UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL – PROFMAT

TÉRCIO RODRIGUES FREIRE

CRIPTOGRAFIA RSA NO ENSINO MÉDIO

UM RECURSO DE MOTIVAÇÃO E APRENDIZAGEM

PALMAS (TO)
2020

TÉRCIO RODRIGUES FREIRE

CRIPTOGRAFIA RSA NO ENSINO MÉDIO

UM RECURSO DE MOTIVAÇÃO E APRENDIZAGEM

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para a obtenção do título de Mestre - Área de Concentração: Matemática.
Orientadora: Prof^a. Dr^a. Hellena Christina Fernandes Apolinário.

PALMAS (TO)

2020

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

F866c Freire, Tércio Rodrigues.

Criptografia RSA no Ensino Médio: um recurso de motivação e aprendizagem . / Tércio Rodrigues Freire. – Palmas, TO, 2020.

101 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2020.

Orientadora : Hellena Christina Fernandes Apolinário

1. Matemática. 2. Criptografia RSA. 3. Ensino e aprendizagem. 4. Sequência didática. I. Título

CDD 510

Elaborado pelo sistema de geração automatica de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

TÉRCIO RODRIGUES FREIRE

CRIPTOGRAFIA RSA NO ENSINO MÉDIO - UM RECURSO DE MOTIVAÇÃO E APRENDIZAGEM

Trabalho de Conclusão de Curso apresentado ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para obtenção do título de Mestre – Área de Concentração: Matemática. Orientadora: Dra. Hellena Christina Fernandes Apolinário.

Aprovada em 28 / 08 / 2020

BANCA EXAMINADORA

Hellena Christina F. Apolinário

Prof. Dra. Hellena Christina Fernandes Apolinário (UFT)

Rogério Azevedo Rocha

Prof. Dr. Rogério Azevedo Rocha (UFT)

José Elias dos Santos

Prof. Dr. José Elias dos Santos Filho (UFPB)

AGRADECIMENTOS

Agradeço a Deus por todas as bênçãos e ao apoio fundamental da minha família e amigos, em especial da minha amada esposa Alexsandra Carlos Souza.

Lembrar também de agradecer a Sociedade Brasileira de Matemática (SBM) pela coordenação deste importante programa de mestrado e aos professores desse programa que trabalham na Universidade Federal do Tocantins (UFT).

Importante salientar a grande contribuição da Prof^a. Dr^a. Hellena Christina Fernandes Apolinário, por ter dedicado o seu tempo para contribuir na elaboração dessa dissertação e consequentemente no meu crescimento pessoal e profissional.

Comprimento aos meus colegas e amigos de curso pelos memoráveis momentos vivenciados nesses anos de aperfeiçoamento.

E por fim, agradeço a você leitor e espero que sua leitura seja agradável e que essa dissertação possa contribuir de alguma forma com a sua busca.

RESUMO

A desmotivação dos educandos da última série do Ensino Médio, após realizarem as avaliações de seleção para cursos de graduação, é vivenciada em muitas escolas brasileiras. Devido a este fato, essa dissertação buscou criar uma sequência didática que estimulasse o educando em sua aprendizagem. Atualmente vivenciamos uma evolução tecnológica nas nossas relações com o mundo e com isso houve o aumento na busca de segurança dos dados e informações trocados na Internet. Essa dissertação tem como tema a Criptografia RSA (Rivest-Shamir-Adleman) e o objetivo de investigar e trabalhar os elementos matemáticos necessários no desenvolvimento dos algoritmos da Criptografia RSA, com o objetivo de instigar a curiosidade e o interesse dos educandos em estudar Matemática. Foram planejadas oito intervenções didáticas para a apresentação do tema e o desenvolvimento dos algoritmos de codificar e decodificar mensagens. Os resultados da análise das intervenções apontaram que os educandos tiveram interesse no tema e no desenvolvimento dos algoritmos e conseguiram realizar as atividades propostas, de codificar e decodificar mensagens, com êxito. Concluímos que essa sequência didática estimulou o interesse dos educandos nas aulas de Matemática e proporcionou momentos de estudos matemáticos que potencializou o Ensino e Aprendizagem em sala de aula.

Palavras-chave: Matemática. Criptografia RSA. Ensino e aprendizagem.

ABSTRACT

The demotivation of students in the last grade of high school, after carrying out the selection evaluations for undergraduate courses, is experienced in many Brazilian schools. Due to this fact, this dissertation sought to create a didactic sequence that would stimulate the student in his learning. We are currently experiencing a technological evolution in our relations with the world and, going on this way, there has been an increase in the search for security of data and information exchanged on the Internet. This dissertation has as its theme RSA Cryptography (Rivest-Shamir-Adleman) and the objective of investigating and working on the mathematical elements, which are necessary in the development of RSA Cryptography algorithms, in order to instigate the curiosity and interest of students in going deeper into Mathematics. Eight didactic interventions were planned for the presentation of the theme and the development of algorithms for encoding and decoding messages. The results of the analysis of the interventions pointed out that the students were interested in the theme and in the development of the algorithms and were able to successfully carry out the proposed activities (about encoding and decoding messages). We conclude that this didactic sequence stimulated the students' interest in Mathematics classes and provided moments of mathematical studies that potentiated Teaching and Learning in the classroom.

Keywords: Mathematics. Cryptography RSA. Teaching and learning.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Comumente as avaliações de seleção para cursos do Ensino Superior são realizadas no último bimestre do ano. Esse fato influencia diretamente no rendimento escolar dos educandos de turmas do 3º ano do Ensino Médio, pois eles começam a apresentar perda de interesse em acompanhar as aulas do restante desse último bimestre escolar.

Baseando em experiências profissionais de trabalhos com turmas do 3º ano do Ensino Médio, sentiu-se a necessidade de desenvolver uma Sequência Didática nessas turmas que estimule a curiosidade e o interesse dos educandos no desenvolvimento das aulas de Matemática no final do ano letivo. Assim o público alvo escolhido para o desenvolvimento dessa dissertação são os educandos de três turmas do 3º ano do Ensino Médio, da escola Centro de Ensino Frei Gil, localizado no município de Estreito no estado do Maranhão.

Com base na dificuldade exposta, essa dissertação apresenta uma proposta de intervenção didática com o tema Criptografia RSA (esse método recebeu esse nome devido a seus criadores R. L. Rivest, A. Shamir e L. Adleman), objetivando a motivação dos educandos no estudo de conteúdos matemáticos. O tema escolhido se deu pela sua importância em situações cotidianas que envolvem a segurança na transmissão de dados e informações pela Internet, e com isso, possivelmente, os educandos se identificarão com o tema e apresentarão maior interesse no final do ano letivo.

Atualmente a Criptografia RSA é uma ferramenta de segurança amplamente adotada no cotidiano, pelo motivo de estarmos vivenciando uma evolução tecnológica jamais vista anteriormente. Com tal evolução surgem diversos meios de trocas de dados e informações e com isso se dá a preocupação pela busca de segurança nessas transações.

Nos algoritmos de codificação e decodificação da Criptografia RSA, são necessários conhecimentos prévios a respeito de alguns conteúdos matemáticos básicos. Tais como números primos, multiplicação de números inteiros, potenciação, algoritmo da divisão, entre outros.

Existem diversos autores, como Silva (2019a), Silva (2019b), Machado (2018), entre outros, que discorrem a respeito dos algoritmos da Criptografia RSA em suas dissertações do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT).

A dissertação da Silva (2019a) discorre a respeito de diversos conceitos matemáticos envolvidos nos algoritmos da Criptografia RSA, mas desenvolveu uma atividade, voltada aos educandos do 2º ano do Ensino Médio, que introduz a noção de Criptografia utilizando o conceito matemático de matriz.

A dissertação do Silva (2019b) discorre a respeito dos conceitos matemáticos de Frações Contínuas e sua ligação com a Criptografia RSA. No entanto não desenvolve nenhuma intervenção escolar.

A dissertação do Machado (2018) criou um minicurso, para educandos voluntários do 8^o e 9^o ano do Ensino Fundamental, trabalhando conceitos matemáticos necessários para a compreensão dos algoritmos da Criptografia RSA.

Esses autores abordam em suas dissertações os algoritmos da Criptografia RSA por meio do conteúdo de Congruência, que é um conteúdo matemático trabalhado apenas em alguns cursos de graduação e pós-graduação, como no Programa de Mestrado Profissional em Matemática em Rede Nacional, ofertado na Universidade Federal do Tocantins, na disciplina de Aritmética.

Diante do exposto, decidiu-se desenvolver esta dissertação visando à criação de uma Sequência Didática, voltada para turmas do Ensino Médio, com o tema Criptografia RSA e que utilize os conceitos matemáticos do Ensino Básico no seu desenvolvimento. Tendo como objetivo desenvolver os algoritmos desse método criptográfico, buscando a motivação dos educandos e potencializar a compreensão dos conteúdos matemáticos básicos envolvidos.

Buscaremos realizar um estudo histórico a respeito da evolução dos métodos criptográficos, além do estudo dos conceitos matemáticos básicos essenciais para o desenvolvimento da Criptografia RSA e o estudo de seus algoritmos.

Ao propor uma intervenção que aborda um tema presente no cotidiano dos educandos, como a Criptografia, estimula-se a curiosidade e o interesse dos educandos no estudo de conteúdos matemáticos básicos envolvidos no desenvolvimento da Criptografia RSA.

Esta dissertação está dividida em cinco capítulos. No Capítulo 1 é apresentado um breve histórico da evolução da Criptografia até os dias atuais. No Capítulo 2 são apresentados os conceitos matemáticos básicos necessários para o desenvolvimento dos algoritmos de codificar e decodificar da Criptografia RSA. No Capítulo 3 são apresentados os algoritmos da Criptografia RSA seguido de exemplos. No Capítulo 4 apresentaremos a nossa proposta de Sequência Didática. E finalmente, no Capítulo 5 exporemos as nossas considerações finais a respeito da elaboração e execução da Sequência Didática.

1 CRIPTOGRAFIA

Neste capítulo será apresentado o contexto histórico da criptografia. Dos primeiros relatos de uso de técnicas para criptografar, passando por momentos onde a criptografia teve grande importância na história da humanidade, como seu uso durante a Segunda Guerra Mundial, até chegar aos códigos criptográficos dos dias atuais.

Discorre também a respeito da Criptografia RSA, que é o código mais utilizado nos dias atuais e apresentará por quais motivos isso ocorre, assim como seu algoritmo para codificar e decodificar mensagem.

Tomou como base Bezerra, Malagutti e Rodrigues (2010), Bonfim (2017),Cavalcante (2005), Coutinho (2014), entre outros autores.

1.1 Evolução histórica da Criptografia

Na evolução humana, sempre houve uma busca por meios eficazes para se comunicar. Com isso também surgiu à necessidade de criar uma comunicação onde apenas o interlocutor e o receptor conseguiriam compreender o conteúdo da mensagem. E é a partir dessa necessidade que é desenvolvida o conceito de Criptografia, também chamada de linguagem de códigos.

Segundo a autora Bonfim (2017, p. 50), “Os indícios são que a criptografia começou a ser usada no antigo Egito quando o faraó Amenemhet II governava, por volta de 1900 a.C”. A Criptografia teria sido usada pelo arquiteto Khnumhotep II, com o intuito de dificultar que ladrões encontrassem os tesouros do faraó, realizando trocas de palavras importantes por símbolos nos documentos que indicavam a localização de tesouros.

Desse tempo até os tempos atuais, a linguagem de códigos sempre esteve em constantes transformações, que ainda ocorrem, na busca de aprimorar os métodos de codificação. É possível notar na história humana que a criptografia sempre foi usada como recurso militar, político, comerciais, guerras e até mesmo em motivos sentimentais (SINGH, 2005).

A codificação com o Scytale (bastão, em grego) ou Cítala Espartana, é considerada por alguns autores, como Bonfim (2017), o primeiro aparelho criptográfico militar, com sua utilização no século V a.C.

Consiste em enrolar uma faixa de couro (cítala) em um bastão de madeira, de determinado formato e largura, e escrever a mensagem nessa faixa. Então a cítala é enviada ao destinatário de

forma disfarçada, como por exemplo, um cinto para segurar a calça. Ao chegar ao destinatário, a faixa de couro deve ser enrolada em um bastão de mesmo formato e largura, conforme Figura 1, para que a mensagem possa ser lida corretamente (OLGIN, 2011).

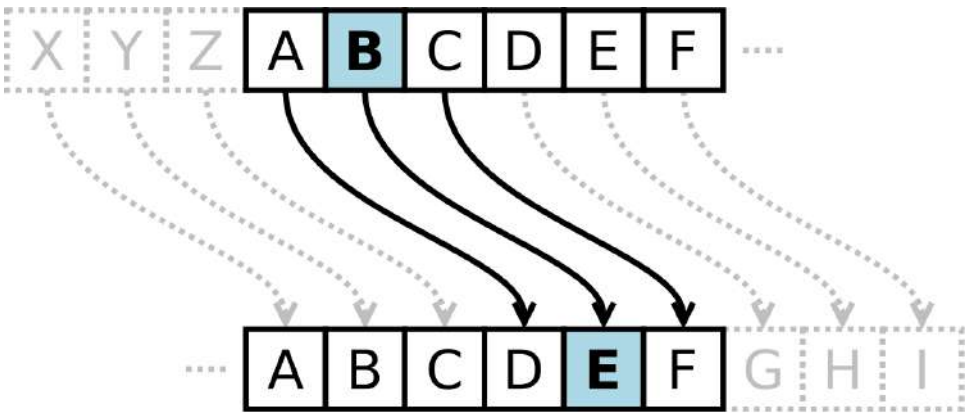
Figura 1 – A Cítala Espartana.

Fonte: http://cryptograma.blogspot.com.br/2015/06/historia-da-criptografia-cifras-e.html (Acesso em: 05 out. 2019).

Essa codificação também é conhecida como Bastão de Licurgo ou cifra de transposição, que pode ser aplicada com uma função bijetiva para codificar e a sua inversa para decodificar mensagens, como foi realizado na dissertação de mestrado do Moura (2019).

Uma cifra bastante conhecida pela sua importância histórica, foi utilizada pelo ditador da República Romana, de 49 a.C. a 44 a.C., Caio Júlio César. Essa cifra consiste em trocar cada letra da mensagem original pela terceira letra que a segue no alfabeto, fazendo assim com que as pessoas que não conhecessem essa cifra não conseguissem entender o significado da mensagem enviada, normalmente para seus exércitos que se encontravam na linha de frente da batalha.

Figura 2 – Relação alfabética da Cifra de César.



Fonte:http://setesys.com.br/blog/como-produzir-senhas-criativas-utilizando-a-cifra-de-cesar (Acesso em: 05 out. 2019).

Júlio César utilizava o alfabeto original para escrever suas mensagens e as codificavam utilizando o alfabeto cifrado para serem enviadas aos seus exércitos que estavam em linha

de batalha. Esse método de criptografia até hoje é conhecido como Cifra de César. Métodos semelhantes a esse são chamados de monoalfabéticas, pois realizam a substituição de uma letra por outra ou por um símbolo que constam em um determinado alfabeto cifrado.

Como o método de criptografia monoalfabética era muito simples de se decifrar por intermediários, tomando como base a análise das frequências que cada letra aparece no texto, surgiu então a necessidade de criar métodos criptográficos novos, com maior elaboração e dificuldades para serem decifrados.

