da volta. Com a mensagem escrita bastava desenrolar a fita e enviar. O destinatário enrolava a fita de couro em seu bastão e assim era possível ler a mensagem original. (BONFIM, 2017)

A figura 1 mostra um exemplo de uma Citale Espartano. (FIARRESGA, 2010)

Figura 1: Citale Espartano

Fonte: (FIARRESGA, 2010)

Por volta de 1440, Leon Battista Alberti, uma importante figura da época propôs utilizar dois ou mais alfabetos, utilizados alternadamente, para cifrar mensagens de modo a confundir os criptoanalistas. Apesar de toda contribuição de Alberti para a evolução da criptografia, ele não conseguiu chegar a um resultado final que gerava um sistema de criptografia completo. Alguns nomes como Johannes Trithemius e Giovanni Porta conseguiram desenvolver as idéias de Alberti e por fim um diplomata francês chamado Blaise de Vigenère tomou conhecimento do trabalho desenvolvido pelos seus antecessores e chegou a um sistema poderoso e concreto. Apesar de todas as contribuições anteriores, a cifra levou o nome de Vigenère por ter sido ele o responsável pela sua formulação final. (BONFIM, 2017 e SINGH, 2004)

Para criptografar uma mensagem utilizando essa técnica utiliza-se uma tabela que representa as 26 letras do alfabeto, e uma palavra chave aleatória, que será tratada como chave secreta, ou seja, um componente essencial à descriptografia da informação e que precisa ser conhecida pelo destinatário. Essa palavra chave deve ser menor que o texto a ser cifrado. A mensagem deve ser escrita sem espaços, como uma linha contínua de letras, e então a palavra-chave deve ser escrita abaixo da mensagem, de forma que cada letra da mensagem seja associada a uma letra da palavra chave. A letra da palavra chave é localizada na linha da tabela de Vigenère, assim como a letra da mensagem na coluna. A interseção da linha e coluna correspondente às letras da mensagem e da palavra chave corresponde à letra criptografada. Para decifrar o processo inverso deve ser feito, e assim o receptor encontrará o texto limpo. A tabela 2 é utilizada para cifrar uma mensagem com a cifra de Blaise de Vigenère. (BONFIM, 2017 e SINGH, 2004)

Tabela 2: Tabela para a cifra de Blaise de Vigenère.

	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: (BONFIM, 2017)

Na tabela 3 está mostrado um exemplo de aplicação da cifra de Blaise de Vigenère que cifra a mensagem “Cifra de Blaise” e utiliza a palavra chave “mágica”. (BONFIM, 2017)

Tabela 3: Exemplo de aplicação da cifra de Blaise de Vigenère.

Mensagem	C	i	f	r	a	d	e	B	l	a	i	s	e
Palavra chave	m	a	g	i	c	a	m	a	g	i	c	a	m
Mensagem	o	i	l	z	c	d	o	b	r	i	k	s	q

Fonte: (BONFIM, 2017)

A grande vantagem da cifra de Vigenère é a imunidade à análise de freqüência, técnica utilizada pelos criptoanalistas para decifrar uma mensagem. Essa técnica consiste em analisar a freqüência que uma letra aparece no texto cifrado e presumir que essa letra representa a letra mais comum do alfabeto que teoricamente aquela cifra foi elaborada. No caso da língua portuguesa é a letra “a”. Outra vantagem da cifra de Vigenère é o grande número de chaves que pode ser utilizada, que pode ser qualquer palavra do dicionário ou combinação de palavras, acordadas pelo remetente e destinatário. (SINGH, 2004)

A cifra de Vigenère perdurou por muito tempo, até meados do século XIX quando ela foi quebrada pelas contribuições de dois homens. O primeiro deles foi o britânico Charles Babbage, conhecido por ter desenvolvido o precursor do computador moderno. O outro foi Friedrich Wilhelm Kasiski, que foi um oficial da reserva do exército prussiano. (SINGH, 2004)

2.2 Tecnologia: vulnerabilidades e impulsos à criptografia

Já no final do século XIX, Marconi iniciou experimentos com circuitos elétricos, o que culminou na invenção do rádio. A grande vantagem da invenção de Marconi em relação ao telégrafo, que já era utilizado há meio século, era a ausência de cabos e fios para se ter uma comunicação. No novo sistema o sinal era propagado através do ar do emissor até o receptor. Poucos anos depois da invenção, Marconi conseguiu a primeira comunicação de rádio transatlântica. (SINGH, 2004)

O rádio fascinou os militares da época, que viram as limitações de comunicações causadas pela distância acabarem com a utilização desse novo equipamento. Este foi um ponto de grande evolução para as comunicações militares. Porém, a nova forma de comunicação trazia um grande problema para eles, já que todas as mensagens enviadas poderiam ser interceptadas por qualquer pessoa, inclusive um possível inimigo. Com isso a corrida por novas cifras seguras foi iniciada. (SINGH, 2004)

Em 1918, Arthur Scherbius e Richard Ritter fundaram uma empresa que trabalhava com diversas linhas de produção. Scherbius era encarregado da área de pesquisa e desenvolvimento e um de seus projetos focava em novos sistemas de criptografia, a fim de substituir os antigos, considerados inadequados, que foram utilizados na Primeira Guerra Mundial. Com seus conhecimentos em engenharia elétrica, ele desenvolveu uma máquina criptográfica que era a versão elétrica do disco de cifras de Alberti. À nova invenção de Scherbius foi dado o nome de Enigma. (SINGH, 2004)

Os militares alemães viram um grande potencial na máquina Enigma e apostaram na idéia de Scherbius. Em 1925 ele iniciou a produção em série das máquinas, que foram adotadas no ano seguinte. Nos 20 anos seguintes a Alemanha comprou 30 mil máquinas Enigma e se tornou o sistema de criptografia mais seguro do mundo. (SINGH, 2004)

Os primeiros que tentaram decifrar a Enigma foram os poloneses, que apesar de não estarem em guerra com a Alemanha, existia uma ameaça de invasão por parte dos alemães na Polônia. Essa preocupação fez com que os poloneses montassem uma equipe de matemáticos para estudar a Enigma. O que mais se destacou foi Marian Rejewski, principal responsável pela quebra da máquina Enigma. (SINGH, 2004)

No entanto a quebra do seu principal sistema de criptografia foi percebido pelos alemães, que logo aumentaram a capacidade de segurança da Enigma. Em 1938, Rejewski chegou ao seu limite intelectual e ficou incapaz de decifrar as mensagens dos alemães. (SINGH, 2004)

Os ingleses criaram uma equipe de criptoanalistas para buscar decifrar as novas e mais seguras máquinas Enigma. Muitos deles deram importantes contribuições para o desenvolvimento dos estudos ingleses, mas um que merece destaque é Alan Turing. Ele foi responsável pela descoberta das maiores fraquezas da Enigma, o que mais tarde proporcionou que ela fosse decifrada. (SINGH, 2004)

Na figura 2 é possível ver uma imagem do modelo I, uma das diversas versões da máquina Enigma. (KRISCHER, 2012)

Figura 2: Modelo I da máquina Enigma.

Fonte: (KRISCHER, 2012)

Historiadores relatam a importância da quebra da Enigma para o fim da guerra. Muitos deles afirmam que sem a descoberta daquela cifra a guerra duraria mais alguns anos e muitas vidas seriam perdidas. Assim, se defende que esse fato foi um fator decisivo para a vitória dos aliados. O historiador David Kahn conseguiu sintetizar muito bem o significado da quebra da Enigma: “Ela salvou vidas. Não apenas vidas aliadas e russas, ao encurtar a guerra, mas vidas alemãs, italianas e japonesas também. Algumas das pessoas que estavam vivas depois da Segunda Guerra Mundial não teriam sobrevivido se não fossem essas soluções. Esta é a dívida que o mundo tem para com os quebradores de códigos, este é o valor humano de seus triunfos.” (SINGH, 2004)

2.3 O uso do computador na criptografia

Com o advento do computador no pós-guerra, pode-se dizer que se iniciou uma nova era da criptografia. As possibilidades cresceram bastante para os criptógrafos, que podiam fazer códigos mais complexos e seguros, assim como para os criptoanalistas, que poderiam

utilizar a velocidade e flexibilidade do computador para buscar decifrar esses novos códigos. (SINGH, 2004)

Podem-se notar três diferenças básicas significativas entre a criptografia computadorizada daquela praticada antes do final da guerra. Primeiramente, a máquina de criptografia mecânica está limitada ao que se pode implementar na prática, entretanto o computador tem a capacidade de simulação de qualquer máquina que se possa imaginar com muito mais complexidade. A segunda diferença é simplesmente a questão da velocidade, que em um computador é diversas vezes maior que uma máquina mecânica – assim, um computador pode realizar uma operação em um tempo consideravelmente menor que na máquina mecânica. E por fim uma diferença que pode ser considerada a mais significativa, que é modo como o computador opera, visto que nele são processados números binários (*bits*). (SINGH, 2004)

Na década de 1960, os computadores foram modernizados e ficaram mais baratos, o que possibilitou o uso deles por mais empresas. Isso aumentou a utilização de criptografia nas demais áreas que não se limitava apenas ao governo e militares, como se observou anos atrás. Essa difusão para diversos setores causou um problema para os criptógrafos, que foi a falta de padronização. Sem um padrão não é possível que as informações sejam trocadas entre entidades diferentes, o que inviabiliza o seu uso. (SINGH, 2004)

