UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

FERNANDA RODRIGUES GOMES

UM ESTUDO EXPLORATÓRIO ENVOLVENDO CRIPTOGRAFIA E FATORAÇÃO NUMÉRICA

SOROCABA

SETEMBRO DE 2022

Fernanda Rodrigues Gomes

Um estudo exploratório envolvendo criptografia e fatoração numérica

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Ensino de Ciências Exatas (PPGECE), da Universidade Federal de São Carlos, como parte dos requisitos para obtenção do título de Mestre em Matemática, sob orientação do(a) Professor(a) Doutor(a) Profa. Dra. Silvia Maria Simões de Carvalho.

Universidade Federal de São Carlos
Centro de Ciências Exatas e Tecnológicas

Orientadora: Profa. Dra. Silvia Maria Simões de Carvalho

Sorocaba
Setembro de 2022

Gomes, Fernanda Rodrigues

Um estudo exploratório envolvendo criptografia e fatoração numérica. / Fernanda Rodrigues Gomes -- 2022.
87f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus Sorocaba, Sorocaba
Orientador (a): Silvia Maria Simões de Carvalho.
Banca Examinadora: Mayk Vieira Coelho, Antonio Luís Venezuela.
Bibliografia

1. 1. Criptografia RSA. 2. Fatoração Numérica. 3. Hacker. I. Gomes, Fernanda Rodrigues. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Maria Aparecida de Lourdes Mariano - CRB/8 6979

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ensino de Ciências Exatas

Folha de Aprovação

Defesa de Dissertação de Mestrado da candidata Fernanda Rodrigues Gomes, realizada em 02/09/2022.

Comissão Julgadora:

Profa. Dra. Silvia Maria Simões de Carvalho (UFSCar)

Prof. Dr. Mayk Vieira Coelho (UNIFAL - MG)

Prof. Dr. Antonio Luís Venezuela (UFSCar)

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Ensino de Ciências Exatas.

Dedico este trabalho aos meus pais, Rosália e Vicente, por todo apoio, paciência e incentivo para que concluisse esta etapa de estudo com grande dedicação.

Agradecimentos

Primeiramente agradeço aos meus pais pelo apoio e paciência que ajudaram a me impulsionar até este momento, me incentivando a realizar este grande desejo, que surgiu desde a conclusão do curso de licenciatura.

Agradeço também a todos os professores e professoras do curso na Universidade Federal de São Carlos, campus Sorocaba, por terem compartilhado seus conhecimentos, mostrando a habilidade e o amor que possuem com a Matemática.

Gostaria de agradecer aos meus colegas de curso pelo companheirismo, mas em especial a Cintia, que sempre esteve ao meu lado, me ajudando e incentivando a continuar, e que se tornou uma grande amiga.

Agradeço a minha orientadora, Professora Doutora Silvia Maria Simões de Carvalho, por toda a paciência e empenho durante a orientação deste trabalho. Muito obrigada por me ter corrigido quando necessário, por ter abraçado as minhas ideias e por todo conhecimento que compartilhou comigo com tanto carinho e dedicação.

"A persistência é o caminho do êxito".

Charles Chaplin

Resumo

Esta pesquisa tem por objetivo investigar as implicações da aplicação de uma sequência de ensino utilizando criptografia e fatoração numérica na aprendizagem de estudantes da 1ª série do Ensino Médio. A criptografia possui diversas aplicações na sociedade atual, desde a segurança de acessar uma rede social até mesmo a proteção de dados bancários; neste sentido a pesquisa buscou apresentar aos estudantes desde o histórico da criptografia até o funcionamento da criptografia RSA e o papel de um hacker neste ambiente. Procuramos fazer uma abordagem didática utilizando vídeos, texto, certificados das redes sociais e um desafio final. Os estudantes se tornaram "hackers do bem", realizando a fatoração de números compostos contidos nas chaves do desafio e decodificando a mensagem de cada urna utilizando uma tabela pré-codificada, para chegar ao resultado.

Palavras-chave: Criptografia RSA. Fatoração Numérica. Hacker. Ensino.

Abstract

This research aims to investigate the implications of applying a teaching sequence using cryptography and numerical factoring in the learning of 1st grade high school students. Cryptography has several applications in today's society, from the security of accessing a social network to even the protection of banking data; In this sense, the research sought to present students from the history of cryptography to the functioning of RSA cryptography and the role of a hacker in this environment. We tried to make a didactic approach using videos, text, certificates from social networks and a final challenge. The students became "hackers of good", performing the factorization of compound numbers contained in the keys of the challenge and decoding the message of each urn using a pre-coded table, to arrive at the result.

Keywords: Cryptography RSA. Numerical Factorization. Hacker. Teaching.

Lista de ilustrações

Sumário

1 Introdução

A disseminação da internet e a globalização estão cada vez mais presentes na vida dos seres humanos, de maneira a facilitar a comunicação e a propagação da informação. Dessa forma a necessidade de proteção de informações foi se tornando cada vez mais necessária, de maneira que foram sendo inventados diferentes métodos até se chegar na criptografia RSA, que é o mais utilizado atualmente e que possui o mais alto grau de segurança.

O desenvolvimento da criptografia é tão antigo quanto o da escrita, é um conjunto de técnicas que permitem tornar uma mensagem imcompreensível e teve sua difusão devido a necessidade de proteger uma informação, para garantir a sua privacidade. A utilização é de longa data, de maneira que a criptografia marcou a história com fins militares, políticos e religiosos. Teve diferentes fases: artesanal, mecânica e digital. Em cada uma foram desenvolvidas invenções, métodos e cifras que vem evoluindo até os dias atuais, junto com o progresso tecnológico e o estudo de conceitos matemáticos de forma aprofundada.

A criptografia mais utilizada é a RSA e recebe este nome devido aos seus inventores Ronald Rivest, Adi Shamir e Leonard Adleman e é um método que codifica a mensagem utilizando dois números primos grandes, o produto desses números gera uma chave, um número inteiro ainda maior.

O estudo relacionado a criptografia levou a alguns questionamentos que impulsionaram a pesquisa desta dissertação: Qual o papel da Matemática e da criptografia na proteção e segurança de dados? Onde podemos encontrar a aplicação da criptografia RSA nos dias atuais? Os estudantes conhecem a criptografia e tem noção de como ela está presente em suas vidas através dos meios digitais que eles utilizam?

Assim foi definido o objetivo geral: Investigar as implicações da aplicação de uma sequência de ensino utilizando criptografia e fatoração numérica na aprendizagem de estudantes da 1ª série do Ensino Médio. E os objetivos específicos: Realizar o estudo da criptografia RSA e seu papel na proteção de dados; Analisar a criptografia em elementos presentes no cotidiano dos estudantes e inseri-los em uma sequência didática.

A importância e a diversa aplicabilidade da criptografia RSA na vida da sociedade atual, que necessita da proteção de seus dados, levou ao desenvolvimento uma sequência didática que utiliza a criptografia RSA como base, além disso a profissão de hacker para engajar os estudantes e a urna eletrônica como parte do desafio proposto, onde foi necessário o estudo de algumas propriedades Aritméticas, que são mostradas nos capítulos.

No capítulo 2, é apresentada a história e a evolução da criptografia, o significado

da palavra criptografia e seu desenvolvimento no decorrer da história. Posteriormente foi explanado sobre o conjunto dos números inteiros, algumas proposições e definições no capítulo 3.

Na sequência temos o capítulo 4, onde foram apresentadas algumas propriedades relacionadas a divisibilidade, números primos, fatoração e a criptografia RSA. Além disso foi discorrido sobre sites e plataformas que utilizam a criptografia RSA, juntamente com o conceito de hacker.

Já no capítulo 5 é mostrada uma sequência didática de 4 aulas, que foi desenvolvida com alunos da 1ª série do ensino médio de uma escola estadual, considerando as suas dificuldades devido ao afastamento de cerca de dois anos por conta da pandemia de COVID. Nessas aulas eles responderam um questionário inicial, para a obtenção dos conhecimentos prévios dos estudantes em relação a criptografia, software, hardware e hacker, posteriormente foi realizada uma competição para que os estudantes descobrissem o resultado de uma eleição utilizando fatoração numérica e mensagens codificadas, e no final outro questionário relacionado aos conhecimentos adquiridos pelos estudantes. Posteriormente temos as conclusões da pesquisa e por último as referências bibliográficas.

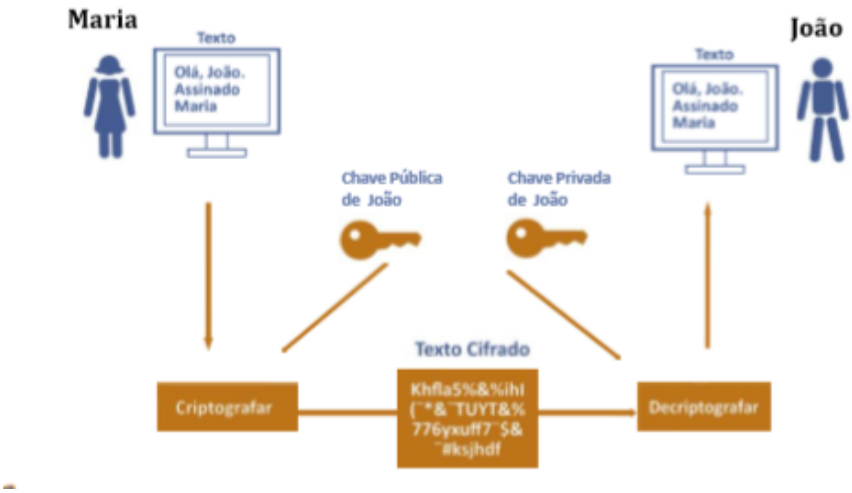
2 CRIPTOGRAFIA: HISTÓRIA E EVOLUÇÃO

Criptografia é uma palavra que deriva do grego, de kriptos tem por significado “secreto” e de graphia que significa “escrita”. Teve seu desenvolvimento paralelo a esteganografia, esta segunda forma de comunicação buscava esconder a existência de uma mensagem enquanto a primeira tinha por objetivo ocultar a informação da mensagem (FRANÇA, 2014).

De acordo com um protocolo ocorre o processo de encriptação, neste o texto passa a ser misturado de modo que com este protocolo preestabelecido entre o transmissor e o receptor se obtém a mensagem. A criptografia tem por objetivo proteger a informação de uma mensagem, essa pode ser a matéria prima que irá produzir conhecimento e isso é poder. Nesta linguagem encontramos as cifras, que codificam uma mensagem e tem como propósito garantir a privacidade, escondendo a informação de uma pessoa não autorizada. Já decifrar é o processo contrário, que busca transformar o que foi criptografado na sua forma legível e original.

Na Figura 1 podemos observar o prococolo de um método de criptografia chamado RSA, onde Maria é a emissora da mensagem e João o receptor, de maneira que a mensagem é criptografada em forma de um código e posteriormente é descriptografada.

Figura 1 – Transmissor e receptor de uma mensagem



Fonte: CERTISING, 2018.

A mensagem criptografada quando é recebida pode ser decodificada ou decifrada,

a primeira situação diz respeito a um receptor que já possui o procedimento usado na codificação e o utiliza para retirar o código e alcançar a mensagem, enquanto a segunda é utilizada para desvendar o procedimento de codificar a mensagem, sendo realizada por um receptor não legítimo, alguém não autorizado.

A necessidade de sigilo na comunicação é tão velha quanto a escrita, e com a evolução da tecnologia e dos meios de comunicação se tornou necessário aumentar a complexidade de ocultar as mensagens.

Com a evolução da tecnologia utilizadas nos computadores e da comunicação a criptografia desenvolveu alguns objetivos principais: confidencialidade, integridade da informação, autenticação de informação e a não repudiação (evita que qualquer das partes, emissor ou receptor neguem o envio ou a receptação da informação). Desde o desenvolvimento da humanidade vem sendo utilizadas diversas cifras, de transposição ou de substituição. A primeira funciona de maneira que cada letra mantém sua identidade, mas muda de posição na mensagem, já na segunda a letra mantém a posição na mensagem, mas é substituída por outra letra ou símbolo (FIARRESGA, 2010).

Segundo Fiarresga (2010) o histórico da criptografia é longo, um dos registros mais antigos é de cerca de 4000 anos, encontrado no antigo Egito, onde foram descobertos hieróglifos que não eram compreendidos por parte da população no túmulo de um membro da nobreza, Khnumhotep II. Os hebreus utilizavam na antiguidade as cifras atbash (a primeira letra do alfabeto é substituída pela última, a segunda pela penúltima e assim consecutivamente), albam (a primeira letra é substituída pela décima quarta letra, a segunda pela décima quinta e assim consecutivamente) e atbah, que também consiste na substituição das letras.

Ao longo da história foi desenvolvido, por volta de 487 a.C, o bastão de Licurgo pelos espartanos, este consiste em uma cifra de transposição, que era utilizado para transmitir mensagens confidenciais. Foi um engenho militar, que através de um cilindro com uma tira de couro ou papiro enrolada que tinha uma mensagem escrita no sentido do seu comprimento.

Uma cifra que também foi desenvolvida na antiguidade é a de Políbio (200 a.C, 118 a.C) que utilizava cinco letras, e que através de uma tabela podiam ser transmitidas mensagens por tochas de fogo. Outro caso que surge no decorrer da história é a cifra de César, utilizada pelo imperador Julio César (100 a.C, 44 a.C) para trocar mensagens com os generais, que utilizava a substituição das letras do alfabeto, de maneira que essas letras em cifra eram resultado do avanço da ordem das letras do alfabeto em três posições para a direita (FIARRESGA, 2010).

A criptografia marcou a história devido a seus fins militares, políticos e religiosos, ocorrendo assim a evolução dos métodos de crifragem. O seu desenvolvimento é marcado

por três fases: artesanal, mecânica e digital. A primeira fase, a artesanal, registra a utilização inicial da criptografia em paralelo com o desenvolvimento da escrita, que ocorreu nas idades Antiga (4000 a.C - 476) e Média (476 - 1453), foi nesta fase em que foram desenvolvidos o bastão de Licurgo, conforme a Figura 2, e o código de César.

Figura 2 – Bastão de Licurgo

Fonte: MEDEIROS, 2013.

Ainda nesta primeira fase temos o Cifrário de Francis Bacon (1561, 1626), que desenvolveu um sistema de substituição utilizando um alfabeto de 24 letras, para cada letra do alfabeto temos um grupo de cinco caracteres utilizando as letras “a” e “b”. Criando assim uma cifra que pode ser considerada binária, com cinco bits (menor unidade de informação que pode ser armazenada ou transmitida na comunicação de dados), onde “a” e “b” podem ser substituídos por 0 e 1. Na cifra de Bacon, por exemplo, através do seu método a letra A pode ser substituída pelo grupo aaaaa, ou de forma binária por 00000, ou a letra Z que pode ser substituída pelo grupo babbb, ou de forma binária por 10111, que podemos observar na Figura 3 a seguir (FRANÇA, 2014).

Figura 3 – Cifra de Bacon

Letra	**Grupo**	**Binário**		**Letra**	**Grupo**	**Binário**
A	aaaaa	00000		N	abbaa	01100
B	aaaab	00001		O	abbab	01101
C	aaaba	00010		P	abbba	01110
D	aaabb	00011		Q	abbbb	01111
E	aabaa	00100		R	baaaa	10000
G	aabba	00110		T	baaba	10010
H	aabbb	00111		U/V	baabb	10011
I/J	abaaa	01000		W	babaa	10100
K	abaab	01001		X	babab	10101
L	ababa	01010		Y	babba	10110
M	ababb	01011		Z	babbb	10111

Fonte: FRANÇA, 2014, p. 25

Neste período, na fase artesanal, houve a criação da criptoanálise, descoberta realizada pelos estudiosos árabes do Oriente Médio, através da combinação linguística, estatística e devoção religiosa. Esse método utiliza a análise de frequências para "quebrar" códigos monoalfabéticos (substituição de uma letra do texto por outra letra). Diante dessa fraqueza das cifras monoalfabéticas foi proposto o uso de dois ou mais alfabetos por Leon Alberti, que levou a criação da cifra de Vigenère por Blaise de Vigenère (1523, 1596). Essa cifra utiliza 26 alfabetos cifrados distintos na criação de uma mensagem cifrada, resistindo à análise de frequências, para decifrar a mensagem o receptor precisa saber qual alfabeto deve utilizar, isto era informado de forma prévia por uma palavra-chave. Essa cifra foi utilizada até 1856, quando o matemático Charles Babbage (1791, 1871) descreveu um método que quebrava essa cifra.

O código Braille, criado por Louis Braille (1809, 1852), é outro sistema de escrita em que uma mensagem é codificada utilizando um sistema de símbolos, que através de uma matriz de seis pontos são formados os caracteres utilizados na formação da mensagem. Outra forma de enviar uma mensagem é o microponto, este consiste em reduzir fotograficamente uma página de texto a ponto de transformá-la em um ponto, com diâmetro menor que um milímetro, e colocar essa informação sobre um ponto final, esse método foi utilizado na Segunda Guerra Mundial por agentes alemães.

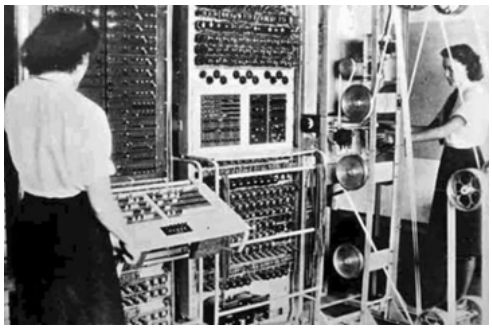
A segunda fase da criptografia, a mecância, teve origem no início da Idade Moderna (1453 - 1789), mas seu apogeu foi durante a Segunda Guerra Mundial, com as máquinas de cifragens. A primeira máquina criptográfica foi o Disco de Cifras com o sistema polialfabético, um misturador que era feito com dois discos de cobre, cada um com um alfabeto na borda. O disco menor (alfabeto cifrado) era fixado sobre o maior (alfabeto original), de maneira que giravam independentemente, foi utilizado para cifrar mensagens por cerca de cinco séculos.

O código Morse, desenvolvido por Samuel Morse (1791, 1872), utiliza um alfabeto baseado em cinco posições no máximo, de maneira que todas as letras e números são padronizados. Nesse código cada caractere possui um conjunto de traços e pontos, podendo ser transmitido até mesmo através de sinais elétricos.

Outra invenção mecânica pertencente a esta fase é a máquina Enigma, criada após a Primeira Guerra Mundial (1791 - 1872) pelo alemão Arthur Scherbuis (1878, 1929). Esta é uma versão elétrica do disco de cifras, possui um elevado número de chaves, com alta complexidade por poder ser regulada de diversas maneiras (150 trilhões de regulagens possíveis) e foi utilizada para fins militares pelos nazistas. Sua complexidade foi quebrada pelo criptoanalista Alan Turing (1912, 1954) e seus colaboradores através das máquinas: Bomba e a segunda Colossus, que foi um computador projetado em 1943, utilizado na Segunda Guerra Mundial na decodificação dos códigos da máquina Enigma (FRANÇA, 2014).

A fase digital da criptografia se deu durante os século XX e XXI, com o desenvolvimento e aperfeiçoamento dos computadores, devido a algumas necessidades como o uso da criptografia por comércios e bancos. No computador temos a informação representada por sequências de zeros e uns, de forma binária, e para iniciar uma cifragem no mesmo existem vários protocolos para fazer a transformação. A American Standard Code for Information Interchange (ASCII) é um exemplo onde cada letra do alfabeto é destinada a um número binário de sete dígitos. A seguir na Figura 4, temos a imagem da máquina Colossus:

Figura 4 – Colossus



Fonte: KLEINA, 2013.

Neste sentido temos a criptografia simétrica e a criptografia assimétrica, a primeira diz respeito a utilização de uma chave privada e um algoritmo de criptografia, que transforma um texto conhecido por todos em um texto cifrado.

O poder da cifra na criptografia simétrica é medido pelo tamanho da chave, de forma que chaves de 40 bits podem ser consideradas fracas e chaves de 256 bits ou mais, como fortes. Utiliza uma única chave secreta e apresenta alguns problemas que estão na distribuição da chave, pois sua disponibilização pode não ocorrer de forma totalmente segura, além de não garantir a identidade do emissor ou do receptor da mensagem, de forma que a quantidade de usuários pode dificultar o gerenciamento das chaves.