No ano de 1466, o italiano Leon Battista Alberti publicou o livro Modes scribendi in ziferas, onde discorre a respeito do Disco de Cifras, que é considerado o primeiro sistema poli alfabético conhecido. Conforme Kahn (1996), Alberti é conhecido como o pai da cifra poli alfabética.

O Disco de Cifras de Alberti é composto por dois discos de diâmetros distintos que são montados de forma concêntrica. Um disco é móvel e outro fixo. O disco externo é fixo, com vinte e quatro casas contendo vinte letras latinas escritas em ordem alfabética e em maiúsculo (incluindo o Z, com U = V e excluindo H, J, K, W, Y) e os números 1, 2, 3 e 4 também escritos em ordem. O disco interno é móvel, possui vinte e quatro letras latinas escritas sem ordenação e em minúsculo.

Figura 3 – O Disco de Cifras.

Fonte: http://www.mateureka.it/wp-content/uploads/2012/11/disco-cifrante-leon-battista-alberti.jpg (Acesso em: 05 out. 2019).

É importante a escrita das letras minúscula, do disco interno, de forma desordenada, pois se estivessem em ordem essa cifra seria uma generalização da Cifra de César. E com isso esse

disco permite realizar a mudança de cifra de forma fácil e rápida, bastando girar o disco móvel em torno de seu eixo para obter uma cifra diferente.

Uma das dificuldades para a utilização do Disco de Cifras é que o emissor e o receptor da mensagem devem ter os discos iguais e bem guardados, pois quem tiver acesso ao disco utilizado consegue facilmente compreender a mensagem transmitida.

No ano de 1553, segundo Kahn (1996), foi descrita a cifra conhecida como Cifra de Vigenère, no livro La cifra del Sig Giovan Batista Belaso escrito pelo italiano Giovanni Battista Belaso. Essa cifra recebe esse nome, pois sua criação é atribuída erroneamente ao francês Blaise Vigenère. Seu sistema consiste na utilização de vinte e seis Cifras de César colocadas em uma tabela, como na figura abaixo.

Figura 4 – Sistema da Cifra de Vigenère.

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

Fonte: http://cryptograma.blogspot.com.br/2015/06/historia-da-criptografia-cifras-e.html (Acesso em: 05 out. 2019).

Para realizar a codificação com a Cifra de Vigenère, primeiramente é preciso escolher uma palavra chave e repetir esta palavra até completar a quantidade de letras da mensagem a ser enviada. Veja um exemplo com a palavra chave "Lua" e a mensagem a ser codificada "Bela noite", observe a tabela abaixo.

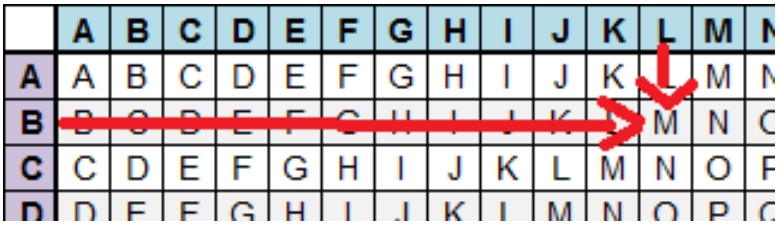
Tabela 1 – Exemplo da codificação com a Cifra de Vigenère.

Palavra chave	L	U	A	L	-	U	A	L	U	A
Mensagem	B	E	L	A	-	N	O	I	T	E
Texto criptografado	M	Y	L	L	-	H	O	T	X	E

Fonte: Elaborada pelo autor.

Agora ao utilizar a Cifra de Vigenère, identifique cada letra do texto criptografado considerando o encontro da coluna da letra da palavra chave com a linha da letra da mensagem. No exemplo acima, a primeira letra do texto criptografado "M" foi encontrada olhando para o encontro da coluna da primeira letra da palavra chave "L" com a linha da primeira letra da mensagem "B".

Figura 5 – Como encontrar a cifra usando o sistema da Cifra de Vigenère.



Fonte: Produzida pelo autor.

Passando para a segunda letra "Y" do texto criptografado, observe o encontro da coluna da segunda letra da palavra chave "U" com a linha da segunda letra da palavra da mensagem "E". E assim sucessivamente até criptografar todas as letras da mensagem.

Dessa época em diante a criptografia teve uma evolução contínua devido à evolução tecnológica no mundo. No entanto uma máquina criada com o objetivo de criptografar mensagens foi criada apenas durante a Segunda Guerra Mundial.

A primeira máquina eletromecânica de criptografia foi denominada Enigma. Ela foi criada pelo engenheiro alemão Arthur Scherbius, por volta de 1918 e tinha a aparência de uma máquina de escrever. Para decodificar uma mensagem criada pela máquina Enigma, o receptor precisaria também ter uma Enigma e uma cópia do livro de códigos que contém o ajuste inicial dos misturadores que eram trocados diariamente para manter a segurança da codificação.

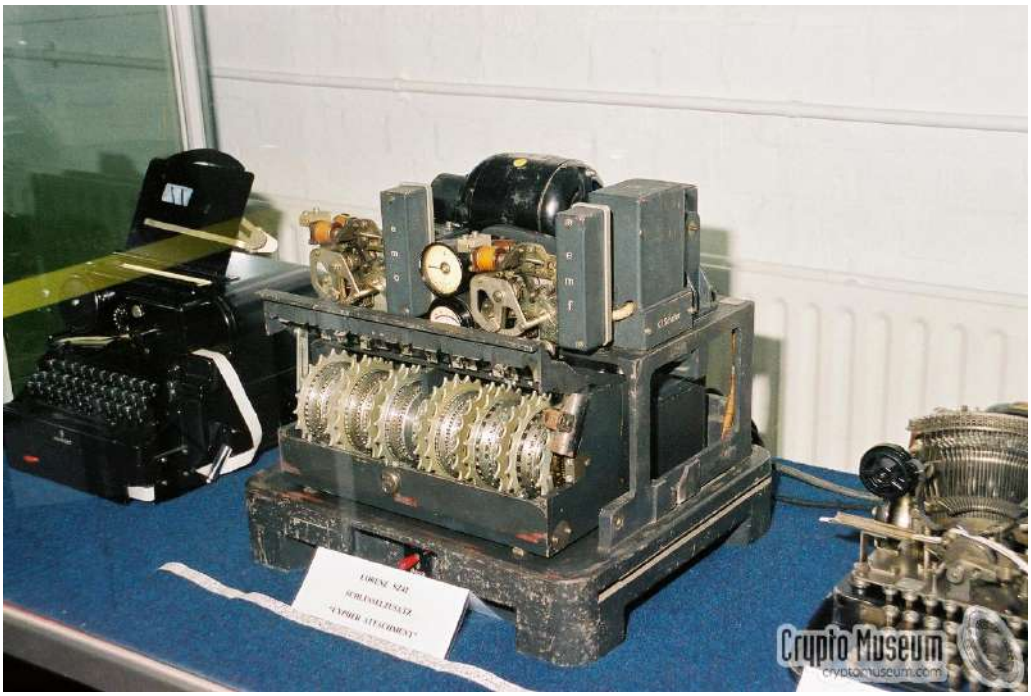
Figura 6 – A máquina Enigma.

Fonte: http://horizontes.sbc.org.br/wp-content/uploads/2016/11/enigma-300x234.jpeg (Acesso em: 05 out. 2019).

Os militares alemães foram aperfeiçoando ainda mais a Enigma, a partir do ano de 1930, usando uma combinação maior de rotores e ligações elétricas. Isso fez com que as mensagens do exército alemão, apesar de serem facilmente interceptadas, fossem indecifráveis e assim proporcionando vantagens táticas aos alemães durante a Segunda Guerra Mundial.

Outra máquina criptográfica utilizada pelos militares alemães foi denominada Lorenz SZ 40/42, criada e usada por eles durante a Segunda Guerra Mundial. Essa foi uma evolução da máquina Enigma, aumentando ainda mais a segurança das mensagens transmitidas do exército alemão.

Figura 7 – A máquina Lorenz SZ 40/42.

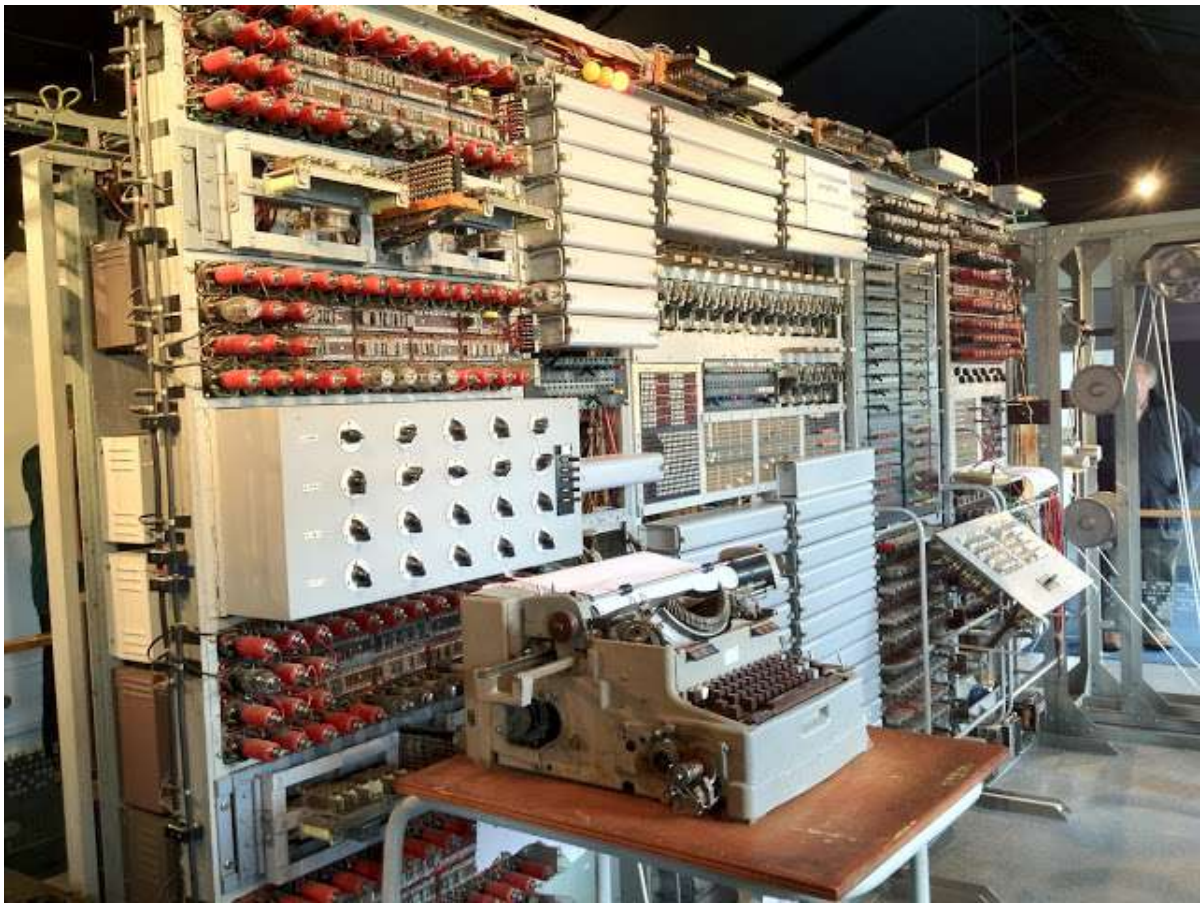


Fonte: https://www.cryptomuseum.com/crypto/lorenz/sz40/img/301491/000/full.jpg (Acesso em: 05 out. 2019).

Por causa de sua maior complexidade e tamanho, as máquinas Lorenz eram guardadas pelos alemães em seus lugares mais seguros. Tanta segurança em torno dessas máquinas que os criptógrafos britânicos conseguiram decodificar as mensagens criadas pela Lorenz sem nem mesmo terem se quer visto uma dessas máquinas antes.

No ano de 1943, foi projetada a máquina Colossus, pela equipe do engenheiro elétrico inglês Tommy Flowers. Foi usada para decodificar os códigos criados pela Lorenz. A Colossus possuía mais de 1700 válvulas e é conhecida como o primeiro computador eletrônico programável da história.

Figura 8 – A máquina Colossus.



Fonte: http://www.tipografos.net/internet/Colossus2.JPG (Acesso em: 05 out. 2019).

A máquina Colossus é considerada como um marco para o início da era moderna da criptografia, onde os computadores começam a apresentarem programações com chaves de codificações mais complexas do que as utilizada pelas máquinas desse tempo, como a Lorenz e Enigma.

1.2 A Criptografia na atualidade

É comum encontrar a palavra Criptografia em nosso cotidiano. Isso se dá por conta da evolução tecnológica que é vivenciada atualmente, por exemplo, hoje é possível enviar e receber mensagens particulares em instantes, no entanto o que garante sua privacidade é a Criptografia que o meio de comunicação utiliza para realizar essa troca de mensagens.

Um aplicativo de comunicação muito utilizado atualmente é o WhatsApp e ele utiliza o que chamam de criptografia de ponta-a-ponta. Segundo o site desse aplicativo, é assegurado aos usuários que somente quem envia e quem recebe a mensagem consiga ler, nem mesmo o WhatsApp pode ler a mensagem.

Outro exemplo da evolução tecnológica vivenciada atualmente são os aplicativos bancários. É possível um cliente do Banco do Brasil ou Caixa Econômica Federal, entre outros, realizar diversas operações bancárias utilizando um smartphone cadastrado. Para que isso aconteça, os aplicativos dos bancos necessitam de uma Criptografia que proporcione segurança aos clientes para digitarem suas senhas bancárias.

Além dos dois exemplos citados acima, é possível listar mais uma infinidade de situações cotidianas que hoje se faz necessária a utilização da Criptografia. Assim temos que sua importância na atualidade é indiscutível, pois a Criptografia:

> [...] é utilizada para proteger informações e manter o sigilo de dados confidenciais. A criptografia utiliza métodos para a produção e distribuição segura de chaves e estuda algoritmos que permitem transformar mensagens claras em formas de comunicação só inteligíveis pelos emissores e pelos receptores envolvidos no processo (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 5).

Assim compreende-se que a Criptografia é a ciência que emprega as formas de se escrever uma mensagem em código, objetivando uma comunicação segura e sem interferências, ou seja, resume-se em um conjunto de técnicas para permitir tornar enigmática uma mensagem de forma que apenas o destinatário a decifre e compreenda o conteúdo da mensagem claramente.

Para o processo de tornar uma mensagem incompreensível, é criada de modo confidencial uma chave de segurança. Tal chave é a base para que uma mensagem seja corretamente codificada e futuramente decodificada pelo destinatário.

A Criptografia Digital, ao qual é vivenciada atualmente, se desenvolveu juntamente com a evolução tecnológica nos últimos anos. Com o aperfeiçoamento dos computadores, conseguindo realizar cálculos cada vez maiores e em menor tempo, contribuiu na criação de códigos mais

complicados de serem quebrados, mas por outro lado, também contribuiu para a criação de métodos de decodificação mais eficazes.

O sistema de codificação mais usado atualmente é denominado Criptografia RSA. Recebe esse nome devido às letras iniciais dos nomes dos criadores desse código, R. L. Rivest, A. Shamir e L. Adleman. Esse código é utilizado amplamente hoje para a transmissão segura de dados e informações via internet e será apresentado mais a respeito desse método na próxima seção.