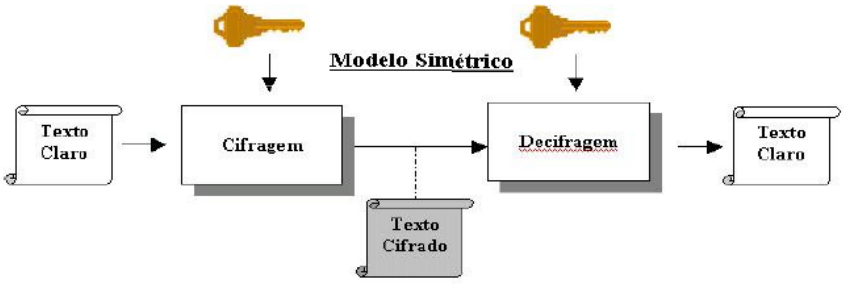
Até então todos os algoritmos criptográficos utilizavam as chaves simétricas. Esse modelo é composto por cinco itens básicos, listados nas alíneas abaixo. (STALLINGS, 2015)

a) **Texto claro**: mensagem original, inteligível, que faz o papel de entrada do algoritmo simétrico.
b) **Algoritmo de encriptação**: executa substituições e transformações no texto claro.
c) **Chave secreta**: funciona também como uma entrada do algoritmo de encriptação, independente do texto claro e do algoritmo. Com isso será produzida uma nova saída que depende da chave utilizada.
d) **Texto cifrado**: mensagem embaralhada, resultante da saída do algoritmo de encriptação. A dependência dessa mensagem em relação ao texto claro e à chave secreta implica na produção de dois textos cifrados diferentes, se utilizadas duas chaves distintas. Esse texto tem uma natureza aleatória de formato ininteligível.

e) **Algoritmo de decriptação**: basicamente o mesmo algoritmo de encriptação executado de modo inverso. Ele utiliza o texto cifrado e a chave secreta e gera como saída o texto claro.

Para utilizar o modelo de criptografia simétrico de forma segura, é necessário cumprir dois requisitos. Primeiramente, precisa-se de um algoritmo de encriptação forte. O inimigo deve ser incapaz de decriptar o texto cifrado ou descobrir a chave secreta, mesmo que possua alguns textos cifrados com seus respectivos textos claros. Outro requisito é a necessidade de emissor e receptor obtenham cópias da chave secreta de forma segura e mantenha protegida. Na figura 3 está mostrado um esquema simplificado do modelo de encriptação simétrico. (STALLINGS, 2015)

Figura 3: Esquema simplificado do modelo de encriptação simétrico.



Fonte: (MORENO, 2005)

Finalmente em 1977, o *Data Encryption Standard* – DES foi adotado pelo *National Bureau of Standards*, que é o atual *National Institute of Standards and Technology* (NIST). Na época todos os problemas de padronização foram resolvidos e as empresas passaram a utilizar o novo padrão. O DES era seguro o suficiente para que nenhum computador de uso civil fosse capaz de quebrar um código que o utilizasse, devido ao elevado número de possíveis chaves secretas. Porém as empresas esbarraram em um antigo problema que era a distribuição de chaves. (SINGH, 2004 e STALLINGS, 2015)

Existem dois tipos de algoritmos simétricos: os cifradores de fluxo e os cifradores de bloco. Os primeiros cifram bit a bit o conjunto que forma a mensagem, já os cifradores de bloco utilizam blocos de n bits da mensagem. Bloco de dados são conjuntos de bits que carregam alguma informação relevante. (STALLINGS, 2015)

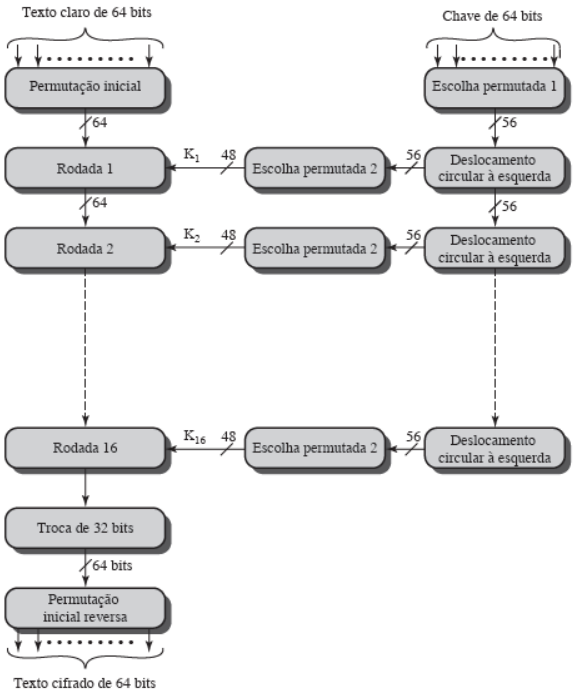
A segurança do DES estava relacionada com a dimensão da chave secreta. Para cifrar utilizando o DES, o texto claro deve possuir 64 bits de comprimento e a chave 56 bits. Isso

significa que o total de chaves possíveis é igual ao ‘espaço’ de bits utilizado. Seguindo essa lógica e sabendo que um bit pode conter dois estados (0 ou 1), temos um total de 2 elevado a 56 possibilidades de chaves, ou aproximadamente 72 quatrilhões de chaves. (STALLINGS, 2015 e BARBOSA et al, 2003)

O texto cifrado produzido possui os mesmos 64 bits do texto claro. Para criar uma segurança maior, o algoritmo utiliza um mecanismo que processa desta forma o texto claro com a chave 16 vezes, utilizando diferentes partes da chave. Uma versão mais recente desse algoritmo é o 3-DES, que utiliza três chaves de 56 bits. (STALLINGS, 2015 e BARBOSA et al, 2003)

A figura 4 mostra um esquema do algoritmo de encriptação DES. Nela pode-se notar a presença de dois componentes básicos no processo de encriptação, o texto claro e a chave secreta. No caso do DES o texto claro possui 64 bits e a chave 56 bits de extensão. O primeiro passo é permutar o texto claro, a fim de produzir uma entrada permutada. A segunda fase é composta por 16 rodadas de que envolvem funções de permutação e substituição. Isso produz, ao fim da 16ª rodada, uma saída de 64 bits que são função do texto claro e da chave secreta. As metades direita e esquerda da saída são trocadas para produzir uma pré-saída, em um esquema conhecido como Feistel (LUBY, 1988 e MORRIS et al., 2009). Esta é passada por uma permutação, que é o inverso da função de permutação inicial, para produzir o texto cifrado de 64 bits. A parte direita da figura 4 mostra como a chave de 56 bits é empregada. Primeiramente, a chave é permutada e parada cada uma das 16 rodadas, é gerada uma sub-chave (K_i), através da combinação de um deslocamento circular à esquerda e uma permutação. A permutação utilizada é a mesma nas 16 rodadas, para cada rodada uma sub-chave é produzida, devido aos deslocamentos repetidos dos bits da chave. (STALLINGS, 2015)

Figura 4: Representação do algoritmo de encriptação DES.



Fonte: (STALLINGS, 2015)

Em 2001, o NIST, padronizou um novo algoritmo de criptografia que ficou conhecido como AES. Este algoritmo também é simétrico (utiliza as mesmas chaves para codificar e decodificar a informação) e pode utilizar chaves de 128, 192 ou 256 bits com blocos de dados de 128 bits. (STALLINGS, 2015 e BARBOSA et al, 2003)

2.4 O problema da distribuição de chaves

A distribuição de chaves é um problema para os criptógrafos em toda a história. Quando uma pessoa cifra uma mensagem utilizando o DES e envia para uma segunda pessoa, ela (o receptor) precisa conhecer qual foi a chave que criptografou a informação para poder acessar a mensagem original. E para o receptor receber a chave de forma segura deve ser apenas pessoalmente, já que de outra forma a cifra pode ser interceptada por pessoas que não devem ler a mensagem original. Esse fato requer bastante recurso financeiro e tempo, para que se tenha uma distribuição de chaves de modo seguro. (SINGH, 2004)

O grau de segurança de um sistema de criptografia simétrico está diretamente ligado à técnica de distribuição de chave, que é o modo como as duas partes interessadas compartilham a chave secreta sem que outras partes tenham conhecimento dela, o que pode

ser um desafio em situações de guerra, devido às grandes distâncias, e uso de canais de comunicação inseguros ou não confiáveis. (STALLINGS, 2015)

No mesmo ano da padronização do DES, três pesquisadores descobriram uma forma de criptografar mensagens que revolucionou o mundo da criptografia. Diffie, Hellman e Merkle resolveram o problema de distribuição segura de chaves. (SINGH, 2004)

No conceito de cifra assimétrica, existem duas chaves diferentes que são utilizadas para criptografar e para descriptografar, respectivamente. Essas chaves receberam o nome de chave-pública e chave-privada. A primeira é utilizada para cifrar mensagens enquanto a segunda para decifrar. A grande vantagem desse novo sistema de chaves é conseguir estabelecer a troca de uma chave-secreta de forma segura, mesmo utilizando canais inseguros. Ou seja, mesmo que essa troca seja interceptada, o interceptador não terá acesso à informação ou à chave criptográfica que foi utilizada para codificá-la. (SINGH, 2004)

Diffie e Hellman apresentaram os conceitos da criptografia de chaves assimétricas (pública e privada)ao público em 1976. Hellman dá crédito também a Merkle pela descoberta, independente e simultânea do conceito, apesar deste não ter publicando o resultado dessa descoberta antes de 1978. O primeiro documento descrevendo a distribuição de chave pública e a criptografia assimétrica foi uma proposta de projeto de 1974 por Merkle. (STALLINGS, 2015)

Interessante notar que o almirante Bobby Inman, como diretor da National Security Agency (NSA), aponta que a criptografia de chave pública tenha sido descoberta na NSA em meados da década de 1960, ou seja, mais de uma década antes de Merkle e Diffie/Helmann. (STALLINGS, 2015)