Alguns exemplos da criptografia simétrica são: DES, AES e IDEA. O Data Encryption Standard (DES) é um algoritmo de criptografia em blocos, foi criado em 1977, este permite cerca de 72 quadrilhões de combinações com uma chave de 56 bits e 16 estágios de criptografia, em 2001 o DES foi substituído pelo AES. O Advanced Encryption Standard (AES) é uma cifra de bloco, aplicado nas conexões wi-fi atuais, um dos algoritmos considerados padrão. Seu bloco fixo possui 128 bits e sua chave 128, 192 ou 256 bits. O International Data Encryption Algorithm (IDEA), criado em 1991, utiliza uma chave de 128 bits (FRANÇA, 2014).

A criptografia assimétrica por sua vez possui algoritmos de chave pública, uma chave cifrante de domínio público e uma chave decifrante de domínio privado. Alguns

exemplos de criptografia assimétrica são: RSA, El-Gamal e Curvas Elípticas.

O RSA é o método mais conhecido de criptografia, foi inventado em 1977. As letras RSA dizem respeito as iniciais dos inventores desse algoritmo: R. L. Rivest, A. Shamir, e L. Adleman. Na codificação de uma mensagem usando esse método são necessários dois números primos grandes que resultam em um terceiro através do produto deles, o que pode gerar uma dificuldade na fatoração desse número, sendo o mais usado em aplicações comerciais.

O El-Gamal foi criado em 1984 pelo egípcio Taher Elgamal e utiliza um logaritmo discreto, sua segurança se baseia na dificuldade de calcular logaritmos discretos em um corpo finito. As curvas elípticas por sua vez têm sua segurança baseada no fato de não existir nenhum algoritmo sub-exponencial conhecido que possa ser utilizado para resolver o problema do logaritmo discreto em uma curva elíptica simples.

Quando existe uma chave pública a assinatura digital se faz necessária, para que se permita a autenticidade do emissor da mensagem, evitando que alguém possa "fingir" ser o emissor da mensagem. Para isso é utilizado uma espécie de resumo especial, empregado em processos de assinatura digital chamado de hash (PÓVOA, 2019).

A base dos protocolos de segurança são os certificados digitais emitidos por autoridades certificadoras. Estas, divulgam as chaves públicas dos usuários, conhecida como certificado digital (conjunto de informações padronizadas que contém os dados do proprietário) utilizado pelos mais diversos tipos de usuários. Esses certificados são utilizados por exemplo para que se possa realizar uma compra com o cartão de crédito de forma segura.

A autoridade certificadora no Brasil é a AC-raiz, administrada pelo Instituto Nacional de Tecnologia da Informação (ITI). Esta realiza a gestão da Infraestrutura de Chaves Públicas Brasileira (ICP - Brasil), certificando as autoridades certificadoras de níveis mais baixos, com um certo custo.

A ICP - Brasil é uma cadeia de hierarquia de confiança que viabiliza a emissão de certificados digitais. Esta é composta por uma cadeia de entidades credenciadas, formada por Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (ACs), Autoridades de Registro (ARs), Autoridades Certificadoras do Tempo (ACTs), Prestadores de Serviço Biométrico (PSBios), Prestadores de Serviço de Suporte (PSS) e, ainda, por uma autoridade gestora de políticas, que é o Comitê Gestor da ICP-Brasil.

A Autoridade Certificadora Raiz e as Autoridades Certificadoras não têm acesso às chaves privadas dos titulares de certificados digitais e o par de chaves criptográficas deve ser gerado sempre pelo titular, sua chave privada de assinatura é de seu exclusivo controle.

As Autoridades Certificadoras são entidades públicas ou pessoas jurídicas de direito

privado credenciadas à AC-Raiz e realizam a emissão de certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. O artigo 6º da Medida Provisória 2.200/01, determina que as ACs emitem, expedem, distribuem, revogam e gerenciam os certificados, disponibilizando aos usuários lista de certificados revogados e outras informações necessárias, e mantendo o registro de suas operações.

A seguir temos a cronologia da criptografia na Tabela 1:

Tabela 1 – Evolução Histórica da Criptografia

Período	**Personagens, conteúdo matemático ou tipo de criptografia**
487 a.C.	Tucídides e o Bastão de Licurgo, cifra de transposição.
± 300 a.C.	Os Elementos de Euclides, teoria dos números e números primos.
276 a 194 a.C.	O Crivo de Erastótenes, números primos.
204 a 122 a.C.	O Código de Políbio, substituição poligrâmica.
50 a.C.	O Código de César, substituição simples.
79 d.C.	A Fórmula Sator ou Quadrado Latino.
801 a 873	al-Kindi e a Criptanálise.
1119 a 1311	Templários, substituição simples por símbolos.
1466	Leon Battista Alberti: inventor da substituição polialfabética.
1518	Johannes Trithemius, esteganografia.
1533	Cifra de Pig Pen: substituição simples por símbolos.
1550	Girolamo Cardano, esteganografia e substituição com auto-chave.
1553	Giovanni Battista Bellaso, substituição polialfabética com palavra-chave.
1558	Philibert Babou, substituição homofônica.
1563	Giambattista Della Porta, substituição polialfabética com palavra-chave.
1586	Blaise de Vigenère, substituição polialfabética com palavra-chave.
1854	Charles Babbage e as Máquinas de Diferenças Cifra Playfair.
1917	William F. Friedman considerado o pai da criptoanálise norte-americana.
1920	A cifra de Bazeries: uma recifragem com métodos clássicos.
1974	A cifra de bloco DES - O NBS publica o padrão dos EUA.
1977	Método RSA: criado por R. Rivest, A. Shamir e L. Adleman.

Fonte: OLIVEIRA LOPES e SILVEIRA LOPES, 2018, p. 06

De forma geral a criptografia nasceu da necessidade de reis, rainhas e generais para realizar uma comunicação eficiente para governar e comandar seus países e exércitos, garantindo o segredo de suas mensagens. Atualmente, devido ao crescimento de transações comerciais através da internet e do surgimento das criptomoedas, a criptografia vem sendo a principal tecnologia dos sistemas de segurança eletrônica (OLIVEIRA LOPES e

SILVEIRA LOPES, 2018).

Existe uma grande dependência dos indivíduos e das organizações dos meios eletrônicos para armazenar informações e o alto grau de conectividade entre os sistemas informatizados certa preocupação em relação ao armazenamento dessas informações é causada nos usuários. Neste sentido a segurança de informação e a segurança em rede são objetivos básicos da criptografia, visto que o armazenamento, a produção e a distribuição de informações por recursos computacionais vêm tendo um aumento significativo ao decorrer dos anos.

Um sistema seguro depende do nível de segurança que este necessita, assim as políticas de segurança devem ir de acordo com as necessidades de segurança das organizações. No dia a dia são utilizadas técnicas de criptografia e ferramentas de segurança, por exemplo na internet e no e-mail.

Um programa de segurança utilizado para correio eletrônico é o PGP (Pretty Good Privacy), criado pelo engenheiro Phil Zimmermann, é um programa livremente disponível que usa a combinação do IDEA (criptografia de chave privada) com um protocolo RSA (chave pública), sendo o software de criptografia de e-mail mais utilizado no mundo.

Os ataques a sistemas computacionais ocorrem quando uma ação, sem autorização de acesso, compromete a segurança de uma informação. Alguns exemplos são: violação de segredo ou privacidade, passar-se por outra pessoa, negar responsabilidade por informação originada, negar recebimento de informação, falsear informação recebida, troca de informação, impedir que uma informação seja disponibilizada ou transmitida entre duas pessoas. Esses ataques podem ser passivos ou ativos, no primeiro caso o objetivo do atacante é ganhar conhecimento da informação sem ser percebido, já no segundo caso ocorre a modificação da informação.

No início de 1990 começaram as pesquisas para se construir um computador quântico e desenvolver uma criptografia quântica. Os ensaios iniciais relatam a utilização de fótons para fazer a transmissão de um fluxo de bits, publicados por Charles H. Bennett, Gilles Bassard e colaboradores (COSTA e FIGUEIREDO, 2010).

Atualmente muitas empresas utilizam tecnologias de "criptografia forte", insuperável até pelas empresas criadoras do software de criptografia, de forma que não oferecem um mecanismo de acesso nem quando há um processo legal. A criptografia continua com a mesma essência de sua criação, mas com maior complexidade devido ao avanço da tecnologia computacional, utilizando fórmulas complexas de matemática (algoritmos) para cifrar as mensagens ou informações.

O uso da criptografia nasceu e se difundiu devido a necessidade de confidencialidade, integridade e autenticidade de informações e comunicações sensíveis, mas atualmente está sendo desenvolvida de forma independente, ou seja, fora das entidades estatais, dando

oportunidade de acesso ao público em geral. Não há nada que possa proibir empresas de internet e de tecnologia desenvolvam sistemas seguros de armazenamento de dados e comunicação, algumas empresas importantes que utilizam a criptografia como configuração padrão são: Apple Inc e WhatsApp (ABREU, 2017).

Assim com a evolução da criptografia a Matemática vem a acompanhando, explorando suas virtudes e fraquezas. O ramo mais utilizado da Matemática na criptografia é a Teoria dos Números. No capítulo 3 será abordado uma introdução a Teoria dos Números.

3 NÚMEROS INTEIROS

A Aritmética é a área da Matemática que da base teórica da ciência capaz de manter o sigilo da informação transmitida entre duas fontes contra terceiros, a criptografia. Devido a isto foi realizado o estudo dos Números Inteiros em relação a: adição e multiplicação, ordenação, Princípio da Boa Ordenação e Princípio de Indução Matemática.

O método de contagem foi revolucionado através do surgimento dos números naturais, relacionando quantidades e números. Com o decorrer dos anos houve a expansão comercial na Europa, o que estendeu ainda mais a circulação de dinheiro e consequentemente passou a existir a necessidade de expressar situações de lucros e prejuízos, surgindo o conjunto dos números inteiros, representado por $\mathbb{Z}$ em referência a palavra alemã Zahlen (números ou algarismos).

O conceito de número inteiro se originou do conceito de número natural, criado com objetivo de resolver problemas de contagem. Devido a essa necessidade, e a outras, como fazer agrupamentos e relacionar quantidades o homem desenvolveu símbolos para resolver essas situações no conjunto dos números inteiros através das operações de adição (+) e multiplicação (.), com propriedades que serão enunciadas posteriormente de acordo com HEFEZ (2016).

Alguns subconjuntos se destacam no conjunto dos números inteiros:

Conjunto dos inteiros não nulos: $\mathbb{Z}_* = \{ \pm1, \pm2, \pm3, ...\}$;

Conjunto dos inteiros não negativos: $\mathbb{Z}_+ = \{ 0, 1, 2, 3, ...\}$;

Conjunto dos inteiros não positivos: $\mathbb{Z}_- = \{...\text{-}3, \text{-}2, \text{-}1, 0 \}$;

Conjunto dos inteiros positivos: $\mathbb{Z}_+^* = \{ 1, 2, 3, ...\}$;

Conjunto dos inteiros negativos: $\mathbb{Z}_-^* = \{... \text{ -}3, \text{-}2, \text{-}1 \}$.

Em $\mathbb{Z}$, o subconjunto $\mathbb{Z}_+^* = \{ 1, 2, 3, ... \}$ se destaca por também ser chamado de naturais, representado por $\mathbb{N}$.

Denota-se o conjunto dos números inteiros como: $\mathbb{Z} = \{..., \text{-}3, \text{-}2, \text{-}1, 0, 1, 2, 3, ...\}$. As operações de adição e multiplicação em $\mathbb{Z}$, possuem as propriedades:

1) A adição e a multiplicação são bem definidas. Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a.b = a'.b'$.

1.1) Fechamento: $a + b \in \mathbb{Z}$ e $a.b \in \mathbb{Z}$.

2) A adição e a multiplicação são comutativas. Para todos $a, b \in \mathbb{Z}$, $a + b = b + a$ e $a.b = b.a$.

3) A adição e a multiplicação são associativas. Para todos $a, b, c \in \mathbb{Z}$, $(a+b)+c = a+(b+c)$ e $(a.b).c = a.(b.c)$.

4) A adição e a multiplicação possuem elementos neutros. Para todo $a \in \mathbb{Z}$, $a+0 = a$ e $a.1 = a$.

5) A adição possui elementos simétricos. Para todo $a \in \mathbb{Z}$, existe $b(= -a)$ tal que $a+b = 0$.

6) A multiplicação é distributiva com relação à adição. Para todos $a, b, c \in \mathbb{Z}$, tem-se $a.(b+c) = a.b + a.c$.

Os axiomas acima caracterizam que $(\mathbb{Z}, +, .\ )$ é um anel.

3.1 Adição e multiplicação dos números inteiros

Destes axiomas, temos como consequência:

Proposição 3.1. *Seja $a.0 = 0$ para todo $a \in \mathbb{Z}$.*

Demonstração. Temos das propriedades 4 e 6 que:

(I) $a.0 = a(0+0) = a.0 + a.0$.

Somando – $(a\ .\ 0)$ aos membros extremos da igualdade, pelas propriedades 5, (I), 3, 5 e 4, obtemos:

$0 = -(a.0) + a.0 = -(a.0) + (a.0 + a.0)$

$= (-(a.0) + a.0) + a.0 = 0 + a.0 = 0$

□

Proposição 3.2. *A adição é compatível e cancelativa com respeito à igualdade. Para todos $a, b, c \in \mathbb{Z}, a = b$ se, e somente se, $a + c = b + c$.*

Demonstração. A implicação $a = b \Rightarrow a + c = b + c$ é consequência do fato de a adição ser bem definida (propriedade 1).

A subtração pode ser definida a partir da operação de adição. Dados dois números inteiros a e b, define-se o número b menos a, denotado por $b - a$, como sendo:

$b - a = b + (-\ a)$.

Assim $b - a$ é o resultado da subtração de a de b.

Supondo que $a + c = b + c$. Somando $(-c)$ a ambos os lados, obtemos que $c + (-c) = 0 \in \mathbb{Z}$. Logo, $a + 0 = b + 0$ e, assim, $a = b$.

□

De acordo com a ordenação dos inteiros, admitimos também os seguindo axiomas em $\mathbb{Z}$:

7) Fechamento de $\mathbb{N}$: O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todos a, $b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $a \,.\, b \in \mathbb{N}$.

8) Tricotomia: Dados a, $b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

i) $a = b$; ou

ii) $b - a \in \mathbb{N}$; ou

iii) - $(b - a) = a - b \in \mathbb{N}$.

Utilizando a notação $b > a$, onde lemos "b é maior que a", podendo ser representada também como $a < b$. Como $a - 0 = a$, decorre das definições que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,$\{x \in \mathbb{Z};\, x > 0\} = \mathbb{N}$ e $\{x \in \mathbb{Z};\, x < 0\} =$ - $\mathbb{N}$.

Daí decorre que $a > 0$ se, e somente se, - $a < 0$ (HEFEZ, 2016).

3.2 Ordenação dos números inteiros

Proposição 3.3. *A relação "menor do que" é transitiva. Para todos a, b, $c \in \mathbb{Z}$, $a < b$ e $b < c \Rightarrow a < c$.*

Demonstração. Para todo a, b, $c \in \mathbb{N}$, temos que $(c-a) \in \mathbb{N}$, de fato pois $c-a = (c-a)+0 = (c-a)+(b-b)$, devido as propriedades comutativa e assossiativa $(c-b)+(b-c) \in \mathbb{N}$

Supondo $a < b$ e $b < c$, temos que $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é aditivamente fechado, temos que $c - a = (b - a) + (c - b) \in \mathbb{N}$.

Assim $b - a + c - b = c - a$. Como $c - a \in \mathbb{N}$, logo $a < c$. □

Proposição 3.4. *A adição é compatível e cancelativa com respeito à relação "menor do que". Para todos a, b, $c \in \mathbb{Z}$, $a < b$ se, e somente se, $a + c < b + c$*

Demonstração. Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Portanto, $(b + c) - (a + c) = b - a \in \mathbb{N}$, o que implica que $a + c < b + c$.

Reciprocamente, suponha que $a + c < b + c$. Podemos somar (- c) a ambos os lados da desigualdade, o que nos conduz a: $a + c +$ (- c) $< b + c +$ (- c). Devido a adição ser cancelativa, conclui-se que $a < b$. □

Proposição 3.5. *A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor do que". Para todos a, $b \in \mathbb{Z}$, para todo $c \in \mathbb{N}$, $a < b$ implica que $a \,.\, c < b \,.\, c$.*

Demonstração. Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Assim, se $c \in \mathbb{N}$, como $\mathbb{N}$ é multiplicamente fechado, temos que $b \,.\, c - a \,.\, c = (b - a) \,.\, c \in \mathbb{N}$. Logo, $a \,.\, c < b \,.\, c$.

De forma reciproca, suponhamos que $a \,.\, c < b \,.\, c$, com $c \in \mathbb{N}$. Pela tricotomia, temos três possibilidades para analisar:

i) $a = b$. Acarretando $a \,.\, c = b \,.\, c$, o que não é verdade.

ii) $b < a$. Acarretando, pela primeira parte da demonstração, que $b \,.\, c < a \,.\, c$, o que também não é verdade.

iii) $a < b$. Sendo a única possibilidade válida. □

Proposição 3.6. *A multiplicação é compatível e cancelativa com respeito à igualdade: Para todos a, b ∈ ℤ, para todo c ∈ 0, a = b se, e somente se, a . c = b . c.*

Demonstração. A implicação $a = b$, implica que $a \,.\, c = b \,.\, c$, o que também vale quando $c = 0$, sendo consequência imediata da multiplicação ser bem definida.

Agora supondo que $a \,.\, c = b \,.\, c$, temos duas possibilidades:

i) Caso $c > 0$. Se $a < b$, pela proposição 1.5, temos que $a \,.\, c < b \,.\, c$, o que é um absurdo. Se $b > a$, pelo mesmo argumento, $b \,.\, c < a \,.\, c$, o que é absurdo. Logo, a única alternativa válida é $a = b$.

ii) Caso – $c > 0$. Se $a < b$, tem-se que $a \,.\, c > b \,.\, c$, o que é absurdo.

Se $b > a$, $a \,.\, c < b \,.\, c$, o que é um absurdo. Logo, $a = b$.

Temos a noção de valor absoluto:

Seja $a \in \mathbb{Z}$, define-se que:

$|a| = a$, se $a \geq 0$,

ou $|a| = -a$, se $a < 0$.

O número inteiro $|a|$ é chamado de módulo ou valor absoluto de a. A seguir algumas propriedades básicas do módulo. □

Proposição 3.7. *Para a, b ∈ ℤ e r ∈ ℕ, temos:*

i) $|a.b| = |a| \,.\, |b|$;

ii) $|a| \geq r$ *se, e somente se,* $-r \geq a \geq r$;

iii) - $|a| \geq a \geq |a|$;

iv) a desigualdade triangular: $||a|$ - $|b|| \leq |a \pm b| \leq |a|$ + $|b|$.

Demonstração. $|a + b| \leq |a| + |b|$, para $a, b \in \mathbb{Z}$.

(1) Como ambos os lados da desigualdade são positivos, basta mostrarmos que $|a+b|^2 \leq (|a|+|b|)^2$.

Então $|a+b|^2 = (a+b)^2 = a^2 + 2ab + b^2 = |a|^2 + 2ab + |b|^2 \leq |a|^2 + 2|ab| + |b|^2$, pois $ab \leq |ab| = |a|^2 + 2|a||b| + |b|^2 = (|a|+|b|)^2$.

Ou seja, $|a+b|^2 \leq (|a|+|b|)^2$. No caso de ser $ab \geq 0$ teremos $ab = |ab| = |a||b|$. Assim, ocorrerá igualdade.

(2) Temos que $|a| \geq a$, $|b| \geq b$

E que $|a| \geq -a$, $|b| \geq -b$

Assim, por adição obtemos que $|a| + |b| \geq a + b$, e que $|a| + |b| \geq -(a+b)$

Implicando que que $|a| + |b| \geq |a+b|$. E se for $ab \geq 0$, então podemos ter $a \geq 0$ e $b \geq 0$ ou $a \leq 0$ e $b \leq 0$.

No primeiro caso teremos consequentemente que $|a| = a$, $|b| = b$ e $|a+b| = a+b$, ou seja, ocorrerá a igualdade. O segundo caso implicará que $|a| = -a$, $|b| = -b$ e $|a+b| = -(a+b)$, ou seja, também teremos igualdade. Portanto, $|a+b| \leq |a| + |b|$, com igualdade se, e somente se, $ab \geq 0$. □

3.3 Princípio da Boa Ordenação

Existe uma propriedade adicional que somente os números inteiros possuem, o Princípio da Boa Ordenação (PBO), que o diferencia dos Racionais e dos Reais.