1.3 A Criptografia RSA

Esse código criptográfico foi um dos primeiros, da criptografia moderna, a utilizar uma chave pública e é considerado um dos códigos mais seguros do mercado atualmente e por essa razão é utilizado na segurança das assinaturas digitais, como as de banco, e-mails, entre outros, tão comuns nos dias atuais.

A respeito do código da Criptografia RSA tem-se que:

> Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais (COUTINHO, 2014, p. 3).

Elucidando o seu uso atualmente, esse método de codificação é empregado em diversas operações do cotidiano, como compra online, operações bancárias, envio de e-mails, entre outras diversas atividades que envolvem o uso de internet.

A criptografia RSA funciona da seguinte maneira: são criadas duas chaves diferentes, uma pública e outra privada (que apenas quem irá decodificar o código pode saber). A chave pública é utilizada para codificar as informações enquanto a chave privada se utiliza para decodificar as informações.

A segurança desse código criptográfico se encontra na dificuldade de fatoração de um número muito grande, denominado semiprimo, o qual é resultado da multiplicação de dois números primos tão grandes quantos se queiram. Tem-se que:

> Segundo pesquisadores, a fatoração de um número de 200 dígitos requer 4 milhões de anos para ser processada. Fatorar um número de 500 dígitos exige 10^{25} anos. Mesmo que os computadores se tornem mais velozes, muito tempo irá passar até que seja possível fatorar um número de 500 dígitos, e até lá poderão escolher a fatoração de um número ainda maior (CAVALCANTE, 2005, p. 4).

Por conta dessa segurança que a Criptografia RSA transmite aos usuários, é que motiva seu uso em nosso dia a dia e que também motivou o tema de pesquisa dessa dissertação.

O próximo capítulo apresentará os conteúdos matemáticos básicos que são necessários para a codificação e decodificação de palavras e frases da linguagem formal para a linguagem de códigos utilizando a Criptografia RSA.

2 CONCEITOS MATEMÁTICOS DO ALGORITMO DA CRIPTOGRAFIA RSA

Neste capítulo serão abordados os conteúdos matemáticos necessários para compreender a parte aritmética do algoritmo da codificação e decodificação de mensagens utilizando a Criptografia RSA. Os algoritmos da Criptografia RSA utilizam o resto natural da divisão entre dois números naturais, algo que é estudado com maior aprofundamento teórico em alguns cursos de graduação, como no de Matemática, e em disciplinas como Teoria dos Números.

Essa parte da dissertação discorre a respeito dos conteúdos de Números Primos, Divisibilidade, Divisão Euclidiana, Potências e Congruência, este último citado é um conteúdo matemático trabalhado no Ensino Superior, no entanto os demais são conteúdos trabalhados no Ensino Básico, onde se encontra o público alvo dessa pesquisa.

Será utilizado $\mathbb{N}$ para se referir ao conjunto dos números naturais e $\mathbb{Z}$ ao conjunto dos números inteiros, assim: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ e $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. As definições e proposições apresentadas nesse capítulo são baseadas nos autores Hefez (2016), Ribenboim (2001), entre outros.

2.1 Números Primos

O estudo dos números primos possui uma grande importância, desde o Ensino Básico até o Ensino Superior. Não é difícil encontrar livros ou pesquisas que discorrem a respeito desse conjunto numérico e apresentando sua definição assim como sua importância no desenvolvimento de várias áreas. Por exemplo, como já foi dito nessa dissertação, o número primo é quem proporciona a segurança na codificação da Criptografia RSA.

Definição 2.1. *Todo número natural maior que 1 que é divisível apenas por um e por ele mesmo é chamado de primo. Os demais naturais maiores que 1 são chamados de compostos.*

Todo número composto é o produto de números primos e esse produto é único, independente da ordem dos fatores. Esse é o resultado do Teorema Fundamental da Aritmética.

Abaixo se encontra a figura que mostra os cem primeiros números primos.

Figura 9 – Os cem primeiros números primos.

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541

Fonte: Produzida pelo autor.

O fato de o número primo possuir apenas dois divisores positivos é o que proporciona a estes números sua importância. Ainda hoje é um desafio descobrir se um número muito grande é primo ou não, pois não existe uma única forma aritmética de descrever um número primo qualquer.

O projeto de pesquisa mundial chamado Great Internet Mersenne Prime Search (GRIMPS), criado em 1996, concede o download de um software para encontrar números primos e oferece prêmios para quem conseguir encontrar algum número primo de Mersenne ainda desconhecido. No ano de 2018 foi descoberto o número 51º de Mersenne, um número de uma classe especial de primos.

Segundo o site do Instituto de Matemática Pura e Aplicada (APLICADA, 2019), "os primos de Mersenne, assim nomeados em homenagem ao monge francês Marin Mersenne, que estudou primos há cerca de 350 anos, têm uma fórmula simples: 2^n – 1" onde n é primo. O número 51º de Mersenne possui 24.862.048 dígitos e foi descoberto por Patrick Laroche, profissional de TI que recebeu um prêmio de aproximadamente 11 mil reais.

Conhecendo um pouco mais a respeito da dificuldade de identificar se um número muito grande é primo ou composto, é possível compreender melhor um dos porquês da Criptografia RSA ser uma das mais seguras atualmente. Esse fato da segurança desse código será mais bem explicado no próximo capítulo, mas a base da explicação está nessa dificuldade.

Definição 2.2. *O número denominado semiprimo é o resultado do produto de dois números primos.*

É importante conhecermos a definição de um número semiprimo, pois os algoritmos da Criptografia RSA, que serão estudados no próximo Capítulo, sempre trabalham com esse número para realizar as suas codificações e decodificações.

2.2 Divisibilidade

Essa parte da dissertação inicia com algumas definições e em seguida teremos algumas proposições, decorrentes das definições, que serão necessárias para o desenvolvimento do algoritmo da Criptografia RSA.

Definição 2.3. *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$. Diremos que a divide b quando existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$, denotaremos por $a \mid b$. Neste caso diremos que b é um múltiplo de a ou, ainda, a é um divisor de b e mais, c é chamado de quociente de b por a e é denotado por $c = \frac{b}{a}$.*

Serão enunciadas e demonstradas a seguir, três proposições de divisibilidade que serão utilizadas nos processos dos algoritmos de codificação e decodificação da Criptografia RSA no decorrer desta dissertação.

Proposição 2.1. *Sejam $a, b, c \in \mathbb{Z}$, temos que:*

(a) $1 \mid a$, $a \mid a$ e $a \mid 0$;

(b) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Prova: Temos que $1 \mid a$ e $a \mid a$, pois ambas decorrem da igualdade $a = 1 \cdot a$. Já $a \mid 0$ decorre da igualdade $0 = 0 \cdot a$. Agora se $a \mid b$ e $b \mid c$, então existem $r, s \in \mathbb{Z}$ tal que

$$b = a \cdot r \tag{1}$$

e

$$c = b \cdot s. \tag{2}$$

Substituindo o valor de b da equação (1) na equação (2) obtemos

$$c = (a \cdot r) \cdot s \Rightarrow c = a \cdot (r \cdot s).$$

Ou seja, $a \mid c$.

□

Note que o item (a) da Proposição 2.1 nos diz que todo número é divisível por 1 e por ele mesmo, e isso é um item importante para identificarmos se um número é primo ou não, como foi exposto na Definição 2.1 do início desse capítulo.

Proposição 2.2. *Sejam $a, b, c, d \in \mathbb{Z}$, temos que se $a \mid b$ e $c \mid d$ então $a \cdot c \mid b \cdot d$.*

Prova: Da hipótese $a \mid b$ e $c \mid d$ temos que existem $r,s \in \mathbb{Z}$ tal que $b = a \cdot r$ e $d = c \cdot s$. Se multiplicarmos as duas equações obteremos

$$b \cdot d = (a \cdot r) \cdot (c \cdot s) \Rightarrow b \cdot d = (a \cdot c) \cdot (r \cdot s).$$

Ou seja, $a \cdot c \mid b \cdot d$.

□

Em particular, como $c \mid c$ pelo item (a) da Proposição 2.1, se $a \mid b$ então $a \cdot c \mid b \cdot c$, para todo $c \in \mathbb{Z}$.

Proposição 2.3. *Sejam a, b, c ∈ ℤ, tal que a | (b + c) ou a | (b - c). Temos que a | b se, e somente se, a | c.*

Prova: Suponha que $a \mid (b+c)$, assim existe $r \in \mathbb{Z}$ tal que

$$b + c = a \cdot r. \tag{3}$$

Se $a \mid b$, então existe $s \in \mathbb{Z}$ tal que

$$b = a \cdot s. \tag{4}$$

Substituindo o valor de b da equação (4) na (3) obtemos

$$(a \cdot s) + c = a \cdot r \Rightarrow c = a \cdot r - a \cdot s \Rightarrow c = a \cdot (r - s).$$

Como $(r-s) \in \mathbb{Z}$, logo $a \mid c$.

Por outro lado, se $a \mid c$, então existe $t \in \mathbb{Z}$ tal que

$$c = a \cdot t. \tag{5}$$

Substituindo o valor de c da equação (5) na (3) obtemos

$$b + (a \cdot t) = a \cdot r \Rightarrow b = a \cdot r - a \cdot t \Rightarrow b = a \cdot (r - t).$$

Como $(r-t) \in \mathbb{Z}$, logo $a \mid b$. Agora, suponha que $a \mid (b-c)$, assim existe $r' \in \mathbb{Z}$ tal que

$$b - c = a \cdot r'. \tag{6}$$

Se $a \mid b$, então existe $s' \in \mathbb{Z}$ tal que

$$b = a \cdot s'. \tag{7}$$

Substituindo o valor de b da equação (7) na (6) obtemos

$$(a \cdot s') - c = a \cdot r' \Rightarrow c = a \cdot s' - a \cdot r' \Rightarrow c = a \cdot (s' - r').$$

Como $(s' - r') \in \mathbb{Z}$, logo $a \mid c$. Além disso, se $a \mid c$, então existe $t' \in \mathbb{Z}$ tal que

$$c = a \cdot t'. \tag{8}$$

Substituindo o valor de c da equação (8) na (6) obtemos

$$b - (a \cdot t') = a \cdot r' \Rightarrow b = a \cdot r' + a \cdot t' \Rightarrow b = a \cdot (r' + t').$$

Como $(r' + t') \in \mathbb{Z}$, logo $a \mid b$.

□

Considerando as definições e proposições apresentadas a respeito de Divisibilidade, seguirá na próxima seção o conceito do algoritmo da Divisão Euclidiana para auxiliar no desenvolvimento do algoritmo da Criptografia RSA no Ensino Médio.

2.3 Divisão Euclidiana

Essa divisão também é conhecida como divisão com resto e é ensinada nas escolas desde os anos iniciais de estudo no Ensino Básico.

Teorema 2.1. *Sejam $a, b \in \mathbb{N}$, com $b \neq 0$. Existem dois únicos números q e r tais que $a = b \cdot q + r$, com $0 \leq r < \mid b \mid$.*

Os números q e r são denominados quociente e resto, respectivamente, da divisão de a por b.

Prova: Considere o conjunto

$$T = \{a - b \cdot k, \text{ com } k \in \mathbb{Z} \text{ e } a - b \cdot k > 0\}.$$

(Existência): Como $a - b \cdot 0 \in T$, temos que o conjunto T não é vazio. Note que o conjunto é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação [1], já que $T \subset N$, o conjunto T possui um menor elemento

$$r = a - b \cdot q.$$

[1] (*LIMA*, 2016) Todo subconjunto $T \subset \mathbb{N}$ possui um menor elemento, isto é, existe um único elemento $n \in T$ tal que $n < k$ para todo $k \in T$.

Sabemos que $r \geq 0$ então vamos mostrar que $r < |b|$. Suponha que $r \geq |b|$, portando existe $s \in \mathbb{N}$ tal que

$$r = |b| + s,$$

logo $0 \leq s < r$. Mas isso é um absurdo, pois contradiz o fato de r ser o menor elemento do conjunto T, pois

$$s = a - (q \pm 1) \cdot b \in T, \text{ com } s < r.$$

(Unicidade): Suponha que

$$a = b \cdot q + r = b \cdot q' + r', \text{ onde } q, q', r, r' \in \mathbb{Z},\ 0 \leq r < |b| \text{ e } 0 \leq r' < |b|.$$

Assim, temos que $-|b| < -r$, $-r \leq r' - r$ e $r' - r < |b|$, o que implica em $-|b| < -r \leq r' - r < |b|$. Logo, $| r' - r | < |b|$.

Por outro lado,

$$b \cdot (q - q') = r' - r,$$

o que implica em

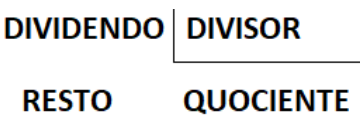
$$|b| \cdot |q - q'| = |r' - r| < |b|.$$

O que só é possível se $q = q'$ e $r = r'$.

□

Abaixo, apresenta a estrutura do algoritmo da divisão que é ensinado no Ensino Básico.

Figura 10 – Algoritmo da divisão, o método conhecido como "chave".



Fonte: Produzida pelo autor.

Esse algoritmo será de extrema importância para o bom desenvolvimento da nossa Sequência Didática, pois como já foi dito e veremos mais detalhadamente no próximo capítulo, a Criptografia RSA envolve resto de divisões. A seguir veremos a respeito de potências de números naturais, outro conteúdo que será trabalhado no desenvolvimento da codificação e decodificação usando a Criptografia RSA.

2.4 Potência

Nessa parte da dissertação, explanaremos a respeito de potências de números naturais, pois no desenvolver da nossa proposta em sala de aula os educandos precisaram relembrar algumas propriedades para nos dar suporte nos cálculos do algoritmo da Criptografia RSA.

Potenciação é considerada uma operação de multiplicação de números reais. Veremos nesse capítulo a potenciação de números naturais com expoente também naturais e algumas propriedades decorrentes da sua definição.

Definição 2.4. *Sejam $a \in \mathbb{R}$ e $n \in \mathbb{N}$. Chamamos de potência de base **a** e expoente **n** o produto de **n** fatores iguais a **a**, ou seja, potência de expoente natural é o resultado da multiplicação de um número por si mesmo um certo número de vezes. Usamos a notação: a^n.*

Abaixo veremos duas propriedades de operações com potências de números naturais que são consequências da definição e que será útil no desenvolvimento do algoritmo RSA.

Proposição 2.4. *Sejam $a, b, c \in \mathbb{N}$, temos que:*

(a) $a^b \cdot a^c = a^{b+c}$;

(b) $(a^b)^c = a^{b \cdot c}$.

Esse conceito matemático, juntamente com os demais citados anteriormente, dará aporte teórico básico para desenvolvermos em sala de aula do Ensino Médio o algoritmo da Criptografia RSA.

2.5 Congruência

Nessa parte da dissertação será apresentado o conteúdo matemático, estudado no Ensino Superior, que fundamenta os algoritmos da Criptografia RSA. No entanto, é importante salientar que esse conteúdo que será exposto agora, não será trabalhado em sala de aula com os educandos do Ensino Médio, visto que para a real compreensão desse conteúdo é necessário ter uma maior maturidade no pensamento matemático.

Apesar de não conhecer o conteúdo de Congruência, os educandos do Ensino Básico conseguirão realizar as codificações e decodificações da Criptografia RSA, pois abordaremos seus cálculos utilizando os conteúdos matemáticos citados anteriormente.