O algoritmo possui dois parâmetros, p e g, que podem ser públicos. O parâmetro p é um número primo e g, que é chamado de chave geradora, é um número inteiro menor que p, tal que para cada número n entre 1 e p, existe um expoente k de g, tal que se relacionam segundo a equação 1.

$$n = g^k mod\ p \qquad \text{(Equação 1)}$$

Para exemplificar o algoritmo serão adotadas as entidades “A” e “B”. Supondo que essas entidades estão interessadas em ter uma nova chave de criptografia, a entidade “A” gera um número aleatório a e “B” gera um numero aleatório b, tal que a e b pertencem a um conjunto de inteiros {1,...,p-2}. Com isso as entidades calculam p e g de suas chaves. A chave pública de “A” é $g^a\ mod\ p$ enquanto a chave pública de “B” é $g^b\ mod\ p$. Nesse momento eles

trocam as suas chaves públicas. Com isso "A" calcula $g^{ab} = (g^b)^a \ mod \ p$ e "B" calcula $g^{ba} = (g^a)^b \ mod \ p$. Como $g^{ab} = g^{ba} = k$, tem-se que as entidades "A" e "B" possuem uma chave secreta simétrica *k*. (BARBOSA et al, 2003)

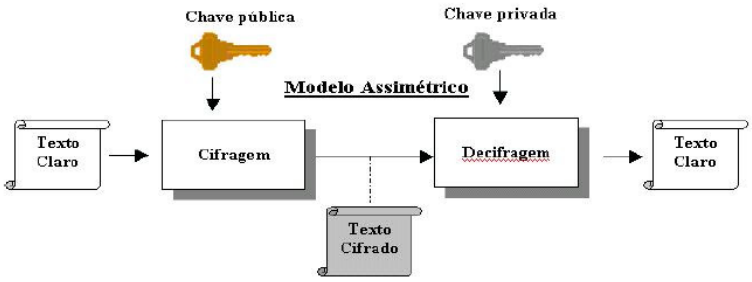
O algoritmo de Diffie e Hellman é vulnerável a um ataque chama *man-in-the-middle*. Este ataque acontece quando duas entidades acreditam que estão se comunicando uma com a outra, quando a comunicação está passando por um dispositivo atacante intermediário, e o tráfego de informações está sendo capturado por uma terceira entidade, que não deveria ter acesso àquelas informações. As redes *wireless* são bem vulneráveis a esse tipo de ataque. (STALLINGS, 2015)

Hellman estava focado em seu método de troca de chaves, ao mesmo tempo em que Diffie trabalhava em algum método que viesse a resolver o velho problema da distribuição de chaves. Logo ele inventou um novo conceito de chave criptográfica, que viria a ser conhecida como "chave assimétrica". (SINGH, 2004)

Até aquele momento as técnicas de criptografia utilizavam o processo de criptografia simétrica, que sempre utiliza para descriptografar um processo inverso ao de criptografar, isto é, a mesma chave utilizada nos dois processos. (SINGH, 2004)

Na figura 5 está mostrado um esquema simplificado do modelo de encriptação assimétrico, que pode ser comparado com o modelo simétrico mostrado na figura 3. No modelo assimétrico é possível observar que são utilizadas a chave pública e a chave privada, o que se diferencia do modelo simétrico, que existe apenas uma chave. (MORENO et al, 2005)

Figura 5: Esquema simplificado do modelo de encriptação assimétrico.



Fonte: (MORENO, 2005)

2.5 O RSA

Em 1978, três pesquisadores, Ron Rivest, Adi Shamir e Len Adleman publicaram no MIT (*Massachusetts Institute of Technology*) um novo algoritmo de criptografia. O RSA (Rivest-Shamir-Adleman) desde então se tornou a técnica de chave pública mais usual dentre as existentes. (STALLINGS, 2015 e RIVEST et al., 1978)

Um problema que existia no algoritmo de Diffie e hellman , quanto ao ataque *man-in-the-middle*, foi resolvido pelo RSA. A chave secreta usada nos algoritmos simétricos que era enviada do emissor para o receptor já não tinha mais o risco de ser interceptada por um terceiro, e assim este não tinha acesso à mensagem clara. (STALLINGS, 2015)

O RSA tem como principal fator de segurança a fatoração de números inteiros enormes. Ao ser criado, seus inventores imaginavam que para uma chave composta por 200 bits seriam necessários 10^{15} anos para realizar a sua quebra, entretanto chaves com 155 bits foram quebradas em apenas oito meses, aproximadamente. Com isso foi necessário aumentar o tamanho das chaves e atualmente se consegue implementá-las com um tamanho suficientemente seguro para que não seja possível quebrá-las. (BARBOSA et al, 2003)

As chaves públicas e privadas no RSA são geradas a partir de números primos enormes, que são multiplicados e seu produto (resultado) usado como chave-criptográfica para criptografar e descriptografar a informação. O esquema RSA apóia-se na dificuldade de se descobrir esse número e seus componentes via fatoração, um processo demorado e que pode durar milhares de anos nos casos de números enormes. Quanto maiores forem esses números, maior será a dificuldade de descobri-los pela fatoração. Atualmente esses números primos, quando convertidos para o sistema binário, podem chegar ao comprimento de 2048 bits. (MORENO et al, 2005)

Existem cinco técnicas que possibilitam atacar o algoritmo RSA, e estão listas nas alíneas abaixo. (STALLINGS, 2015)

a) Força bruta: todas as chaves possíveis são testadas até que a correta seja descoberta.
b) Ataques matemáticos: diversas técnicas são utilizadas com objetivo de fatorar números compostos pelo produto de dois primos.
c) Ataque de temporização: dependem da duração de execução do algoritmo de descriptação.

d) Ataques baseados em falha de hardware: relacionados a falhas de hardware no processador que está gerando as chaves.
e) Ataques de texto cifrado escolhido: este último ataca propriedades do algoritmo RSA.

O RSA, assim como outros cripto-sistemas, utiliza um grande espaço de chaves para se defender contra ataques de força bruta. Assim, quanto maior o número de bits que compõe a chave, mais difícil de quebrá-la. Por outro lado quando se aumenta a chave, a complexidade dos cálculos aumenta bastante na geração da chave e nos processos de encriptação e decriptação, o que torna o sistema lento. (STALLINGS, 2015)

Muitos estudos são realizados a fim de se encontrar números primos cada vez maiores para assim proporcionar maior segurança nas chaves criptográficas. Porém o grande avanço no poder de processamento dos sistemas computacionais causa preocupação para os que dependem da segurança dessas chaves, já que eles são capazes de fatorar números e menos tempo. Diversos setores são usuários do RSA, por exemplo, sistemas bancários, lojas virtuais, empresas das mais variadas áreas, entre outros. (MORENO et al, 2005)

O algoritmo utilizado para gerar as chaves pública e privada está descrito nas alíneas a seguir: (BARBOSA et al, 2003)

a) Dois números primos gigantes (***p*** e ***q***), são escolhidos de forma aleatória;
b) Gera-se um número n através da multiplicação dos números escolhidos anteriormente (***n = p . q***);
c) Calcula-se ***Φ(n) = (p-1).(q-1)***;
d) Escolhe-se um número inteiro ***1 < e < Φ(n)***, tal que ***e*** e ***Φ(n)*** sejam primos entre si;
e) Calcula-se ***d*** de forma que ***d.e ≡ 1 mod Φ(n)***, ou seja, ***d*** deve ser o inverso multiplicativo de ***e*** em ***mod Φ(n).***

Com isso para criptografar a mensagem clara (M) e obter a mensagem criptografada, deve-se fazer as seguintes operações matemáticas para criptografar (equação 2) e descriptografar (equação 3) uma informação. (BARBOSA et al, 2003)

$$C = M^e \bmod n \qquad \text{(Equação 2)}$$

$$M = C^d \ mod \ n \qquad \text{(Equação 3)}$$

Para cada bloco de dados a ser cifrado é necessário realizar os cálculos das equações 2 e 3. Para ambas as operações é preciso conhecer o valor de *n.* A partir disso tem-se a chave pública, que é o par *(n,e)* e a chave privada que é a dupla *(n,d)*. (BARBOSA, 2003)

A cada dia que os computadores aumentam seus poderes de processamento, a força do RSA baseada na fatoração de números grandes compostos de números primos está ameaçada. O fato que comprova essa observação foi o desafio propostos pelos inventores do algoritmo quando foi elaborado. Eles desafiaram leitores de uma revista americana a decodificarem uma mensagem em troca de uma recompensa de 100 dólares. A previsão feita por eles era que o texto criptografado levaria algo em torno de 40 quatrilhões de anos. Entretanto, com o avanço das tecnologias dos computadores, um grupo reivindicou o prêmio em 1994. Isso leva a crer que em algum momento o algoritmo RSA não será considerado seguro. (STALLINGS, 2015)

2.6 A computação quântica

Nas últimas décadas, o computador vem sofrendo rápida evolução, ficando mais velozes e eficientes. Eles sofrem um processo de redução de tamanho físico, o que é proporcionado pela miniaturização dos componentes eletrônicos que estão presentes em grande número nos computadores. Porém com esse processo os pesquisadores da área esbarraram em um problema de limitação física. (SANTOS, 2018 e JORCUVICH, 2018)

Ao mesmo tempo em que a eletrônica vinha se desenvolvendo, as pesquisas na área da física moderna estudavam as menores partículas da matéria, e como elas se comportam. Foi então que foram aplicadas na prática as leis da mecânica quântica, que muito se diferem das leis clássicas da física. Nesse contexto nasce a computação quântica, que busca trabalhar o processamento de informações no nível atômico. Um computador quântico é projetado de tal forma que suas operações elementares devem ser baseadas na mecânica quântica. (SANTOS, 2018 e JORCUVICH, 2018)

