INSTITUTO FEDERAL GOIANO - CAMPUS CERES
BACHARELADO EM SISTEMAS DE INFORMAÇÃO
WILLIAN WALLACE DE MATTEUS SILVA

A EVOLUÇÃO DA CRIPTOGRAFIA E SUAS TÉCNICAS AO LONGO DA HISTÓRIA

CERES - GO
2019

WILLIAN WALLACE DE MATTEUS SILVA

A EVOLUÇÃO DA CRIPTOGRAFIA E SUAS TÉCNICAS AO LONGO DA HISTÓRIA

Trabalho de curso apresentado ao curso de Sistemas de Informação do Instituto Federal Goiano – Campus Ceres, como requisito parcial para a obtenção do título de bacharel em Sistemas de Informação, sob orientação do Prof. Me. Rangel Rigo.

CERES - GO

2019

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

WSI586 e

Wallace de Matteus Silva, Willian
A Evolução da Criptografia e Suas Técnicas ao Longo da História / Willian Wallace de Matteus Silva;orientador Rangel Rigo. -- Ceres, 2019.
17 p.

Monografia (em Bacharelado em Sistemas de Informação) -- Instituto Federal Goiano, Campus Ceres, 2019.

1. chave simétrica. 2. chave assimétrica. 3. chave pública e privada. 4. criptossistema. 5. cifras. I. Rigo, Rangel , orient. II. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

Identificação da Produção Técnico-Científica

[ ] Tese	[ ] Artigo Científico
[ ] Dissertação	[ ] Capítulo de Livro
[ ] Monografia – Especialização	[ ] Livro
[X] TCC - Graduação	[ ] Trabalho Apresentado em Evento
[ ] Produto Técnico e Educacional - Tipo: _____	

Nome Completo do Autor: Willian Wallace de Matteus Silva
Matrícula: 2016103202030252
Título do Trabalho: A Evolução da Cristalografia e suas Técnicas ao Longo da História

Restrições de Acesso ao Documento

Documento confidencial: [X] Não [ ] Sim, justifique: _____

Informe a data que poderá ser disponibilizado no RIIF Goiano: 20/12/2013
O documento está sujeito a registro de patente? [ ] Sim [X] Não
O documento pode vir a ser publicado como livro? [ ] Sim [X] Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Luziânia-GO, 13/12/2013
Local Data

Willian Wallace de Matteus Silva
Assinatura do Autor e/ou Detentor dos Direitos Autorais

Ciente e de acordo:

Rangel

ANEXO IV - ATA DE DEFESA DE TRABALHO DE CURSO

Ao(s) 21 dia(s) do mês de Novembro do ano de dois mil e dezenove, realizou-se a defesa de Trabalho de Curso do(a) acadêmico(a) William Wallace de Matteus Silva, do Curso de Bacharelado em Sistemas de Informaç matrícula 20161303202030257, cujo título é " A evolução da criptografia e suas técnicas ao longo da história ". A defesa iniciou-se às 21 horas e 10 minutos, finalizando-se às 21 horas e 35 minutos. A banca examinadora considerou o trabalho apto com média 9,0 no trabalho escrito, média 8,8 no trabalho oral, apresentando assim média aritmética final 8,9 de **pontos,** estando o(a) estudante apto para fins de conclusão do Trabalho de Curso.

Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, o(a) estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

Assinatura Presidente da Banca

Assinatura Membro 1 Banca Examinadora

Assinatura Membro 2 Banca Examinadora

Dedico este trabalho a todos que me apoiaram
e que contribuíram para a sua realização.

AGRADECIMENTOS

Agradeço primeiramente ao Instituto Federal Goiano Campus Ceres pela oportunidade de me capacitar e aos professores que tanto me ajudaram e ensinaram. Quero fazer um agradecimento especial ao professor Rangel Rigo que tanto ajudou na confecção deste trabalho, aplicando seu tempo e conhecimento na orientação do mesmo.

Quero deixar meu muito obrigado a todos os colegas que me apoiaram e me deram forças para continuar. E acima de tudo deixo meus agradecimentos à minha família por acreditar em mim e me apoiar em todos os aspectos da minha vida.

"Nós só podemos ver um pouco do futuro, mas o suficiente para perceber que há muito a fazer."

Alan Mathison Turing

RESUMO

Considerada a arte de esconder ou proteger informações, a criptografia está presente em várias ações que são executadas em nosso cotidiano, como por exemplo, quando executamos transações bancárias ou fazemos compras pela Internet ou ainda quando utilizamos as redes sociais como meio de comunicação. Este trabalho destaca os principais acontecimentos ocorridos relacionados à criptografia, sua evolução ao longo do tempo e qual sua importância para a sociedade. São abordados conceitos como cifras, chaves simétricas, públicas e privadas além de investigar se existe relação direta entre as evoluções das técnicas criptográficas e dos computadores.

Palavras-chave: chave simétrica; chave assimétrica; chave pública e privada; criptossistema; cifras.

ABSTRACT

Considered an art of hiding or protecting information, encryption is present in several actions that are performed in our daily lives, such as when we perform bank checks or purchases on the Internet or when used as social networks as a means of communication. This paper highlights the major events that have occurred in connection with cryptography, its evolution over time and how important it is to society. Concepts such as ciphers, symmetric keys, public and private, as well as investigating if there is a direct relationship between the evolution of cryptographic techniques and computers.