Dito isto, então o motivo de discorrermos a respeito de Congruência é para que os leitores, que já possuírem afinidades com esse conteúdo, possam melhor compreender os cálculos que serão realizados com o algoritmo da Criptografia RSA.

Congruência trata-se de um conteúdo aritmético que trabalha com restos da divisão euclidiana por um número fixado inicialmente.

Definição 2.5. *Sejam a, b, $m \in \mathbb{Z}$, com $m > 0$, dizemos que os números a e b são congruentes módulo m se seus restos da divisão euclidiana por m forem iguais.*

Quando dois números a e b são congruentes módulo m, escrevemos

$$a \equiv b \mod m.$$

Exemplo 2.1. *Temos que* 39 *é congruente a* 25 *módulo* 7*, pois* $39 = 7 \cdot 5 + 4$ *(*39 *deixa resto* 4 *na divisão euclidiana por* 7*) e* $25 = 7 \cdot 3 + 4$ *(*25 *deixa resto* 4 *na divisão euclidiana por* 7*). Assim*

$$39 \equiv 25 \mod 7.$$

Proposição 2.5. *Sejam a, b, $m \in \mathbb{Z}$, com $m > 0$, os números a e b serão congruentes módulo m se, e somente se, o número m divide a diferença entre a e b, ou seja, $m \mid a$ - b.*

Prova: Se $a \equiv b \mod m$, temos que existem $q, q' \in \mathbb{Z}$ tais que

$$a = m \cdot q + r$$

e

$$b = m \cdot q' + r,$$

com r < m. Subtraindo o valor de a por b obtemos

$$a - b = m \cdot q + r - (m \cdot q' + r) = m \cdot q + r - m \cdot q' - r = m \cdot (q - q').$$

Como $(q - q') \in \mathbb{Z}$, logo $m \mid a - b$.

Por outro lado, considere $m \mid a - b$. Se dividirmos a e b por m, temos que existem $q, q', r, r' \in \mathbb{Z}$ únicos pelo Teorema 2.1, tais que

$$a = m \cdot q + r$$

e

$$b = m \cdot q' + r',$$

com $r < m$ com $r' < m$. Subtraindo a de b obtemos

$$\begin{aligned} a - b &= m \cdot q + r - (m \cdot q' + r') \\ &= m \cdot q + r - m \cdot q' - r' \\ &= m \cdot (q - q') + (r - r'), \end{aligned} \tag{9}$$

com $r - r' < m$. Por hipótese temos que $m \mid a - b$, logo, pela Definição 2.3, existe $c \in \mathbb{Z}$ tal que

$$a - b = m \cdot c. \tag{10}$$

E com o Teorema 2.1, concluímos das equações (9) e (10) que

$$q - q' = c \text{ e } r - r' = 0.$$

Portanto, $r = r'$ e assim temos por definição que $a \equiv b \mod m$.

□

Exemplo 2.2.

(a) Temos que $36 \equiv 4 \mod 8$*, pois* $36 - 4 = 32 = 8 \cdot 4$.

(b) Note que $51 - 9 = 42$*. Como* $42 = 6 \cdot 7$*, podemos concluir que* $51 \equiv 9 \mod 6$ *ou que* $51 \equiv 9 \mod 7$.

Corolário 2.1. *Sejam $n \in \mathbb{N}$ e $a, b, m \in \mathbb{Z}$, com $m > 0$, temos que se $a \equiv b \mod m$, então temos que*

$$a^n \equiv b^n \mod m.$$

Prova: Conferir, Hefez (2016)([168], Corolário 9.4).

□

Proposição 2.6. *Sejam $a, b, c \in \mathbb{Z}$ e $d, m \in \mathbb{N}^*$. Temos que se $a \equiv b \mod m$ e $a^d \equiv c \mod m$, então $b^d \equiv c \mod m$.*

Prova: Por hipótese temos que $a \equiv b \mod m$ e $a^d \equiv c \mod m$. Assim pelo Corolário 2.1 sabemos que $a^n \equiv b^n \mod m$. Fazendo $n = d \in \mathbb{N}^*$ temos que

$$a^d \equiv b^d \mod m.$$

No entanto como $a^d \equiv c \mod m$, concluímos que $b^d \equiv c \mod m$.

□

Exemplo 2.3. *Qual o resto da divisão de* 5^8 *por 16?*

Usando o conceito de Congruência, devemos determinar $r \in \mathbb{N}$, *com* $r < 16$ *tal que*

$$5^8 \equiv r \mod 16.$$

Utilizando as propriedades de potenciação, temos que $5^8 = (5^2)^4 = 25^4$. *No entanto,*

$$25 \equiv 9 \mod 16,$$

pois $25 = 16 + 9$. *Daí,*

$$5^8 \equiv r \mod 16 \Rightarrow 25^4 \equiv r \mod 16 \Rightarrow 9^4 \equiv r \mod 16.$$

Novamente, utilizando as propriedades de potenciação, temos que $9^4 = (9^2)^2 = 81^2$. *No entanto,*

$$81 \equiv 1 \mod 16,$$

pois $81 = 16 \cdot 5 + 1$. *Daí,*

$$9^4 \equiv r \mod 16 \Rightarrow 81^2 \equiv r \mod 16 \Rightarrow 1^2 \equiv r \mod 16 \Rightarrow 1 \equiv r \mod 16.$$

Assim, $16 \mid 1 - r$. *E como* $0 \leq r < 16$, *logo* $r = 1$.

Portanto o resto da divisão de 5^8 *por* 16 *é* 1.

Proposição 2.7. *Sejam* $a, m \in \mathbb{Z}$, *com* $m > 0$. *Então existe* $b \in \mathbb{Z}$ *com* $a \cdot b \equiv 1 \mod m$ *se, e somente se,* $mdc(a,m) = 1$.

Dizemos que a é invertível módulo m e chamamos b de inverso de a módulo m.

Prova: Se $a \cdot b \equiv 1 \mod m$ temos que $m \mid a \cdot b - 1$. Assim

$$m \cdot (-k) = a \cdot b - 1,$$

com $k \in \mathbb{Z}$. Isolando o número 1 obtemos

$$m \cdot k + a \cdot b = 1.$$

Como $mdc(a,m) \mid m \cdot k + a \cdot b$ e $m \cdot k + a \cdot b = 1$, logo $mdc(a,m) = 1$.

Por outro lado, pelo Teorema de Bézout [2], se $mdc(a,m) = 1$ então existem $b,k \in \mathbb{Z}$ tal que $a \cdot b + m \cdot k = 1$. Assim

$$m \cdot k = 1 - a \cdot b \Leftrightarrow m \cdot (-k) = a \cdot b - 1 \Leftrightarrow \text{a} \cdot b \equiv 1 \mod m.$$

□

Com a definição, as proposições e o corolário apresentados nesta seção, que trata a respeito do conteúdo de Congruência, é possível compreender a codificação e decodificação de mensagens criptografadas pelo método RSA.

No capítulo seguinte, serão apresentados os algoritmos de codificação e decodificação, assim como exemplos, para potencializar a compreensão por parte do leitor.

[2] Seja $d = mdc(a,b)$, então existem x e $y \in \mathbb{Z}$ tais que $d = a \cdot x + b \cdot y$, ou seja, d é uma combinação linear de a e b.

3 ALGORITMOS DA CRIPTOGRAFIA RSA

O objetivo principal da Sequência Didática proposta nessa dissertação é desenvolver os algoritmos da Criptografia RSA, para codificar e decodificar mensagens simples em sala de aula, com educandos do terceiro ano do Ensino Médio da escola Centro de Ensino Frei Gil, no município de Estreito, estado do Maranhão.

Os algoritmos da Criptografia RSA, que serão explicados nesse capítulo, possuem como conceito matemático principal a Congruência. Tanto para codificar quanto para decodificar devemos calcular o número b tal que a e b sejam congruentes módulo m, onde a e m serão números conhecidos.

Através da Proposição 2.5, temos que

$$a \equiv b \mod m \Leftrightarrow m \mid a-b.$$

Daí, se $m \mid a-b$, então existe $k \in \mathbb{Z}$, tal que

$$a-b = m \cdot k \Leftrightarrow a = m \cdot k + b.$$

E pela Divisão Euclidiana, temos dessa última parte que, o número b é o resto da divisão de a por m. E será esse conceito da divisão, que os educandos já conhecem, que trabalharemos em sala de aula para conseguirmos codificar e decodificar utilizando os algoritmos da Criptografia RSA.

Para uma melhor compreensão do desenvolvimento dos algoritmos, por parte do leitor, serão explicados os processos da codificação e decodificação passo a passo e então será mostrado um exemplo para cada passo do desenvolvimento. Esses exemplos que serão apresentados, vão seguir o raciocínio que será apresentado e desenvolvido pelos educandos em sala de aula.

Ao final desse Capítulo, será apresentada a prova matemática do por que o método de Criptografia RSA funciona.

3.1 Algoritmo de Codificação

Para codificar uma mensagem, inicialmente precisamos escolher dois números primos (p e q) para criar a nossa chave pública de codificação (N). Essa chave pública de codificação do nosso código é o produto dos dois números primos escolhidos inicialmente ($N = p \cdot q$). Observe

que quanto maior forem os números primos selecionados, mais difícil será de alguém conseguir, a partir da chave pública N, encontrar os valores de p e q escolhidos.

Iniciando nosso exemplo, vamos escolher $p = 3$ e $q = 11$. Assim a nossa chave de codificação é $N = 3 \cdot 11 = 33$.

Agora temos que realizar uma pré-codificação monoalfabética da mensagem que queremos transmitir, transformando cada letra em um número. Nessa dissertação faremos essa pré-codificação utilizando um número de dois dígitos para cada letra, para evitar confusões de misturar duas letras e pensar ser apenas uma, como por exemplo, seja A transformado em 1, B transformado em 2, C transformado em 3, e assim por diante. Se nos depararmos com o código 12, pode surgir a dúvida se a palavra possui as letras AB ou a letra L, pois L é a décima segunda letra do alfabeto. Então para que isso não ocorra, fizemos a pré-codificação considerando o seguinte alfabeto cifrado relacionando cada letra a um número de dois dígitos, como na tabela abaixo.

Tabela 2 – Alfabeto cifrado utilizado em sala de aula com os educandos.

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: Elaborada pelo autor.

Como exemplo, vamos codificar a palavra RSA. Utilizando o alfabeto cifrado acima, a pré-codificação da nossa palavra é: 272810.

No caso de codificação de uma frase, que sempre existe espaços entre as palavras, o pesquisador Coutinho (2015, p.147) afirma que o "espaço entre duas palavras será substituído pelo número 99". No entanto, com o intuito de simplificar o desenvolvimento dos códigos em sala de aula, não codificaremos os espaços como o método criptográfico faz, deixaremos os espaços entre os códigos assim como eles aparecem entre as palavras.

Para exemplificar, observe a tabela abaixo com exemplo da pré-codificação da frase "Aula legal" como é com o método criptográfico RSA e como utilizamos em sala de aula:

Tabela 3 – Pré-codificação da frase AULA LEGAL.

Criptografia RSA faz	Como faremos em sala
10302110992114161021	10302110 2114161021

Fonte: Elaborada pelo autor.

Após realizar a pré-codificação, iremos separar em blocos numéricos o nosso código inicialmente encontrado. Existem diversas possibilidades de fazer essa separação em blocos, pois os mesmos não precisam ter a mesma quantidade de algarismos, apenas obedecer a regra de que os números formados em cada bloco não sejam maiores que o número da chave pública de codificação.

Um modo de fazer essa separação dos blocos é separar em blocos unitários e é o que foi proposto aos educandos na codificação em sala de aula, pois com isso conseguimos trabalhar com números menores, que irão se repetir, e também para sempre seguirmos as mesmas regras iniciais.

Voltando ao exemplo da codificação para a palavra RSA (272810), um modo que não podemos separar o código em blocos é: $2-72-8-10$, pois o bloco 72 é maior que nossa chave pública $N = 33$. Então separando em blocos unitários, assim obtemos: $2-7-2-8-1-0$.

Próximo passo do algoritmo é realizar a codificação de cada bloco. Para isso faremos o seguinte: elevamos o valor numérico de cada bloco a um expoente λ e calculamos qual o valor do resto da divisão dessa potência pela nossa chave de codificação N, esse valor numérico do resto é o nosso código criptografado.

O expoente λ é um número escolhido por quem está realizando a criptografia e deve ser informado a quem irá decodificar a mensagem. Por questão de uniformidade, na prática se usa o $\lambda = 3$ e será esse valor o usado na codificação proposta aos educandos em sala de aula.

Para finalizar a codificação do nosso exemplo, da palavra RSA, temos então que calcular os restos das divisões das potências 0^3, 1^3, 2^3, 7^3 e 8^3 pela chave de codificação $N = 33$. Observe a tabela abaixo.

Tabela 4 – Cálculos da codificação da palavra RSA utilizando a Divisão Euclidiana.

Potência	Divisão euclidiana	Resto
$0^3 = 0$	$0 = 33 \cdot 0 + 0$	0
$1^3 = 1$	$1 = 33 \cdot 0 + 1$	1
$2^3 = 8$	$8 = 33 \cdot 0 + 8$	8
$7^3 = 343$	$343 = 33 \cdot 10 + 13$	13
$8^3 = 512$	$512 = 33 \cdot 15 + 17$	17

Fonte: Elaborada pelo autor.

Temos então que as potências 0^3, 1^3, 2^3, 7^3 e 8^3 divididas por 33 deixam restos, respectivamente, iguais a: 0, 1, 8, 13 e 17. Com isso temos que os blocos unitários $2-7-2-8-1-0$, foram transformados no código $8-13-8-17-1-0$. Dessa forma a nossa mensagem está codificada pela Criptografia RSA.

É importante manter os blocos do código encontrado iguais aos restos calculados, pois esses números serão utilizados no algoritmo de decodificação, que realiza operações semelhantes às operações matemáticas realizadas até aqui, o que veremos a seguir.

3.2 Algoritmo de Decodificação

Para realizarmos a decodificação da mensagem precisaremos da chave de decodificação, que é formada por dois números (N,d). O número N é a nossa chave de codificação e o número d é o número tal que

$$d \cdot \lambda \equiv 1 \mod (p-1) \cdot (q-1)$$

e que é denominado inverso do número λ módulo $(p-1) \cdot (q-1)$. Assim antes de realizarmos o algoritmo de decodificação, primeiro temos que calcular o valor numérico de d.

Mas o valor numérico de λ, p e q são conhecidos e então é possível calcular o valor numérico de d, por exemplo, resolvendo a seguinte equação Diofantina que decorre da congruência acima, pois segundo a Proposição 2.5 nos garante que $(p-1) \cdot (q-1) \mid d \cdot \lambda$ e pela Definição 2.3, temos que existe $k \in \mathbb{Z}$ tal que

$$d \cdot \lambda - 1 = (p-1) \cdot (q-1) \cdot k \Rightarrow \mathrm{d} \cdot \lambda - (p-1) \cdot (q-1) \cdot k = 1$$

No entanto, como trabalharemos com educandos do Ensino Médio, apresentaremos para eles a seguinte equação, que decorre da equação acima, para calcularem o valor numérico do número d, lembrando que λ é igual a três:

$$d = \frac{(p-1)\cdot(q-1)\cdot k+1}{3}.$$

O desafio para os educandos aqui é, por meio de testes, encontrar o primeiro número natural k que torne o valor de d também natural. A limitação do valor de k nos números naturais foi feita para trabalharmos com números positivos e facilitar as operações matemáticas. No exemplo usado, temos que calcular o valor de d, tal que

$$\begin{aligned} d &= \frac{(3-1)\cdot(11-1)\cdot k+1}{3} \\ &= \frac{2\cdot 10\cdot k+1}{3} \\ &= \frac{20\cdot k+1}{3}. \end{aligned}$$

Na tabela a seguir, encontramos os testes dos valores naturais de k para calcularmos o valor numérico de d no nosso exemplo.