O avanço da computação foi previsto em 1965 por Gordon Earl Moore, co-fundador e presidente da Intel. Segundo Moore, o limite da evolução da tecnologia esbarra em dois fatores. São eles o grau de miniaturização dos componentes eletrônicos e as interferências eletromagnéticas entre estes componentes. Diante desse fato, quando os limites físicos dos componentes forem atingidos, a alternativa será o computador quântico. (ALEGRETTI, 2004 e JORCUVICH, 2018)

Já em 1981, um físico americano chamado Paul Benioff formulou uma teoria sobre uma máquina de Turing quântica, que aplicava princípios quânticos à computação. Com sua teoria ele demonstrou teoricamente a possibilidade da implementação de um computador quântico. Ele escreveu três artigos científicos que fundamentaram a teoria da computação quântica. (SOBRAL, 2019)

Richard Feynman foi um físico americano que em 1982 considerou pela primeira vez que efeitos quânticos poderiam produzir algo de inovador e mostrou como a resolução de cálculos poderia ser feita ao se utilizar um sistema quântico. Além disso, ele mostrou que seria possível realizar experimentos de simulação para a física quântica. Feynman afirmou que nenhuma máquina de Turing nos modelos clássicos poderia realizar simulações quânticas sem introduzir um fator exponencial em seu desempenho. Com isso foi formulada a idéia do computador quântico. (SOBRAL, 2019)

Em 1985, David Deutsch descreveu um algoritmo quântico simples capaz de determinar se uma função qualquer era constante ou balanceada e demonstrou que um computador quântico teria de fato maior poder de processamento se comparado a uma máquina de Turing probabilística. (SOBRAL, 2019)

Alguns anos depois, em 1994, Peter Shor demonstrou que a utilização de um computador quântico poderia resolver de forma eficiente a fatoração de enormes primos e o problema do logaritmo discreto, justamente onde os algoritmos assimétricos como Diffie-Hellman e RSA apóiam suas seguranças criptográficas, respectivamente. Esse fato seria uma relevante aplicação do computador quântico. (SOBRAL, 2019)

Esse trabalho propiciou um grande aumento de pesquisas na área e trouxe aflição para os pesquisadores de segurança da informação digital. A criptografia assimétrica, que se baseia no uso de números primos gigantes e obtém sua segurança no tempo necessário para fatorá-los, estava ameaçada com os novos desenvolvimentos de Shor. (SANTOS, 2018)

O computador quântico realiza cálculos matemáticos que utilizam propriedades da mecânica quântica. A superposição de estados ocorre quando uma partícula se encontra em diferentes condições ao mesmo tempo e o entrelaçamento quando a alteração em uma partícula provoca o mesmo efeito em outra que se encontra distante. (SOBRAL, 2019)

Na computação clássica o bit é considerado a menor unidade de informação que se tem, e pode assumir valor 0 ou 1. Já na computação quântica, a menor unidade de informação recebe o nome de bit quântico, ou Q-bit. Eles também assumem valores 0 e 1, porém, diferente da computação clássica, os Q-bits podem assumir valores de 0 e 1 simultaneamente. (SANTOS, 2018)

Um estado quântico é considerado qualquer estado possível que um sistema quântico possa se encontrar e pode ser descrito por um vetor de estado, uma função de onda ou por um conjunto completo de números quânticos. O estado quântico fundamental é chamado aquele de menor energia possível. (SOBRAL, 2019)

Para exemplificar o que seria o comportamento de um q-bit e a definição de estado quântico, pode-se usar uma moeda simples de duas faces distintas, “cara” ou “coroa”. Ao ser lançada a moeda o resultado pode ser apenas “cara” ou “coroa”. Mas ao assumir que essa moeda se comporta segundo princípios quânticos, pode-se dizer que o resultado “cara” e “coroa” existem simultaneamente, devido à propriedade de superposição de estados. Fazendo analogia ao sistema clássico, os resultados básicos seriam 0 ou 1, que são os estados básicos, e no caso quântico são representados por $|0\rangle$ e $|1\rangle$. Portanto um estado quântico genérico desse Q-bit deve ser representado pela equação 4. (SOBRAL, 2019)

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{(Equação 4)}$$

Na equação 4 os valores de α e β representam números complexos, que são a probabilidade de se encontrar $|0\rangle$ e $|1\rangle$, respectivamente, ao ser lançada a moeda. O sinal de operação “+” na equação significa sobreposição. Quando é realizada uma medição em um sistema desse tipo um dos estados deixa de existir (colapsa) e o de maior probabilidade é detectado. (SOBRAL, 2019)

A superposição de estados, que é um dos princípios básicos da mecânica quântica e permite a criação de um computador quântico, dificulta a construção desses estados quânticos. Isso porque a sobreposição é muito sensível a micro ruídos eletromagnéticos, que podem modificar o estado do Q-bit, fazendo com que a informação contida no estado seja perdida. (SOBRAL, 2019)

A estrutura básica de um algoritmo quântico é composta por:

- Especificação de *n* Q-bits;
- Aplicação seqüencial de ‘*k*’ operadores quânticos sobre quaisquer subconjuntos dos *n* Q-bits;
- Medição realizada sobre qualquer subconjunto de Q-bits.

Com isso o resultado pode ser obtido apenas de maneira probabilística. Ao serem utilizadas redundâncias, ou seja, o mesmo algoritmo executado diversas vezes, e estratégias de projeto podem aproximar para um resultado determinístico. (SOBRAL, 2019)

Esse é o conceito de computadores Quantum Anealing (ou 'recozimento' em tradução literal), que submetem os dados diversas vezes no algoritmo quântico de forma a extrair aqueles resultados que estatisticamente aparecem com mais probabilidade. (DWAVE, 2017)

Um dos mais conhecidos computadores a operar nesse conceito é o D-Wave, sendo utilizado pela NASA e pela GOOGLE. Entretanto, esse tipo de computador quântico não é reconhecido como "true quantum" (verdadeiramente quântico) apesar de usar as propriedades da mecânica quântica em seu processamento. Devido ao estágio tcnológico do momento, computadores "verdadeiramente quânticos" eram impossíveis de serem contruídos devido aos desafios relacionados a custo e/ou ambiente, lembrando que as partículas quânticas sofrem interferências por temperatura, gravidade e eletromagnetismo - e por isso os "Anealing" fazem diversos processamentos. (DWAVE, 2017)

Entertanto, outros fabricantes, como a IBM, trabalharam nos últimos anos em computadores "verdadeiramente quãnticos", que nãoprecisam reprocessar a informação por diversas vezes e fossem invulneráveis a essas "perturbações". Em 2019 a IBM apresentou o "System Q One", que vem revolucionar a computação quântica mundial e está mostrado na figura 6. (DWAVE, 2017)

Figura 6: System Q One da IBM

Fonte: (IBM, 2019)

2.7 A criptografia quântica

Criptografia quântica pode ser entendia como uma ciência que explora as propriedades da mecânica quântica a fim de realizar criptografia de dados e informações. Ela utiliza a natureza probabilística da mecânica quântica para prover troca de informações e dados com segurança. Para isso serão utilizados os futuros computadores quânticos, que são constantes objetos de pesquisa nos centros tecnológicos dos países mais desenvolvidos. (COSTA, 2008 e DINIZ, 2019)

Abaixo são descritos alguns componentes básicos da criptografia quântica. (DINIZ, 2019)

- Fóton: considerado a menor partícula da luz. Possui três spins: horizontal, vertical e diagonal, que pode ser considerado uma polarização da direita para esquerda.
- Polarização: os fótons são polarizados, e os filtros de polarização são utilizados a fim de retirar os tipos de spins indesejados. O fóton possui os três tipos de estados de spin simultaneamente. Os filtros de polarização manipulam o fóton ao longo do caminho, para que ele tenha um giro específico que se deseja.
- Spin: é uma propriedade de partículas elementares como fótons e elétrons. Campos magnéticos alteram seus estados, desviando-os como se tivessem propriedades de pequenos ímãs. O spin do fóton não muda e pode ter duas orientações possíveis.
- LED: são diodos emissores de luz usados para criar fótons. Os LEDs criam luz não polarizada. Uma sequência de fótons é criada e usada no canal quântico para gerar e distribuir as chaves no processo de distribuição de chaves quânticas entre dois usuários. Na criptografia quântica, apenas um fóton é enviado para ser polarizado na entrada do canal ótico e a polarização é verificada na saída.