Keywords: symmetric keys; asymmetric Keys; public and private key; cryptosystem; cipher.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A Internet transformou a maneira como diversas atividades são executadas no dia-a-dia, uma vez que realizar uma transação bancária, fazer compras ou mesmo conversar com um amigo visualizando sua imagem em tempo real, só podiam ocorrer de forma presencial. Atualmente, graças aos serviços disponibilizados pela grande rede, é possível fazer este tipo de atividade além de muitas outras de forma remota. Mas para que estes benefícios possam ser desfrutados de forma satisfatória, a infraestrutura de comunicação deve zelar pelo não repúdio juntamente com os três pilares da segurança da informação: Confidencialidade, Integridade e Disponibilidade (KIM; SOLOMON, 2014).

De acordo com (KIM; SOLOMON, 2014) o não repúdio significa a impossibilidade de que uma mensagem enviada possa ser negada pelo remetente, uma vez que é possível confirmar o emissor. A Integridade diz respeito à confiabilidade da informação, ou seja, apenas as pessoas autorizadas podem inserir e/ou modificar os dados utilizados na transmissão. Já a Disponibilidade diz respeito ao fornecimento de serviços, ou seja, o serviço deve estar disponível no momento em que dele um usuário necessitar. Por fim, a Confidencialidade preza pela visibilidade das informações, uma vez que somente as pessoas autorizadas possam visualizar de forma inteligível os dados. Neste trabalho será explorada a criptografia, técnica relacionada ao pilar da Confidencialidade, que trata-se da arte de esconder a informação de pessoas não autorizadas, além de sua evolução ao longo do tempo.

Um dos problemas que sempre esteve presente desde o princípio da civilização é a necessidade de atingir a confidencialidade, considerada fundamental para se manter a informação segura (KIM; SOLOMON, 2014). Para que a confidencialidade seja alcançada, são utilizadas várias técnicas e métodos para cifrar informações legíveis com a intenção de transformá-las em um texto ilegível. Desta forma, mesmo que o texto seja adquirido por pessoas não autorizadas, a informação contida nele estará segura. As pessoas autorizadas podem realizar o processo inverso sobre o texto cifrado, recuperando assim a informação original (SINGH, 2011).

As técnicas de cifragem de textos são utilizadas há muito tempo para transmitir ou armazenar informações secretas. O primeiro exemplo da utilização da escrita cifrada ocorreu aproximadamente no ano de 1900 a.C., quando um escriba de Khnumhotep II, um nobre egípcio que viveu durante o reinado dos faraós Amenemhat II e Senusret II, decidiu trocar algumas palavras ou partes do texto, com o propósito de proteger o caminho para o tesouro. Desta forma, se o documento fosse roubado, os ladrões se perderiam dentro do labirinto e morreriam

de fome (LAREW; KAHN, 1968). Um dos primeiros relatos sobre transmissão de informações secretas são datadas de Heródoto, a partir da descrição do filósofo Cícero a respeito dos conflitos entre Grécia e a Pérsia, ocorridos no século V antes de Cristo (SINGH, 2011).

Apesar do termo "criptografia" ter sido criado em 1920, um dos métodos clássicos foi definido há mais de mil anos, no século IX por volta de 850, quando um matemático árabe chamado Al-Kindi (Iraque, 801-853), conhecido como AlKindus, publicou um manuscrito sobre a decifração de mensagens criptografadas (WAZLAWICK, 2016).

Atualmente a utilização da criptografia é muito intensa pois são realizadas inúmeras trocas de informações por meio da Internet e é desejável que somente as pessoas autorizadas tenham condições de acessar e entender o que está sendo transmitido. E no passado, quais áreas utilizavam esta forma de escrever informações? E nos dias de hoje, qual sua importância para a sociedade? Este trabalho tem como finalidade analisar, por meio de estudo bibliográfico, o avanço da criptografia ao longo da história, sua importância tanto para a sociedade antiga quanto para a atual. Além disso, foi verificado se existe relação direta entre as evoluções da criptografia e dos computadores.

2 A EVOLUÇÃO DA CRIPTOGRAFIA

2.1 Método utilizado

Este trabalho é de natureza exploratória com uma abordagem qualitativa, pois visa pesquisar a linha evolutiva da criptografia e suas técnicas. Para a realização da pesquisa bibliográfica, foram definidos pontos de referência ao longo da história, sendo esta dividida em quatro pontos: período anterior ao século XX, durante o século XX, o mundo moderno representado pelos dias atuais e o que se espera do futuro.

Para a coleta do material bibliográfico foram realizadas buscas por título utilizando combinações com as seguintes palavras: criptografia, evolução, história e criptossistemas nas bases de dados Periódicos CAPES e Google Acadêmico. Foi verificado que o material levantado poderia ser enriquecido ao se utilizar da técnica de *snowball*, ou bola de neve, que consiste em utilizar do referencial de um artigo para se alcançar outras fontes de informação úteis para o trabalho. Como resultado da bola de neve foram encontrados alguns livros conceituados na área como The CodeBreakers: The Story of Secret Writing (LAREW; KAHN, 1968), Criptografia em Software e Hardware (ORDONEZ; PEREIRA; CHIARAMONTE, 2005) e O livro dos códigos (SINGH, 2011) além de artigos que explicam alguns métodos criptográficos como (SINGH, 2013), (SINGHAL; RAINA, 2011) e (BENNETT; BRASSARD, 1984).