Todo subconjunto não vazio formado por números inteiros positivos possui um menor elemento. A seguir algumas propriedades, de acordo com Hefez (2016), do conjunto dos Inteiros que utilizam o Princípio da Boa Ordem.

Proposição 3.8. *Não existe nenhum inteiro n tal que 0 < n < 1.*

Demonstração. Suponha por absurdo que exista n, $0 < n < 1$.

Logo, o conjunto $S = \{\ x \in \mathrm{Z}\ /\ 0 < x < 1\ \}$ é não vazio, além de ser limitado inferiormente. Portanto, S possui um menor elemento a, com $0 < a < 1$. Multiplicando esta última desigualdade por a, obtemos $0 < a^2 < a < 1$, logo $a^2 \in S$ e $a^2 < a$, uma contradição. Portanto $S = \oslash$. □

Corolário 3.9. *Dado um número inteiro n qualquer, não existe nenhum número inteiro m tal que n < m < n + 1.*

Demonstração. Suponha por absurdo que exista um número inteiro m satisfazendo as desigualdades $n < m < n + 1$, logo $0 < m$ - $n < 1$, o que contradiz a proposição. □

Corolário 3.10. *Sejam $a, b \in \mathbb{Z}$. Se $a \,.\, b = 1$, então $a, b \in \{-1, 1\}$.*

Demonstração. Note que $a \neq 0$ e $b \neq 0$, pois, caso contrário $a \,.\, b = 0$.

Vamos supor que $a > 0$ (o outro caso é semelhante). Como $a \,.\, b = 1 > 0$, temos que $b > 0$, pois se $a = 0$ ou $b = 0$, teremos $a \,.\, b = 0$. Segue-se da proposição que $a \geq 1$ e $b \geq 1$. Logo $1 = a \,.\, b \geq b \geq 1$, implicando em $b = 1$. Como $a \,.\, b = 1$, temos também que $a = 1$. □

Corolário 3.11. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então $|a.b| \geq |a|$.*

Demonstração. Como $b \neq 0$ e pela proposição 1.8: não existe nenhum inteiro n de maneira que $0 < n < 1$, temos que $|b| \geq 1$. Desta forma, $|a.b| = |a|.|b| \geq |a|$. □

Corolário 3.12 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $n \,.\, b > a$.*

Demonstração. Como $|b| \neq 0$, pela proposição 1.8: não existe nenhum inteiro n de maneira que $0 < n < 1$, temos que $|b| \geq 1$. Logo, $(|a| + 1) \,.\, |b| \geq |a| + 1 > |a| \geq a$.

Tomando $n = |a| + 1$, se $b > 0$ e tomando $n =$ - $(|a| + 1)$, se $b < 0$. □

Corolário 3.13. *Se T é um subconjunto de $\mathbb{Z}$ não vazio e limitado superiormente, então T possui um maior elemento.*

Demonstração. Supondo que d seja uma cota superior para T.

Logo $x \leq d$ para todo $x \in T$. Considerando o conjunto $S = \{\ y \in$ Z; $y = d$ - x, com $x \in T\ \}$.

O conjunto S é não vazio e como $y = d - x \geq 0$, para todo $x \in T$, ele é limitado inferiormente. Logo, pelo Princípio da Boa Ordenação, ele tem um menor elemento, sendo $d - b$, com $b \in T$. Vamos mostrar que $b = maxT$. De fato, se $x \in T$, temos que $d - x \in S$, portanto, $d - x \geq d - b$, o que implica $x \leq b$. □

3.4 Princípio de Indução Matemática

Desde a antiguidade a indução finita é utilizada como método de demonstração, este princípio é uma consequência do Princípio da Boa Ordenação, a seguir são apresentados alguns teoremas de acordo com Hefez (2016).

Teorema 3.14 (Princípio de Indução Matemática)**.** *Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que:*

i) $a \in S$.

ii) S é fechado com respeito à operação de "somar 1" a seus elementos, ou seja, para qualquer n, $n \in S$, implicando em $n + 1 \in S$.

Demonstração. Ponhamos $S' = \{ x \in \mathrm{Z} ; x \geq a \}$ e suponhamos por absurdo que S' não está contido em S, logo S' *setminus* $S \neq \oslash$. Como esse conjunto é limitado inferiormente (por a), existe um menor elemento x em S' *setminus* S. Pelo fato de $c \in S'$ e $c \notin$ a S, temos que $c > a$. Portanto, $c - 1 \in S'$ e c -1 $\in S$.

Pela hipótese sobre S, temos que $c = (c - 1) + 1 \in S$, como $c \in S'$, obtemos uma contradição com o fato de $c \in S' \setminus S$. □

Teorema 3.15 (Prova por Indução Matemática)**.** *Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma sentença aberta em n. Suponha que:*

i) $p(a)$ é verdadeiro, e que

ii) Para qualquer que seja $n \geq a$, $p(n) \Rightarrow p(n + 1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

Demonstração. Seja $V = \{ n \in \mathbb{Z}; p(n) \}$, ou seja, V é um subconjunto dos elementos de $\mathbb{Z}$ para os quais $p(n)$ é verdadeiro.

Como por:

i) $a \in V$ e por

ii) n, $n \in V \Rightarrow n + 1 \in V$, seguindo o Princípio de Indução Matemática temos que $\{ x \in \mathbb{Z}; x \geq a \} \subset V$. □

Teorema 3.16 (Prova por Indução Completa)**.** *Seja $p(n)$ uma sentença aberta tal que:*

i) $p(a)$ é verdadeiro, e que:

ii) Para qualquer que seja n, $p(a)$ e $p(a + 1)$ e . . . e $p(n) \Rightarrow p(n + 1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

Demonstração. Considerando o conjunto $V = \{ n \in a + \mathbb{N}; p(n) \}$.

Supondo, por absurdo, que $W = (a + \mathbb{N}) \setminus V$ não é vazio. Logo pelo Princípio da Boa Ordenação, W teria um menor elemento k, e, como sabemos de (i) que a não pertence a W, segue-se que existe n tal que $k = a + n > a$.

Portanto, a, $a + 1$, ... , $k - 1 \notin W$; logo a, $a + 1$, ... , $k - 1 \in V$. Por (ii) conclui-se que $k = k - 1 + 1 \in V$, o que contradiz o fato de $k \in W$. Então temos que $W = (a + \mathbb{N}) \setminus V$ é vazio. □

No capítulo 4 veremos algumas propriedades relacionadas a divisibilidade, números primos e fatoração, essenciais para o entendimento da criptografia RSA. Além disso

estudaremos a aplicabilidade da criptografia em diversos sites e quais foram os maiores hackers do mundo e os sistemas que invadiram. Estes conteúdos serão fundamentais para o desenvolvimento da sequência didática.

4 DIVISIBILIDADE E FATORAÇÃO

Devido a aplicação da sequência de ensino ser relacionada a fatoração numérica de números compostos foi necessário a realização do estudo de propriedades relacionadas a divisibilidade, fatoração e números primos tendo como base Hefez (2016).

Podemos realizar a divisão de um número inteiro por outro, essa possibilidade é demonstrada através da relação de divisibilidade.

Podemos dizer que a divide b, sendo a e b números inteiros, com a seguinte escrita $a \mid b$, se existir $c \in \mathbb{Z}$, de maneira que $b = ca$. A negação dessa sentença é representada por $a \nmid b$, indicando que não existe nenhum número inteiro c de maneira que $b = ca$.

A seguir temos algumas propriedades da divisibilidade:

Proposição 4.1. *Sejam a, b, $c \in \mathbb{Z}$, tem-se que:*

i) $1 \mid a$, $a \mid a$ e $a \mid 0$.

ii) $0 \mid a \Leftrightarrow a = 0$.

iii) $a \mid b$ se, e somente se, $\mid a \mid \mid \mid b \mid$.

iv) se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. Temos que:

(i) Ocorre devido as desigualdades $a = a \,.\, 1$, $a = 1 \,.\, a$ e $0 = 0 \,.\, a$.

(ii) Suponhamos que $0 \mid a$; desta forma, existe $c \in \mathbb{Z}$ tal que $a = c$.

Tendo que $a \,.\, 0 = 0$, para todo $a \in \mathbb{Z}$, que foi demonstrado anteriormente, conclui-se que $a = 0$. Na recíproca podemos observar que $0 \mid 0$, o que foi provado no item (i).

(iii) Temos que:

($\Rightarrow$) Por hipótese $b = ac$, c $\in \mathbb{Z}$.

Daí $\mid b \mid = \mid ac \mid = \mid a \mid \mid c \mid$, implicando que $\mid a \mid \mid \mid b \mid$.

($\Leftarrow$) Por hipótese $\mid b \mid = \mid a \mid c$, $c \in \mathbb{Z}$.

Como $\mid b \mid \geq 0$ e $\mid a \mid \geq 0$, então se pode concluir que $c \geq 0$ e portanto $c = \mid c \mid$. Assim $\mid b \mid = \mid a \mid \mid c \mid = \mid ac \mid$. Mas $\mid b \mid = \pm\, b$ e $\mid ac \mid = \pm\, ac = a(\pm c)$. Logo $b = a(\pm c)$ e daí a divide b.

(iv) $a \mid b$ e $b \mid c$ implica que existem f, g $\in \mathbb{Z}$ de maneira que $b = fa$ e $c = gb$. Substituindo o valor de b da primeira equação na outra, temos que:

$c = gb = g(fa) = (gf)a$.

Mostrando que $a \mid c$. □

A relação de divisibilidade não é uma relação de ordem em $\mathbb{Z}$, apesar de ser reflexiva e transitiva, ela não é antissimétrica, por exemplo, -3 | 3, 3 | -3, porém $3 \neq$ -3.

Proposição 4.2. *Se $a, b, c, d \in \mathbb{Z}$, então $a \mid b$ e $c \mid d \Rightarrow ac \mid bd$*

Demonstração. Se $a \mid b$ e $c \mid d$, então $\exists\ f$ e $g \in \mathbb{Z}$, de modo que $b = fa$ e $d = gc$. Portanto, $bd = (fg)\ (ac)$, logo $ac \mid bd$. □

Proposição 4.3. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então $a \mid b \Leftrightarrow a \mid c$.*

Demonstração. Suponhamos que $a \mid (b+c)$. Logo, existe $f \in \mathbb{Z}$, tal que $b+c = fa$. Agora, se $a \mid b$, temos que existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as duas igualdades acima temos: $ga + c = fa$, donde segue-se que $c = (f - g)a$, logo $a \mid c$.

A prova da implicação contrária é análoga.

Por outro lado se $a \mid (b - c)$ e $a \mid b$, pelo caso anterior, temos $a \mid -c$, o que implica que $a \mid c$. □

Proposição 4.4. *Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, para todo $x, y \in \mathbb{Z}$, temos que $a \mid (xb + yc)$.*

Demonstração. $a \mid b$ e $a \mid c$ implicam que existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$.

Logo, $xb + yc = x(fa) + y(ga) = (xf + yg)a$, provando o resultado. □

Proposição 4.5. *Dados $a, b \in \mathbb{Z}$, onde $b \neq 0$, temos que $a \mid b \Rightarrow \mid a \mid \leq \mid b \mid$.*

Demonstração. Se $a \mid b$, existe $c \in \mathbb{Z}$ de maneira que $b = ca$. Tomando módulos, temos que $\mid b \mid = \mid a \mid \mid c \mid$. Como $b \neq 0$, temos que $c \neq 0$, logo $1 \leq \mid c \mid$ e, consequentemente, $\mid a \mid \leq \mid a \mid\mid c \mid = \mid b \mid$. □

O fato de sempre ser possível efetuar a divisão de b por a, com resto, foi enunciado por Euclides, e será demonstrado a seguir. Os números q e r são chamados, respectivamente, de quociente e resto na divisão de a por b.

Teorema 4.6 (Divisão Euclidiana)**.** *Sejam a e b dois números inteiros com $b \neq 0$. Existe dois únicos números inteiros q e r tais que:*

$a = bq + r$, *com* $0 \leq r \leq \mid b \mid$.

Demonstração. Considerando o conjunto $\mathrm{S} = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.

Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n.(-b) > -a$. Logo, $a - n.b > 0$, mostrando que S é um conjunto não vazio. O conjunto S é limitado inferiormente por 0,

pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - b.q$. Sabendo que $r \geq 0$. Iremos mostrar que $r \leq \mid b \mid$. Supondo por absurdo que $r \geq \mid b \mid$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = \mid b \mid + s$, logo $0 \leq s < r$. Mas, isto contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1).b \in S$, com $s < r$.

Logo, $0 \leq r \leq \mid b \mid$.

Supondo que $a = b.q + r = b.q' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < \mid b \mid$ e $0 \leq r' \leq \mid b \mid$, para provar que q e r são únicos .

Assim, temos que $- \mid b \mid < -r \leq r' - r \leq r' < \mid b \mid$. Logo, $\mid r' - r \mid < \mid b \mid$. Por outro lado, $b.(q - q') = r' - r$, o que implica que $\mid b \mid . \mid q - q' \mid = \mid r' - r \mid < \mid b \mid$. Sendo possível somente se $q = q'$ e, consequentemente, $r = r'$. □

Na divisão euclidiana, o resto da divisão de a por b será zero se, e somente se, b divide a.

4.1 Números Primos

Um número natural e maior que 1, que possui apenas os divisores positivos 1 e ele próprio, é número primo. Estes desempenham papel fundamental e são associados a muitos problemas matemáticos famosos.

Dados a, $b \in \mathbb{Z}$, distintos ou não. Um número d será dito um divisor comum de a e b se $d \mid a$ e $d \mid a$. E se um inteiro $d \geq 0$ é um máximo divisor comum (mdc) de a e b, deve possuir as seguintes propriedades:

i) d é divisor comum da a e b, e

ii) d é divisível por todo divisor comum de a e b. Ou seja se c é um divisor comum de a e b, então $c \mid d$.

O mdc de a e b será denotado por (a, b).

Considerando os números primos p e q e um número inteiro a qualquer, decorrem da definição acima os fatos:

I) Se $p \mid q$, então $p = q$.

De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > q$, o que acarreta $p = 1$.

II) Se $p \nmid a$, então $(p, a) = 1$.

De fato, se $(p, a) = d$, temos que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo é chamado composto.

Logo, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Desta forma, existirá um número natural n_2 tal que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

4.2 Fatoração

Podemos escrever os números naturais através da multiplicação de números primos. A fatoração corresponde a decomposição de qualquer número composto, através da divisão do mesmo por números primos. Este método, o mais utilizado atualmente, se torna inviável quando se trata de números muito grandes, mesmo que seja utilizado um computador potente. Por exemplo para fatorar um número primo de 47 algarismos, utilizando o super computador inaugurado pela USP em 2015, seria necessário cerca de 1 ano e 4 meses para realizar as divisões (OBMEP, 2020).

A técnica de fatoração desenvolvida pelo o matemático francês Pierre de Fermat (1601 – 1665), ficou conhecida como fatoração de Fermat, tem como base a representação de um inteiro como a diferença de dois quadrados.

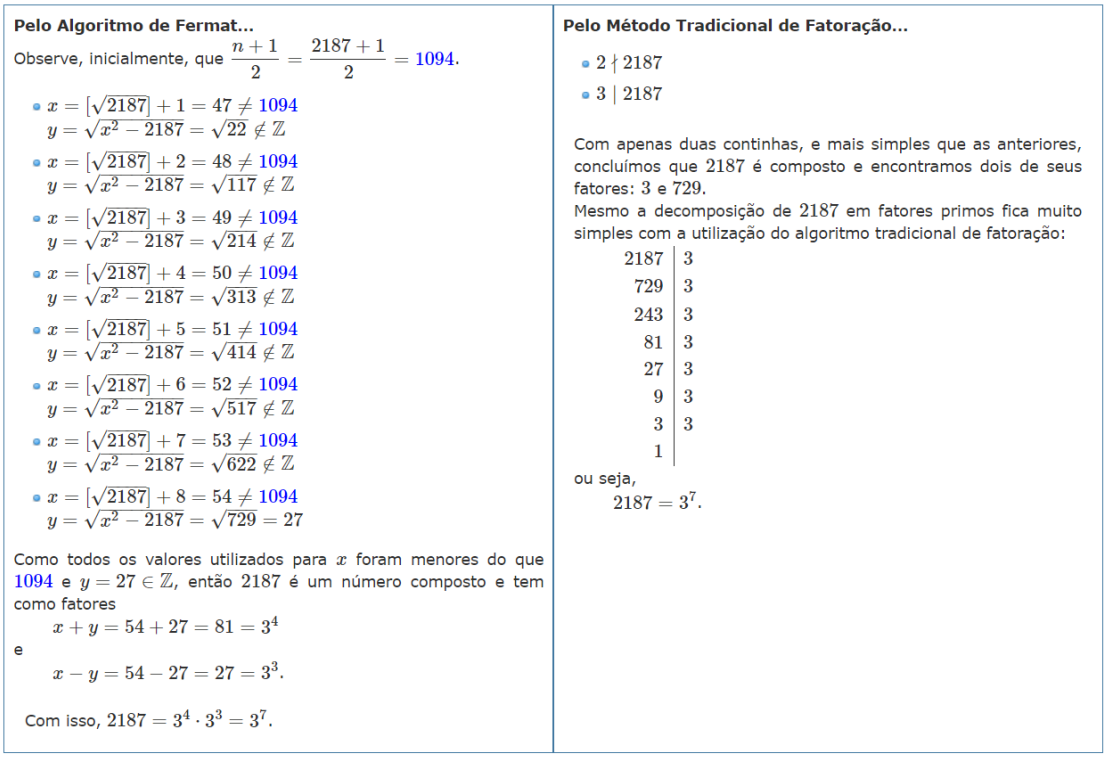
O objetivo é fatorar n inteiro maior que 1, de maneira que deve-se encontrar inteiros não negativos x e y, com $x > y$, tais que $n = x^2 - y^2$, pois $x^2 - y^2 = (x + y).(x - y)$ e dessa forma, obter-se uma fatoração de n, não precisamente em fatores primos, mas com a precisão de que n é composto.

Assim pode ser considerado n ímpar, pois se fosse par seria escrito como $n = 2(a.b)$ para algum $a \in \mathbb{Z}_+$ e algum $b \in \mathbb{Z}_+$ ímpar. Dessa forma para realizar a fatoração de n bastaria conhecer a fatoração de b devido a 2 ser um número primo, e assim haveria a necessidade de fatorar um número ímpar. Neste processo de obter x e y pode-se encontrar números que não são inteiros.

Na figura 5, pode ser observado que utilizando o algoritmo de Fermat conclui-se que 2187 é um número composto, onde se obtém os fatores $x + y = 81$ e $x - y = 27$. E que de forma mais simples e rápida pode-se encontrar a fatoração numérica de 2187, utilizando os números primos, e conclui-se que a fatoração deste número é 3^7 pois são utilizados 7 fatores 3 na decomposição deste número.

A seguir, na Figura 5, temos a fatoração do número 2187 pelo algoritmo de Fermat em comparativo com o método tradicional de fatoração.

Figura 5 – Fatoração



Pelo Algoritmo de Fermat...

Observe, inicialmente, que $\frac{n+1}{2} = \frac{2187+1}{2} = 1094$.

- $x = \lfloor\sqrt{2187}\rfloor + 1 = 47 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{22} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 2 = 48 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{117} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 3 = 49 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{214} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 4 = 50 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{313} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 5 = 51 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{414} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 6 = 52 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{517} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 7 = 53 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{622} \notin \mathbb{Z}$
- $x = \lfloor\sqrt{2187}\rfloor + 8 = 54 \neq 1094$
  $y = \sqrt{x^2 - 2187} = \sqrt{729} = 27$

Como todos os valores utilizados para x foram menores do que 1094 e $y = 27 \in \mathbb{Z}$, então 2187 é um número composto e tem como fatores

$$x + y = 54 + 27 = 81 = 3^4$$

e

$$x - y = 54 - 27 = 27 = 3^3.$$

Com isso, $2187 = 3^4 \cdot 3^3 = 3^7$.

Pelo Método Tradicional de Fatoração...