O primeiro protocolo criado em 1984, por Charles Bennett e Gilles Brassard, denominado BB84, foi baseado na polarização de fótons de um feixe LASER como unidade básica para implementação de um mecanismo seguro na transmissão de informação de forma segura. Depois disso, diversos protocolos e algoritmos vêm sendo desenvolvidos, baseados no mesmo princípio. (COSTA, 2008)

Já na década de 1990, o emaranhamento, uma propriedade quântica, foi muito estudado com o intuito de ser utilizado em problemas de processamento de informações. Esta propriedade é a capacidade quântica que permite que partículas divididas e colocadas em distância infinita se comportem como “apenas uma”, ou seja, tudo que é feito com uma delas será imediatamente refletido na outra. Dessa forma não é necessário “transmitir chaves” (ou transmitir partículas como chaves), bastando apenas alterar a partícula na origem para que aquela no destino assuma imediatamente o mesmo valor. Com isso muitos trabalhos foram publicados com esse enfoque. Em 1991, Arthur Ekert (EKERT, 1991) demonstrou como o emaranhamento poderia ser utilizado na distribuição de chaves criptográficas imunes a espionagem. (ALBUQUERQUE, 2009)

Em 1992, Charles Bennett e Stephen Wiesner demonstraram uma forma de transmitir dois bits clássicos de informação de forma que apenas fosse usado apenas um bit quântico. Esse trabalho ficou conhecido como codificação superdensa. (BENNETT, 1992) Em 1993, uma equipe formada por seis pesquisadores de diferentes países, explicou como estados quânticos podem ser deslocados de um lugar para outro, mesmo não existindo um canal de comunicação, utilizando o emaranhamento. Esse processo ficou conhecido como teletransporte quântico, sem canal de comunicação, portanto sem risco de interceptação, e assim atendendo a requisitos de segurança propostos. (ALBUQUERQUE, 2009)

Algumas propostas desenvolvidas para criptografia quântica foram baseadas em algumas famílias de protocolos citados nas alíneas abaixo. (COSTA, 2008)

a) **BB84**: Utiliza fótons polarizados em duas bases ortogonais entre si gerados por um usuário da comunicação e utilizados para estabelecer uma chave e verificar a presença de espiões;
b) **B92**: Esse protocolo simplificou o BB84, e utiliza apenas uma base de polarização para o fóton, com o mesmo funcionamento do protocolo original. Existe outra modificação do protocolo que utiliza três bases diferentes;
c) **EPR**: Protocolo que originou diversos outros que utilizam as propriedades de fótons emaranhados previamente preparados para estabelecer uma chave e verificar a presença de espionagem. Ele difere dos anteriores no processo de geração de fótons, sendo feito de forma conjunta pelos dois usuários;
d) **Lo-Chau**: Protocolo baseado no EPR. Utiliza a técnica de correção de erro quântico a fim de obter um método de distribuição de chave.

O protocolo EPR possui algumas vantagens se comparado ao protocolo BB84. Por exemplo, foram verificados menores níveis de erros no protocolo EPR. Porém, devido à simplicidade do BB84, e o desenvolvimento de técnicas de implementação eficientes, este protocolo tem tido grande evolução nas pesquisas de algoritmos criptográficos quânticos. (COSTA, 2008)

Uma característica considerada vantajosa, que leva à utilização de sistemas quânticos na transmissão de informações é a limitação física para realizar medição simultânea de algumas grandezas. Essa propriedade se baseia no princípio da incerteza de Heisenberg (BARROS, 2018) e faz com que sinais quânticos sejam invariavelmente alterados na ocorrência de qualquer tipo de interferência. O fato de um sinal quântico se manter constante quando se tem uma interferência leva a teorema utilizado como um dos fundamentos no método de transmissão seguro baseado em propriedades quânticas. (COSTA, 2008)

Pelo teorema da não-clonagem, é mostrado que é impossível copiar um sinal quântico sem que o sinal original sofra uma modificação significativa, já que por serem partículas em um universo infinitesimal, qualquer tentativa de visualização já traz consigo fatores físicos (como temperatura, pressão, magnetismo e luz) que criam distorções no sinal original. Essas propriedades fundamentam o desenvolvimento de um novo método utilizado para distribuição de chaves criptográficas. (COSTA, 2008)

Uma importante propriedade da distribuição de chaves quânticas é o fato de dois usuários quando se comunicam possuírem a capacidade de detectar a presença de um terceiro desconhecido que tente a interceptação da chave secreta. Com a utilização de entrelaçamento quântico e superposição quântica para transmissão de informações em estados quânticos, o sistema pode detectar uma espionagem. Caso o nível de interceptação esteja abaixo de um limite, uma chave poderá ser produzida com garantia de segurança e o terceiro não conseguirá interceptar a chave. Em caso contrário, não será encontrada nenhuma chave segura e a comunicação será cancelada. (DINIZ, 2019)

A distribuição de chaves quânticas é utilizada para produzir e distribuir uma chave, e não para a transmissão de dados. Essa chave pode ser utilizada com qualquer algoritmo criptográfico. Dentre alguns algoritmos, o que mais se associa à distribuição de chaves quânticas é o One-Time-Pad (SHARMA, 2013), que utiliza a chave uma única vez, e logo após destrói a mesma. (DINIZ, 2019)

A distribuição de chaves quânticas pode ser dividida em duas principais categorias, de acordo com suas propriedades. Elas são descritas a seguir. (DINIZ, 2019)

- **Preparar e medir protocolos**: a medição de um estado quântico desconhecido muda o estado quântico dele de alguma forma. Dessa forma a indeterminação quântica pode ser explorada para detectar uma invasão na comunicação, e ainda mais importante, é possível calcular a quantidade de informação interceptada.
- **Protocolos baseados em entrelaçamento**: os estados quânticos de objetos separados podem ser unidos de forma que eles devem ser caracterizados por um estado quântico combinado, e não separadamente. Esse efeito é chamado de entrelaçamento, e com isso ao tentar realizar medição em uma das partes, a ligação é quebrada de entrelaçamento e a segunda parte fica afetada com esta medição. Se um par de objetos entrelaçados for compartilhado entres duas partes, qualquer interceptação altera o sistema geral, o que revela a presença de terceiros.

Essa duas propriedades são divididas em três famílias de protocolos, que são chamados de “Variável Discreta”, “Variável Contínua” e “Codificação de Referência de Fase Distribuída”. Os protocolos de variável discreta são os mais antigos, entretanto continuam sendo implementados. As outras duas famílias são utilizadas visando reduzir as limitações encontradas. Os protocolos BB84 e E91 utilizam codificação de variáveis discretas. (DINIZ, 2019)

Esses protocolos de distribuição de chave quântica fornecem aos usuários da comunicação chaves compartilhadas quase idênticas e uma estimativa de diferenças entre as chaves. As diferenças podem ser causadas por efeitos de tentativas de interceptação externa ou por imperfeições na linha de transmissão e nos detectores. Visto que não é possível discriminar qual foi o tipo de erro ocorrido, deve-se supor que todos os erros são ocorridos em virtude de tentativas de interceptação. Isso é considerado para se ter uma garantia de segurança. (DINIZ, 2019)

A taxa de erro das chaves deve ser menor que um determinado valor limite para que duas etapas sejam executadas a fim de que os bits errados sejam removidos e o nível de conhecimento do interceptador da chave secreta seja reduzido a um valor baixo. Essas duas etapas são conhecidas como “reconciliação de informações” e “amplificação de privacidade”. (DINIZ, 2019)

Reconciliação de informações é uma maneira de corrigir erros nas chaves de dois usuários, a fim de garantir que as elas sejam idênticas. É implementado em um canal público,

e por isso é necessário minimizar as informações a respeito das chaves, para que não seja interceptado por um invasor. Já a amplificação de privacidade é um método para reduzir e eliminar as informações parciais que o invasor possui das chaves dos usuários. As informações parciais podem ser obtidas por espionagem no canal quântico durante a transmissão de chaves ou no canal público durante a reconciliação de informações. (DINIZ, 2019)

2.7.1 O protocolo BB84

No protocolo BB84 dois usuários são interconectados por um canal de comunicação quântica, permitindo que os estados quânticos sejam transmitidos. Para os fótons o canal geralmente é uma fibra ótica e os usuários comunicam-se por um canal público clássico utilizando uma transmissão de rádio ou Internet. O protocolo foi projetado com a idéia que um interceptador pode tentar interferir no canal quântico e uma autenticação é feita pelo canal clássico. (DINIZ, 2019)

Neste protocolo a segurança é embasada através da codificação da informação em estados não ortogonais. Ele usa dois pares de estados de estados ortogonais entre si, que são chamados de base. Os pares de estados de polarização mais comumente utilizados são a base retilínea vertical e horizontal (0º e 90º respectivamente) e a base diagonal (45º e 135º). (DINIZ, 2019)

A primeira etapa do protocolo é a transmissão quântica. Um usuário cria aleatoriamente um bit e da mesma forma aleatória escolhe uma base, retilínea ou diagonal, para então transmitir. A preparação do estado de polarização dos fótons varia de acordo com o valor do bit e a base escolhida, conforme mostrado na tabela 4. Um fóton é transmitido por um usuário utilizando o canal quântico. O processo de transmissão se repete a partir do estágio de bit aleatório, e o transmissor registra o estado, a base e o tempo de todos os fótons encaminhados. (BENNETT, 1984 e DINIZ, 2019)

Tabela 4: Estados de polarização dos fótons.

Bits Bases	0	1
+	↑	→
x	↗	↘

Fonte: (BENNETT, 1984)

Baseado nos conceitos da mecânica quântica, uma medida capaz de diferenciar os quatro estados de polarização não existe, devido a não ortogonalidade entre todos os estados. A realização dessa medida apenas é possível entre dois estados ortogonais. Caso uma medição seja realizada na base retilínea e o fóton criado foi na polarização vertical ou horizontal, então a medição é correta. Porém se o fóton criado foi em 45º ou 135º, a medida retornará horizontal ou vertical aleatoriamente. A informação só é considerada válida se a medição for correta. (BENNETT, 1984 e DINIZ, 2019)

Tendo em vista que o receptor não conhece a base dos fótons recebidos, ele escolhe uma base aleatoriamente para realizar a medição. Ao receber ele registra o tempo, a base de medição e o resultado da medição, repetindo esse processo para todos os fótons chegados. De posse de todos os fótons recebidos e medidos, o receptor se comunica com o emissor pelo canal público clássico, e eles trocam a informação de qual base foi utilizada para enviar os fótons e qual base foi medida na recepção de cada um. Após isso são descartadas medidas de fótons incorretas, em que o receptor utilizou uma base diferente da utilizada na emissão. Em média esses excluídos representam metade dos fótons, e a metade correta representa a chave compartilhada. (BENNETT, 1984 e DINIZ, 2019)

A comparação de uma sequência predefinida de fótons corretos é feita entre os usuários, a fim de verificar a presença de possíveis interceptadores na comunicação. A ação externa de alguém durante a comunicação insere erros nas medidas do receptor. Além de possíveis ataques, esses erros podem ser causados por condições ambientais. Se o erro for acima de um limiar aceitável, a chave é descartada e repete-se o processo, através de um novo canal quântico. (BENNETT, 1984 e DINIZ, 2019)

Na tabela 5 é mostrado um exemplo de como funciona esse processo de troca de chave entre os usuários.