2.2 Definição de conceitos

A evolução da criptografia sempre esteve acompanhada pela evolução da criptoanálise, área de estudo que visa entender os métodos criptográficos e descriptografar informações. Uma observação que pode ser feita a respeito dos processos criptográficos é que geralmente estão divididos em dois elementos, sendo eles: algoritmo e chave, conforme explica (MENDES; PAULICENA; SOUZA, 2011). Ainda segundo o autor, o algoritmo é o procedimento que será executado para cifrar a informação, já a chave seria a especificação para aquele procedimento.

A chave, na criptografia, é um valor fornecido como uma entrada para um criptossistema. A chave funciona como um manual de como a mensagem deve ser criptografada contendo instruções do processo (KIM; SOLOMON, 2014).

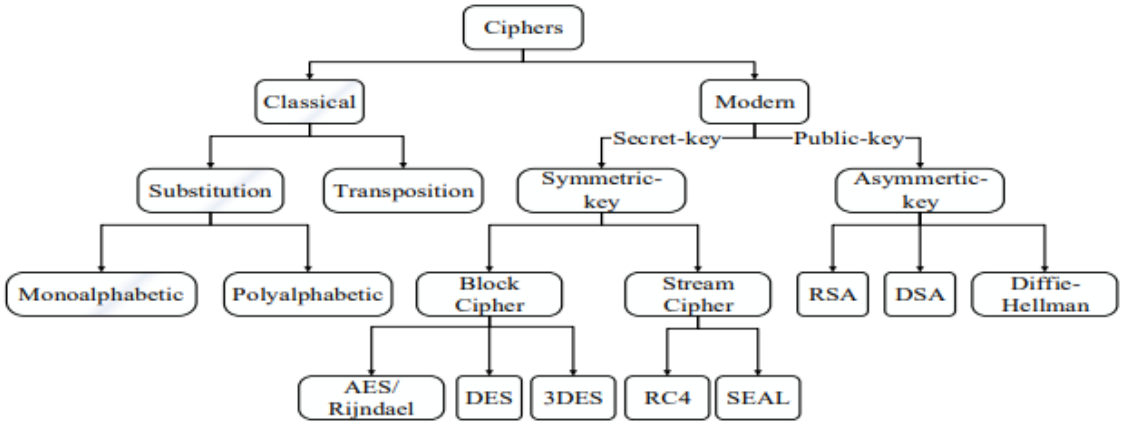
De acordo com (ORDONEZ; PEREIRA; CHIARAMONTE, 2005), para se criptografar uma informação podem ser utilizadas duas formas: a de códigos e a de cifras. O método de códigos transforma parte da informação em códigos predefinidos, geralmente seguindo algum

padrão de códigos, como por exemplo, o código morse. Já o método de cifras utiliza-se de duas técnicas para encriptar a informação sendo essas a transposição e/ou substituição do conteúdo original da mensagem por meio de algoritmos.

Ainda segundo (ORDONEZ; PEREIRA; CHIARAMONTE, 2005), as cifras mais utilizadas são as de transposição, que consistem de embaralhar os caracteres da informação contida no texto original. Um exemplo simples é cifrar a palavra "SEGURANÇA" e escrevê-la "GRUAÇNAES". Por outro lado, as cifras de substituição utilizam-se de tabelas de substituição predefinidas, que trocam ou substituem um ou mais caracteres da informação original.

A figura 1 mostra uma representação visual de como os métodos criptográficos estão classificados, sendo divididos entre métodos clássicos e modernos.

Figura 1 – Classificação dos métodos criptográficos



Fonte: SINGH, 2013, p.34..

2.3 Um pouco de história

De acordo com (ORDONEZ; PEREIRA; CHIARAMONTE, 2005), a criptografia é uma técnica que existe há milênios, sendo utilizada até mesmo no hieróglifo, antiga forma de escrita dos egípcios. Desta forma, é possível perceber que a criptografia já estava sendo utilizada, debatida e aprimorada há aproximadamente 4000 anos. Uma utilização da criptografia muito comum era proteger informações militares. Segundo o mesmo autor, na Roma antiga, os planos de guerra eram criptografados antes de serem enviados aos campos de batalha. Desta forma, caso os inimigos interceptassem as mensagens enviadas, os mesmos não conseguiriam fazer bom uso delas, pois estariam ilegíveis.

2.3.1 **Cifra de César**

A Cifra de César, também conhecida como Cifra de Troca, utilizada para proteger comunicações governamentais, é uma técnica de cifragem por substituição na qual cada letra é substituída por outra, que está logo após ela, definida por um número fixo. Por exemplo, ao utilizar o número três, cada letra do texto original será substituída pela letra que está três posições sucessivas , ou seja, para formar o texto cifrado a letra A torna-se D, B se torna E, e assim por diante (SALES, 2015). A Figura 2 ilustra as substituições, sendo que a letra original será substituída com a que está abaixo dela.