- $2 \nmid 2187$
- $3 \mid 2187$

Com apenas duas continhas, e mais simples que as anteriores, concluímos que 2187 é composto e encontramos dois de seus fatores: 3 e 729.
Mesmo a decomposição de 2187 em fatores primos fica muito simples com a utilização do algoritmo tradicional de fatoração:

2187	3
729	3
243	3
81	3
27	3
9	3
3	3
1	

ou seja,

$$2187 = 3^7.$$

Fonte: OBMEP, 2020

4.3 Criptografia RSA

A troca de informações utilizando a internet requer sigilo, desta forma é essencial que seja utilizado algum método para que essa informação seja protegida e somente o destinatário consiga ter acesso a informação disponibilizada (BONFIM, 2017).

A criptografia é o método utilizado para codificar a mensagem, e vem sendo utilizada a muito tempo, como: o Bastão de Licurgo, o Crivo de Erastótenes, o Código de Políbio, o Código de César, a Substituição Simples, a Fórmula Sator ou Quadrado Latino, os Templários, a Substituição Polialfabética, o Método RSA, entre outros.

Atualmente têm-se dois tipos de criptografia, a simétrica e a assimétrica. A primeira utiliza uma mesma chave para criptografar e posteriormente descriptografar uma mensagem, um método relativamento rápido mas inseguro devido a necessidade de compartilhar a chave, o algoritmo mais utilizado para esta criptografia é o AES (Advanced Encryption Standard). Enquanto na segunda são utilizadas duas chaves, uma para criptografar (chave pública) e outra para descriptografar a mensagem(chave privada, de uso exclusivo do destinatário), é um método relativamente mais lento, porém oferece maior segurança.

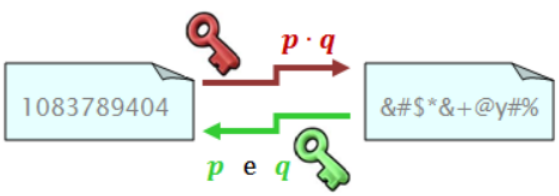
Na criptografia assimétrica cada chave privada deve ser referente a uma única chave

pública, pois somente ela poderá decifrar a mensagem. O algoritmo mais utilizado para esta criptografia é o RSA (Rivest Shamir Adleman), este método utiliza como parte do processo de criptografar dois números primos grandes, que ao serem multiplicados geram um número inteiro ainda maior. Para quebrar essa criptografia é necessário encontrar os dois fatores primos que geraram o número inteiro, para isso é necessário realizar a fatoração do mesmo.

A criptografia RSA funciona da seguinte forma: são escolhidos dois números primos p e q distintos entre si. Posteriormente multiplica-se p e q, obtendo $N = p.q$ e define-se $\varphi_{(N)} = (p-1).(q-1)$. Em seguida é escolhido um número e, que faz parte da chave pública, de maneira que o máximo divisor comum entre ele e $\varphi_{(N)}$ seja 1 e que $1 < e < \varphi_(N) \mid e.d-1$. Depois é resolvida a seguinte congruência para encontrar d (inverso multiplicativo de e) que faz parte da chave privada $(N, d) : e.d \equiv 1(mod\varphi_(N))$. Existe a necessidade de uma tabela pré formulada de domínio público (todos os números da tabela devem possuir a mesma quantidade de dígitos) para que seja realizada a transformação dos caracteres da mensagem em números e assim obter a mensagem numérica em um único bloco que será dividida em blocos b, de maneira que, $1 \leq b < N$. Garantido que ao utilizar a a congruência será obtido um único resultado na decodificação. Com a chave pública (N, e) criptografa-se os blocos b de acordo com a congruência $b^e \equiv C(b)(modN)$, de forma que $C(b)$ é a mensagem criptografada. Possuindo a chave privada (N, d) descriptografa-se usando a congruência $C(b)^d \equiv D(C(b))(modN)$, de modo que $D(C(b))$ é a mensagem descriptografada, com $1 \leq D(C(b)) < N$. Por último, cada bloco $D(C(b))$ deve ser colocado na sequência e deve-se usar novamente a tabela do pré formulada de domínio público, já utilizada no inicio do processo para realizar a conversão dos números em caracteres (BONFIM, 2017).

Assim tem-se duas grandes dificuldades com este algoritmo, os números inteiros utilizados, que são muito grandes e a dificuldade de descobrir quantos números representam cada letra, na sequência numérica que deve ser decifrada.

Figura 6 – Criptografia RSA



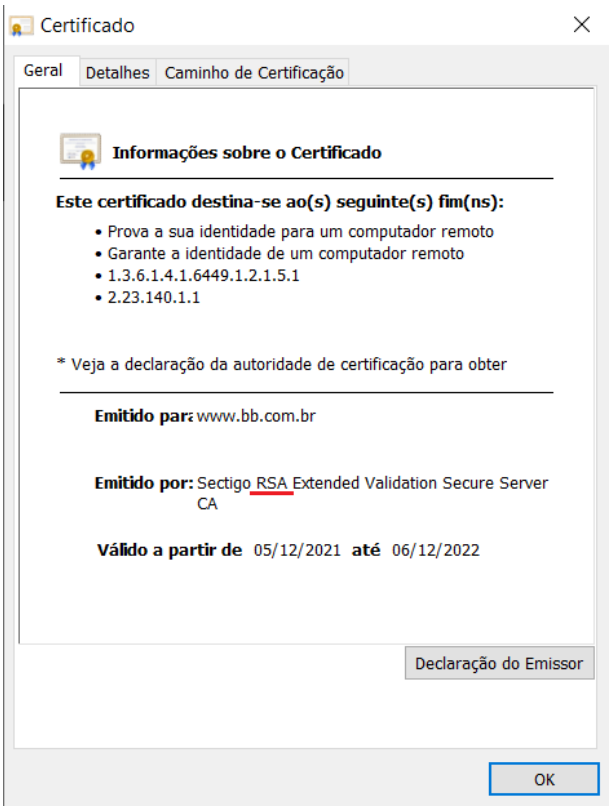
Fonte: OBMEP, 2020.

Podemos ver a criptografia RSA sendo aplicada em diferentes sites e plataformas digitais, que serão apresentadas posteriormente.

4.4 Sites e plataformas que utilizam a Criptografia RSA

Os bancos utilizam o sistema de criptografia para segurança e privacidade, o Banco do Brasil para a proteção dessas informações instituiu uma metodologia de classificação das informações corporativas, que utiliza a criptografia. A seguir na Figura 7 temos o certificado do site do Banco do Brasil:

Figura 7 – Criptografia no site do Banco do Brasil



Fonte: Banco do Brasil.

O WhatsApp que surgiu como uma alternativa ao sistema de SMS e atualmente possibilita o envio e recebimento de diversos arquivos de mídia: textos, fotos, vídeos, documentos e localização, além de chamadas de voz. Utiliza a criptografia que tem como chaves públicas: um par de chaves de identidade (chaves Curve25519 de longo prazo gerado no momento da instalação), pré-chave assinada (chaves Curve25519 de médio prazo gerado no momento da instalação assinado pela chave de identidade e alternada periodicamente) e pré-chaves de uso único (fila de pares de chaves Curve25519 para uso único, gerados no momento da instalação e repostos conforme necessário). E utiliza como chaves de sessão: chave raiz (valor de 32 bytes que é usado para criar chaves corrente, chave corrente (valor de 32 bytes que é usado para criar chaves de mensagem) e chave de mensagem (valor de 80 bytes que é usado para criptografar o conteúdo das mensagens, 32 bytes são usados para uma chave AES-256, 32 bytes para uma chave HMAC-SHA256 e 16 bytes para uma

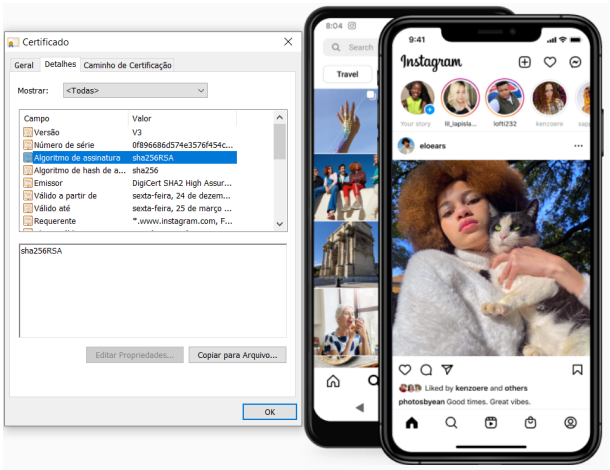
chave IV). Na Figura 8 temos a tela do WhatsApp, que mostra uma mensagem referente a presença da criptografia para manter a segurança dos usuários.

Figura 8 – Criptografia no WhatsApp

Fonte: WhatsApp.

Além dos bancos e do WhatsApp podemos encontrar a criptografia como proteção de diversos outros sites e redes sociais, como Instagram um aplicativo criado em 2010 por Kevin Systrom e Mike Krieger, que é uma rede social, assim como o Facebook, onde os usuários possuem "login"e senha em que o usuário pode rolar o "feed"de notícias para ver fotos e vídeos das pessoas a quem segue e também compartilhar, conforme a figura 9:

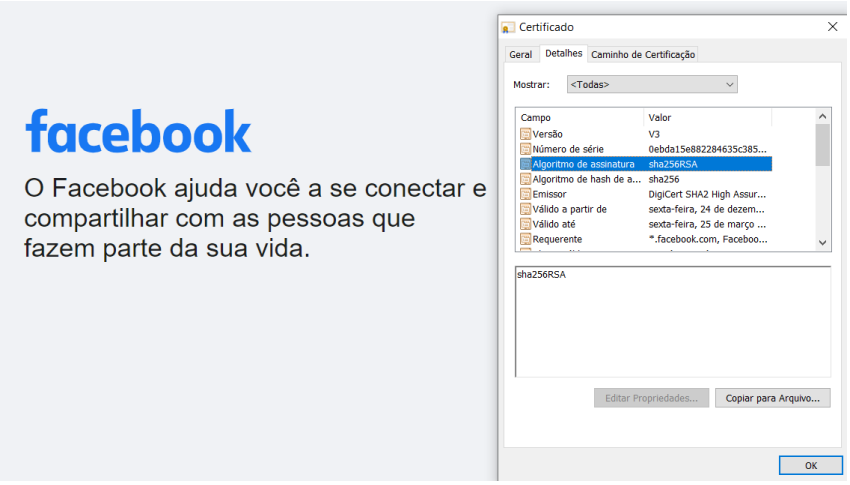
Figura 9 – Criptografia no Instagram



Fonte: Instagram.

No Facebook, criado em 2004 por Mark Zuckerberg, que é uma rede social que permite conversar com amigos e compartilhar mensagens, links, vídeos e fotografias também podemos encontrar a criptografia, como podemos observar na Figura 10 a seguir.

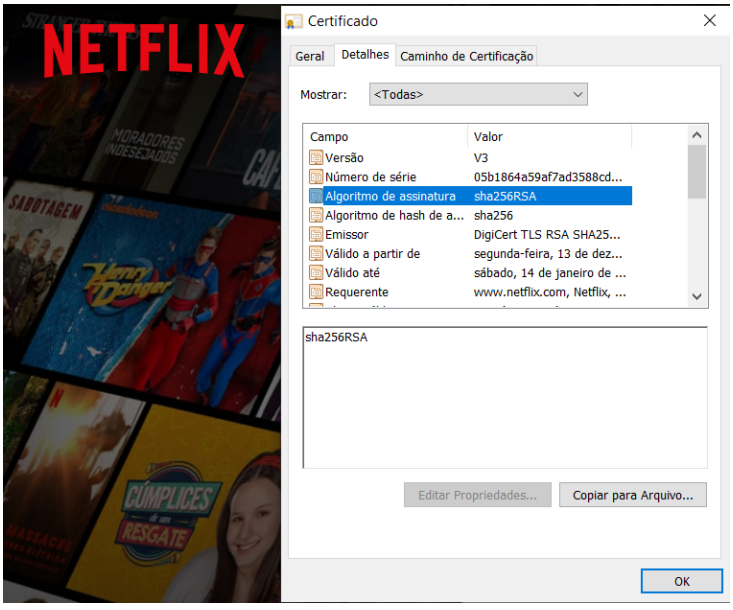
Figura 10 – Criptografia no Facebook



Fonte: Facebook.

Na Netflix, que é um serviço de transmissão online, utilizado para assistir séries, documentários e filmes também podemos visualizar a criptografia presente, conforme a Figura 11:

Figura 11 – Criptografia na Netflix



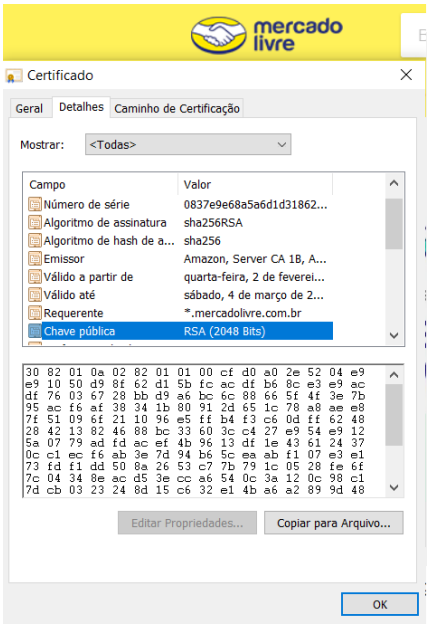
Fonte: Netflix.

Além dessas plataformas podemos encontrar a criptografia em plataformas de compra ou venda, como no Mercado Livre, na Netshoes e na Shopee por exemplo.

O Mercado Livre que é uma empresa especializada no setor de comércio eletrônico com sede em Buenos Aires, na Argentina, fundada em 1999 e que atualmente opera em 19 países incluindo o Brasil também tem presente a criptografia em seu site, de acordo

com o certificado na Figura 12.

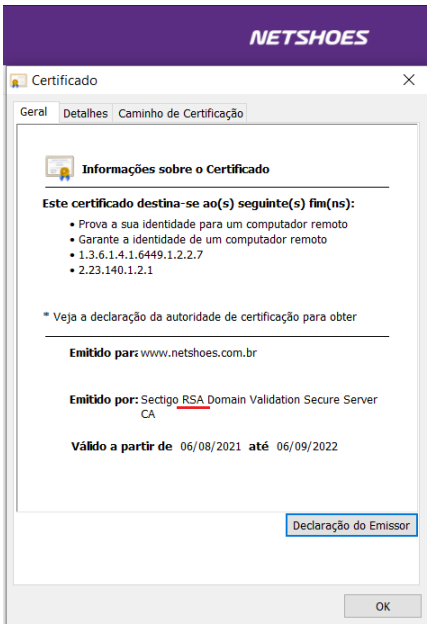
Figura 12 – Criptografia no Mercado Livre



Fonte: Mercado Livre.

A Netshoes, uma empresa brasileira criada em 2010, é uma plataforma de comércio eletrônico de artigos esportivos, nela também podemos encontrar a criptografia, como mostra no certificado na Figura 13 a seguir:

Figura 13 – Criptografia na Netshoes

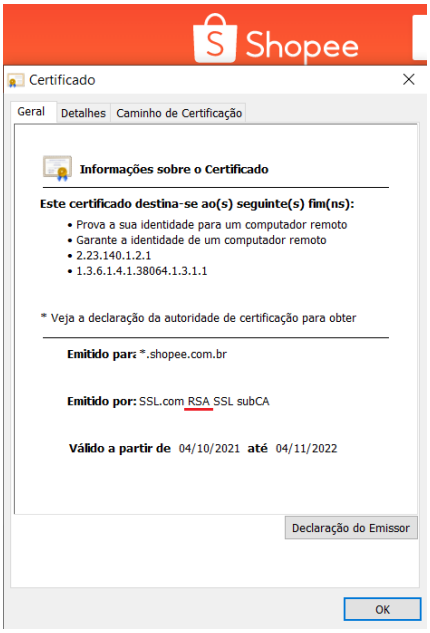


Fonte: Netshoes.

A Shopee uma plataforma asiática que chegou ao Brasil em 2019 é utilizada para

o comércio eletrônico, onde também podemos encontrar a criptografia, conforme a Figura 14:

Figura 14 – Criptografia na Shopee



Fonte: Shopee.

Então de forma geral é possivel encontrar a criptografia no certificado dos diversos sites utilizados na atualidade, que permitem a segurança e a privacidade dos dados emitidos, recebidos e armazenados.

4.5 Os maiores "hackers"do mundo

O termo "hacker"já possuiu diversas denominações, como: carpinteiros que produziam móveis com Machados, devido a "hack"ser uma onomatopeia para essas ferramentas no idioma inglês; utilizado para descrever radioamadores e "hobbystas"de mecânica ou eletrônica no período entre 1940 e 1950; aplicado à informática, o termo "hack"passou a ser utilizado por estudantes do Massachussetts Institute of Technology (MIT), na década de 60 para trotes e brincadeiras na instituição (ROCHA, 2016).

De acordo com Menezes e Cordeiro (2019):

> "Hackers"não são criminosos digitais tal como se popularizou no imaginário social. A origem do termo “hacker” vem do verbo em inglês "to hack"cujo significado é esculpir, entalhar. Ao se acrescentar a partícula “er”, se refere ao entalhador, o artista que transforma a madeira em arte, e começou a ser usada como um elogio aos integrantes do The Tech Model Railroad Club (TMRC), um clube de ferromodelismo do Massachusetts Institute of Technology (MIT), já na década de 50, se dedicavam a desenvolver locomotivas e aparelhagens de controle para

> o tráfego nas maquetes. Quando bonita e inovadora, a produção era considerada como um hacking. No MIT, o hacking era associado a brincadeiras do tipo "pegadinhas" criativas e inusitadas, bem como era considerado um hacking se aventurar caminhando por trilhas e caminhos pouco frequentados no terreno do instituto. De tal forma, o termo hackear guarda em si esse sentido de ser algo desafiador, divertido, inovador e criativo, cujo resultado é compartilhado com outras pessoas. (**MENEZES e CORDEIRO: 2019 p. 08-09**)

De forma geral o termo hacker pode ser utilizado para descrever uma pessoa que possui abrangente conhecimento na área de informática, possuindo habilidades em software e hardware. Ao redor do mundo existem milhares, talvez milhões de hackers em ação, alguns utilizando seus conhecimentos de forma lícita e outros de forma ilícita.

O Hacker mais famoso do mundo, Kevin Mitnick, se tornou uma das maiores autoridades no assunto de invasão, começou jovem na área de tecnologia da informação e aos 12 anos descobriu comando terá cartões perfurados de controle de balde ações de ônibus em Los Angeles, andando o dia todo para qualquer local da cidade sem ter que pagar por isto. O desafio chamava sua atenção, desta forma invadiu o computador do professor Tsutomu Shimomura do MIT, que recebeu este ato como uma ofensa pessoal e uma afronta a seus conhecimentos, dessa forma passou a persegui-lo e a preparar armadilhas para localizá-lo, assim em 1995, Kevin cometeu um erro e foi localizado e preso, com a sentença de 5 anos em regime fechado. Depois de cumprir a pena, Kevin passou a trabalhar com consultorias de segurança, realizando palestras pelo mundo ensinando empresas sobre as práticas de defesa contra os ataques hacker.

Existem diversos tipos de hackers: os do bem chamados White Hats, os que estão em cima do muro Gray hats e os que agem de forma criminosa chamados Black Hats ou Crackers. O diferencial entre os tipos de hackers é a motivação que possuem, entre elas temos: curiosidade, necessidade profissional, vaidade, espírito competitivo, patriotismo, ativismo e crime.

Podem ocorrer diversos tipos de ataques a redes e sistemas, como: Botnet (vírus criado com intuito de infectar o computador sem que seja percebido), DDoS/Dos (Distributed Deny Of Service attack, que derruba algum tipo de sistema online ou web sites), BruteForce (script web rodado que testa vários caracteres seguidos, a procura de senhas padrões de sistemas ou sites), Phising (spams enviados de forma aleatória, imitando banco e operadoras solicitando atualizações cadastrais) e a Engenharia social (utilização de disfarces para visitas ao local físico, buscando conhecer pessoas, informações nas redes sociais e até mesmo tentar interações com funcionários descontentes). Competindo assim aos profissionais de segurança, hackers do bem, zelar e identificar fragilidades nos sistemas, antes dos demais (ROCHA, 2016).

De acordo com Polessa (2017) a primeira geração de hackers no Brasil se deu na década de 80, com a fundação de uma editora, com intuito de difundir a boa prática de

programação e a ética hacker. A comunidade hacker brasileira foi inicialmente formada entre 1981 e 1984, limitada a universidades, empresas e pessoas que possuíam maior valor financeiro, com maior concentração na região de São Paulo.