Tabela 5 – Teste de valores naturais de k para cálculo do valor numérico de d.

Valor de k	Valor de d
0	$\frac{20\cdot 0+1}{3} = \frac{1}{3} \notin \mathbb{N}$
1	$\frac{20\cdot 1+1}{3} = \frac{21}{3} = 7 \in \mathbb{N}$

Fonte: Elaborada pelo autor.

Assim a chave de decodificação do nosso exemplo é (33, 7).

Encontrado o valor numérico de d, podemos então começar a decodificação do código. Realizaremos cálculos semelhantes aos realizados para a codificação. Pegaremos os valores numéricos dos blocos codificados, elevaremos ao expoente d e calcularemos o resto da divisão dessa potência pela chave de codificação N.

Como exemplo, vamos decodificar o código $8-13-8-17-1-0$, criado no exemplo anterior, para confirmar que seu significado é a palavra RSA. Então temos que calcular os restos das divisões das potências 0^7, 1^7, 8^7, 13^7 e 17^7 pelo número da nossa chave que é 33. Observe a tabela abaixo.

Tabela 6 – Cálculos da decodificação do código "8 – 13 – 8 – 17 – 1 – 0" utilizando a divisão.

Potência	Divisão euclidiana	Resto
$0^7 = 0$	$0 = 33 \cdot 0 + 0$	0
$1^7 = 1$	$1 = 33 \cdot 0 + 1$	1
$8^7 = 2.097.152$	$2.097.152 = 33 \cdot 63.550 + 2$	2
$13^7 = 62.748.517$	$62.748.517 = 33 \cdot 1.901.470 + 7$	7
$17^7 = 410.338.673$	$410.338.673 = 33 \cdot 12.434.505 + 8$	8

Fonte: Elaborada pelo autor.

Assim, os restos das divisões das potências 0^7, 1^7, 8^7, 13^7 e 17^7 por 33 são, respectivamente, 0, 1, 2, 7 e 8. Portanto o código 8 – 13 – 8 – 17 – 1 – 0 após decodificado se torna o seguinte: 2 – 7 – 2 – 8 – 1 – 0.

Realizada a decodificação, temos que desconstruir os blocos formados pelo criador do código. Logo temos que unir os algarismos de acordo com a separação dos blocos inicialmente escolhida, para formar os números da pré-codificação e então verificar qual letra do alfabeto cifrado corresponde ao valor numérico encontrado, obtendo assim a mensagem na linguagem formal. No nosso exemplo, sabemos que foram formados blocos unitários e que o alfabeto cifrado utilizado obedece a regra que cada letra é relacionada a um número de dois dígitos. Assim temos que o código se dá por: 27 – 28 – 10. E esses números correspondem as letras RSA.

3.3 Prova matemática da funcionalidade do Algoritmo RSA

Para realizarmos essa prova, vamos relembrar os passos para realização da codificação. Inicialmente escolhemos dois números primos (p e q) e fazemos uma pré-codificação da mensagem a ser transmitida, relacionando cada letra com um número e assim formando uma sequência de números. Essa sequência de números deve ser dividida em blocos de modo que o número (D), obtido em cada bloco unitário, deve ser menor que o número da chave de codificação ($N = p \cdot q$). Assim

$$1 \leq D < N.$$

Feito isso, é realizada a codificação de cada um desses blocos. Para isso temos que calcular o número α, que deve ser congruente a D^{λ} módulo N, onde λ escolhemos ser igual a 3, ou seja

$$D^3 \equiv \alpha \mod N,$$

com $0 \leq \alpha < N$. E esse número α representa a codificação do bloco D.

Agora para fazer a decodificação, temos que procurar um número β tal que ele seja congruente a α^d módulo N, lembrando que d é a chave de decodificação e é secreta. Assim:

$$\alpha^d \equiv \beta \mod N,$$

com $0 \leq \beta < N$. E esse número β representa a decodificação de α.

Então se ocorrer de encontrarmos $\beta = D$, significa que esse método de codificação está correto, pois ao encontrarmos essa igualdade chegamos aos blocos formados inicialmente e desfazendo esses blocos encontramos uma sequência de números que, ao ser relacionado com as letras do alfabeto, formaremos a mensagem na linguagem formal.

Vamos então a prova matemática.

Note que $\beta \equiv \alpha^d \mod N$ e $\alpha \equiv D^3 \mod N$, logo $\beta \equiv (D^3)^d \mod N$. Ou seja:

$$\beta \equiv D^{3d} \mod N. \tag{11}$$

Como vimos na seção anterior a respeito da chave de decodificação (d), temos que

$$3 \cdot d \equiv 1 \mod (p-1)\cdot(q-1) \Rightarrow 3 \cdot d = 1 + (p-1)\cdot(q-1)\cdot k,$$

com $k \in \mathbb{Z}$. Assim, substituindo $3 \cdot d$ na congruência (11) obtemos

$$\beta \equiv D^{1+(p-1)\cdot(q-1)\cdot k} \mod N,$$

observe ainda que $D^{1+(p-1)\cdot(q-1)\cdot k} = \mathrm{D} \cdot D^{(p-1)\cdot(q-1)\cdot k}$.

Agora, vamos tomar como objetivo provar que $D^{3d} \equiv D \mod p$ e $D^{3d} \equiv D \mod q$, para assim obtermos um sistema de congruências e finalmente provar que $D = \beta$.

Para provar que $D^{3d} \equiv D \mod p$, vamos dividir essa demonstração em dois casos.

Primeiro caso: Consideraremos $mdc(p,D) \neq 1$ e p é primo, então D é um múltiplo de p. Assim $D \equiv 0 \mod p$ e $D^{3d} \equiv 0 \mod p$, logo

$$D^{3d} \equiv D \mod p.$$

Segundo caso: Consideraremos $mdc(p,D) = 1$, logo o D não é múltiplo de p. Sabemos que $D^{3d} = D \cdot D^{(p-1)\cdot(q-1)\cdot k} = D \cdot (D^{(p-1)})^{(q-1)\cdot k}$. Observe agora que como $mdc(p,D) = 1$ então o Pequeno Teorema de Fermat [1] me garante que $D^{(p-1)} \equiv 1 \mod p$. Então $D^{3d} \equiv D \cdot (1)^{(q-1)\cdot k} \mod p$, ou seja

[1] Se p é um número primo e se a é um número não divisível por p, então p divide $a^{p-1} - 1$.

$$D^{3d} \equiv D \mod p.$$

Assim, acabamos de provar que de fato temos que $D^{3d} \equiv D \mod p$.

Analogamente, prova-se que $D^{3d} \equiv D \mod q$.

Com as congruências $D^{3d} \equiv D \mod p$ e $D^{3d} \equiv D \mod q$, obtemos o seguinte sistema de congruência

$$\begin{cases} D^{3d} \equiv D \mod p \\ D^{3d} \equiv D \mod q \end{cases}$$

Do sistema acima obtemos $p \cdot m = D^{3d} - D$, com $m \in \mathbb{Z}$ e $q \cdot n = D^{3d} - D$, com $n \in \mathbb{Z}$. Ou seja, $D^{3d} - D$ é múltiplo de p e de q. Como p e q são primos, temos que $D^{3d} - D$ é múltiplo de $p \cdot q$. Assim temos que

$$D^{3d} - D = p \cdot q \cdot g,$$

com $g \in \mathbb{Z}$. Logo, lembrando que $N = p \cdot q$, podemos escrever a seguinte congruência

$$D^{3d} \equiv D \mod N.$$

Daí, como $\beta \equiv D^{3d} \mod N$, temos que

$$\beta \equiv D \mod N.$$

Agora, β e D serem congruentes não implicam que são iguais. No entanto, como β e D são congruentes módulo N, temos que ao dividir β e D por N eles deixaram o mesmo resto. Mas $\beta < N$, então a divisão de β por N deixa resto β, por se tratar de uma divisão euclidiana no conjunto dos números naturais. De forma análoga, conclui-se que o resto da divisão de D por N é D. O fato de β e D serem congruente módulo N, conclui-se então que β é igual a D.

E assim então está provado matematicamente que ao decodificar o bloco α obtemos exatamente o bloco inicial formado, que é o bloco D.

4 PROPOSTA DA SEQUÊNCIA DIDÁTICA

Este capítulo trará uma breve discussão a respeito de Sequência Didática e apresentaremos, também nessa parte, a análise da nossa intervenção didática, onde tivemos como tema a Criptografia RSA.

Como já discorremos nos capítulos anteriores, criamos uma Sequência Didática com o objetivo principal de investigar e trabalhar os conceitos matemáticos básicos necessários no desenvolvimento dos algoritmos da Criptografia RSA, com o objetivo de instigar a curiosidade e o interesse dos educandos em estudar Matemática. Além disso, implementar a discussão a rdisciplinares de forma espeito da importância da segurança de dados e informações pessoais na Internet, pois caminhamos para um cotidiano cada vez mais tecnológico.

O público alvo desta Sequência Didática são educandos do 3º ano do Ensino Médio do Centro de Ensino Frei Gil, no município de Estreito do Estado do Maranhão. No entanto entendemos que essa Sequência Didática pode ser proposta a educandos a partir do 9º ano do Ensino Fundamental, por abordar conteúdos matemáticos básicos, como descrito no Capítulo 2.

Nesta perspectiva apresentamos o conceito de Sequência Didática e a análise da nossa intervenção com o aporte teórico de autores como Zabala (1998), Oliveira (2013), Miguel (2005), entre outros.

4.1 Sequência Didática

Na vida escolar de um professor, um dos desafios na docência está presente no processo do planejamento das atividades diárias, de modo que os objetivos pedagógicos sejam alcançados. Neste trabalho vamos elaborar uma proposta de ensino denominada de Sequência Didática.

Consentimos com Zabala (1998, p.18) quando afirma que Sequência Didática é “um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecidos tanto pelos professores como pelos alunos".

Compreendemos a definição de Sequência Didática como:

> [...] um procedimento simples que compreende um conjunto de atividades conectadas entre si, e prescinde de um planejamento para delimitação de cada etapa e/ou atividade para trabalhar os conteúdos disciplinares de forma integrada para uma melhor dinâmica no processo ensino-aprendizagem. (OLIVEIRA, 2013, p. 39).

Pudemos perceber, tanto para (ZABALA, 1998) como para (OLIVEIRA, 2013), que uma Sequência Didática deve ser criada com a visão de um ensino por meio de atividades sequenciadas, estruturada com seus objetivos definidos e explicitados para os educandos. Objetivando assim uma potencialização no processo de ensino e aprendizagem, contribuindo com a construção do conhecimento dos educandos.

Com a intenção de contribuir no processo de ensino e aprendizado dos educando, organizamos uma Sequência Didática com a realização de três etapas:

1. Apresentações teóricas;
2. Exposições de exemplos;
3. Realização de atividades em grupos.

Para o desenvolvimento destas três etapas, foi planejado oito aulas de 50 minutos cada, com diferentes atividades em cada um dos momentos. Pois concordamos que:

> [...] sequências didáticas, são uma maneira de encadear e articular as diferentes atividades ao longo de uma unidade didática. Assim, pois, poderemos analisar as diferentes formas de intervenção segundo as atividades que se realizam e, principalmente, pelo sentido que adquirem quanto a uma sequência orientada para a realização de determinados objetivos educativos. (ZABALA, 1998, p. 20).

Posto isto, proporemos uma Sequência Didática pelo motivo de que ela pode ser disposta como uma atividade de ensino e aprendizagem em que pode proporcionar aos educandos uma discussão a respeito de certa problemática do cotidiano, que no nosso caso é a segurança dos dados na rede de Internet, e em cima dessa problemática trabalhar conteúdos matemáticos específicos. Desse modo o educando é desafiado a encontrar argumentos embasados nos conteúdos teóricos para obter uma resposta ou solução.

4.2 Análise da intervenção

Nessa parte, discorreremos a respeito do desenvolvimento da Sequência Didática que foi proposta para três turmas do Ensino Médio. Seu desenvolvimento iniciou no dia 11 de novembro e finalizou no dia 21 de novembro do ano letivo de 2019. Nesse período foi ministradas oito aulas em cada uma das turmas. As turmas tinham exatamente 39, 29 e 32 educandos cada, totalizando assim 100 educandos que participaram do desenvolvimento da Sequência Didática.

Como foi dito acima, a Sequência Didática foi planejada com a realização de três etapas, organizada do seguinte modo: duas aulas com apresentações teóricas, outras duas aulas com exposição e discussão de exemplos e mais quatro aulas destinada a realização de atividades em

grupos. Sendo assim, deverão ser reservadas oito aulas com duração de 50 minutos cada. Os oito planejamentos de intervenções em sala de aula estão no Apêndice A.

4.2.1 Primeira aula

É o primeiro momento de apresentação teórica. Essa aula foi planejada com a utilização de notebook e data show para a exposição de slides, presentes no Apêndice B, que abordam o desenvolvimento da Criptografia, expondo os métodos criptográficos apresentados no Capítulo 1, e apresenta um vídeo de 4 minutos e 54 segundos que discorre a respeito da Criptografia RSA. Esse vídeo é um recorte, exatamente de 17 minuto e 22 segundos até 22 minuto e 16 segundos, do documentário "Luta contra os hackers" (CHANNEL, 18 ago. 2014). O objetivo dessa primeira intervenção é despertar a curiosidade dos educandos a respeito do tema Criptografia e fazer com que eles percebam que hoje em dia, devido a evolução tecnológica, a utilização de métodos criptográficos são comuns e necessários em nosso cotidiano.

Nesta aula houve boa participação da grande maioria dos educandos ao serem indagados e também no decorrer de cada um dos slides. Ao serem perguntados se conheciam algum método criptográfico, inicialmente disseram que não, mas então ao serem indagados se alguém conhecia a brincadeira da Língua do P, alguns falaram que conheciam essa brincadeira e então foi proposto a esses educando que codificassem uma frase simples, para que eles consigam perceber que em algum momento de suas vidas eles já realizaram algum tipo de codificação, mesmo que em uma brincadeira.

Ao prosseguir na apresentação dos slides, os educandos se mostraram curiosos a respeito dos métodos criptográficos apresentados como exemplos (Cítala Espartana e Cifra de César) e discutimos a respeito de sua eficiência na época e se atualmente tais métodos ainda seriam eficientes para a transmissão de mensagens. Partindo dessas discussões, foi mencionado a respeito do estudo sobre as frequências que cada letra apresenta em cada língua. Foi exibida nos slides uma tabela com essas frequências nas línguas francesa, espanhola, italiana e portuguesa. Com isso chegaram à conclusão que atualmente esses métodos conseguem ser eficientes em transmissões de mensagens simples entre amigos durante brincadeiras, mas não seriam tão eficientes em transmissões de mensagens importantes, como dados bancários, pois os códigos seriam facilmente interpretados por pessoas não desejáveis.