Figura 2 – Cifra de César

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
T	U	V	W	X	Y	Z	A	B	C

Disponível em: http://www.fernandosilva.pro.br/portal/index.php/en /para-pensar/curiosidades/item/214-criptografia-e-a-cifra-de-césar. Acesso em 15 de abril.2019.

César utilizava outras maneiras de reforçar seu método de grafar mensagens trocando caracteres latinos por gregos. Apesar dessa técnica ser simples é uma técnica da antiguidade que ainda é útil, como ocorreu na Guerra de Secessão Americana, onde oficiais sulistas utilizaram da técnica em uma situação precária onde não havia equipamentos modernos para proteger suas informações estratégicas do exército russo em 1915. (ORDONEZ; PEREIRA; CHIARAMONTE, 2005).

2.3.2 **Bastão de Licurgo**

Outro exemplo de técnica utilizada por civilizações antigas é o Bastão de Licurgo, utilizada pelos espartanos para esconder informações militares (OLIVEIRA; CRUZ; GOMES, 2018). Trata-se de um bastão de madeira denominado cítala no qual era enrolada uma tira de couro ou pergaminho onde a mensagem era escrita no sentido do comprimento do bastão, como pode ser visto na Figura 3. Eram utilizados diversos bastões com diâmetros diferentes sendo que para decifrar a mensagem era necessário enrolar novamente a mensagem em um bastão de diâmetro igual ao que foi utilizado para criptografar a mensagem (COSTA, 2014).

Figura 3 – Bastão de Licurgo

Disponível em: https://www.ebah.com.br/content/ABAAAfvW4AE/criptografia. Acesso em 15 de abril. 2019.

2.3.3 **Quadrado de Polybius**

Outra técnica utilizada na antiguidade é chamada Quadrado de Polybius. Consiste em associar de uma maneira fácil letras com números. Utilizando o formato de tabela de dimensão 5x5, as letras do alfabeto eram ali colocadas, sendo que o I e o J ocupam a mesma posição, conforme ilustra a figura 4. O método de criptografar utilizando esse quadrado consiste em associar uma letra a dois números formados pelo número da linha e coluna de cada letra. Deste modo basta trocar a letra pelo respectivo número, para dificultar que a mensagem fosse descriptografada, a numeração das linhas e colunas não era fixa (COSTA, 2014).

Figura 4 – Quadrado de Polybius

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fonte: Elaborado pelo autor.

2.3.4 **ADFGX**

A criptografia de sobreposição junto ao método de substituição serviu como base para a criação de diversos outros algoritmos utilizados durante a primeira guerra mundial. A invenção do telégrafo no século XIX possibilitou a comunicação entre grandes distâncias sem a necessidade de um mensageiro. Isto fez com que as trocas de mensagens entre remetente e destinatário se tornassem mais seguras. Entretanto, o uso desta tecnologia trouxe alguns inconvenientes, como o vazamento de informações pelos operadores dos telégrafos ou ainda a possibilidade da linha telegráfica ser "grampeada" por parte dos inimigos (COSTA, 2014).

Com o intuito de evitar os problemas obtidos com a invasão da comunicação à distância, os alemães desenvolveram uma cifra utilizando o Quadrado de Polybius, o qual substitui os números 12345 pelas letras ADFGX, letras estas que formam o nome da técnica de criptografia utilizada para grafar as mensagens dos alemães (COSTA, 2014).

De acordo com (COSTA, 2014) para codificar uma mensagem usando o sistema ADFGX é necessário criar uma matriz parecida com o Quadrado de Polybius, substituindo os números 12345 pelas letras ADFGX, como poder ser visto na figura 5.

Figura 5 – Quadro ADFGX-Primeira Etapa

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

Fonte: Elaborado pelo autor.

Para ilustrar o funcionamento da referida técnica, vamos utilizar um exemplo. Vamos supor que a mensagem escolhida para ser enviada seja "HOJE A NOITE". Ao substituir os caracteres da mensagem original pela combinação obtida por meio da posição dos caracteres da primeira linha com os da primeira coluna que representa o caractere a ser substituído teremos: H=DF, O=FG, J=DG, E=AX, A=AA, N=FF, O=FG, I=DG, T=GG, E=AX. Assim, a sequência de caracteres obtida é DFFGDGAXAAFFFGDGGGAX.

O passo seguinte é definir uma palavra-chave, podendo ser de qualquer tamanho, mas que não contenha letras repetidas. No exemplo que está sendo descrito, será utilizada a palavra "FRIO". O próximo passo é formar uma nova tabela onde a primeira linha é composta pela palavra-chave e as demais células de cada linha são preenchidas com a mensagem cifrada, conforme ilustrado na Figura 6.

Figura 6 – Quadro ADFGX-Segunda Etapa

F	R	I	O
D	F	F	G
D	G	A	X
A	A	F	F
F	G	D	G
G	G	A	X

Fonte: Elaborado pelo autor.

As colunas devem ser organizadas em ordem alfabética tendo como base os caracteres que compõem a palavra-chave, ou seja, a primeira linha. Assim a coluna que possui na primeira linha a letra I deve ser movida para a posição à direita da coluna que possui o caractere F. Em seguida, a coluna que possui na primeira linha a coluna O deve ser movida para a posição á direita da coluna I. Por fim, a coluna R ocupa a ultima posição. O resultado pode ser visto na figura 7.