Tabela 5: Exemplo do processo de troca de chaves entre os usuários.

O bit aleatório da Alice	0	1	1	0	1	0	0	1
A base de envio aleatório da Alice	+	+	×	+	×	×	×	+
Polarização dos fotões que a Alice enviou	↑	→	↘	↑	↘	↗	↗	→
Base de medição aleatória do Bob	+	×	×	×	+	×	+	+
Medição da polarização do fotão do Bob	↑	↗	↘	↗	→	↗	→	→
DISCUSSÃO PÚBLICA DA BASE								
Chave secreta compartilhada	0		1			0		1

Fonte: (BENNETT, 1984)

Os protocolos quânticos, apesar de serem considerados seguros, sofrem alguns tipos de ataques que exploram algumas vulnerabilidades deles. Para serem contextualizados, esses tipos de ataque serão destacados nesta subseção, considerando o protocolo BB84.

2.7.1.1 Ataque “Man-in-the-middle”

O protocolo BB84 está vulnerável quando se fala de autenticação do canal clássico. Quando o protocolo é implementado para distâncias grandes, como acontece na realidade, se faz necessário algum mecanismo que permita os dois usuários se certificarem que estão se comunicando com a pessoa que realmente espera. Caso não exista tal mecanismo, existe a possibilidade de que um terceiro mal intencionado se passe um dos usuários para o outro e

vice e versa, estabelecendo a chave de comunicação com os usuários da comunicação sem que eles notassem essa presença externa. (COSTA, 2008)

Nesse caso o protocolo BB84 se assemelha aos algoritmos clássicos, com problemas de autenticação dos usuários, para se ter uma comunicação segura sem ter um segredo compartilhado inicial. Diversos métodos foram criados a fim de criar este segredo compartilhado inicial, utilizando teoria dos terceiros ou de caos, porém apenas a família de funções *hash* pode ser utilizada para autenticação segura. (DINIZ, 2019)

Uma função hash funciona a partir de uma entrada de tamanho variável que é convertida em uma saída de tamanho fixo. Uma função hash considerada boa, a partir de um grande conjunto de entradas, produz saídas distribuídas igualmente e aparentemente de modo aleatório. O seu objetivo principal é manter a integridade dos dados. (STALLINGS, 2015)

2.7.1.2 Interceptação-reenvio

Esse ataque é considerado o mais simples para o interceptador, que recebe os Q-bits vindos de um usuário e faz uma medição em uma das duas bases de medida do protocolo BB84, assim como faria o segundo usuário. Nesse momento, o interceptador prepara os Q-bits no mesmo estado ao que foi medido e encaminha para o segundo usuário, que receberia a mensagem original. Essa interceptação, entretanto, produz erros na partilha de chaves entre os usuários. (COSTA, 2008 e DINIZ, 2019)

A probabilidade de o interceptador realizar uma medição correta dos Q-bits enviados pelo usuário é de 50% e ele enviará para o segundo usuário o estado correto, o que permite que ele não seja detectado. Porém 50% da informação do interceptador provocará descorrelação entre os resultados dos usuários, o que permitirá a detecção do invasor. O interceptador, para não ser detectado, aplica seu ataque apenas em uma pequena parcela dos Q-bits enviados pelo primeiro usuário, gerando uma pequena taxa de erro e assim obtendo uma pequena parte da informação original. (COSTA, 2008 e DINIZ, 2019)

2.7.1.3 Outros tipos de ataques

Existem alguns outros tipos de ataques que serão apenas citados neste trabalho. O ataque de negação de serviço (*Denial of Service*), visa a necessidade de uma linha dedicada de fibra ótica entre dois pontos ligados pela distribuição de chaves quânticas. Esse ataque pode ser implementado cortando ou bloqueando a linha. (DINIZ, 2019)

No ataque tipo Cavalo de Tróia, um interceptador pode testar um sistema de distribuição de chaves quânticas enviando luz brilhante no canal quântico e fazendo avaliações das reflexões. (DINIZ, 2019)

Outro ataque que permite a obtenção de informação utiliza a imperfeição das implementações físicas do canal quântico, visando obter a chave trocada pelo protocolo, é chamado de “Beam-Splitting”. Para a implementação do protocolo BB84 são utilizados geradores de pulsos de laser que não produzem apenas um fóton por pulso e eventualmente são produzidos mais de um fóton por pulso. Esse fóton excedente pode ser capturado por um interceptador, utilizando uma técnica de divisão de feixe, que permite a medição em um dos fótons deixando o outro intacto e este último é enviado para o usuário real. A detecção do interceptador nesse ataque é difícil, já que os estados dos Q-bits não são alterados na transmissão de informações. (COSTA, 2008)

2.7.2 Comunicações quânticas e seus desafios

Os estudos elaborados a respeitos dos protocolos de criptografia quântica, principalmente aqueles baseados no BB84, teoricamente, são uma alternativa para futuras gerações de sistemas de criptografia resistentes a tecnologias de processamento de informações avançadas. Porém existem alguns fatores a serem considerados para que esses protocolos sejam aplicados em sistema com infraestrutura padrão de telecomunicações. (COSTA, 2008)

O primeiro ponto a ser considerado é que os protocolos quânticos foram desenvolvidos para serem aplicados em comunicações ponto-a-ponto, entre dois usuários. Isso limita a aplicação uso da técnica em diversas áreas que necessitam de mais de dois usuários na comunicação. O segundo ponto é a limitação máxima de distância e taxa de transferência no processo de comunicação. Outro aspecto relevante está na implementação de uma estrutura de telecomunicações para operar com os protocolos quânticos. Essa estrutura está se chamando de rede quântica, que tem a ideia de ampliar a comunicação para grandes distâncias e múltiplos usuários, e será operada em paralelo com a rede de telecomunicações já existente. (COSTA, 2008)

Para se ter uma ampla aplicação das comunicações quânticas alguns outros desafios práticos e teóricos são objetos de estudos e pesquisas. Dentre eles alguns são citados abaixo. (NETO, 2004)

- Fontes geradoras de fótons, com tamanho reduzido e a baixo custo, devem ser implementadas;
- Desenvolvimento de fotodiodos com baixos ruídos em altas temperaturas e alta eficiência quântica;
- Repetidores quânticos que façam aumentar o alcance na comunicação entre usuários na rede,
- Protocolos quânticos que utilizam sistemas quânticos de mais de dois estados;
- Integrar a infraestrutura da rede quântica com a rede de comunicações já existente;
- Implementar métodos de testes de segurança dos protocolos.

Ao longo dos anos muito tem sido feito para avançar no desenvolvimento da tecnologia e diferentes institutos de pesquisa privados, governamentais ou ligados a universidades trabalham na área. Empresas ligadas a tecnologia como IBM, HP e NEC têm pessoal qualificado e dedicado em seus laboratórios específicos sobre comunicação quântica. O NIST é um exemplo de instituto governamental que promove diversas pesquisas relacionadas. Existem ainda empresas quem são financiadas com recursos provenientes do governo, por exemplo, BBN Technologies, QinetiQ, MagiQ e IdQuantique. Essas duas últimas implementaram os primeiros dispositivos comerciais de criptografia quântica. (COSTA, 2008)

2.8 A criptografia pós-quântica

A criptografia pós-quântica estuda algoritmos criptográficos considerados seguros a ataques provenientes de computadores quânticos. Os algoritmos clássicos baseiam sua segurança em basicamente três problemas matemáticos. São eles: a fatoração de números inteiros gigantes formados pelo produto de dois números primos grandes, o problema do logaritmo discreto e o problema do logaritmo discreto da curva elíptica. Quando o computador quântico for uma realidade prática, esses problemas matemáticos serão facilmente resolvidos devido à sua característica de processamento paralelo, podendo testar todas as possíveis combinações numéricas de forma não-sequencial, invalidando a segurança na qual tais problemas matemáticos se apoiam. (DINIZ, 2019)

Muitos criptógrafos ao redor do mundo estudam e desenvolvem algoritmos a espera do momento em que os computadores quânticos serão uma real ameaça aos sistemas

criptografados. Desde 2006, com a conferência PQCrypto, muitos trabalhos ganharam atenção especial em todas as áreas onde se deseja ter segurança da informação e comunicações. Recentemente esses estudos cresceram com diversos workshops sobre criptografia segura de Quantum, realizados pelo Instituto Europeu de Padrões de Telecomunicações (ETSI) e pelo Instituto de Computação Quântica. (DINIZ, 2019)

Os sistemas criptográficos de chave pública, que são muito utilizados, estarão sobre forte ameaça quando o computador quântico for uma realidade. Com o algoritmo de Peter Shor é possível resolver os problemas matemáticos que são a base para a segurança desses algoritmos. Para o RSA, por exemplo, seriam devastadoras as conseqüências da aplicação do algoritmo de Shor, visto que o aumento das chaves não resolveria o problema. Em face ao exposto, os algoritmos de chave pública perderiam seu valor e deveriam ser inutilizados, sendo substituídos por outros que garantissem a segurança. (OLIVEIRA et al., 2017)