Na parte dos slides que tratam a respeito das primeiras máquinas de criptografar, os educandos começaram a fazer relações com as aulas de história, que o professor abordou o tema

da Primeira Guerra Mundial. Nessa parte foi explorada a evolução da máquina Enigma até chegar à máquina Lorenz SZ 40/42, para que os educandos conseguissem compreender a importância histórica e científica da criação da máquina Colossus. Ficaram bastante curiosos e intrigados com a criação da máquina Colossus, pois com essa máquina a equipe do inglês Tommy Flowers conseguiu decodificar as mensagens da máquina Lorenz SZ 40/42, que era a mais evoluída na época, sem ao menos os criadores da máquina Colossus terem tido acesso a máquina Lorenz SZ 40/42.

Ao perceber a curiosidade dos educandos a respeito dessas máquinas, sugerimos a eles o filme O Jogo da Imitação, que trata a respeito desse tema. Esse filme não foi exibido em sala de aula, pois ele tomaria pelo menos duas aulas e não é a respeito do tema principal dessa dissertação, que é a Criptografia RSA. Nas aulas seguintes, alguns educandos nos relataram que assistiram ao filme e gostaram bastante, surgindo assim mais discussões e maior aprofundamento teórico a respeito desse tema. Pudemos notar um grande envolvimento desses educandos que assistiram ao filme no decorrer da Sequência Didática

Chegando à parte dos slides que tratam a respeito da Criptografia na atualidade, foi exibido parte do documentário "Luta contra os hackers" (CHANNEL, 18 ago. 2014), que discorre sobre a Criptografia RSA, e percebemos que grande parte dos educandos prestaram bastante atenção ao vídeo e após sua apresentação foi dedicado um momento para perguntas e apontamentos a respeito do que tinham assistido. Nesse momento percebemos a curiosidade dos educandos a respeito dos números primos, pois a segurança desse código é baseada nesses números.

Optamos por exibir imagens em slides e um pequeno vídeo nessa aula, visto que o material didático audiovisual é reconhecido por potencializar o processo de ensino e aprendizagem. Selecionamos o vídeo com cuidado, pois concordamos que:

> Embora também possam assumir um caráter meramente recreativo ou de lazer, em determinadas situações os filmes devem, sempre, ser pensados como recursos didáticos, ou seja, como mediadores do processo ensino-aprendizagem. Nesse sentido, a escolha deve recair sobre filmes de curta duração, que realmente auxiliem na compreensão da área do currículo que se propõe abordar, sendo adequados ao assunto e à faixa etária. (FREITAS, 2009, p. 45).

Assim, a seleção do vídeo que trata a respeito da Criptografia RSA, foi proposital para a potencialização da aprendizagem por parte dos educados.

Ao final dessa primeira aula, foi falado a respeito do que eles produziriam nas próximas aulas e como que seriam avaliados. Buscamos deixar claro nossos objetivos, assim como (ZA-

BALA, 1998) e (OLIVEIRA, 2013) defendem a respeito de uma Sequência Didática. Não houve muitas perguntas nesse momento, mas demonstraram interesse e curiosidades a respeito dos algoritmos da Criptografia RSA.

4.2.2 Segunda aula

Foi o segundo momento de apresentação teórica. Foi ministrada com a utilização de quadro branco e pincéis. Nessa aula falamos a respeito dos conteúdos matemáticos envolvidos nos algoritmos da Criptografia RSA, que são os apresentados na seção 2.1, seção 2.3 e seção 2.4. No entanto, nesse momento ainda não fizemos a ligação entre os conteúdos matemáticos com os algoritmos da Criptografia. Foram expostos os seguintes conteúdos matemáticos de: números primos, algoritmo da divisão e potenciação de números naturais. Como esses conteúdos já são conhecidos pelos educandos do 3º ano do Ensino Médio, a explicação foi breve e seguida de exemplos numéricos. Foi proposto aos educandos que resolvam os exemplos expostos e então o professor comentou essas resoluções no quadro. Neste momento é preciso deixar explícito que esses conteúdos matemáticos serão necessários para o desenvolvimento dos algoritmos das próximas aulas.

Reservamos apenas uma aula para expor os conteúdos citados acima, pois eles já foram ensinados aos educandos no Ensino Fundamental e ainda continuam a serem trabalhados frequentemente no Ensino Médio. Pudemos perceber que os educandos se lembravam dos primeiros números primos, mas não sua definição. Sobre as propriedades de potenciação, grandes partes dos educandos não se lembravam delas e sobre o algoritmo da divisão, apenas uma pequena parte dos educandos não lembrava ou admitiu não saber.

A respeito do algoritmo da divisão, ficamos surpreendidos de encontrar educandos, no final do Ensino Básico, que não sabiam como utilizá-lo. Mas no decorrer dessa aula conseguimos notar que esses educandos que não sabiam o algoritmo da divisão tinham aprendido, pois conseguiram responder os exemplos propostos.

Tais dificuldades nos conteúdos matemáticos se dão devido a uma falha no aprendizado durante o Ensino Fundamental, onde esses conteúdos são introduzidos inicialmente. Um dos possíveis motivos da falha no aprendizado dos educandos se dá, provavelmente, ao estereótipo de a Matemática ser uma disciplina com conteúdos difíceis, e fazendo assim eles desistirem de aprender antes mesmo de começar a estudar. Vivenciamos que:

> [...] Os alunos, apesar de manterem uma boa relação com certos conteúdos matemáticos

> antes da escolarização, mesmo sem assim reconhecê-los, mostram na escola certa resistência à disciplina, fruto de crenças e convenções sociais e culturais, que impedem de reconhecer a Matemática como parte integrante de suas vidas. (MIGUEL, 2005, p. 414).

Deste modo, buscaremos sanar ao máximo essas dificuldades matemáticas apresentadas pelos educandos, utilizando esses conteúdos na execução dos algoritmos da Criptografia RSA nas próximas aulas.

4.2.3 Terceira aula

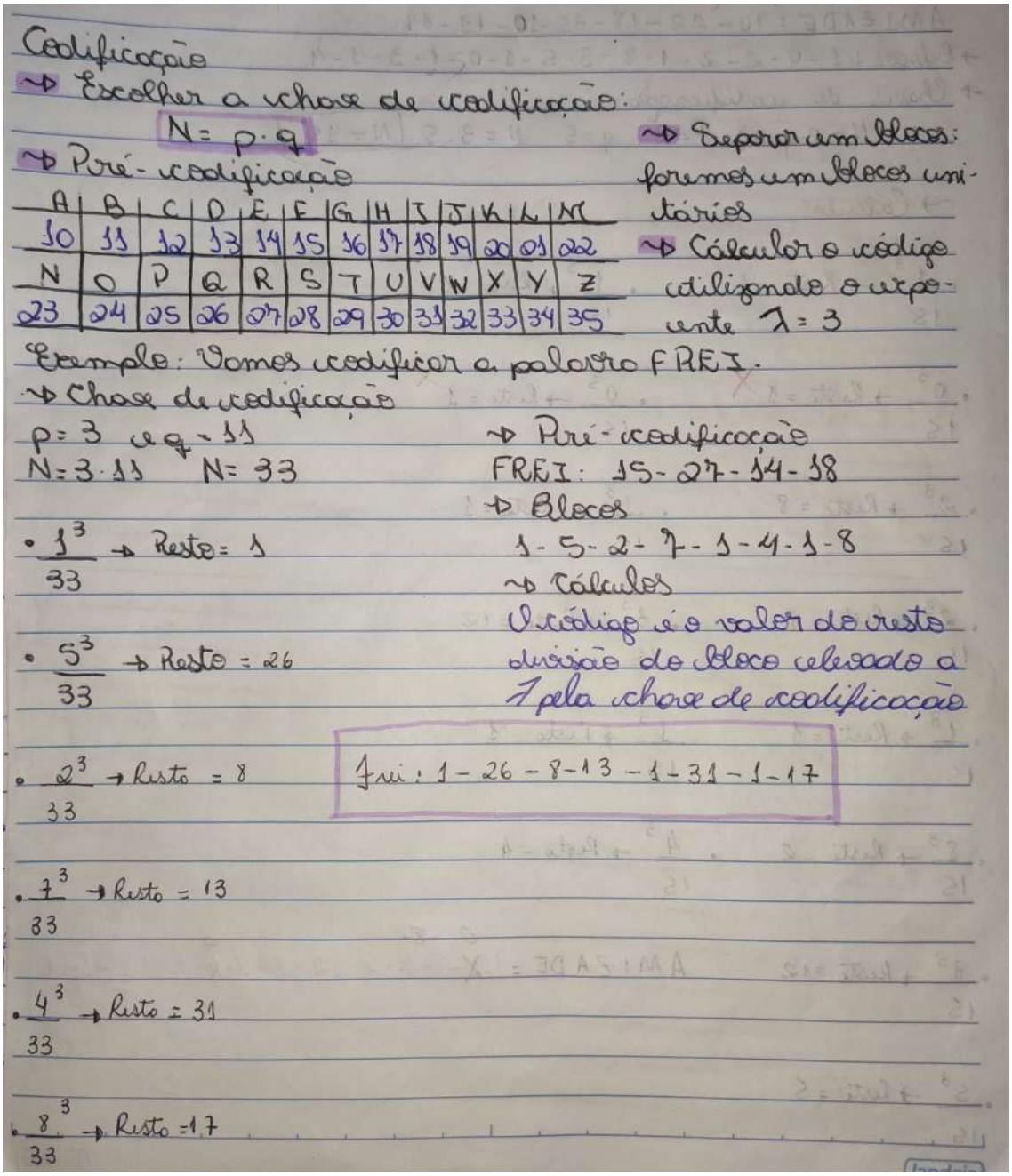
Foi realizada a apresentação do algoritmo de codificação da Criptografia RSA, apresentado na seção 3.1. Foi iniciada com uma discussão a respeito do vídeo "Luta contra os hackers" (CHANNEL, 18 ago. 2014) assistido na primeira aula. Para elucidar sobre a dificuldade de fatorar um número semiprimo (lembrando que semiprimo é um número formado pelo produto de apenas dois números primos, não necessariamente distinto), foi proposto aos educandos que fatorem alguns semiprimos, como por exemplo, o número 391 que possui como fatores 17 e 23.

Propomos aos educandos que fatorassem, além do número 391 já citado, os números 119 e 2257. Autorizamos o uso de calculadora para agilizar os cálculos e notamos que mesmo com o auxilio dessa ferramenta, eles apresentaram dificuldades, mas conseguiram calcular. Com isso eles puderam perceber a real dificuldade para se fatorar um número semiprimo e assim conseguiram compreender melhor a segurança da Criptografia RSA, que discorremos na seção 1.3.

Após esse momento, apresentamos os processos matemáticos envolvidos no algoritmo de criptografar, por meio de um exemplo da palavra Frei, e foi mostrado o passo a passo da codificação dessa palavra como foi descrito na seção 3.1.

Os educandos demonstraram interesse no desenvolvimento dessa aula e não tiveram muitas dificuldades na compreensão dos cálculos do algoritmo, como é possível observar na Figura 11, que é a foto das anotações de um dos grupos a respeito da codificação da palavra Frei.

Figura 11 – Anotações de um grupo a respeito da codificação da palavra FREI.



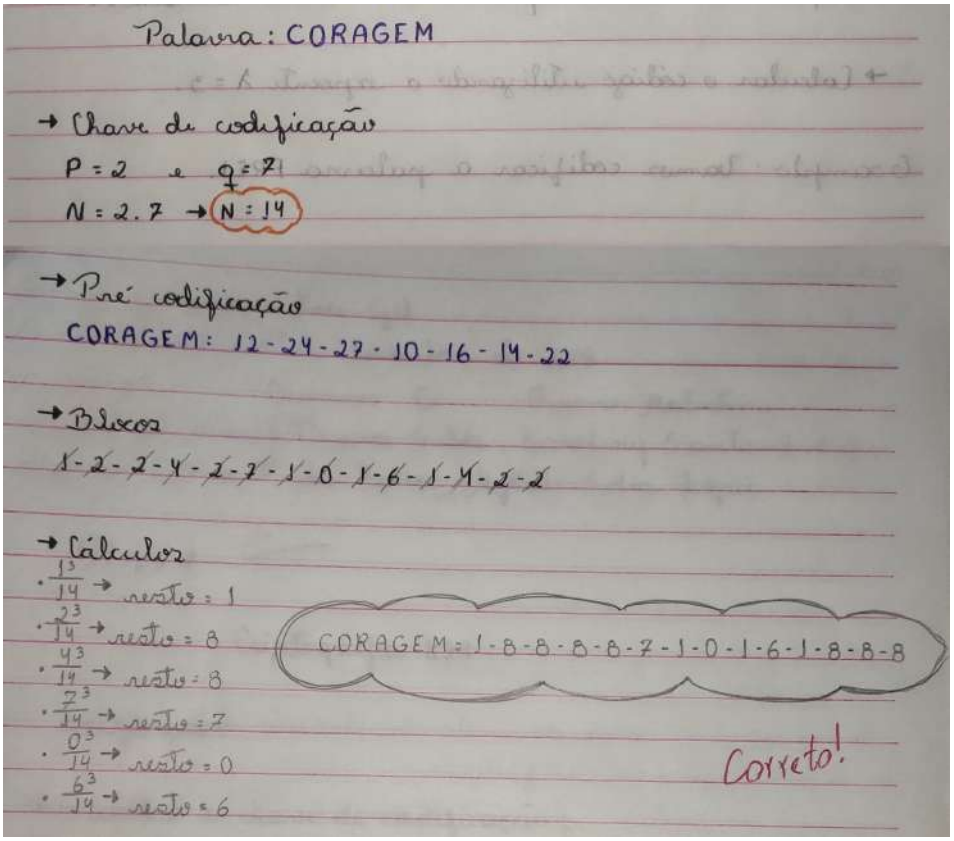
Fonte: Produzida pelo autor.

Foi proposto então que os educandos formassem grupos de até quatro pessoas e foi sorteada uma palavra para cada grupo codificar. Optamos pelo desenvolvimento das atividades em sala de aula em grupos de educandos, pois temos a mesmo concepção que Silva (1998, p.143) quando afirma que "no trabalho em grupo, o indivíduo exercita, desenvolve as possibilidades não só de discutir e argumentar, como, sobretudo, de se responsabilizar pelas decisões do pequeno grupo e do Grupão (formado por toda a turma)".

Nesta atividade ficou em aberto para os educandos escolherem os números primos que

formarão a chave de codificação. Como podemos observar na Figura 12, houve grupos que escolheram números primos diferentes aos números escolhidos no exemplo da codificação da palavra Frei apresentados.

Figura 12 – Codificação de uma palavra com a chave de codificação diferente da apresentada.



Fonte: Produzida pelo autor.

Como podemos ver na Figura 12, esse grupo escolheu os números primos 2 e 7, formando assim o número semiprimo 14 como sua chave de codificação.

Essa aula e as próximas aulas que necessitarem de explicações de desenvolvimento dos algoritmos optaram pelo tipo de aula expositiva dialógica, pois:

> Uma alternativa para transformar aula expositiva em técnica de ensino capaz de estimular o pensamento crítico do aluno é dar-lhe uma dimensão dialógica. Essa forma de aula expositiva utiliza o diálogo entre professor e alunos para estabelecer uma relação de intercâmbio de conhecimento e experiências (LOPES, 2013, p. 42).

Portanto, ao optarmos por aulas expositivas dialógicas, pudemos estimular a curiosidade e iniciativa dos educandos, valorizando o diálogo entre professor e educandos e os conhecimentos prévios apresentados pelos educandos sem atrapalhar o planejamento do desenvolvimento da aula.