Figura 7 – Quadro ADFGX-Terceira Etapa

F	I	O	R
D	F	G	F
D	A	X	G
A	F	F	A
F	D	G	G
G	A	X	G

Fonte: Elaborado pelo autor.

Ao final a mensagem cifrada é formada pelos grupos de caracteres de cada coluna da tabela representada na figura 7. No exemplo aqui descrito, a mensagem que deverá ser enviada pelo telégrafo é a seguinte: FDDAFG IFAFDA OGXFGX RFGAGG. Para que a mensagem original possa ser lida, basta que seja realizado o processo inverso e que o destinatário saiba a chave utilizada no processo e a composição do diagrama de substituição. A técnica ADFGX

deu origem a outra denominada ADFGVX, que inseriu algarismos de 0 a 9 aumentando a complexidade do mesmo, sendo que esta foi utilizada no final da primeira guerra mundial pelos Alemães (COSTA, 2014).

2.3.5 **Máquina Enigma**

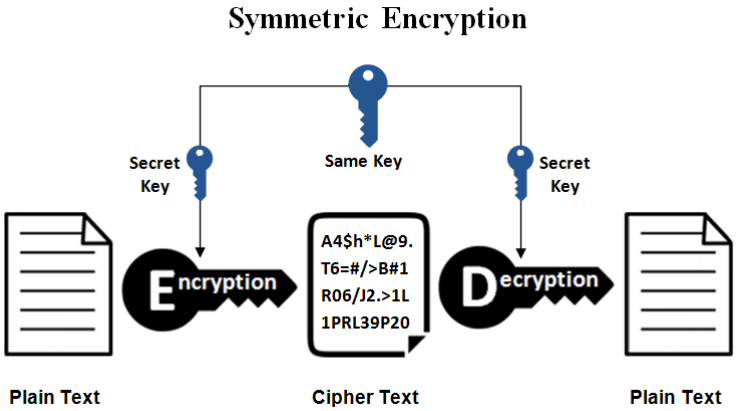
As forças armadas Alemãs utilizaram na segunda guerra mundial a máquina de cifra mais conhecida de todos os tempos, denominada Enigma, criada pelo DR. Arthur Scherbius. Devido a dificuldade de decifrar as mensagens geradas pela Enigma, foram reunidos vários criptoanalistas, que são profissionais responsáveis por estudar um método criptográfico e tentar quebra-lo sem o conhecimento prévio da chave utilizada, dentre eles Marian Rejewski, Henryk Zygalski e Alan Turing. Este último escreveu o artigo "*Treatise on the Enigma*", no qual a máquina Enigma serviu de exemplo para se explicar vários métodos da criptoanálise (HAMER; SULLIVAN; WEIERUD, 1993).

A atuação do *Bletchley Park*, também conhecida como *Station X*, era um centro de pesquisa secreto britânico, o local foi utilizado durante a segunda guerra mundial como centro da *Government Code and Cypher School*(GC&CS), responsável por decifrar os códigos militares Alemães. Uma das criações com maior importância realizado na *Station X* foi a da bomba eletromecânica dispositivo que deu origem ao computador chamado de Bomb, inventado por Alan turing e sua equipe de criptoanalistas desenvolvido em 1939, passando por um refinamento feito por Gordon Welchman em 1940 que tornou possível entender o funcionamento de algumas partes da Enigma como por exemplo, as configurações diárias da máquina utilizada pela marinha alemã, ajudando a entender como as mensagens eram cifradas (LYCETT, 2011).

2.4 Chave simétrica

O conceito de chave mais antigo é conhecido como chave privada ou modelo de chave simétrico. Este modelo consiste de uma única chave que é utilizada tanto para criptografar a mensagem que o remetente deseja enviar quanto para o destinatário descriptografar a mensagem como pode ser observado na figura 8. Com a utilização deste sistema, mesmo que um terceiro intercepte a mensagem e conheça o algoritmo utilizado para grafar, o mesmo não conseguirá decifrar a mensagem, pois ela está protegida pela chave, possibilitando que as partes interessadas em ter uma comunicação segura se preocupe apenas com a segurança da chave (OLIVEIRA, 2012).

Figura 8 – Processo de criptografia utilizando a técnica de chave simétrica



Disponivel em: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. Acesso em 30 de outubro. 2019.

O algoritmo de chave simétrica *The Data Encryption Standard* (DES) desenvolvido pela IBM na década de 1970, foi adotado em 1976 pelo *National Institute of Standards and Technology* (NIST). O DES foi projetado para criptografar e descriptografar blocos de informação de 64 bits de comprimento. Mesmo tendo uma chave de entrada de 64 bits, o tamanho real da chave do algoritmo DES é de 56 bits (SINGH, 2013).

Com a exploração da fraqueza do sistema criptográfico DES relacionado ao tamanho da chave de apenas 56 bits, foi necessário o desenvolvimento de um algoritmo mais seguro sendo denominado 3DES onde a chave passou de 56 bits para 168 bits. De uma forma simplificada o algoritmo é formado por 3 chaves de 56 bits onde a primeira chave encripta a informação, a segunda chave decripta e a terceira chave encripta novamente tornando o 3DES mais lento que o DES porém muito mais seguro (SINGH, 2013).