Nessa época o Brasil vivenciava a Ditadura Militar (1964-1985) o que pode ter influenciado o país a ter uma estrutura de modelo fechado no setor de tecnologia e pesquisa por muito tempo. Diferente dos Estados Unidos, que possuía um modelo de fonte aberta em que eram compartilhados trabalhos de forma livre.

A maioria das notícias hackers que saíram no Brasil aparecem a partir de 1985, envolvendo posicionamentos negativos em torno do tema, distorcendo sua imagem para que fossem interpretados como criminosos. Mas o que os hackers brasileiros realmente buscavam na década de 1980 era o desenvolvimento de manuais que facilitassem a utilização do computador, através de publicações e traduções (POLESSA, 2017).

O primeiro indivíduo preso por crimes digitais, nos Estados Unidos, foi Jonathan James, ele invadiu os sistemas do Departamento de Defesa dos Estados Unidos e da Nasa, além de ter baixado os códigos-fonte de sistemas da Estação Espacial Internacional (ISS) aos 15 anos. Outro nome que ficou marcado na história foi o de Adrian Lamo por conseguir invadir o New Your Times, a Microsoft e Yahoo! O grupo de hackers denominado Anonymous é um dos mais conhecidos do mundo, este é formado por pessoas desconhecidas e é considerado uma organização de ativistas que invadem páginas na internet, derrubam servidores e até mesmo vazam informações confidenciais como forma de protesto. Alguns dos maiores hackers do mundo são: Kevin Mitnick (estadunidense), Jonathan James (estadunidense), Albert Gonzalez (cubano), Kevin Poulsen (estadunidense) e o grupo Anonymous.

De forma geral o principal alvo dos crackers são os bancos e grandes instituições. No Brasil vem se tornando mais frequente o vazamento de informações como o CPF e data de nascimento.

A Universidade de São Paulo (USP), criou uma inciativa chamada "Hackers do Bem", e conta com os alunos do curso de bacharelado em Ciência da Computação do Instituto de Matemática e Estatística, que buscam identificar vulnerabilidades e recomendar correções no sistema da própria instituição.

No mundo atual uma batalha digital vem sendo travada, em que temos hackers que utilizam seus conhecimentos tanto para fins lícitos, quanto para fins ilícitos. Desta forma se torna importante a disseminação de práticas e informações, tendo em vista que os indíviduos que possuem essas habilidades podem ser inseridos no mercado de trabalho de forma legal.

No Capítulo 5 será apresentado uma sequência didática, com o intuito de trabalhar com a criptografia e a fatoração de forma lúdica e divertida com os estudantes, através

de perguntas que os levem a refletir e desafios que os instiguem a pensar e resolver as situações propostas.

5 A CRIPTOGRAFIA COMO RECURSO DIDÁTICO

Neste capítulo será apresentada uma sequência de atividades que foram desenvolvidas buscando realizar a recuperação de habilidades relacionadas a fatoração que estavam em defasagem, desta forma através de atividades em grupos de aproximadamente 4 integrantes, foi realizada a retomada de conceitos relacionados a fatoração numérica e números primos, além da ideia do que é a profissão de um hacker. Utilizando slides, vídeos, questionários e um desafio com premiação no final no decorrer de 4 aulas. Na Figura 15 temos um resumo das atividades que foram desenvolvidas:

Figura 15 – Resumo das atividades

AULAS 1 e 2	Vídeo: Privacidade – Autógrafo (https://youtu.be/BjeR1wZmI-g). Vídeo: Privacidade – Vaga (https://www.youtube.com/watch?v=EMUVPWxLqZc). Formulário Inicial: • O que você conhece por hacker? • Você sabe o que é hardware e software? • Qual seu conhecimento sobre criptografia? Estudo e discussão do conceito de hacker. Texto: Hackers do bem: conheça a profissão que tem salários de até R$ 50 mil - Contratados para identificar vulnerabilidades em sistemas de segurança da informação estão em alta com o aumento das ameaças digitais. Criptografia: • Origem; • Conceito; • Fases: artesanal, mecânica e digital. Criptografia RSA: • Funcionamento; • Certificados digitais sites e plataformas digitais. Fatoração: 60 e 9900; Revisão de conceitos sobre: divisibilidade, fatoração, números primos. Crivo de Eratóstenes. Hackers e criminosos digitais.
AULAS 3 e 4	Segurança da urna eletrônica brasileira; Eleição com três candidatos fictícios → Competição: 3 urnas, 3 chaves, 3 tabelas pré-codificadas e 3 mensagens → Descobrir o resultado da eleição. Formulário Final: • Essas atividades te ajudaram com quais conhecimentos?

Fonte: autor.

5.1 Metodologia

A sequência didática foi desenvolvida nas aulas de Eletiva - Profissões: a escolha certa! – com uma turma da 1ª série do Ensino Médio, de uma escola estadual no município de Sorocaba, conforme plano de aula em Anexo A.

A disciplina faz parte do Inova Educação, um programa do governo de São Paulo, que tem por objetivo preparar os estudantes da rede estadual para o século 21. Este componente possui duas aulas semanais, e os alunos podem escolher no início do período

escolar dentre as eletivas ofertadas qual possui maior interesse, e irá cursar esse componente semestralmente.

Os jovens, na maioria das vezes, não conhecem determinadas profissões. Sendo este momento essencial para futuras tomadas de decisões, esta disciplina tem por objetivo proporcionar o contato dos estudantes com as mais diversas áreas existentes, visando o processo de escolha profissional, a troca de conhecimentos e a socialização do saber.

Assim a profissão que foi trabalhada na sequência de quatro aulas: Hacker do bem e o trabalho de profissionais da área de computação. Inicialmente a aula se deu com dois vídeos do banco Itaú, referentes a proteçãos de dados. O primeiro vídeo diz respeito a um homem com uma camiseta que possuia os números do CPF e do telefone de outro homem que estava andando na mesma rua e finalizado com a mensagem que proteger os dados não é brincadeira, como é mostrado na Figura 16:

Figura 16 – Comercial Itaú sobre pivacidade - camiseta

Fonte: https://www.youtube.com/watch?v=BjeR1wZmI-g

O segundo vídeo começou com uma mulher falando o nome de um homem que estava saindo de seu carro, em seguida fala o número do seu número do cartão e ao perguntar como a mulher havia o reconhecido a mesma responde que foi pela placa do carro, sabendo até a quantidade e o valor das prestações que foram pagas pelo carro como é mostrado na Figura 17. O vídeo foi finalizado com a mesma mensagem da propaganda anterior que proteger os dados não é brincadeira.

Figura 17 – Comercial Itaú sobre pivacidade - vaga

Fonte: https://www.youtube.com/watch?v=EMUVPWxLqZc

Com o objetivo de levantar os conhecimentos prévios dos estudantes em relação aos conceitos que iriam ser trabalhados foi respondido, em grupos de 4 alunos, um questionário com algumas perguntas norteadoras, sobre o que os alunos conheciam por hacker. Em relação a pergunta: o que você conhece por hacker? As respostas obtidas foram:

Grupo 1: A pessoa que tem a capacidade de invadir e coletar dados.

Grupo 2: É uma pessoa que entende de programação, que pode acessar ou invadir softwares.

Grupo 3: É um programador de sistema.

Grupo 4: São pessoas que conseguem invadir sistemas com uma alta segurança para conseguir dados importantes ou até mesmo são contratados pelos próprios bancos para testar a segurança deles mesmos, para que não sejam invadidos futuramente.

Grupo 5: Alguém que sabe mexer com computação, códigos, entrar em servidores. É uma pessoa que usa programação em outra programação, hackeando coisas pessoais (tipo cartão de crédito, CPF, sua conta e clona seu cartão).

Grupo 6: É um especialista em computação que comete crimes virtuais.

Grupo 7: É uma pessoa que invade sistemas para obter dados pessoais, contas, senhas, etc de outros e usa essas informações para roubar.

Já na pergunta: você sabe o que é hardware e software? As respostas obtidas foram:

Grupo 1: Hardware é a parte física do computador (ex: processador e memória) e software é a parte programada (ex: google).

Grupo 2: Ambos são sistemas físicos do computador, ou seja, são peças do computador.

Grupo 3: São sistemas.

Grupo 4: Software são sistemas operacionais, configurações como atualizações de sistema e melhorias. Hardware são as peças que mantém o PC/ smartphone, para PC existem variações onde cada peça tem uma função diferente, podendo deixá-lo mais rápido por exemplo.

Grupo 5: Hardware são as peças do computador que fazem o computador viver, software é o sistema do computador que também faz o computador viver.

Grupo 6: Hardware é a peça física do computador e software são programas que fazem o computador funcionar.

Grupo 7: Hardware é a parte exterior do computador (ex: teclado, mouse, etc). Software é a parte interior do computador (ex: fotos, sites, sistema operacional).

E na pergunta: qual seu conhecimento sobre criptografia? As respostas obtidas foram:

Grupo 1: É uma forma de camuflagem que as pessoas usam para proteger dados, trocando letras por números ou símbolos.

Grupo 2: A criptografia é um código focado na segurança de sites.

Grupo 3: É um sistema de proteção.

Grupo 4: Sites , apps populares da atualidade, Insta, Whats e Facebook ambos usam o mesmo sistema de criptografia para proteger as mensagens de seus usuários.

Grupo 5: Vamos dizer que criptografia é um "caderno"que você pode pesquisar como o google. É usado também para códigos binários.

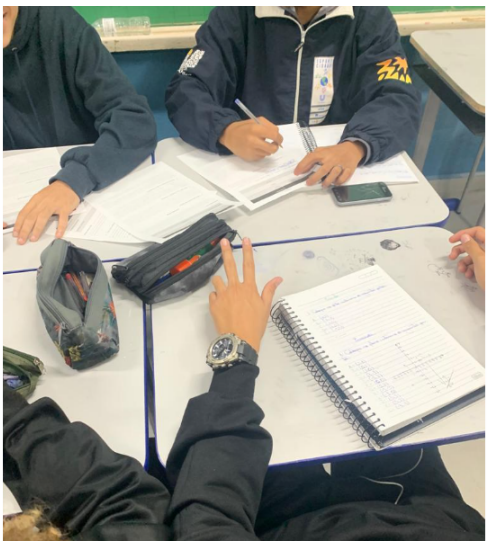
Grupo 6: É uma técnica de comunicação que usa substituição de caracteres.

Grupo 7: É quando pega dados muito importantes como senhas por exemplo e deixa impossíveis de descobrir.

Concluímos que os estudantes demonstraram ter o conhecimento prévio dos assuntos que foram abordados posteriormente. Então foi explicado que os hackers são pessoas que possuem abrangente conhecimento na área de informática, com habilidades de software e hardware. E explicado de forma simples que o hardware são as peças que compõe o computador como o teclado, monitor e placa de vídeo por exemplo, enquanto o software é a parte de programação, que fornece as instruções para o hardware.

Ainda com os 7 grupos formados com 4 alunos cada, na Figura 18, tem-se a imagem de um dos grupos com os estudantes respondendo o primeiro questionário:

Figura 18 – Alunos respondendo o questionário em grupo



Fonte: autor.

Logo em seguida foi realizada a leitura de alguns recortes do texto jornalístico de Bruno Lima, publicado em 30 de novembro de 2021, da revista Forbes - Hackers do bem: conheça a profissão que tem salários de até R$ 50 mil - Contratados para identificar vulnerabilidades em sistemas de segurança da informação estão em alta com o aumento das ameaças digitais:

> O número de ciberataques contra empresas cresceu 220% no primeiro semestre de 2021, de acordo com um relatório publicado pelo grupo Mz, empresa especializada em relações com investidores. Para profissionais de TI, esse cenário soma desafios mas também apresenta oportunidades. Os ethical hackers, também chamados de hackers do bem, contratados pelas organizações para identificar vulnerabilidades em seus sistemas de segurança da informação estão em alta com o aumento desse tipo de crime. "Percebi que as empresas estão buscando um procedimento chamado Pentest, que é um teste feito na infraestrutura da empresa para identificar falhas de segurança", diz Alessandro Alzani, especialista em cibersegurança que se deu conta dessa demanda via anúncios do LinkedIn.
>
> A remuneração de um profissional da área varia de acordo com seu nível de senioridade, mas mesmo na média é atraente. "O salário de um profissional certificado em ethical hacking varia entre R$ 7,5 mil e R$ 15 mil. Mas hoje temos profissionais com mais expertise e mais certificações cujo salário pode chegar até R$ 50 mil", diz Leandro Mainardi, diretor de serviços de segurança cibernética e educação da consultoria de educação ACADI-TI. Segundo o executivo, esses profissionais também podem encontrar colocação fora do Brasil, já que o problema se repete e cresce em todo o mundo.
>
> Quando se fala de C- Level, no entanto, a situação muda um pouco, pois a grande necessidade do mercado está nos profissionais de nível técnico. "Para especialistas, esse é um mercado bem atraente e com bastante possibilidades. Mas, quando falamos de gestores, o número de vagas é um pouco menor."
>
> Os processos de trabalho podem variar de acordo com a organização. Além do já mencionado Pentest, um dos modelos adotados consistem em uma dinâmica divisão de equipes. "Tem o blue team [equipe azul], que é o 'goleiro' que vai defender a infraestrutura. Do outro lado tem a red team [equipe vermelha], que é que vai atacar a infraestrutura", explica Alzani. Toda essa dinâmica tem o objetivo de testar a resiliência da estrutura da empresa, assim como a capacidade defensiva das equipes de TI.
>
> O especialista em cibersegurança Gabriel Castro conta que começou sua trajetória no ethical hacking dentro da equipe azul, mas que não quis parar por aí. Após estudar as dinâmicas de ataque, ele fez uma transição para a equipe vermelha para ter domínio dos dois lados do problema. Quando finalmente voltou ao posto original, o blue team, já tinha mais conhecimento e passou a ocupar um cargo de gestão. "Existe uma carência no mercado de profissionais na equipe azul que também saibam as dinâmicas de ataque", diz Gabriel. O mercado global de cibersegurança lida com uma escassez de 4 milhões de profissionais de TI, segundo levantamento de 2019 realizado pela associação global de profissionais de cibersegurança ISC.
>
> O profissional de ethical hacking já deve ter embasamento no tema antes de embarcar nessa especialização. "Ele precisa entender de sistemas operacionais e de protocolos de comunicação. Esse último é algo que ele

> precisa conhecer do começo ao fim", diz Mainardi. Um embasamento teórico específico para a área, que vai ajudar na conquista de uma vaga, exige tempo e investimento. Essa trajetória de estudos muitas vezes é finalizada com algum tipo de certificação que não é obrigatória, mas exigida por grande parte das empresas. No caso da ACADI-TI, a certificação oferecida é a CEH v11, uma das opções no mercado. Para conquistá-la, o aluno passa por mais de 40 horas de treinamento, além de um exame teórico. O preço dessa etapa atualmente gira em torno de R$ 10 mil.
>
> A procura por essa formação vem aumentando, de acordo com o CEO da fintech de crédito estudantil Elleve, André Dratovsky. "Enxergamos o potencial das pessoas, mesmo aquelas de menor poder aquisitivo, que embarcam nessa formação. Sabemos que as chances delas de obter êxito são grandes, assim como as nossas de recuperar esse crédito."
>
> (**LIMA: 2021**)

Os trechos do texto jornalístico selecionados com a intencionalidade de chamar a atenção dos estudantes foram: "Hackers do bem: conheça a profissão que tem salários de até R$ 50 mil", trechos como: "O número de ciberataques contra empresas cresceu 220% no primeiro semestre de 2021", "Para profissionais de TI, esse cenário soma desafios mas também apresenta oportunidades. Os ethical hackers, também chamados de hackers do bem, contratados pelas organizações para identificar vulnerabilidades em seus sistemas de segurança da informação estão em alta com o aumento desse tipo de crime", "O salário de um profissional certificado em ethical hacking varia entre R$ 7,5 mil e R$ 15 mil. Mas hoje temos profissionais com mais expertise e mais certificações cujo salário pode chegar até R$ 50 mil", "O mercado global de cibersegurança lida com uma escassez de 4 milhões de profissionais de TI, segundo levantamento de 2019 realizado pela associação global de profissionais de cibersegurança ISC", "Ele precisa entender de sistemas operacionais e de protocolos de comunicação. Esse último é algo que ele precisa conhecer do começo ao fim", "No caso da ACADI-TI, a certificação oferecida é a CEH v11, uma das opções no mercado. Para conquistá-la, o aluno passa por mais de 40 horas de treinamento, além de um exame teórico. O preço dessa etapa atualmente gira em torno de R$ 10 mil"e "A procura por essa formação vem aumentando".

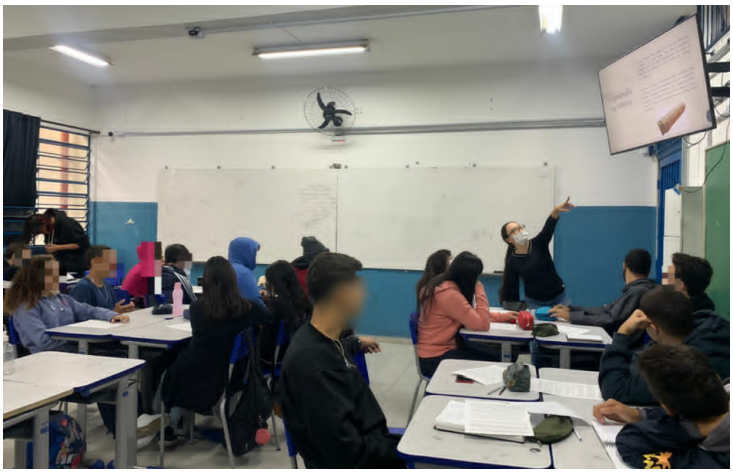
Os estudantes ficaram interessados quanto ao valor do salário dos profissionais citados no texto. Posteriormente em conversa com os alunos foi explicado que os hackers de forma geral testam, protegem e fazem sistemas de segurança, e que nesses sistemas está presente a criptografia, assim foi introduzido o conceito de criptografia.

Foi explicado que a criptografia é utilizada desde a antiguidade para enviar mensagens, de forma que somente o remetente e o destinatário conseguissem compreender o conteúdo da mensagem, com uma breve explanação sobre alguns equipamentos e métodos que foram utilizados ao longo da história.

Os alunos se mostraram surpresos com a presença da criptografia desde a antiguidade, e citaram alguns filmes em que são utilizados o código morse e a máquina

enigma. A seguir, na Figura 19, temos um registro da apresentação dos slides na televisão da sala de aula para os alunos:

Figura 19 – Apresentação dos slides



Fonte: autor.

Buscando fazer com que os estudantes entendessem que a criptografia tem por objetivo esconder uma mensagem ou informação, de maneira que se obtém um código, que pode ser decifrado. Foi explicado que a criptografia RSA é o método mais conhecido, onde são necessários dois números primos grandes, que multiplicados resultam num terceiro número ainda maior, e que para quebrar essa criptografia é necessário encontrar os números primos utilizados inicialmente e para isso é preciso realizar a sua fatoração.

Figura 20 – Apresentação do slide sobre criptografia

Fonte: autor.

Em seguida foram mostrados alguns certificados digitais que mostram a presença

da criptografia RSA, como: Banco do Brasil, WhatsApp, Instagram, Facebook, Netflix, Mercado Livre, Netshoes e Shopee.

Os alunos se surpreenderam com a criptografia tão presente no dia a dia dos mesmos, a seguir temos a Figura 21 com o registro da apresentação de alguns dos certificados digitais que foram mostrados durante as aulas para os estudantes, onde puderam observar a presença da criptografia até mesmo nas redes sociais que eles mais utilizam.

Figura 21 – Apresentação do slide com alguns certificados digitais

Fonte: autor.

Após foi o momento dos alunos fatorarem dois números compostos, um sem explicação para percepção dos conhecimentos prévios dos estudantes, posteriormente foi realizada a correção e relembrado conceitos do que é um número primo e como realizar a fatoração de um número inteiro, em seguida foi lançado outro desafio, a fatoração de um número maior, com o intuito de que percebam que quanto o maior o número maior será a dificuldade de encontrar os números primos que deram origem ao número composto.

O primeiro número que foi solicitado que os estudantes realizassem a fatoração foi o 60, sem nenhuma explicação anterior, e foi percerptível que quase toda a sala já não lembrava mais o que era fatoração. Um comentário que se mostrou interessante foi de uma aluna que relacionou a fatoração com MMC (Mínimo Múltiplo Comum), o que fez com que a classe de certa forma se sentisse mais confortável para realizar as fatorações, como se deixasse mais claro, já que era um conteúdo que eles já haviam estudado. Porém demonstraram grandes dificuldades em realizar as divisões manualmente, sem calculadora. Não lembravam os critérios de divisibilidade, e mostraram certa dificuldade para trabalhar com números primos.