Assim, ao final dessa aula pudemos observar que os educandos haviam compreendido os passos da codificação, pois todos os grupos realizaram a codificação correta da palavra sorteada. Assim, temos que o objetivo dessa aula foi alcançado, pois todos os grupos conseguiram codificar a palavra proposta a eles e demonstraram ter compreendido o algoritmo da codificação assim como os cálculos matemáticos envolvidos.

4.2.4 Quarta aula

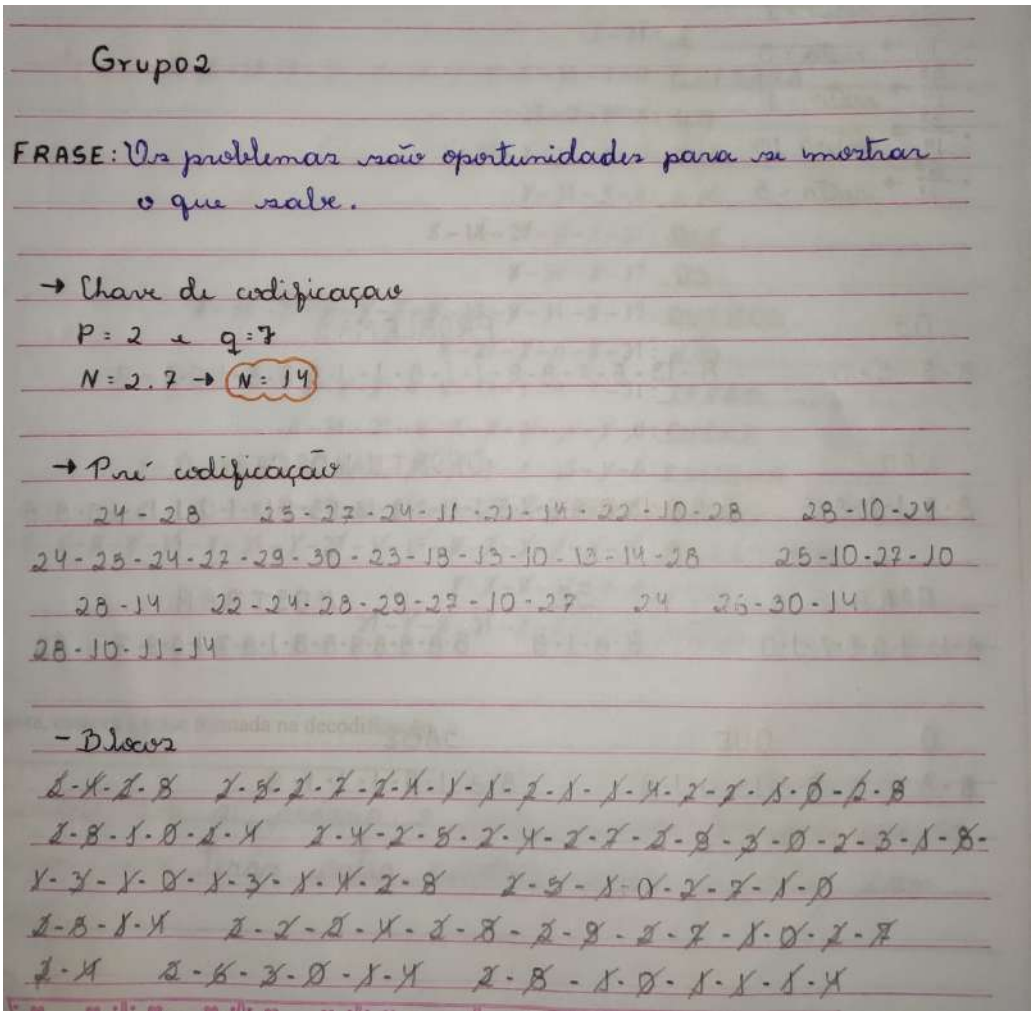
Manteve o tema do algoritmo de codificação abordado na aula anterior. Foram formados os mesmos grupos da aula anterior e esses grupos sempre serão os mesmo daqui em diante.

No primeiro momento foi iniciada uma discussão a respeito do algoritmo de codificação, com o objetivo de relembrar e esclarecer as possíveis dúvidas remanescentes dos educandos. Em seguida foi pedido que formassem os mesmos grupos da aula anterior para o desenvolvimento da atividade dessa aula, que é a realização da codificação de uma frase. Foi proposto que cada grupo criasse uma frase e a codificasse, pois assim que estimularemos ainda mais eles no desenvolvimento dessa atividade ao propormos que eles codificassem uma frase criada por eles mesmos.

Essa aula teve como objetivo, consolidar a compreensão dos educandos a respeito dos passos do algoritmo de codificação e com isso fazer com que os educandos a pratiquem os conceitos matemáticos de potenciação e algoritmo da divisão.

Nesta aula, deixamos a escolha dos números primos para a formação da chave de codificação por conta da escolha de cada grupo. Os educandos não demonstraram muitas dificuldades para realizarem as codificações. Todos os grupos conseguiram terminar essa atividade até o final dessa aula e houve poucos erros de cálculos, que foram corrigidos com o auxilio do professor. A Figura 13 traz a foto da folha de um grupo que realizou essa atividade de codificação com os números da chave de codificação dois e sete, diferentes dos apresentados no exemplo exposto pelo professor no quadro da aula anterior.

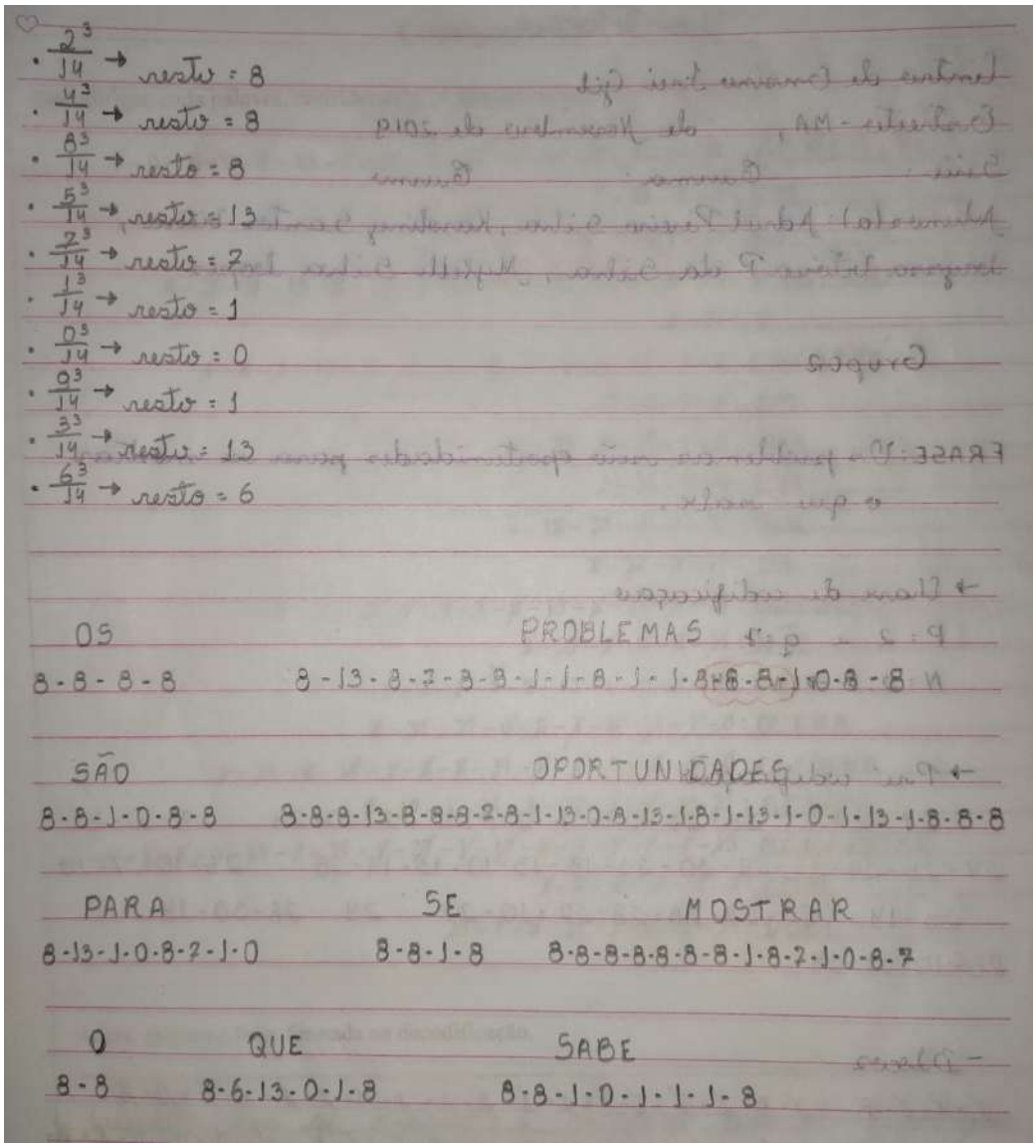
Figura 13 – Anotações da codificação de uma frase de um dos grupos de educandos.



Fonte: Produzida pelo autor.

Nessa Figura 13 podemos observar que após anotar os blocos da pré-codificação, os educandos foram realizando os cálculos e riscando os blocos. Assim a maioria dos grupos percebeu nessa atividade que os cálculos se repetiam, pois os bloco eram dos números zero ao nove, ou seja, eles observaram que deveriam calcular apenas uma vez o resto da divisão de cada um desses números elevado ao expoente três pela sua chave de codificação, como é possível observar na Figura 14 a seguir.

Figura 14 – Finalização da codificação da frase da imagem anterior.

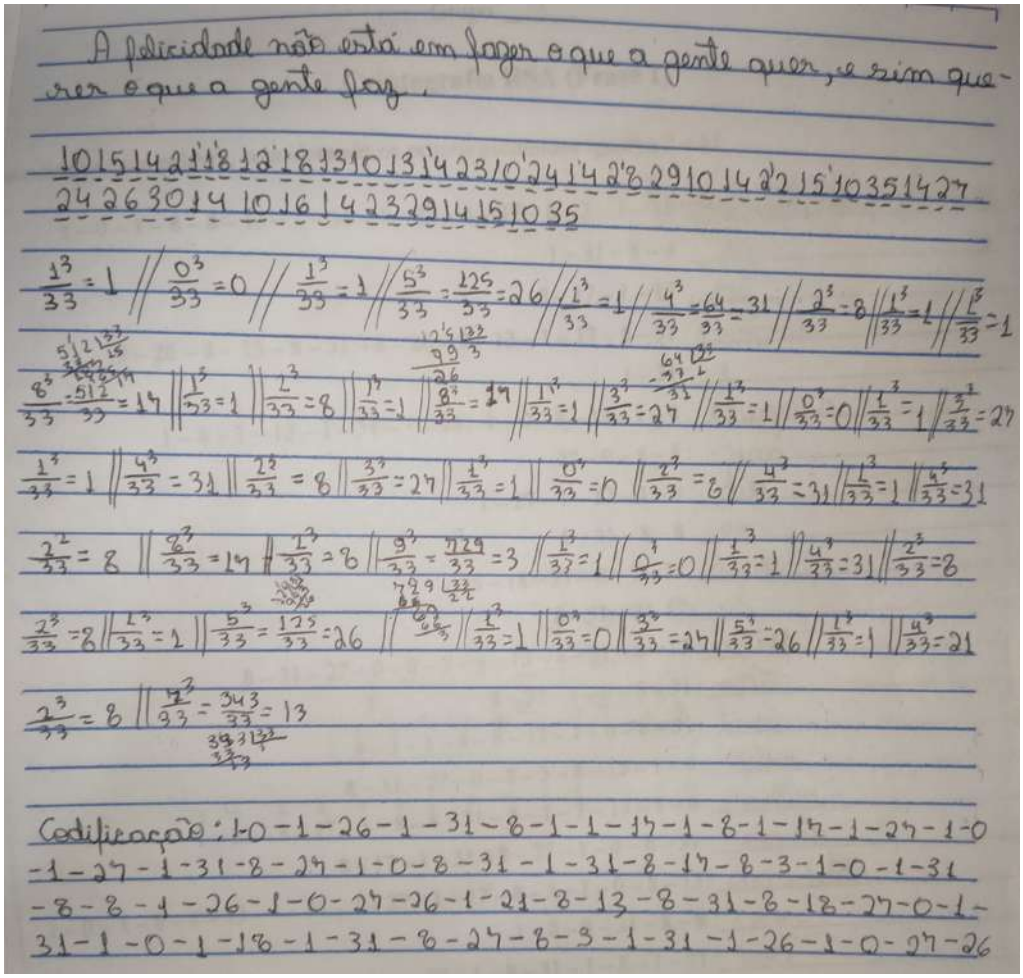


Fonte: Produzida pelo autor.

Note que na Figura 14 acima, esse grupo anotou o resto da divisão apenas uma vez e não repetiu para todos os códigos, como também foi feito por outros grupos.

A Figura 15 a seguir, mostra a foto da atividade de um grupo que realizou os cálculos repetidamente para todos os blocos.

Figura 15 – Anotações da codificação de uma frase de um grupo que repetiu os cálculos.



Fonte: Produzida pelo autor.

O grupo que entregou a folha da Figura 15 notou que os cálculos se repetiam apenas ao final da aula quando os educandos dos outros grupos comentaram sobre a repetição.

É importante observamos também o modo de organização para anotar os restos calculados desse grupo, que vários outros grupos também tiveram a mesma organização. Note que eles escreveram o resto da divisão da potência pela chave de codificação com uma igualdade. No entanto ao indagados a respeito se eram verdadeiras as igualdades, eles afirmaram que não, que aquelas igualdades significavam, para eles, o resto e não o resultado da divisão. E assim como vários grupos, continuaram a usar a notação da igualdade mesmo alertados pelo professor que não era a forma matematicamente correta.

Ao final da aula, pudemos identificar que o objetivo da compreensão do algoritmo de codificação por parte dos educandos foi alcançado, visto que a maioria dos grupos entregou esta atividade no final da aula, os demais ficaram para entregar na próxima aula.

4.2.5 Quinta aula

Foi dedicada à apresentação e explicação do algoritmo de decodificação da Criptografia RSA, como apresentado na seção 3.2. Começamos expondo o código formado no exemplo apresentado na terceira aula e iniciamos uma discussão a respeito do significado desse código, se os educandos conseguem relacionar esse código com a palavra Frei.

Após esse momento de debate de ideias, foi exposto passo a passo o algoritmo de decodificação. Cada passo foi seguindo o exemplo de decodificação do código inicialmente apresentado nesta aula. Ao finalizar a explicação desse algoritmo, foi proposto a cada um dos grupos a decodificação de um código que representa uma palavra, esses códigos e seus significados estão no Apêndice C. As palavras selecionadas para esse exercício foram escolhidas pelo professor da turma, seguindo uma exigência que era o limite de letras, entre seis ou sete.

Os objetivos dessa aula foi fazer com que os educando aprendesse e utilizasse o algoritmo para decodificar um código e assim fazer com que eles praticassem os conceitos básicos da matemática de potenciação e do algoritmo da divisão.

Pudemos notar que, devido à semelhança nos cálculos dos dois algoritmos, codificação e decodificação, os educandos não apresentaram dificuldades para compreenderem as explicações da decodificação. Eles observaram que alguns cálculos seriam maiores, devido ao código que será decodificado possuir números maiores, mas se sentiram desafiados a decodificarem o código propostos a eles, como podemos observar na Figura 16 os educandos concentrados em seus cálculos.