Em 1987 foi desenvolvido o algoritmo *Rivest Cipher 4* (RC4), que diferentemente do DES que encripta blocos de informação, é um algoritmo de criptografia de fluxo. Desenvolvido por Ron Rivest, é considerado mais eficiente para processamento em tempo real (SINGHAL; RAINA, 2011). O algoritmo RC4 era utilizado no protocolo *Secure Socket Layers* (SSL), conhecido hoje em dia como TLS para proteger o tráfego da Internet e *Wired Equivalent Privacy* (WEP) para segurança de redes sem fios (SINGHAL; RAINA, 2011). Hoje em dia o protocolo TLS utiliza-se de um sub-protocolo chamado *Handshake*, que é responsável por especificar qual algoritmo será utilizado na comunicação, por exemplo, o DES (DIAS, 2016).

No ano de 2001, o órgão Americano NIST recomendou um novo algoritmo de criptografia conhecido como *Advanced Encryption Standard* (AES), substituindo o algoritmo DES. O algoritmo AES suporta uma combinação de dados de 128 bits e chaves com o comprimento de

128, 192 e 256 bits (SINGH, 2013).

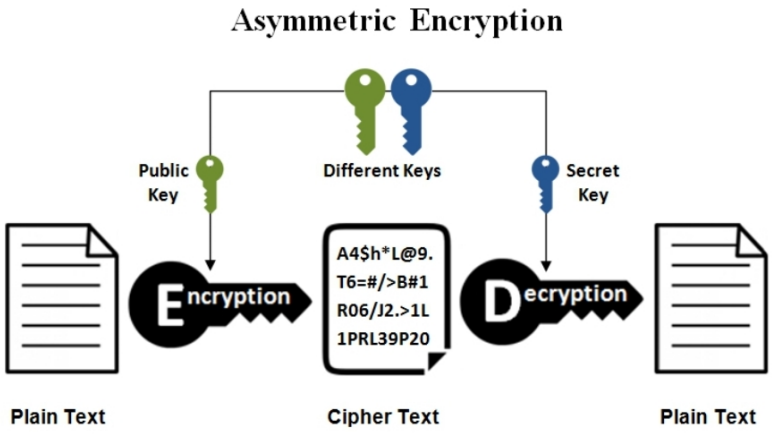
O algoritmo AES suporta um comprimento de 128 bits, que podem ser divididos em 4 blocos operacionais básicos, sendo que estes blocos são organizados como uma matriz de bytes de ordem 4x4, que é chamado de estado. O processo tanto de encriptar quanto de decriptar uma informação passa por dez passos, tendo quatro etapas cada passo(SINGH, 2013).

Utilizando o conceito de chave simétrica, se um terceiro interceptar a chave durante a transmissão, ele tem acesso às instruções para criptografar novas mensagens e descriptografar a informação cifrada enviada, inutilizando qualquer segurança que o algoritmo traria (KIM; SOLOMON, 2014). Neste ponto, surge um problema: se as chave garante a segurança do conteúdo grafado quem garante a segurança da chave?

2.5 Chave assimétrica

Em 1976 foi proposto pela dupla Diffie e Hellman, a criptografia de chave pública ou chave assimétrica (OLIVEIRA; CRUZ; GOMES, 2018). Com a proposta de chave assimétrica, o problema de segurança da chave seria resolvido (MENDES; PAULICENA; SOUZA, 2011). O sistema de chave assimétrica consiste em um par de chaves, uma pública e uma privada, onde esse par de chaves é utilizado para criptografar e descriptografar uma informação, técnica ilustrada na figura 9. A chave privada só tem como função descriptografar a informação encriptada pela chave pública, que é previamente disponibilizada ao usuário que deseja mandar uma informação criptografada, onde somente seu par, a chave privada consegue descriptografar a informação (KIM; SOLOMON, 2014).

Figura 9 – Processo de criptografia utilizando a técnica de chave assimétrica



Disponivel em: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. Acesso em 30 de outubro. 2019.

Com a utilização do sistema assimétrico cada usuário contém um par de chaves, porém somente as públicas são trocadas entre eles, fazendo com que se a chave pública for interceptada por um terceiro ele só irá conseguir criptografar novas mensagens, mas não terá acesso as informações trocadas entre os usuários, pois não poderá descriptografar as mensagens, tornando o processo de envio de informações mais seguro que o sistema de chave simétrica (KIM; SOLOMON, 2014).

Em 1977, Ron Rivest, Adi Shamir e Len Adleman fizeram uma descoberta importante, uma função modular de mão única que foi nomeada com as iniciais dos nomes dos autores da descoberta Rivest, Shamir e Adleman formando RSA, um dos primeiros sistemas de criptografia de chave assimétrica (OLIVEIRA; CRUZ; GOMES, 2018).