Depois foi solicitado que realizassem a fatoração do número 9900, que fizeram com menos dificuldade, consultando uma tabela com os números primos de 0 a 99.

Posteriormente foram apresentados alguns criminosos digitais e o que eles fizeram, de forma ilícita: Kevin Mitnick, Jonathan James, Albert Gonzalez, Kevin Poulsen e o grupo Anonymous.

Nas duas aulas seguintes foi conversado que um mecanismo de segurança para o funcionamento dos programas computacionais é a criptografia digital, tornando os dados embaralhados e inacessíveis a indivíduos que não são autorizados, e que o Tribunal Superior Eleitoral utiliza algoritmos de cifração simétrica e assimétrica na urna eletrônica. Explicado que é criptografado o boletim da urna de maneira segmentada, assinado digitalmente e transmitido e que a descriptografia é o processo em que se realiza a recuperação dos dados que foram criptografados, os desembaralhando.

Assim o desafio foi lançado: o computador que faz o processo de descriptografia quebrou e assim precisamos da sua ajuda para descriptografar os resultados de algumas urnas eletrônicas e chegarmos no resultado de uma eleição utilizando as chaves e as mensagens de cada urna.

Eram três chaves, os alunos receberam as três chaves, nelas estavam dois números que eles precisaram fatorar e encontrar os números primos que lhe deram origem para ter acesso ao conteúdo de cada urna (tabela pré-codificada e mensagem). Sendo os números da chave 1: 2350 e 16380, os números da chave 2: 6486 e 11011 e os números da chave 3: 118121 e 290377.

Eram três urnas, cada uma com sua tabela pré-codificada, e uma mensagem com a quantidade de votos de cada um dos três candidatos, era necessário descobrir o conteúdo das mensagens a seguir através da codificação das mensagens, condiderando 00 como o espaço, sendo que o resultado da mesma era a troca dos números pela letras e vice-versa.

Figura 22 – Urnas com suas respectivas chaves

Fonte: autor.

As mensagens foram:

Mensagem 1

CANDIDATO GIOVANI AMBROSIO 1231 VOTOS

12102313181310292400161824311023180010221127242818240 0CV003124292428

CANDIDATA DANIELA BERNARDI 1232 VOTOS

12102313181310291000131023181421100011142723102713180 0CW003124292428

CANDIDATA NICOLLE COUTINHO 1322 VOTOS

12102313181310291000231812242121140012243029182317240 0DM003124292428

Figura 23 – Codificação 1

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: autor.

Mensagem 2

CANDIDATA DANIELA BERNARDI 3843 VOTOS

38364939443936553600393649444047360037405349365339440 0CH005750555054

CANDIDATO GIOVANI AMBROSIO 3642 VOTOS

38364939443936555000424450573649440036483753505444500 0AG005750555054

CANDIDATA NICOLLE COUTINHO 3747 VOTOS

38364939443936553600494438504747400038505655444943500 0BL005750555054

Figura 24 – Codificação 2

A	B	C	D	E	F	G	H	I	J	K	L	M
36	37	38	39	40	41	42	43	44	45	46	47	48
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
49	50	51	52	53	54	55	56	57	58	59	60	61

Fonte: autor.

Mensagem 3

CANDIDATA NICOLLE COUTINHO 6287 VOTOS

64627565706562816200757064767373660064768281707569760 0AZ008376817680

CANDIDATA DANIELA BERNARDI 6283 VOTOS

64627565706562816200656275706673620063667975627965700 0AV008376817680

CANDIDATO GIOVANI AMBROSIO 6472 VOTOS

64627565706562817600687076836275700062746379768070760OCK008376817680

Figura 25 – Codificação 3

A	B	C	D	E	F	G	H	I	J	K	L	M
62	63	64	65	66	67	68	69	70	71	72	73	74
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
75	76	77	78	79	80	81	82	83	84	85	86	87

Fonte: autor.

Foi necessário que os estudantes somassem os votos que cada candidato obteve, para obter o total dos votos e encontrar qual foi vencedor, que neste caso foi a candidata Daniela Bernardi com 11358 votos.

O grupo 1 foi o vencedor, com as respostas completas e todas as fatorações e o resultado final correto obtido primeiro. Os outros grupos quase finalizaram a contagem dos votos, de forma geral os alunos se mostraram competitivos e determinados a vencer. Cada integrante do grupo vencedor recebeu uma caixa de Bis como prêmio, enquanto os demais ganharam dois chocolates Bis pela participação e desempenho na atividade.

5.2 Resultados

Depois para finalizar os alunos responderam em grupo a seguinte pergunta: essas atividades te ajudaram com quais conhecimentos?

As respostas foram:

Grupo 1: Essa atividade nos ajudou a ter mais conhecimento em Matemática, trabalho em grupo e nos concedeu um raro aprendizado sobre criptografia, que utiliza números primos bem grandes. Aprendemos sobre um tipo de profissão não muito conhecida e também a diferença entre hacker e cracker.

Grupo 2: Ajudaram com a Matemática e aprendemos sobre fatoração, lembramos dos números primos e descobrimos quais letras trocar pelos numerais no papel e tivemos que lembrar coisas que aprendemos a muito tempo atrás.

Grupo 3: Trabalhar em grupo; Exercitar a mente com a Matemática; Usar a mente para resolver códigos; Agilidade; Racíocinio rápido; Competitividade.

Grupo 4: Foi bem legal, nos ajudou a ter mais conhecimento sobre o faturamento de um hacker e foi legal trabalhar em equipe. A criptografia nós entendemos que é uma maneira de esconder informações tipo senhas, palavras e informações.

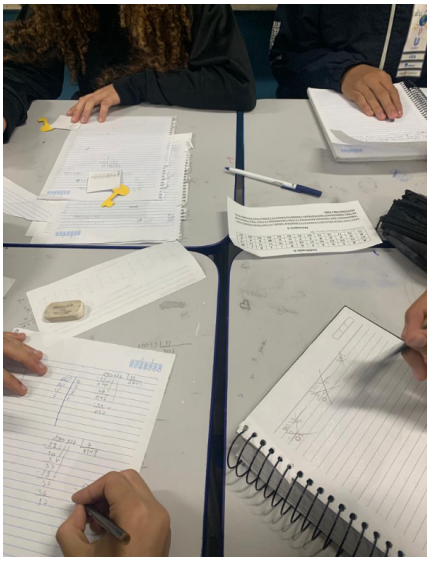
Grupo 5: MMC, coisas sobre criptografia, muitos cálculos e também sobre cracker e hacker. Que é uma chave de segurança feita por uma sequência de números e letras.

Grupo 6: A atividade nos ajudou com o trabalho em grupo e com cálculos rápidos, e estamos cientes de que a criptografia é importante para as nossas vidas para proteger os nossos dados.

Grupo 7: Raciocínio lógico, fatoração, agilidade e trabalhar em grupo, o que valoriza cada integrante do grupo e a troca de conhecimento e experiência. Que a criptografia é um conjunto de técnicas que cifra a escrita, fazendo com que ela fique inteligente.

A seguir temos a Figura 26 de um dos grupos fazendo as divisões de um dos números das chaves, para obter sua fatoração.

Figura 26 – Momento da realização da atividade prática



Fonte: autor.

A criptografia RSA utiliza como parte do processo de criptografar o produto de dois números primos grandes que geram um número inteiro ainda maior, dessa forma criando a dificuldade para encontrar os números que deram origem a este terceiro, assim sendo necessária a fatoração do mesmo.

Assim no decorrer de 4 aulas foi explicado o significado de criptografia e seu contexto histórico. Inicialmente foram expostos dois vídeos do banco Itaú a respeito da proteção de dados, o que prendeu a atenção dos alunos pois diziam respeito ao CPF, telefone, número de cartão e placa de carro. Todos os estudantes já possuiam CPF, um número de telefone e seus pais em sua maioria utilizam cartão de crédito. Assim iniciamos a noção de como a segurança dos dados é importante para os usuários.

Posteriormente os alunos responderam um questionário em grupo sobre o que conheciam por hacker, software, hardware e criptografia algumas respostas surpreenderam, pois boa parte dos alunos tinham uma certa noção do que estava sendo perguntado. Em seguida houve uma conversa entre os alunos da sala e a professora, onde cada grupo expôs

suas respostas de forma que os estudantes entendessem que os hackers não são criminosos digitais.

Os estudantes se mostraram surpresos e interessados em relação a remuneração de um hacker, despertando mais a curiosidade dos mesmos sobre essa profissão que não é tão falada. Seguido de uma breve apresentação do histórico da criptografia onde foi explicado suas três fases: artesanal, mecânica e digital.

Assim após a explicação da fase digital, foi iniciada uma conversa sobre a criptografia RSA, que é um método onde são necessários dois números primos grandes que resultam em um terceiro através do produto deles. Logo após foram expostos alguns certificados digitais que mostram a presença da criptografia RSA em sites como: Instagram, Facebook, Banco do Brasil, Netflix, WhatsApp, Shopee, Netshoes e Mercado Livre.

Posteriormente o desafio, que obteve a participação de todos os estudantes, consistia em descriptografar os resultados de três urnas eletrônicas e chegar no resultado de uma eleição utilizando as chaves e as mensagens de cada urna. Cada chave era referente a uma urna e nela continham dois números que deveriam ser fatorados, após a realização correta da fatoração recebiam uma ficha com uma tabela pré codificada e uma mensagem com o resultado dos votos daquela urna para cada candidato e deveriam descrobrir a mensagem. No final ao somar os votos dos candidatos das três urnas deveriam dizer qual foi o candidato vencedor daquela eleição.

Assim, com a pesquisa constata-se que a criptografia RSA está presente no nosso dia a dia, e que mesmo sendo possível realizar a fatoração, quanto maior o número maior será a dificuldade e o tempo utilizado. Que o hacker tem uma função muito importante para a sociedade e que ajuda a proteger os dados e da maior segurança para os usários. Os alunos gostaram de trabalhar em grupos, acharam a atividade legal e ao mesmo tempo retomaram conteúdos anteriores que estavam em defasagem.

5.3 Análise e discussão

Observando os resultados obtidos durante a aplicação da sequência didática percebemos que havia uma defasagem maior do quer o esperado no conteúdo de fatoração numérica, visto que o conteúdo de MMC (Mínimo Múltiplo Comum) supostamente eles teriam visto por volta de 2019 no 7º ano do Ensino Fundamental, na habilidade (EF07MA01) Resolver e elaborar situações problema com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmo.

Outro fato que chamou a atenção foi que os alunos já não lembravam dos critérios de divisibilidade, por exemplo que qualquer número par seria divisível por 2, que se a soma

dos algarismos de um número fosse divisível por 3, esse número também seria divisível por 3, que qualquer número terminado em 0 ou 5 é divisível por 5. Ao analisar as habilidades essenciais do Currículo Paulista encontramos a habilidade referente ao 6º ano do Ensino Fundamental (EF06MA06) Resolver e elaborar situações problema que envolvam as ideias de múltiplo e de divisor, reconhecendo os números primos, múltiplos e divisores. Os estudantes de forma geral já não lembravam dos critérios de divisibilidade, que foram conteúdos vistos supostamente no 6º ano do Ensino Fundamental.

A sequência didática de quatro aulas fez uma revisão de conteúdos que estavam em defasagem, utilizando os slides do Anexo B, além de diversos recursos para auxiliar no processo de aprendizagem dos estudantes, buscando a participacação e interesse de todos através de vídeos, texto, slides e dinâmica em grupos.

Nas aulas posteriores os alunos foram desafiados a participar de uma competição relacionada a uma eleição, tema pertinente ao ano de 2022. Foi explicado que as urnas utilizam o sistema de criptografia para criptografar o boletim da urna e que posteriormente é necessário fazer a descriptografia, desembaralhando os dados. Os estudantes demonstraram interesse pela atividade e participaram, percebendo a Matemática mais uma vez presente em seu cotidiano e com o incentivo de que no final o grupo vencedor iria receber um prêmio.

Os alunos apresentaram dificuldades em relação a realização das divisões, visto que não deveriam utilizar o celular e nem calculadora para realização dos cálculos, em alguns momentos ficavam desestimulados e a professora buscava dar dicas em relação a quais números primos eles poderiam usar para realizar a fatoração, como por exemplo tentar um número primo entre 30 e 40, relembrando alguns critérios de divisibilidade e com o slide dos números primos na televisão.

Todos os grupos se empenharam para obter a melhor pontuação, responderam todos os questionários com responsabilidade, trabalharam em equipe e participaram positivamente de todas as atividades propostas.

6 Considerações Finais

O trabalho investigou as implicações de uma sequência de ensino para estudantes da 1ª série do Ensino Médio utilizando a criptografia RSA e a fatoração numérica, além de realizar o estudo da criptografia RSA, seu papel na proteção de dados e sua presença no cotidiano na vida dos indivíduos da sociedade atual, principalmente dos adolescentes, em relação a suas redes sociais.

Assim ocorreu a análise da inserção de conteúdos que estão presentes no dia a dia dos estudantes, de maneira a instigar a curiosidade e o interesse dos mesmos. Nos dias atuais os adolescentes estão super antenados em redes sociais e de compartilhamento de informações como: WhatsApp, Youtube, Facebook, Instagram, Netflix entre outras plataformas.

Além das redes sociais temos também os bancos, as plataformas de venda de produtos, entre outros aplicativos que precisam fazer a proteção dos dados, assim precisam proteger a integridade e a segurança de seus usuários, dessa forma o algoritmo mais utilizado é a criptografia RSA.

Após as atividades, as respostas do estudantes sobre os conhecimentos adquiridos se relacionaram de forma geral a: maior conhecimento da Matemática, aprender sobre criptografia e que esta utiliza números primos bem grandes, fatoração relembrando dos números primos, raciocínio rápido, faturamento de um hacker, minímo múltiplo comum e que a criptografia é importante para as vida das pessoas por conta a proteção de dados.

A aplicação inicial para pesquisa seria a criptografia com funções ou com congruências, mas devido a pandemia os alunos apresentaram dificuldades nas operações básicas, levando em consideração que estão na 1ª série do ensino médio e as habilidades essenciais são trabalhadas nas aulas de Matemática, de maneira que na sondagem realizada no início do ano com os estudantes, alguns apresentaram grande dificuldade em realizar divisões, assim a prática foi alterada para a aplicação com fatoração.

Tendo em vista que os primeiros casos de COVID foram em 2019, que em 30 de janeiro de 2020, a OMS declarou que o surto do novo coronavírus e as escolas estaduais suspenderam gradualmente as aulas por volta de março de 2020. Desde então os estudantes ficaram no ensino remoto, e parte se afastou da escola e do ensino, assim alguns conteúdos entre o 8º e 9º ano do Ensino Fundamental podem nem terem sido vistos por parte dos estudantes. Assim podemos deduzir que o MMC foi parte do que eles haviam estudado por último no ensino presencial em 2019, por isso que conseguiram assimilar o MMC a fatoração de um número inteiro.

Alguns pontos positivos foram que todos os estudantes já possuíam dados pessoais ou senhas, o que auxiliou no processo de entendimento da importância da proteção de dados e da criptografia RSA, os estudantes se mostraram surpresos e interessados em relação a remuneração de um hacker, despertando ainda mais a curiosidade dos mesmos sobre essa profissão que não é tão comentada.

De forma geral todos os alunos se mostraram interessados na presença da criptografia RSA, pelas atividades e o desafio que a competição gerou, e que ocorreu de forma lúdica. Os estudantes realizaram as fatorações com empenho, utilizando rascunhos para fazer as divisões. Então todo o esforço e empenho na preparação das aulas valeu a pena, visto que foi imensamente satisfatório ver a participação e a vontade de resolver o desafio por parte dos estudantes.

Após a realização das atividades algumas ideias surgiram como a utilização da calculadora e o uso de números primos maiores como parte do desafio. Além disso a possibilidade de utilizar erros controlados, com um certo raio de erros, para evitar que os estudantes percebam a repetição nas frases das respostas.

O estudo e realização deste trabalho foi impactante em minha carreira como professora, foram adquiridos conhecimentos relacionados a criptografia RSA que já eram vistos como importantes, mas que se mostraram ainda mais devido a sua aplicabilidade e importância para a sociedade, em especial relacionado as urnas eletrônicas que fazem parte do processo eleitoral que futuramente irá definir os governantes do Brasil, em especial o presidente, de forma democrática e segura.

Referências Bibliográficas

ABREU, Jacqueline de Souza. **Passado, presente e futuro da criptografia forte:** desenvolvimento tecnológico e regulação. Revista Brasileira de Políticas Públicas 7, nº 3 (2017): 24-42.

BANCO DO BRASIL. **Certificado**. Disponível em: <https://www.bb.com.br/site/> . Acesso em: 12 de mar. de 2022.

BONFIM, Daniele Helena. **Criptografia RSA**. Dissertação (Mestrado – Programa de Pós Graduação em Mestrado Profissional em Matemática em Rede Nacional). USP. São Carlos, São Paulo, 2017.

CERTISING. **Como a criptografia funciona no Certificado Digital?**. 2018. Disponível em: <https://blog.certisign.com.br/como-a-criptografia-funciona-no-certificado-digital/>. Acesso em: 02 de setembro de 2022.

COSTA, Celso, e FIGUEIREDO, Luiz Manoel. **Introdução à Criptografia**. Volume 1. Fundação CECIERJ, consórcio CEDERJ. Rio de Janeiro: UFF / CEP – EB, 2010.

FACEBOOK. **Certificado**. Disponível em: <https://pt-br.facebook.com/> . Acesso em: 12 de mar. de 2022.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**. Faculdade de Ciências da Universidade de Lisboa. Dissertação de Mestrado em Matemática para Professores. 2010.

FRANÇA, Waldizar Borges de Araújo. **A utilização da criptografia para uma aprendizagem contextualizada e significativa**. 2014. 63 f., il. Dissertação (Mestrado em Matemática) - Universidade de Brasília, Brasília, 2014.

HEFEZ, Abramo; **Aritmética**. Coleção Profmat. Rio de Janeiro: SBM, 2016.

INSTAGRAM. **Certificado**. Disponível em: <https://www.instagram.com/>. Acesso em: 12 de mar. de 2022.

ITAU. **Privacidade – Camiseta**. 8 de abr. de 2021. 1 vídeo (48 seg.). Disponível em: <https://www.youtube.com/watch?v=BjeR1wZmI-g>. Publicado pelo Itaú. Acesso em: 15 de maio de 2022.

ITAU. **Privacidade - Vaga**. 28 de mar. de 2021. 1 vídeo (33 seg.). Disponível em: <https://www.youtube.com/watch?v=EMUVPWxLqZc>. Publicado pelo Itaú. Acesso em: 15 de maio de 2022.

KLEINA, Nilton. **Colossus:** herói de guerra e um dos primeiros computadores do mundo. Publicado em 14 de jun. de 2013. Disponível

em: <https://www.tecmundo.com.br/historia/40576-colossus-heroi-de-guerra-e-um-dos-primeiros-computadores-do-mundo.htm>. Acesso em 11 de mar. de 2022.

LIMA, Bruno de. **Hackers do bem:** conheça a profissão que tem salários de até R$ 50 mil. Forbes, cidade de publicação, 30 de novembro de 2021. Disponível em: <https://forbes.com.br/carreira/2021/11/hackers-do-bem-a-profissao-que-tem-salarios-de-ate-r-50-mil/>. Acesso em: 21 abr. 2022.

MEDEIROS, Fábio. **Criptografia:** Bastão de Licurgo (scytale) em Python. Publicado em 13 maio 2013. Disponível em: <https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/> . Acesso em 10 de mar. de 2022.

MENEZES, Karina Moreira; CORDEIRO, Salete de Fátima Noro. **Crianças, adultos e hackers:** cotidianos e tecnologias. Revista Entreideias: educação, cultura e sociedade, [S. l.], v. 8, n. 2, 2019. DOI: 10.9771/re.v8i2.27625. Disponível em: <https://periodicos.ufba.br/index.php/entreideias/article/view/27625>. Acesso em: 15 abr. 2022.

MERCADO LIVRE. **Certificado**. Disponível em: <https://www.mercadolivre.com.br/> . Acesso em: 13 de mar. de 2022.

NETFLIX. **Certificado**. Disponível em: <https://www.netflix.com/br/> . Acesso em: 13 de mar. de 2022.