Os algoritmos pós-quânticos podem ser implementados em computadores convencionais, enquanto a criptografia quântica depende de uma infraestrutura quântica pronta. Todos os obstáculos encontrados para a realização da criptografia quântica, como dificuldades e altos custos para a realizada da infraestrutura, fazem com que haja um crescente interesse na criptografia pós-quântica. (OLIVEIRA et al., 2017)

Diversos estudos são realizados pelo NIST para que se tenha uma padronização para os sistemas criptográficos pós-quânticos, porém ainda não existe nenhum estabelecido. Possivelmente, alguns anos ainda serão necessários para se chegar à definição de padrões. Isto pode ser um desafio de interoperabilidade para os sistemas que devem oferecer segurança de longo prazo. (OLIVEIRA et al., 2017)

A criptografia assimétrica pós-quântica tem um grande desafio que é a redução do tamanho das chaves públicas e privadas, e o *overhead* de espaço considerável por mensagem a ser criptografada ou assinada. Assim, muitos estudos e pesquisas são realizados com a intenção de tornar tal técnica mais eficiente e competitiva se comparada às técnicas convencionais. Destaca-se que muitos esquemas pós-quânticos já são competitivos e algumas vezes já superam os convencionais quando se fala de tempo de processamento, tamanho de código fonte e ocupação de memória RAM. (BARRETO et al., 2013)

O NIST promove, desde 2016, um concurso que visa avaliar e estabelecer padrões de algoritmos de criptografia de chave pública pós-quânticos. Esse concurso foi nomeado de *Post-Quantum Cryptography Standardization* (PQCS). Esse concurso analisa os algoritmos submetidos em diversos critérios: aplicação do algoritmo, segurança, custo, tempo de execução para gerar as chaves, assinar e verificar e eficiência. (BELARMINO, 2019)

Diversos algoritmos de assinatura digital são analisados no concurso e dentre eles os baseados em “reticulados” (Lattice algorithms) são destacados, pois apresentam demonstrações formais de segurança e implementações eficientes e relativamente simples. Na seção 2.8.1 serão apresentados alguns desses algoritmos. (BELARMINO, 2019)

2.8.1 Algoritmos de assinatura digital submetidos ao PQCS

O algoritmo CRYSTALS-DILITHIUM (*Cryptographic Suite for Algebraic Lattices Dilithium*), foi proposto em 2019, e apresenta uma solução de assinatura digital. (DUCAS et al., 2019) Ele propõe uma opção determinística e uma aleatória para sua implementação, entretanto a versão determinística é sugerida como padrão pelos autores, com exceção em casos que o atacante tem a possibilidade de explorar o determinismo por ataques de canal lateral. O FALCON (*Fast-Fourier Lattice-bases Compact Signatures over NTRU*) foi proposto em 2018. (FOUQUE et al., 2018). O qTESLA (BINDEL et al., 2019) é um algoritmo proposto em duas versões, que são o “qTESLA heurístico” e o “qTESLA demonstravelmente seguro”. (BELARMINO, 2019)

Os três algoritmos atendem diferentes níveis de segurança propostos pelo NIST. A escolha do algoritmo deve ser feita de acordo com a aplicação que será empregado. O CRYSTALS-DILITHIUM é mais lento para assinar e verificar se comparado ao qTESLA. O FALCON apresenta parâmetros com menor tamanho se comparado aos outros. O qTESLA abrange mais níveis de segurança propostos pelo NIST, possui versões demonstravelmente seguras e a geração de chaves é mais lenta. No geral o qTESLA apresenta melhor desempenho. (BELARMINO, 2019)

De acordo com o site do NIST, nove algoritmos de assinatura digital foram para a segunda fase de análises do concurso. Eles são listados abaixo. (NIST, 2019)

- CRYSTALS-DILITHIUM
- FALCON
- GeMSS
- LUOV
- MQDSS
- Picnic
- qTESLA
- Rainbow

- SPHINCS+

2.8.2 Outros algoritmos pós-quânticos

Até o prazo dado pelo NIST para receber trabalhos participantes do PQCS, foram recebidos 82, provenientes de 25 países diferentes de seis continentes. Após o recebimento, todos eles foram analisados e avaliados se participariam ou não do processo, e com isso apenas 69 foram anunciados na primeira fase do concurso. Após dois meses, cinco candidatos foram desclassificados, restando apenas 64 trabalhos. Esses trabalhos aceitos foram divididos em algumas categorias (CHEN et al., 2016). São elas: Lattice-based (baseados em reticulados), Multivariable (Multivariável), HASH-based (baseados em funções Hash), Code-based (baseados em código), entre outras, que está mostrado o resumo dessa distribuição na tabela 6. (CHEN, 2020)

Tabela 6: Distribuição dos algoritmos na primeira fase do concurso.

	Assinatura Digital	Encriptação/Gerenciamento de chave	TOTAL
Baseados em reticulados	5	21	26
Baseados em código	2	17	19
Multivariável	7	2	9
Baseados em funções Hash	3	0	3
Outros	2	5	7
TOTAL	19	45	64

Fonte: (CHEN, 2020)

Em abril de 2018 aconteceu o primeiro Congresso de Padronização de Criptografia Pós-Quântica do NIST, onde foram feitas 52 apresentações a respeito de 60 algoritmos. Cada equipe apresentou seu trabalho mostrando suas vantagens, desvantagens e diferenças para os outros envolvidos no congresso. Esse primeiro evento gerou diversos trabalhos novos e muitos artigos foram publicados abordando pontos discutidos nas apresentações. (CHEN, 2020)

Em janeiro de 2019 o NIST revelou que 26 trabalhos passariam à segunda fase do concurso. Nesse segundo filtro foram levados em consideração fatores como segurança, custo

e desempenho, além de características de implementação dos algoritmos. Nessa etapa a diversificação de algoritmos é importante para se ter a continuidade da pesquisa com variações de abordagens, visto que uma categoria pode completar a outra e vice e versa. A tabela 7 mostra como ficou a distribuição dos algoritmos na segunda fase. (CHEN, 2020)

Tabela 7: Distribuição dos algoritmos na primeira fase do concurso.

	Assinatura Digital	Encriptação/Gerenciamento de chave	TOTAL
Baseados em reticulados	3	9	12
Baseada em código	0	7	7
Multivariável	4	0	4
Baseada em Hash	2	0	2
Outros	0	1	1
TOTAL	19	45	26

Fonte: (CHEN, 2020)

O processo de padronização do NIST foi programado para durar alguns anos. Espera-se que a segunda fase tenha duração de 12 a 18 meses. Ainda pode ser realizada uma terceira fase a critério do NIST. A expectativa é que em 2022 ou 2023 se consiga finalizar o concurso e enfim tenha uma padronização para os algoritmos pós-quânticos. (CHEN, 2020)

3 METODOLOGIA

A metodologia utilizada para elaborar esse trabalho tem um caráter qualitativo, já que as informações foram obtidas a partir de livros, artigos, teses e dissertações a respeito do assunto em questão. A pesquisa envolve apenas dados qualitativos, não sendo utilizados experimentos laboratoriais ou em campo, além de não se fazer uso de métodos numéricos ou matemáticos para encontrar soluções para o problema em análise. Simples equações são mostradas para tentar embasar o assunto de forma mais clara, mas não abrange a exploração matemática delas.

Ao longo deste trabalho serão abordados os princípios básicos da criptografia clássica, do funcionamento do computador quântico e das criptografia quântica e pós-quântica, a fim de mostrar para Marinha do Brasil como será o comportamento dos sistemas criptográficos com o advento do computador quântico, e o que isso impactará para a instituição.

3.1 Classificação da Pesquisa

Uma pesquisa pode ser feita de diversas maneiras e possui algumas classificações que podem enquadrá-la. Ela pode ser classificada quantos aos fins e quanto aos meios. Este subitem do trabalho foi destinado a esse enquadramento da pesquisa.

3.1.1 Quanto aos fins

A pesquisa em questão pode ser classificada quanto aos fins como explicativa, já que foi feita para justificar a necessidade da busca de conhecimento na área da criptografia quântica e pós-quântica.

3.1.2 Quanto aos meios

Quanto aos meios, a pesquisa pode ser classificada como bibliográfica, já foi realizada com base em trabalhos publicados de amplo acesso, como teses de doutorado, dissertações de mestrado, artigos, livros e pesquisas de inovações e produtos já lançados e em uso no mercado.

3.2 Limitações do Método

A limitação do método escolhido é o nível de profundidade que foi dado à parte matemática da criptografia. Isso porque foi proposta apenas uma visão teórica acerca do assunto, visto que não houve tempo hábil para uma abordagem mais prática do tema estudado.

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Deve-se ter em mente que um sistema criptográfico é mais robusto se tanto a criptografia quântica, quanto a pós-quântica, estão disponíveis. Nesse caso, alguns usuários serão beneficiados em um dado grau de segurança a um custo menor enquanto outros utilizarão um método muito mais confiável para obter confidencialidade em longo prazo. Assim, os dois sistemas podem obter ferramentas de segurança com certas peculiaridades que não podem ser obtidas se aplicadas individualmente. (MOSCA, 2015)

Muitas pesquisas devem ser realizadas nos próximos anos a fim de aumentar o conhecimento e ampliar os horizontes do que se tem hoje em termos de criptografia quântica e pós-quântica. Com isso será possível estabelecer padronizações de uso para as diversas aplicações e usuários pelo mundo. (MOSCA, 2015)

Esses padrões deverão estar prontos para serem aplicados na prática quando sistemas quânticos estiverem sendo operados. Os profissionais técnicos da área de criptologia deverão estar prontos para as novas ferramentas e modos de trabalhar na sua área, visto que se dará uma quebra de paradigmas da criptologia. (MOSCA, 2015)

O uso do poder de processamento do computador quântico em larga escala possibilitará para a humanidade a resolução de diversos problemas históricos, na área da saúde por exemplo. Porém, deve-se pensar antes no enorme impacto que este equipamento trará para a segurança cibernética. Por isso é necessário estar pronto no momento certo. (MOSCA, 2015)

5 CONCLUSÃO

Diante do tema apresentado e discutido, a Marinha do Brasil deve ficar atenta à evolução dos algoritmos e sistemas criptográficos, visto que para manter os requisitos citados da segurança da informação e comunicações devem-se investir recursos a fim de estabelecer protocolos para atender as demandas necessárias de criptografia da instituição.