O sistema de chave assimétrica não substituiu totalmente o sistema de chave simétrica. O que ocorre é que os cálculos matemáticos necessários para o sistema de chave assimétrica são muito extensos pois trabalham com números muito grandes além dos próprios problemas matemáticos não resolvidos, como uma fórmula de gerar números primos descrito no artigo "A RELAÇÃO CIENTÍFICA ENTRE A CRIPTOGRAFIA E OS NÚMERO"(OLIVEIRA; CRUZ; GOMES, 2018), o que acarreta em lentidão no processamento computacional em comparação com o sistema simétrico (MENDES; PAULICENA; SOUZA, 2011). Os autores comentam que estes cálculos causam lentidão no processamento computacional, o que torna a utilização do sistema assimétrico na criptografia de grandes quantidades de texto inferior em comparação ao sistema simétrico. Então como solução para esse problema o sistema de chave assimétrico é utilizado não para criptografar toda a informação mas para criptografar pequenos trechos de informação com 128 ou 256 bits, que geralmente é o tamanho de uma chave simétrica. Assim, o sistema assimétrico habitualmente só é utilizado para criptografar a chave que é simétrica, onde a mesma é responsável em criptografar a informação. Esse procedimento é chamado de sistema criptográfico híbrido (MENDES; PAULICENA; SOUZA, 2011) onde o sistema assimétrico protege apenas a chave simétrica utilizada na grafia da informação.

2.6 O que vem por aí?

A tecnologia de criptografia quântica precede os computadores quânticos, pois o sistema de distribuição de chaves quânticas já teve seus protocolos de comunicação definidos e já é utilizada de forma pública mesmo sem precisar de um computador quântico (MENDES; PAULICENA; SOUZA, 2011).

Para se utilizar a criptografia quântica são necessários dois canais de comunicação, sendo um quântico é um clássico. O canal quântico pode ser de fibra ótica, que é capaz de transmitir fótons enquanto o canal clássico pode utilizar qualquer outra fonte como e-mail, ou ondas radiofônicas (MENDES; PAULICENA; SOUZA, 2011). O primeiro protocolo de criptografia quântico ou sistema de distribuição de chaves quânticas foi proposto em 1984 por Charles H. Bennett e Gilles Brassard chamado de BB84 (BENNETT; BRASSARD, 1984). Um fato interessante sobre criptografia quântica é que esse sistema possivelmente não será utilizado em computadores quânticos.

De acordo com o autor (RIGOLIN; RIEZNIK et al., 2005) o envio das chaves utilizando o sistema quântico é efetuado enviando fótons que podem ser previamente modificados em quatro estados de polarização, os fótons são enviados utilizando o canal de comunicação quântico. O autor mostra que a grande vantagem de se utilizar o sistema de distribuição de chaves quânticas é a possibilidade de descobrir se a transmissão está sendo interceptada ou não por meio da comparação de bits, pois se um terceiro interceptar um fóton antes dele chegar ao destinatário é detectá-lo usando uma base diferente, a polarização do fóton é alterada, dando resultados diferente quando comparado ao remetente, mostrando que a comunicação está sendo interceptada.

3 CONSIDERAÇÕES FINAIS

Uma observação que pode ser realizada ao pesquisar o histórico evolutivo da criptografia é como a utilização da criptografia se ramificou principalmente após a invenção dos computadores e a internet, a criptografia antes do surgimento destas tecnologias era basicamente utilizada para proteger informações sensíveis de estado ou utilizada na comunicação em tempos de guerra. Técnicas famosas como a Cifra de César ou Quadrado de Polybius demonstram bem esse fato, pois eram estritamente utilizadas para proteger informações militares ou governamentais.

Após a invenção e aumento da utilização dos computadores e da grande rede, a criptografia tomou um papel mais de utilidade pública, pois com ela pode se ter uma comunicação com algum nível de segurança dentro da internet. A criptografia também tornou possível a realização de operações online como por exemplo, investimento da bolsa de valores, movimentações bancárias e assinaturas digitais, tudo isso graças aos pilares da segurança e ao não repúdio concedido pela criptografia.

Mesmo quando um novo sistema criptográfico é criado são realizados vários estudos com a finalidade de encontrar fraquezas nesta nova técnica. Esse padrão pode ser observado em boa parte das técnicas apresentadas neste trabalho, como pode ser é visto na técnica ADFGX Alemã, que teve que ser aprimorada para a técnica ADFGVX. Outro exemplo seria o algoritmo DES, que logo foi substituído pelo algoritmo 3DES devido à falta de segurança apresentada pelo seu predecessor.

A instabilidade técnica que persegue a criptografia faz com que ela se desenvolva continuamente, pois nunca se sabe quanto tempo uma técnica permanecerá segura. Os ataques contínuos de hackers ou mesmo novas pesquisas para encontrar pontos fracos, realizadas por criptoanalistas, torna a criptografia uma área de estudo muito movimentada, sempre gerando novos mecanismos de segurança cada vez mais complexos e eficientes.

A criptografia quântica é um exemplo de como os estudos na área de criptografia estão avançados em relação aos computadores, pode ser percebido que a técnica está estagnada, sua utilização ainda é baixa e os estudos nesta área são poucos. Um dos fatores para isso seria que o método de criptografia híbrido supra bem as necessidades criptográficas atuais, diminuindo a necessidade de avanço da técnica quântica.