NETSHOES. **Certificado**. Disponível em: <https://www.netshoes.com.br/ >. Acesso em: 13 de mar. de 2022.

OBMEP. **Sala de Estudo:** Fatorando de um jeito diferente (nível avançado). Clubes de matemática da Obmep, 2020. Disponível em: <http://clubes.obmep.org.br/blog/fatorando-de-um-jeito-diferente/>. Acesso em: 09 de março de 2022.

OLIVEIRA LOPES, Gabriela Lucheze de, e SILVEIRA LOPES, Jaques. **Criptografia:** a evolução histórica e seu potencial como ferramenta no ensino de teoria dos números nos cursos de licenciatura em matemática. Anais V CONEDU, Campina Grande: Realize Editora, 2018. Disponível em: <https://editorarealize.com.br/artigo/visualizar/46859>. Acesso em: 02 de mar. de 2022.

PASTOR, Luis Paulo Rodrigues. **Análise e implementação de algoritmo paralelo distribuído para fatoração de números inteiros utilizando Java** RMI. 2013. Monografia (Bacharelado Em Ciência Da Computação). 72 p. Fundação De Ensino "Eurípides Soares Da Rocha".

POLESSA, Ana Carolina Estorani. **Por uma genealogia da cena hacker brasileira**. Revista Sinais: Revista de Ciências Sociais, v. 21 n. 2 (2017): Sinais. DOI: 10.25067/s.v21i2.16761. Disponível em: <https://periodicos.ufes.br/sinais/article/view/16761>. Acesso em: 12 abr. de 2022.

PÓVOA, Tiago Marques Esteves. **Estudo sobre os principais aspectos da criptografia simétrica e assimétrica ao longo da história**. 2019. Dissertação (Mestrado Profissional em Matemática). Universidade de Brasília, Distrito Federal.

ROCHA, Juliano Vieira da. **HACKERS e suas características**. Artigo apresentado ao Instituto de Ciências Exatas e Tecnológicas (ICET) – Universidade Feevale, Novo Hamburgo, 2016.

SHOPEE. **Certificado**. Disponível em: <https://shopee.com/index.html>. Acesso em: 13 de mar. de 2022.

TRIBUNAL SUPERIOR ELEITORAL. **Criptografia**. Disponível em: <https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/criptografia> . Acesso em: 28 abr. 2022.

WHATSAPP. **Certificado**. Disponível em: <https://www.whatsapp.com/> . Acesso em: 12 de mar. de 2022.

ANEXO A – Plano de aula

Figura 27 – Plano de aula

PLANO DE AULA

1. IDENTIFICAÇÃO

Professora: Fernanda	**Disciplina:** Eletiva	**Tema:** Criptografia RSA e fatoração numérica.	**Data/Hora:** 02/06 (duas aulas) e 09/06 (duas aulas).

2. PLANO

	OBJETIVOS	CONTEÚDOS	RECURSOS
GERAL	Investigar as implicações da aplicação de uma sequência de ensino utilizando criptografia e fatoração numérica na aprendizagem de estudantes da 1ª série do Ensino Médio.	**Divisibilidade;** **Fatoração numérica;** **Números primos;** **Criptografia RSA.**	• Televisão ou projetor; • Apresentação PowerPoint; • Lousa; • Atividades impressas;
ESPECÍFICOS	Realizar o estudo da criptografia RSA e seu papel na proteção de dados; Analisar a criptografia em elementos presentes no cotidiano dos estudantes e inseri-los em uma sequência didática.		

HABILIDADES	Envolve Habilidade Socioemocional	Qual:
(EF07MA01) Resolver e elaborar situações problema com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmo. (EF06MA06) Resolver e elaborar situações problema que envolvam as ideias de múltiplo e de divisor, reconhecendo os números primos, múltiplos e divisores.	(X) sim ( ) não	• Foco; • Persistência; • Entusiasmo; • Curiosidade para aprender.

Fonte: autor.

Figura 28 – Plano de aula

3. PROCEDIMENTOS

INTRODUÇÃO	DESENVOLVIMENTO	CONCLUSÃO
Levar os estudantes as seguintes reflexões: • Precisamos da proteção dos nossos dados? • O que é criptografia? • Onde encontramos a criptografia? • Por que a criptografia RSA é importante? Qual é seu papel na proteção de dados? • O que é um hacker? É uma profissão? • A urna eletrônica brasileira é segura?	Apresentação de dois vídeos relacionados a proteção de dados: Vídeo: Privacidade – Autógrafo (https://youtu.be/BjeR1wZml-g). Vídeo: Privacidade – Vaga (https://www.youtube.com/watch?v=EMUVPWxLqZc). Atividades com pontuação: formulários, fatorações e finalização do desafio. **Aulas 1 e 2** (grupos de 4 estudantes) Formulário Inicial: • O que você conhece por hacker? • Você sabe o que é hardware e software? • Qual seu conhecimento sobre criptografia? Estudo e discussão do conceito de hacker. Leitura de trechos do texto: Hackers do bem: conheça a profissão que tem salários de até R$ 50 mil - Contratados para identificar vulnerabilidades em sistemas de segurança da informação estão em alta com o aumento das ameaças digitais. Apresentação sobre a Criptografia: • Origem; • Conceito; • Fases: artesanal, mecânica e digital. Apresentação sobre a Criptografia RSA: • Funcionamento; • Certificados digitais sites e plataformas digitais. Realização da fatoração dos números: 60 e 9900; Revisão de conceitos sobre: divisibilidade, fatoração, números primos. Crivo de Eratóstenes. Hackers e criminosos digitais. **Aulas 3 e 4** (grupos de 4 estudantes) Segurança da urna eletrônica brasileira; Eleição com três candidatos fictícios → Competição: 3 urnas, 3 chaves, 3 tabelas pré-codificadas e 3 mensagens → Descobrir o resultado da eleição.	Formulário Final: • Essas atividades te ajudaram com quais conhecimentos? O grupo com maior pontuação recebe uma premiação para cada integrante (caixa de bis) e os demais recebem uma quantidade menor de chocolate devido a participação na atividade.

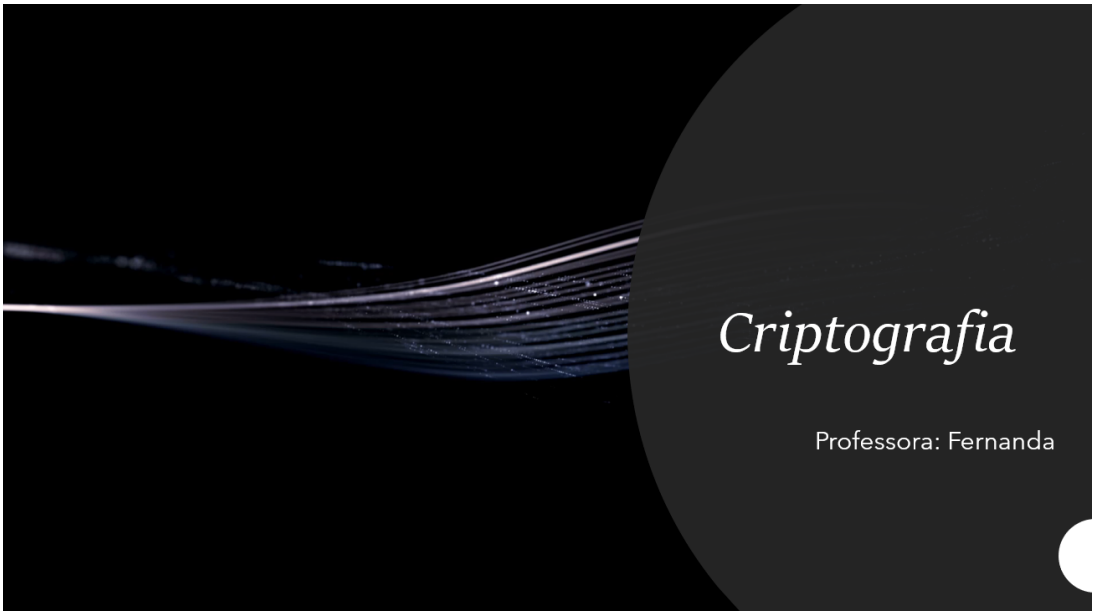
4. AVALIAÇÃO

Pontuação dos grupos, participação e empenho nas atividades.

Fonte: autor.

ANEXO B – Slides das aulas

Figura 29 – Slide 1



Fonte: autor.

Figura 30 – Slide 2

Fonte: autor.

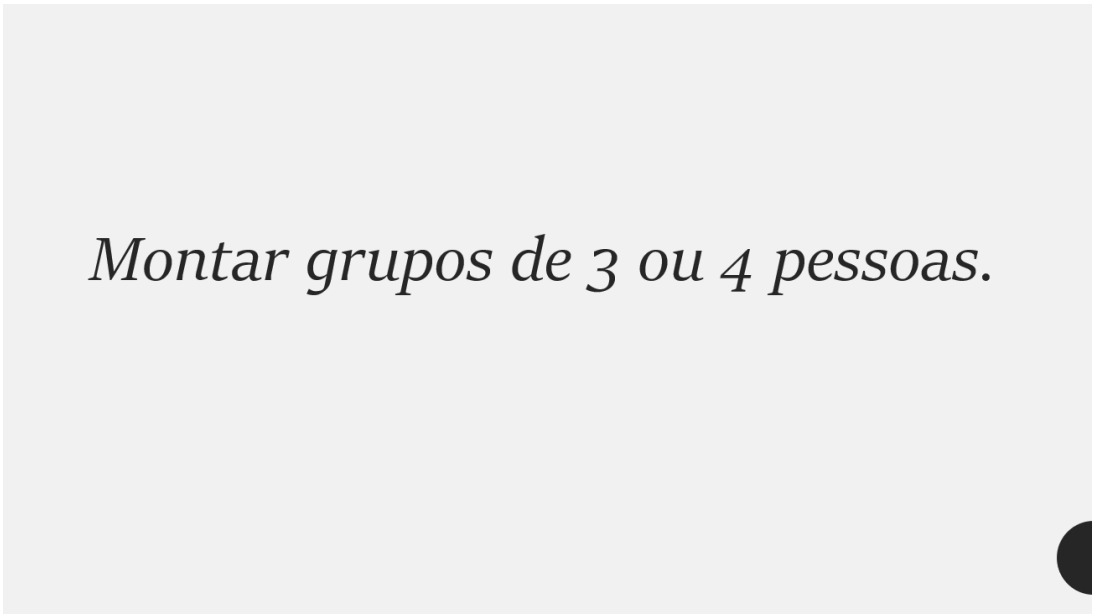
Figura 31 – Slide 3

Fonte: autor.

Figura 32 – Slide 4

Fonte: autor.

Figura 33 – Slide 5



Fonte: autor.

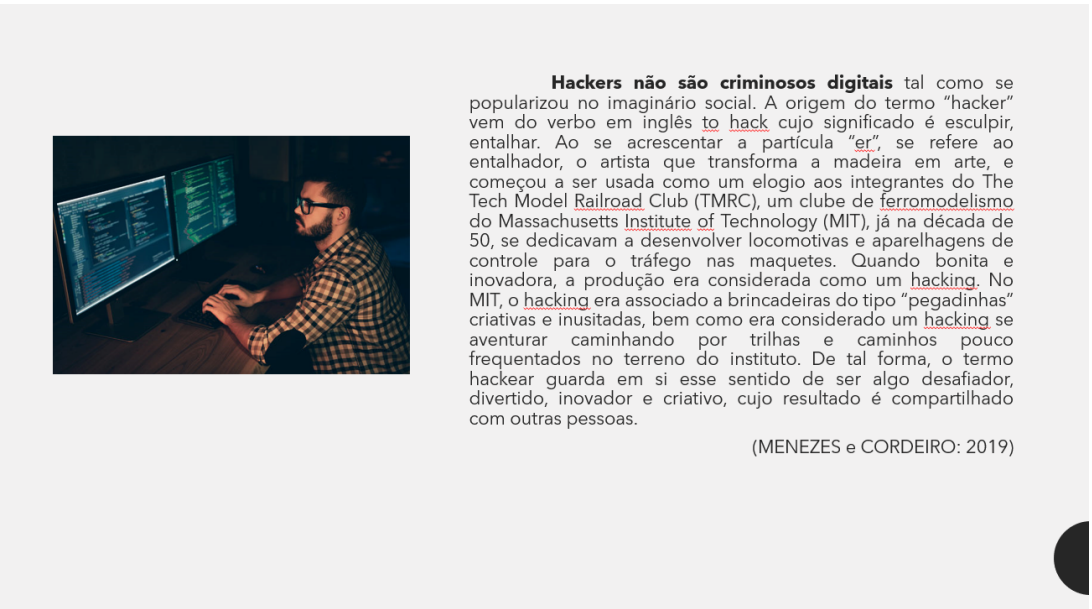
Figura 34 – Slide 6

Fonte: autor.

Figura 35 – Slide 7

Fonte: autor.

Figura 36 – Slide 8



Fonte: autor.

Figura 37 – Slide 9

Texto jornalístico de Bruno Lima, publicado em 30 de novembro de 2021, na revista Forbes - Hackers do bem: conheça a profissão que tem salários de até R$ 50 mil - Contratados para identificar vulnerabilidades em sistemas de segurança da informação estão em alta com o aumento das ameaças digitais.

O número de ciberataques contra empresas cresceu 220% no primeiro semestre de 2021, de acordo com um relatório publicado pelo grupo Mz, empresa especializada em relações com investidores. **Para profissionais de TI, esse cenário soma desafios mas também apresenta oportunidades. Os ethical hackers, também chamados de hackers do bem, contratados pelas organizações para identificar vulnerabilidades em seus sistemas de segurança da informação estão em alta com o aumento desse tipo de crime.** "Percebi que as empresas estão buscando um procedimento chamado Pentest, que é um teste feito na infraestrutura da empresa para identificar falhas de segurança", diz Alessandro Alzani, especialista em cibersegurança que se deu conta dessa demanda via anúncios do LinkedIn.

A remuneração de um profissional da área varia de acordo com seu nível de senioridade, mas mesmo na média é atraente. "**O salário de um profissional certificado em ethical hacking varia entre R$ 7,5 mil e R$ 15 mil. Mas hoje temos profissionais com mais expertise e mais certificações cujo salário pode chegar até R$ 50 mil**", diz Leandro Mainardi, diretor de serviços de segurança cibernética e educação da consultoria de educação ACADI-TI. Segundo o executivo, esses profissionais também podem encontrar colocação fora do Brasil, já que o problema se repete e cresce em todo o mundo.

Quando se fala de C- Level, no entanto, a situação muda um pouco, pois a grande necessidade do mercado está nos profissionais de nível técnico. "Para especialistas, esse é um mercado bem atraente e com bastante possibilidades. Mas, quando falamos de gestores, o número de vagas é um pouco menor."

Os processos de trabalho podem variar de acordo com a organização. Além do já mencionado Pentest, um dos modelos adotados consistem em uma dinâmica divisão de equipes. "Tem o blue team [equipe azul], que é o 'goleiro' que vai defender a infraestrutura. Do outro lado tem a red team [equipe vermelha], que é que vai atacar a infraestrutura", explica Alzani. Toda essa dinâmica tem o objetivo de testar a resiliência da estrutura da empresa, assim como a capacidade defensiva das equipes de TI.

O especialista em cibersegurança Gabriel Castro conta que começou sua trajetória no ethical hacking dentro da equipe azul, mas que não quis parar por aí. Após estudar as dinâmicas de ataque, ele fez uma transição para a equipe vermelha para ter domínio dos dois lados do problema. Quando finalmente voltou ao posto original, o blue team, já tinha mais conhecimento e passou a ocupar um cargo de gestão. "Existe uma carência no mercado de profissionais na equipe azul que também saibam as dinâmicas de ataque", diz Gabriel. **O mercado global de cibersegurança lida com uma escassez de 4 milhões de profissionais de TI, segundo levantamento de 2019 realizado pela associação global de profissionais de cibersegurança ISC.**

O profissional de ethical hacking já deve ter embasamento no tema antes de embarcar nessa especialização. "**Ele precisa entender de sistemas operacionais e de protocolos de comunicação. Esse último é algo que ele precisa conhecer do começo ao fim**", diz Mainardi. Um embasamento teórico específico para a área, que vai ajudar na conquista de uma vaga, exige tempo e investimento. Essa trajetória de estudos muitas vezes é finalizada com algum tipo de certificação que não é obrigatória, mas exigida por grande parte das empresas. **No caso da ACADI-TI, a certificação oferecida é a CEH v11, uma das opções no mercado. Para conquistá-la, o aluno passa por mais de 40 horas de treinamento, além de um exame teórico. O preço dessa etapa atualmente gira em torno de R$ 10 mil.**

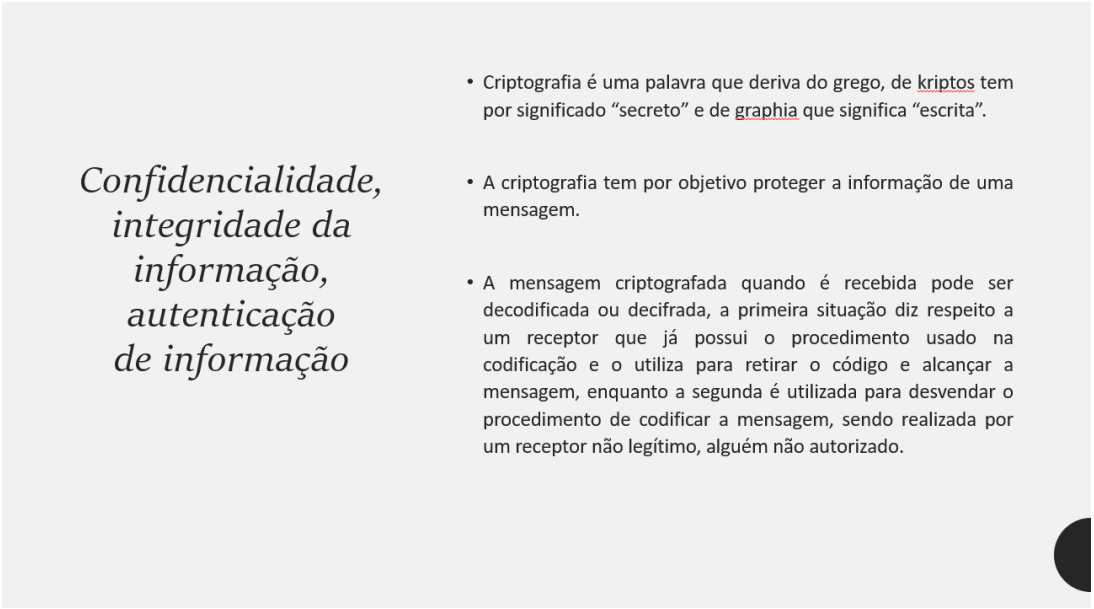
A procura por essa formação vem aumentando, de acordo com o CEO da fintech de crédito estudantil Elleve, André Dratovsky. "Enxergamos o potencial das pessoas, mesmo aquelas de menor poder aquisitivo, que embarcam nessa formação. Sabemos que as chances delas de obter êxito são grandes, assim como as nossas de recuperar esse crédito."

Fonte: autor.

Figura 38 – Slide 10

Fonte: autor.

Figura 39 – Slide 11

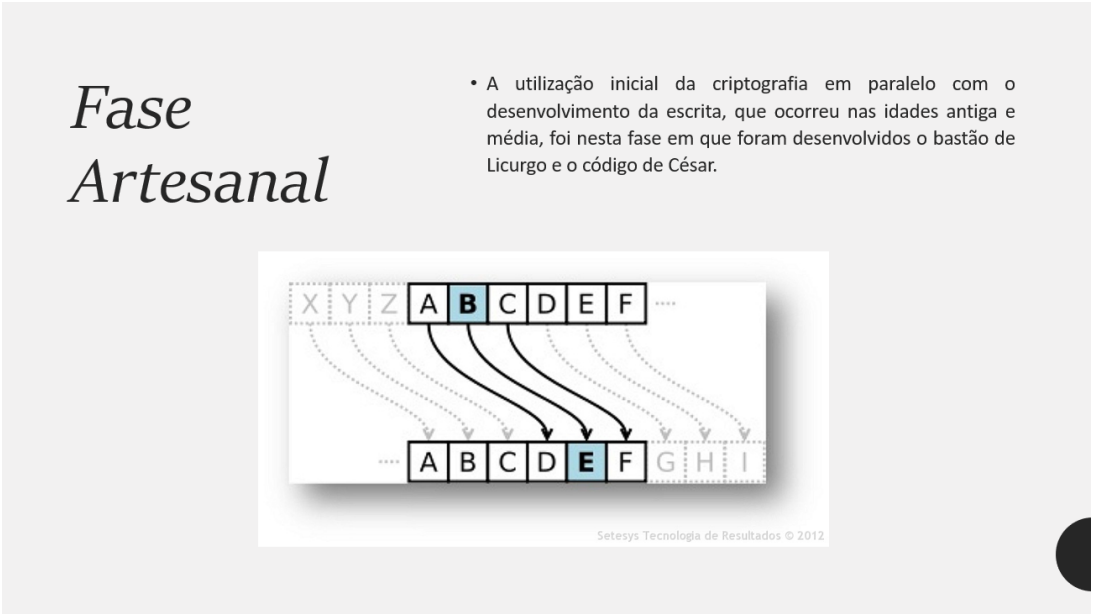


Fonte: autor.