Os riscos de ter informações sigilosas ameaçadas não se restringem apenas para o presente e futuro, mas também para documentos passados. Isto se deve ao fato de que diversos materiais que tenham grau de sigilo com validade de longos períodos e utilizam chaves criptográficas tradicionais estarão ameaçados com a aplicação de algoritmos quânticos com intenção de quebrá-las. Com isso é de extrema importância o desenvolvimento de chaves que garantam o sigilo desses materiais.

Os algoritmos quânticos devem ser adotados não apenas visando o arquivamento de documentos, mas também para serem aplicados nas comunicações entre as autoridades navais visto que elas estarão sujeitas a interceptação em suas trocas de informações.

Existe ainda um risco de países que estão na frente do Brasil em termos de pesquisas na área implementarem um computador quântico e ter acesso às informações sigilosas brasileiras sem nem mesmo chegar ao conhecimento das autoridades, o que caracteriza ações de espionagem. Assim o risco de se ter informações vazadas aumenta ainda mais.

A ideia principal é se precaver às possíveis ações dos computadores quânticos que terão poder de processamento elevadíssimo se comparado melhores computadores que existem atualmente. Comparando-se essas capacidades, os computadores atuais levariam 100 anos para descriptografar uma chave hipotética que utiliza o RSA, enquanto os computadores quânticos levariam horas ou mesmo minutos para cumprir a mesma tarefa.

A Marinha do Brasil deve se preocupar com esse tema e divulgar a importância dele para o futuro da segurança das informações e comunicações. Para isso sugere-se a realização de seminários e simpósios sobre o assunto para que a mentalidade de segurança cresça entre os militares da força e para que todos tenham a consciência da necessidade de se antever ao novo paradigma da criptografia.

5.1 Sugestões para Futuros Trabalhos

Como sugestão para trabalhos futuros pode-se analisar outros protocolos, visto que o presente trabalho focou mais no BB84. Pode-se ter um enfoque maior na questão matemática que envolve a criação de protocolos, visto que este trabalho focou apenas em uma abordagem teórica, mostrando diferenças entre os tipos de algoritmos.

Buscar parcerias com laboratórios de universidades ou institutos de pesquisa que trabalhem as criptografias quântica e pós-quântica para tentar implementar ou acompanhar algum experimento prático de aplicação de um protocolo quântico.

REFERÊNCIAS

ALEGRETTI , F. J. P. **Computação Quântica**. Programa de pós-graduação em computação. Universidade Federal do Rio Grande do Sul**,** 2004.

ARTZ, D. **Digital Steganography: Hiding Data within Data**. IEEE Internet Computing, 2001.

BARBOSA, L. A. de M., BRAGHETTO, L. F. B., BRISQUI, M. L. e DA SILVA, S. C. **RSA Criptografia Assimétrica e Assinatura Digital**. Especialização em Redes de Computadores. Campinas: Universidade Estadual de Campinas, 2003.

BARRETO, P. S. L. M., BIASI, F. P., DAHAB, R., LÓPEZ-HÉRNANDEZ, J. C., MORAIS, E., OLIVEIRA, A. K. D. S., OLIVEIRA, T, PEREIRA, G. C. C. F. e RICARDINI, J. E. **Introdução à criptografia pós-quântica**, Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2013, Cap 2, 2013.

BARROS, A. A. **90 anos do Princípio de incerteza de Heisenberg: das grandezas não comutáveis ao artigo de 1927**. Mestrado em ensino de Ciências e Educação Matemática. Campina Grande: Universidade Estadual da Paraíba, 2018.

BELARMINO, G. D. e GOYA, D. H. **Algoritmos de Assinatura Digital Baseada em Reticulados Candidatos a Padrão Pós-Quântico**. Santo André: Universidade Federal do ABC, 2019.

BENNET, C. H. e WIESNER, S. J. **Communication via 1-and 2-particle operators on Einstein-Podolsky-Rosen states**, 1992.

BENNETT, C. H. e BRASSARD, G. **Quantum cryptography: Public key distribution and coin tossing**, 1984.

BINDEL, N., ALKIM, E., BARRETO, P. S. L. M., AKLEYLEK, S., BUCHMANN, J., , EATON, E., GUTOSKI, G., KRAMER, J., LONGA, P., POLAT, H., RICARDINI, J. E., e ZANON, G. **Submission to NIST's post-quantum project (2nd round): lattice-based digital signature scheme qtesla**, 2019.

BONFIM, D. H. **Criptografia RSA**. Mestrado Profissional em Matemática. São Carlos: Universidade de São Paulo, 2017.

CHEN L. e Moody, D. **New mission and opportunity for mathematics researchers: Cryptography in the quantum era**, 2020.

CHEN, L., JORDAN, S., LIU, Y. K., MOODY, D., PERALTA, R., PERLNER, R. e SMITH-TONE, D., R**eport on Post-Quantum Cryptography**, National Institute of Standards and Technology Internal Report (NISTIR) 8105, 2016.

COSTA, C. H. A. **Criptografia quântica em redes de informação crítica – aplicação a telecomunicações aeronáuticas**. Mestrado em Engenharia da Computação e Sistemas Digitais. São Paulo: Universidade de São Paulo, 2008.

DINIZ, J. M. G. **O Contributo Quântico para a 4ª Revolução Industrial**. Mestrado em Engenharia Informática e de Telecomunicações. Lisboa: Universidade Autónoma de Lisboa, 2019.

DUCAS, L., KILTZ, E., LEPOINT, T., LYUBASHEVSKY, V., SCHWABE, P., SEILER, G., e STEHLÉ, D. **CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation**, 2017.

DWAVE. **The D-Wave 2000TM Quantum Computer. Technology Overview.** 2017. Disponível em <https://www.dwavesys.com/resources/media-resources>. Acesso em: 25 de fevereiro de 2020.

EKERT, A. K. **Quantum cryptography based on Bell's theorem**, 1991.

FIARRESGA, V. M. C. **Criptografia e matemática**. Mestrado em Matemática para Professores. Lisboa: Universidade de Lisboa, 2010.

FOUQUE, P. A., HOFFSTEIN, J., KIRCHNER, P., LYUBASHEVSKY, V., PORNIN, T., PREST, T., RICOSSET, T., SEILER, G., WHYTE, W. e ZHANG, Z. **Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU**, 2018.

JORCUVICH, W. N. S. **Uma introdução à Computação Quântica**. Bacharelado em Matemática Aplicada e Computacional. São Paulo: Universidade de São Paulo, 2018.

KAHN, D. **The Codebreakers: The story of Secret Writing**. New York: Scribner, 1996.

KRISCHER, T. C. **Um estudo da máquina Enigma**. Bacharelado em Ciência da Computação. Porto Alegre: Universidade Federal do Rio Grande do Sul, 2012.

LUBY, M., RACKOFF, C. **How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing**, 1988.

MORENO, E. D., PEREIRA, F. D. e CHIARAMONTE, R. B. **Criptografia em software e hardware**. São Paulo - SP. Novatec, 2005.

MORRIS, B., ROGAWAY, P., STEGERS, T. **How to encipher messages on a small domain: deterministic encryption and the Thorp shuffle**, 2009.

MOSCA, M, **Cybersecurity in an era with quantum computers: will we be ready?**, 2015.

NETO, F. C. J., DUARTE, O. C. M. B. **Criptografia Quântica para Distribuição de Chaves**. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2004.

OLIVEIRA, L. B., PEREIRA, F. M. Q., MISOCZKI, R., ARANHA, D. F., BORGES, F. e LIU, J. **The computer for the 21st century: Security & privacy challenges after 25 years**. 26th International Conference on Computer Communication and Networks (ICCCN), 2017

PETRI, M. **Esteganografia**. Bacharelado em Sistemas de Informação. Joinville: Instituto Superior Tupy, 2004.

NIST. **PQC Standardization Process: Second Round Candidate Announcement**. 30 de janeiro de 2019. Disponível em: <https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates> Acesso em: 20 de fevereiro de 2020.

RIVEST, R. L., SHAMIR, A. e ADLEMAN, L. **A Method for Obtainig Digital Signatures and Public-Key Cryptosystems**, Communications of the ACM, 1978.

SANTOS, P. S. **Q-bit: um novo fundamento lógico**. Bacharelado em Engenharia da Computação. João Molevade: Universidade Federal de Ouro Preto, 2018.

SHARMA, S. e GUPTA, V. **Encryption and Decryption using One Pad Time Algorithm in Mac Layer.** International Journal of Innovative Research in Science, Engineering and Technology, 2013.

SINGH, S. **O livro dos códigos**. A ciência do sigilo – do antigo Egito à criptografia quântica. 4ª ed. Tradução de Jorge Calife. Rio de Janeiro - RJ. Record, 2004.

SOBRAL, J. B. M. e MACHADO, R. B. **Computação Quântica: Aspectos Físicos e Matemáticos - Uma Abordagem Algébrica.** Universidade Federal de Santa Catarina. Florianópolis- SC, 2019.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6ª ed. Tradução: Daniel Vieira. São Paulo – SP. Pearson Education do Brasil, 2015.