A distribuição de chaves quânticas se apresenta como uma grande evolução em relação às técnicas de criptografia atuais, entre tanto ainda não é tão explorada, pelo fato dos computadores atuais não conseguirem quebrar as mensagens proporcionadas pelos métodos

criptográficos atuais. Acredita-se que quando os computadores quânticos se tornarem estáveis, será possível quebrar os códigos criptográficos atuais com muita facilidade, por causa da alta capacidade de processamento dos computadores quânticos. Mesmo que neste trabalho tenha ressaltado a importância da criptografia na segurança de dados, um ponto que deve ser mencionado é que a criptografia sozinha não garante a proteção das informações, mesmo o mais complexo dos sistemas criptográficos pode ser facilmente quebrado se houverem falhas humanas como o vazamento da chave criptográfica.

A engenharia social é uma das mais poderosas armas utilizadas pelos hackers. Existem técnicas e mecanismos que podem induzir o erro humano, o que pode transformar uma informação bem protegida criptograficamente em totalmente vulnerável, pela falta de preparo ou cuidado em realizar o processo de comunicação segura.

Um ponto que é interessante ressaltar é a contribuição da criptografia para a evolução dos computadores. Um período importante na história, que liga a criptografia à evolução dos computadores, pode ser vista no ano de 1939, com a criação da bomba eletromecânica, que posteriormente deu origem ao computador chamado Bomb. Apesar da ligação clara durante esse período, as linhas evolutivas da criptografia e dos computadores parecem ter se dividido a partir deste momento. Porém é um assunto que demanda uma pesquisa mais voltada para a origem dos computadores conjunta com o estudo dos próprios envolvidos na evolução dos computadores, com o intuito de encontrar mais contribuições da criptografia em relação à evolução dos computadores.

A realização deste trabalho traz muitas oportunidades de pesquisas futuras, pois a grande quantidade de informações sobre a criptografia é o tamanho da linha evolutiva da mesma, deixando espaço para que trabalhos futuros mais focados em determinados períodos sejam realizados, descrevendo com maior detalhamento as técnicas, impactos e utilizações da criptografia naquele determinado período, criando assim um conjunto de trabalhos que possam sanar as dúvidas oriundas do passado, presente e até futuro da criptografia.

REFERÊNCIAS

BENNETT, C. H.; BRASSARD, G. Quantum Cryptography: Public Key Distribution and Coin Tossin. In: **In International Conference on Computers, Systems & Signal Processing**. [S.l.: s.n.], 1984.

COSTA, D. D. **A Matemática e os Códigos Secretos: Uma Introdução à Criptografia**. 78 p. Tese (Programa de Mestrado Profissional em Matemática) — UNIVERSIDADE ESTADUAL DE MARINGÁ, 2014.

DIAS, F. J. T. **Estudo de Segurança dos Protocolos SSL/TLS**. Tese (Doutorado), 2016.

HAMER, D. H.; SULLIVAN, G.; WEIERUD, F. Enigma variations: An extended family of machines. In: CITESEER. **Proceedings-A**. [S.l.], 1993. v. 140, n. 3.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: LTC, 2014. 385 p. ISBN 978-0-7637-9025-7.

LAREW, K.; KAHN, D. The Codebreakers: The Story of Secret Writing. **The American Historical Review**, Macmillan, New York, v. 74, n. 2, p. 537, 1968. ISSN 00028762.

LYCETT, A. Breaking germany's enigma code. **Pinching the Codes. Np, nd Web.< http://www. bbc. co. uk/history/worldward/wwtwo/enigma01. shtml**, 2011.

MENDES, A. J. B.; PAULICENA, E. H.; SOUZA, W. A. R. Criptografia Quântica: Uma Abordagem Direta. **Revista de Sistemas de Informação da FSMA**, v. 7, n. 39-48, p. 9, 2011. Disponível em: <http://www.fsma.edu.br/si/edicao7/FSMA_SI_2011_1_Tutorial_1.pdf>.

OLIVEIRA, I. D. H. F.; CRUZ, M. P. M. D.; GOMES, R. L. R. A relação científica entre a criptografia e os números primos. **Revista Atlante: Cuadernos de Educación y Desarrollo**, n. 1-20, p. 20, 2018. Disponível em: <https://www.eumed.net/rev/atlante/2018/05/criptografia-numeros-primos.html>.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, v. 31, p. 11–15, 2012.

ORDONEZ, E.; PEREIRA, F.; CHIARAMONTE, R. **Criptografia em Software e Hardware**. 1st edition. ed. São Paulo: Novatec, 2005. ISBN 85-7522-069-1.

RIGOLIN, G.; RIEZNIK, A. A. et al. Introdução à criptografia quântica. **Revista Brasileira de Ensino de Física**, SciELO Brasil, 2005.

SALES, I. **Cifra de César**. 2015. Disponível em: <http://www.contabilidade-financeira.com/2015/02/cifra-de-cesar.html>.

SINGH, G. A study of encryption algorithms (rsa, des, 3des and aes) for information security. **International Journal of Computer Applications**, Foundation of Computer Science, v. 67, n. 19, 2013.

SINGH, S. **O livro dos códigos**. 9º edição. ed. Rio de Janeiro: Record, 2011. 446 p. ISBN 8501055980.

SINGHAL, N.; RAINA, J. Comparative analysis of aes and rc4 algorithms for better utilization. **International Journal of Computer Trends and Technology**, v. 2, n. 6, p. 177–181, 2011.

WAZLAWICK, R. S. **História da Computação**. 1º edição. ed. Rio de Janeiro: Elsevier, 2016. 584 p. ISBN 9788535285451.