Figura 40 – Slide 12

Fonte: autor.

Figura 41 – Slide 13



Fonte: autor.

Figura 42 – Slide 14

Fonte: autor.

Figura 43 – Slide 15

Fonte: autor.

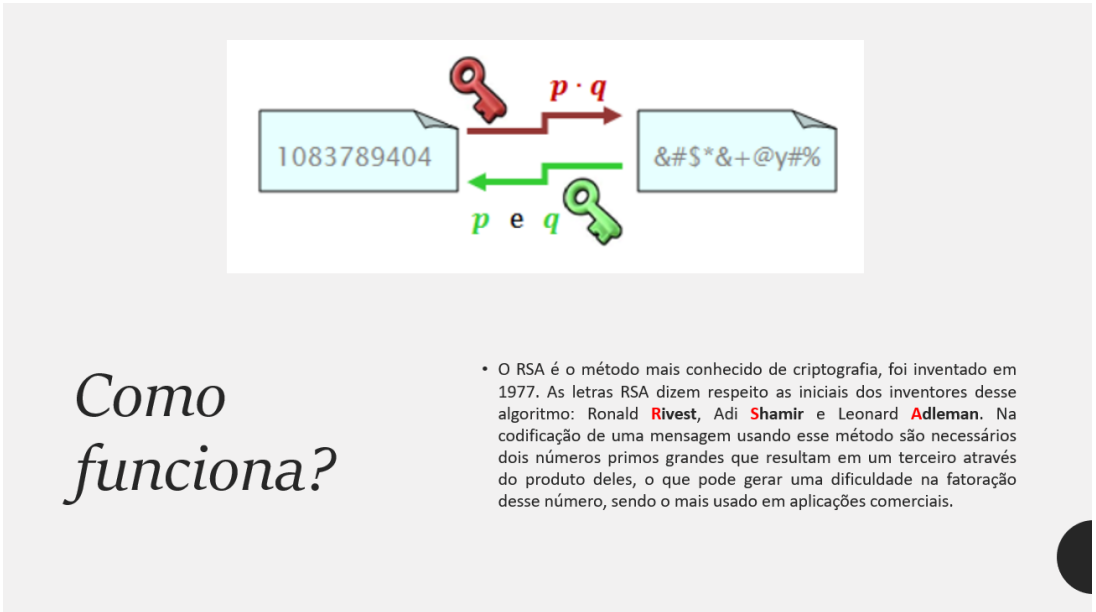
Figura 44 – Slide 16

Fonte: autor.

Figura 45 – Slide 17

Fonte: autor.

Figura 46 – Slide 18

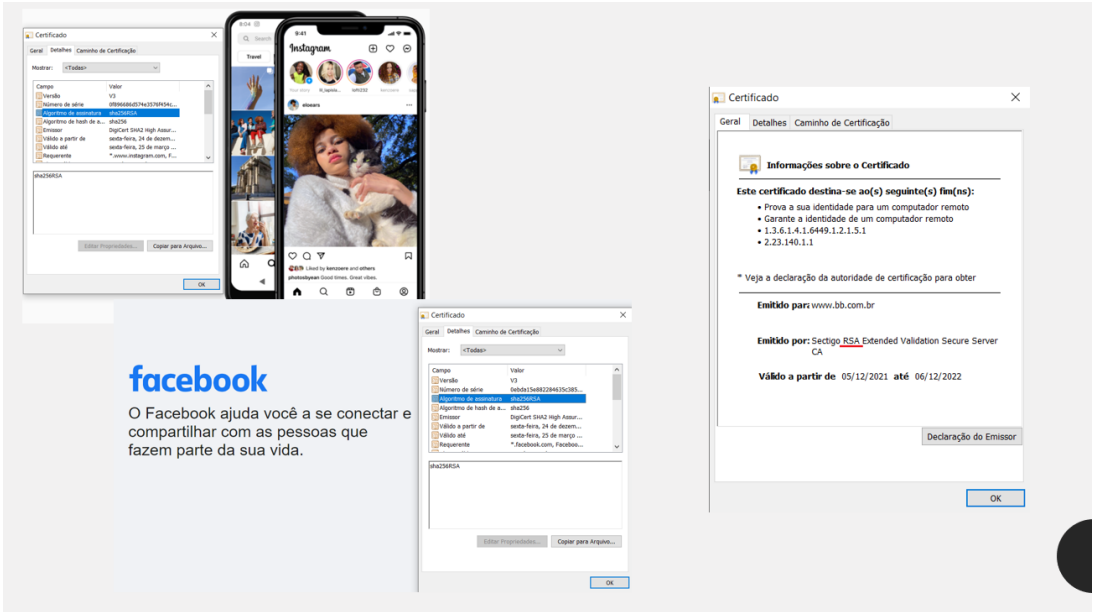


Fonte: autor.

Figura 47 – Slide 19

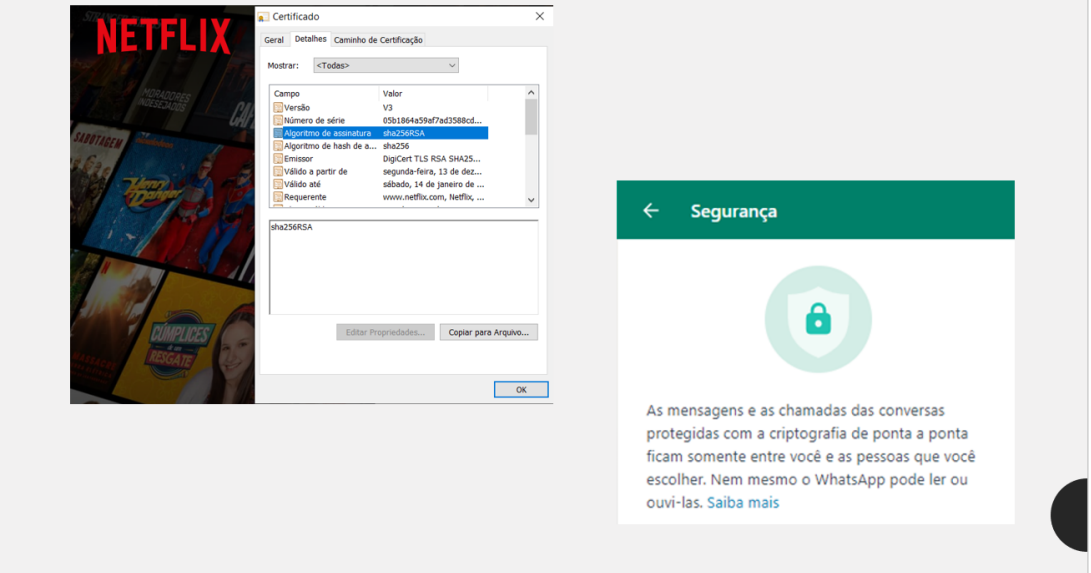
Fonte: autor.

Figura 48 – Slide 20



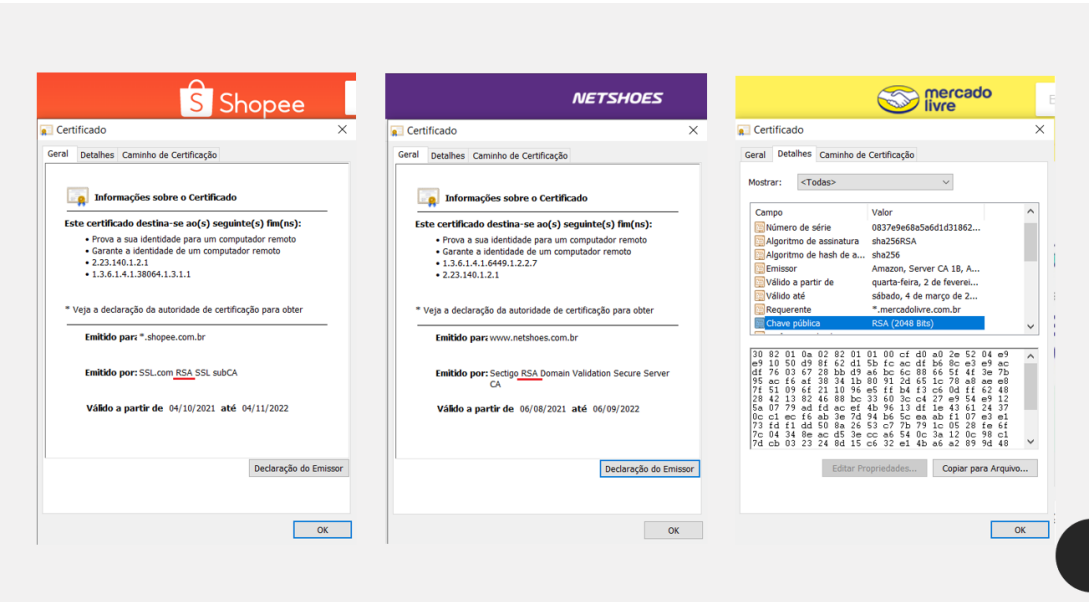
Fonte: autor.

Figura 49 – Slide 21



Fonte: autor.

Figura 50 – Slide 22

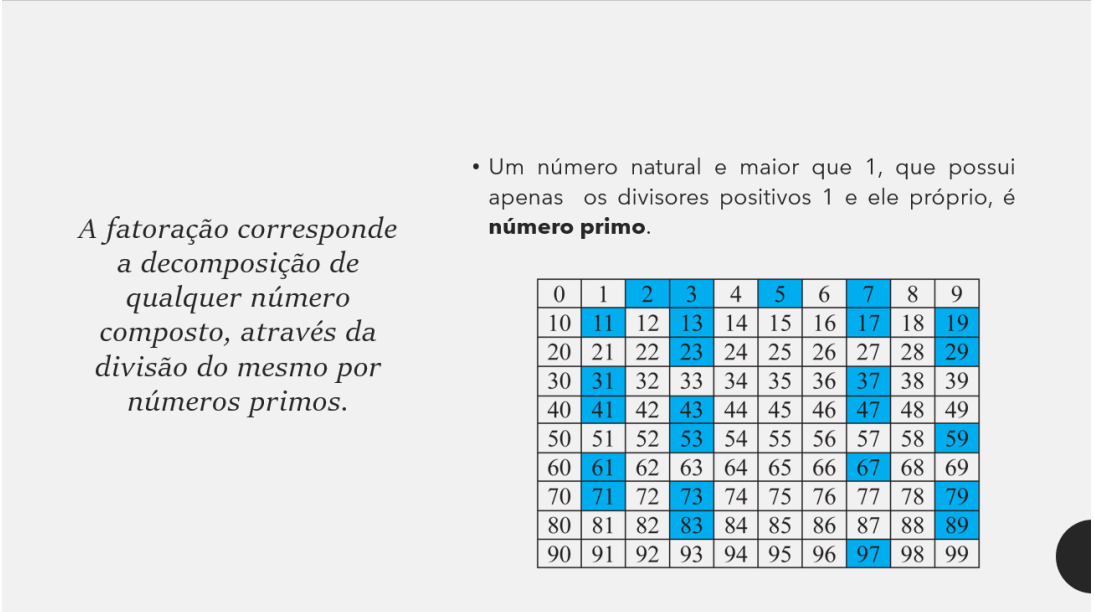


Fonte: autor.

Figura 51 – Slide 23

Fonte: autor.

Figura 52 – Slide 24



Fonte: autor.

Figura 53 – Slide 25

Fonte: autor.

Figura 54 – Slide 26

Fonte: autor.

Figura 55 – Slide 27

Fonte: autor.

Figura 56 – Slide 28

Fonte: autor.

Figura 57 – Slide 29

Fonte: autor.

Figura 58 – Slide 30

Fonte: autor.

Figura 59 – Slide 31

Fonte: autor.

Figura 60 – Slide 32

Fonte: autor.

Figura 61 – Slide 33

Fonte: autor.

Figura 62 – Slide 34

Fonte: autor.

Figura 63 – Slide 35

Um mecanismo de segurança para o funcionamento dos programas computacionais é a criptografia digital, tornando os dados embaralhados e inacessíveis a indivíduos que não são autorizados, o Tribunal Superior Eleitoral utiliza algoritmos de cifração simétrica e assimétrica na urna eletrônica. É criptografado o boletim da urna de maneira segmentada, assinado digitalmente e transmitido. A descriptografia é o processo em que se realiza a recuperação dos dados que foram criptografados, os desembaralhando.

Fonte: autor.

Figura 64 – Slide 36

Tabela de pontuação

ATIVIDADE	PONTUAÇÃO
URNA 1	2 pontos
URNA 2	2 pontos
URNA 3	2 pontos
RESULTADO DAS 3 URNAS	1 ponto
Formulário Final	2 pontos

	DESCONTO NA PONTUAÇÃO
CONSULTA NO CELULAR	2 pontos
CONSULTA NA RESPOSTA DO COLEGA	2 pontos

Fonte: autor.

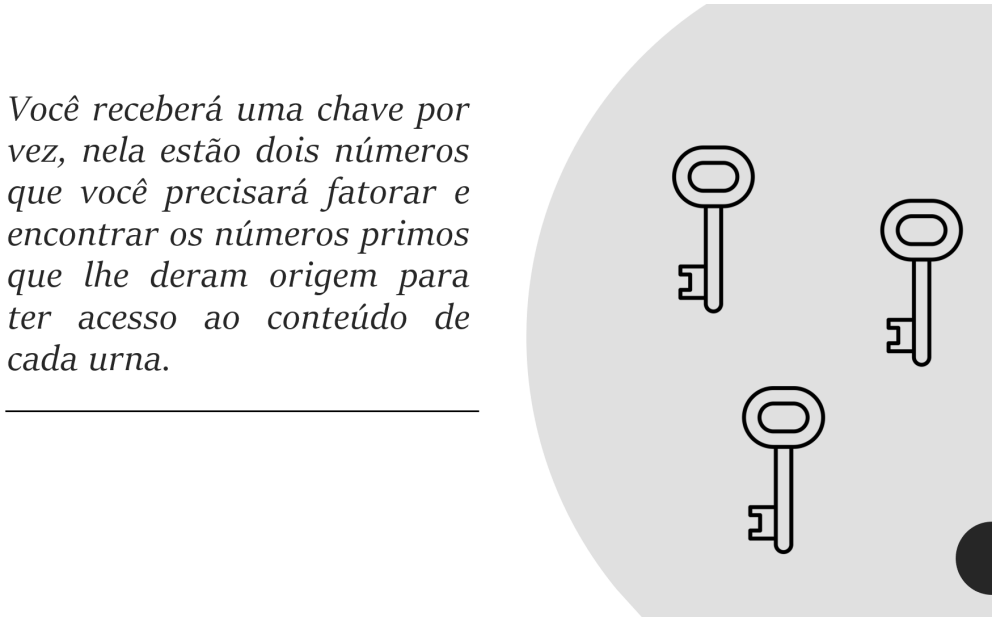
Figura 65 – Slide 37

Fonte: autor.

Figura 66 – Slide 38

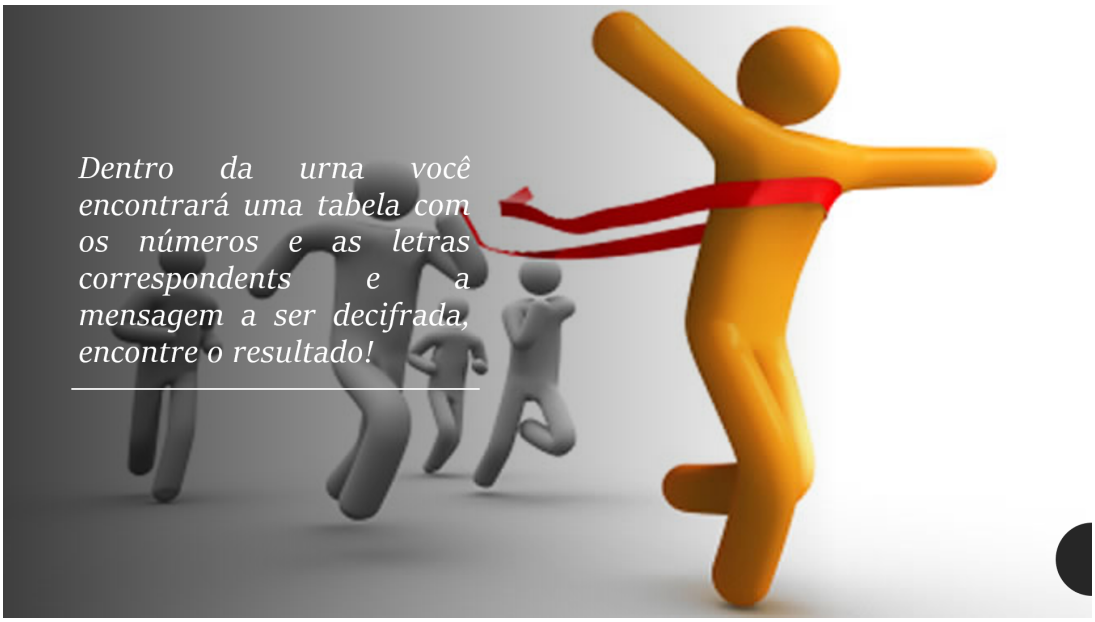
Fonte: autor.

Figura 67 – Slide 39



Fonte: autor.

Figura 68 – Slide 40

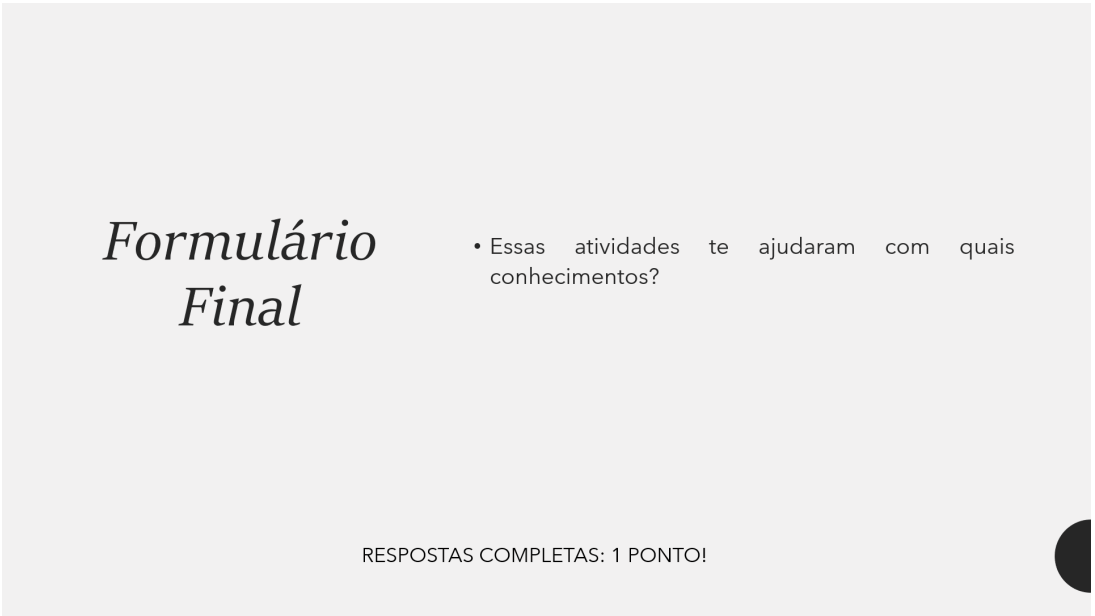


Fonte: autor.

Figura 69 – Slide 41

Fonte: autor.

Figura 70 – Slide 42



Fonte: autor.