Figura 16 – Organização de uma das salas durante o desenvolvimento da decodificação.

Fonte: Produzida pelo autor.

Constatamos que os objetivos dessa aula foram alcançados, pois todos os grupos conseguiram realizar a decodificação proposta. Não apresentaram muitos erros, apesar de aparecerem números grandes com o expoente sete. Isso significa que conseguiram identificar um modo correto para calcular o resto de uma divisão de números naturais.

4.2.6 Sexta aula

Permanecemos com o tema do algoritmo de decodificação. Inicialmente relembramos os passos desse algoritmo e em seguida propomos aos grupos que decodifiquem duas frases, presentes no Apêndice D. Primeiro foi distribuída a folha com a "Frase 1" e quando terminava a decodificação eles recebiam a segunda folha com a "Frase 2". Como essa atividade proposta possui vários códigos, por se tratar de decodificação de frases, foi sugerido aos grupos dividissem esses códigos entre seus integrantes para conseguirem decodificar as frases, seguindo o algoritmo trabalhado na aula anterior, até o final dessa aula.

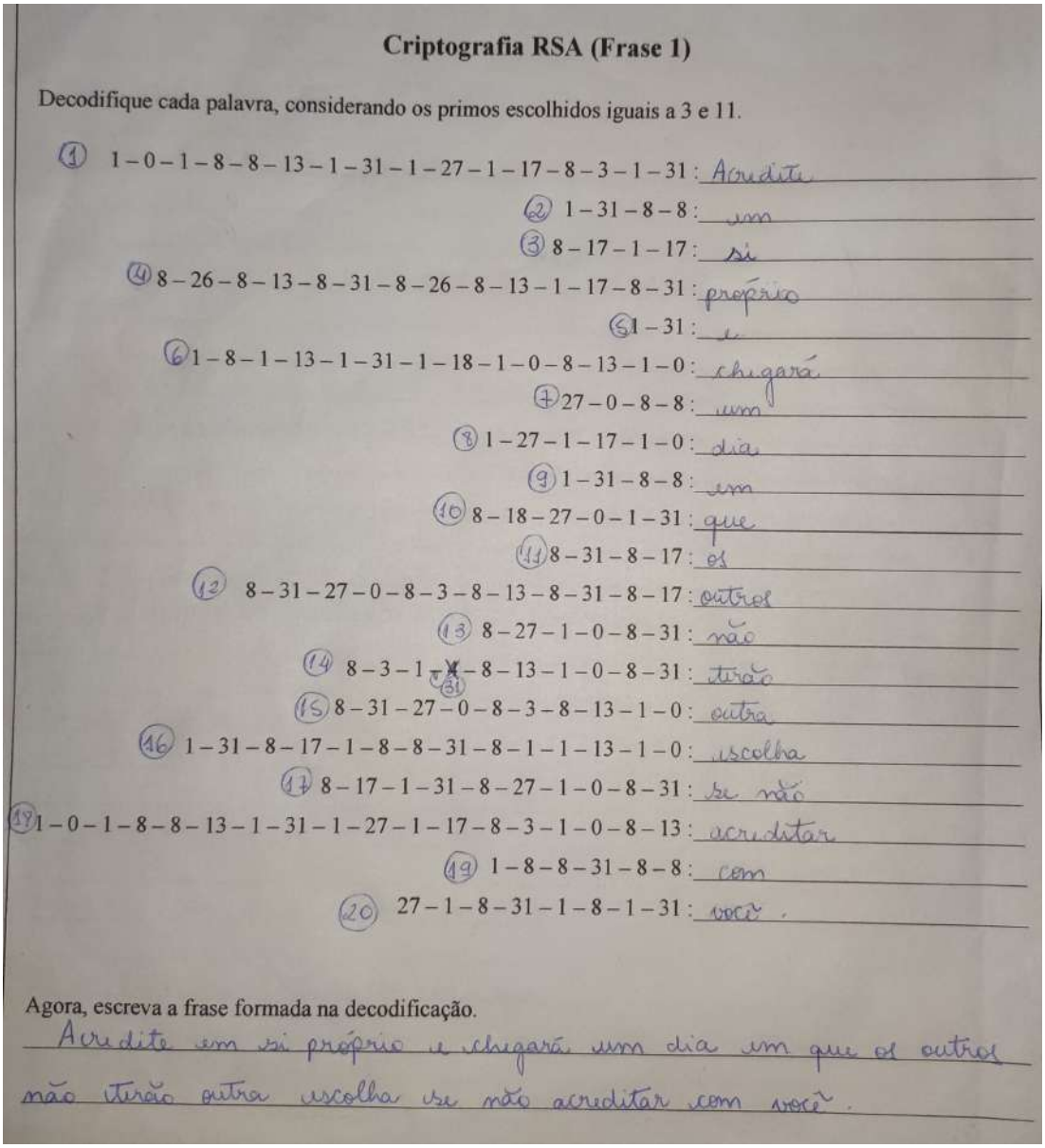
O objetivo dessa aula é firmar a compreensão dos educandos a respeito do desenvolvimento do algoritmo de decodificação e com isso levar os educandos a fortalecer os conceitos básicos da matemática envolvidos nesses cálculos.

Quando um grupo entregava a folha com a "Frase 1" decodificada e pegava a folha com a "Frase 2", eles conseguiam realizar a decodificação dessa segunda frase sem o auxilio do professor.

A maioria dos grupos conseguiu finalizar a decodificação das duas frases nessa aula e o restante que não conseguiu finalizar a atividade em sala, foi proposto para finalizarem em casa e entregar a atividade completa na próxima aula.

A Figura 17 abaixo, apresenta a imagem da atividade da "Frase 1" de um dos grupos de educandos. Essa imagem foi escolhida para mostrar a organização criada pelos educandos e expor o erro de digitação encontrada por eles.

Figura 17 – Folha da atividade 1 de um dos grupos de educandos.



Criptografia RSA (Frase 1)

Decodifique cada palavra, considerando os primos escolhidos iguais a 3 e 11.

① 1 – 0 – 1 – 8 – 8 – 13 – 1 – 31 – 1 – 27 – 1 – 17 – 8 – 3 – 1 – 31 : Acredite
② 1 – 31 – 8 – 8 : em
③ 8 – 17 – 1 – 17 : si
④ 8 – 26 – 8 – 13 – 8 – 31 – 8 – 26 – 8 – 13 – 1 – 17 – 8 – 31 : próprio
⑤ 1 – 31 : e
⑥ 1 – 8 – 1 – 13 – 1 – 31 – 1 – 18 – 1 – 0 – 8 – 13 – 1 – 0 : chegará
⑦ 27 – 0 – 8 – 8 : um
⑧ 1 – 27 – 1 – 17 – 1 – 0 : dia
⑨ 1 – 31 – 8 – 8 : em
⑩ 8 – 18 – 27 – 0 – 1 – 31 : que
⑪ 8 – 31 – 8 – 17 : os
⑫ 8 – 31 – 27 – 0 – 8 – 3 – 8 – 13 – 8 – 31 – 8 – 17 : outros
⑬ 8 – 27 – 1 – 0 – 8 – 31 : não
⑭ 8 – 3 – 1 – ~~X~~ 31 – 8 – 13 – 1 – 0 – 8 – 31 : terão
⑮ 8 – 31 – 27 – 0 – 8 – 3 – 8 – 13 – 1 – 0 : outra
⑯ 1 – 31 – 8 – 17 – 1 – 8 – 8 – 31 – 8 – 1 – 1 – 13 – 1 – 0 : escolha
⑰ 8 – 17 – 1 – 31 – 8 – 27 – 1 – 0 – 8 – 31 : se não
⑱ 1 – 0 – 1 – 8 – 8 – 13 – 1 – 31 – 1 – 27 – 1 – 17 – 8 – 3 – 1 – 0 – 8 – 13 : acreditar
⑲ 1 – 8 – 8 – 31 – 8 – 8 : com
⑳ 27 – 1 – 8 – 31 – 1 – 8 – 1 – 31 : você .

Agora, escreva a frase formada na decodificação.

Acredite em si próprio e chegará um dia em que os outros não terão outra escolha se não acreditar com você.

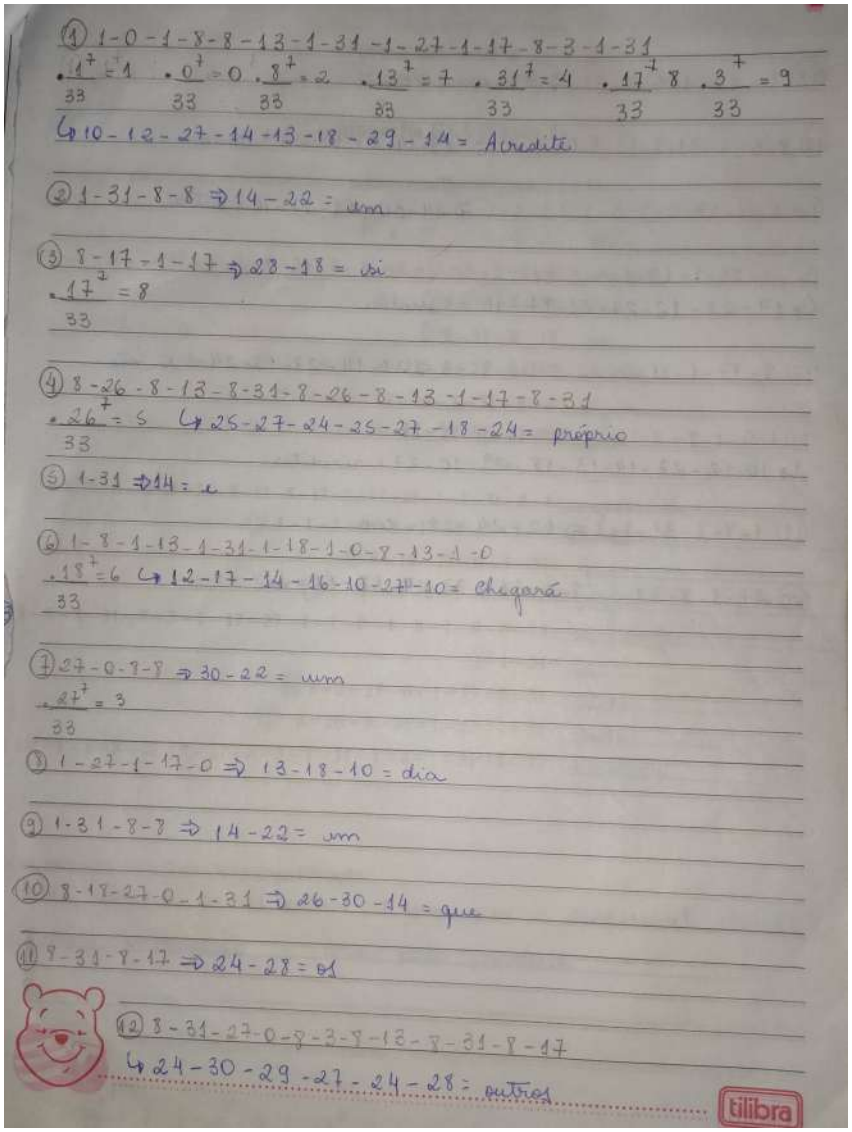
Fonte: Produzida pelo autor.

Na Figura 17 é possível observar a organização do grupo para decodificarem, eles numeraram cada uma das palavras. Tem também um número riscado e marcado em baixo na décima quarta palavra, pois o código riscado estava errado e os educandos identificaram qual código era o correto analisando as palavras já decodificadas (A atividade presente do Apêndice D já foi essa realizada a correção). Esse erro se deu na digitação da atividade e se mostrou interessante, pois os educandos tiveram que raciocinar a respeito do código e da palavra decodificada para perceberem que se tratava de um erro de e assim conseguirem encontrar qual deveria ser o código correto para dar sentido a frase.

Nas Figuras 18 e 19 abaixo, apresentaremos as duas folhas de anotações do grupo da

Figura 17, onde é possível observar o desenvolvimento dessa atividade de decodificação.

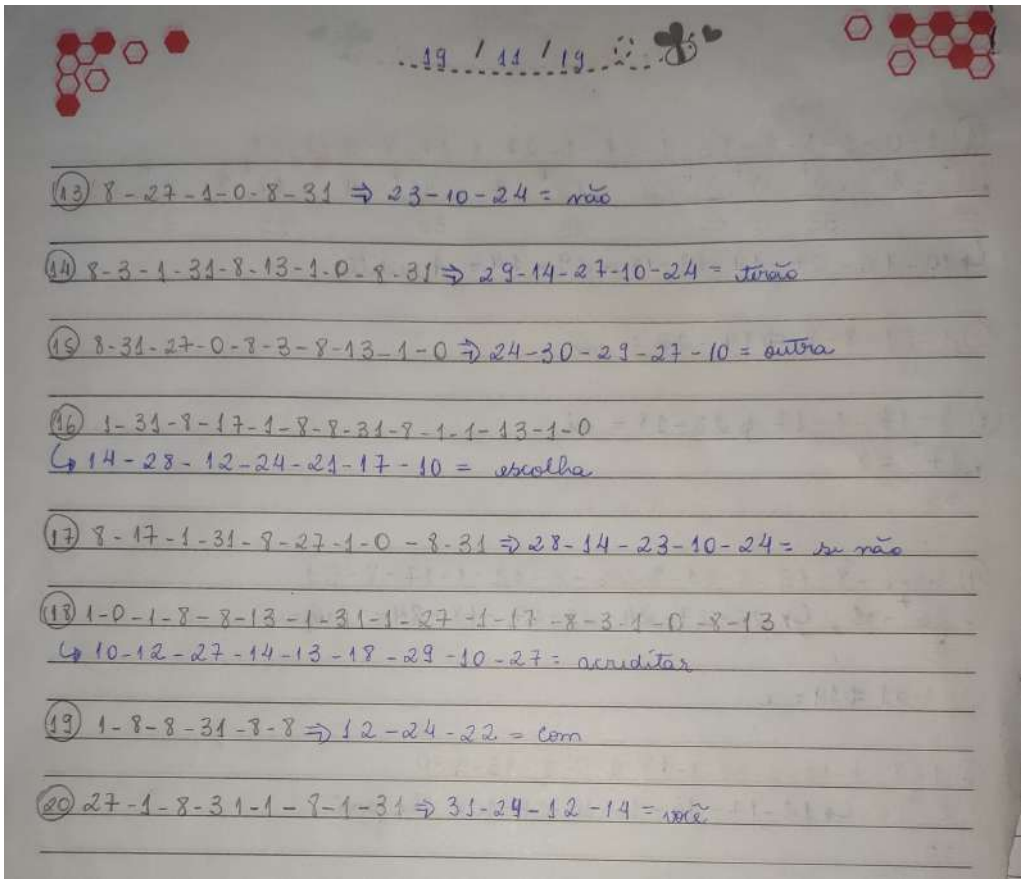
Figura 18 – Anotações de um dos grupos relacionado aos cálculos da atividade.



Fonte: Produzida pelo autor.

A Figura 18 mostra que na primeira palavra foram realizados sete cálculos e na palavra seguinte nenhum cálculo, pois já haviam calculado o código que precisavam e notaram que os códigos da palavra seguinte eram iguais.

Figura 19 – Verso da folha das anotações da figura anterior.

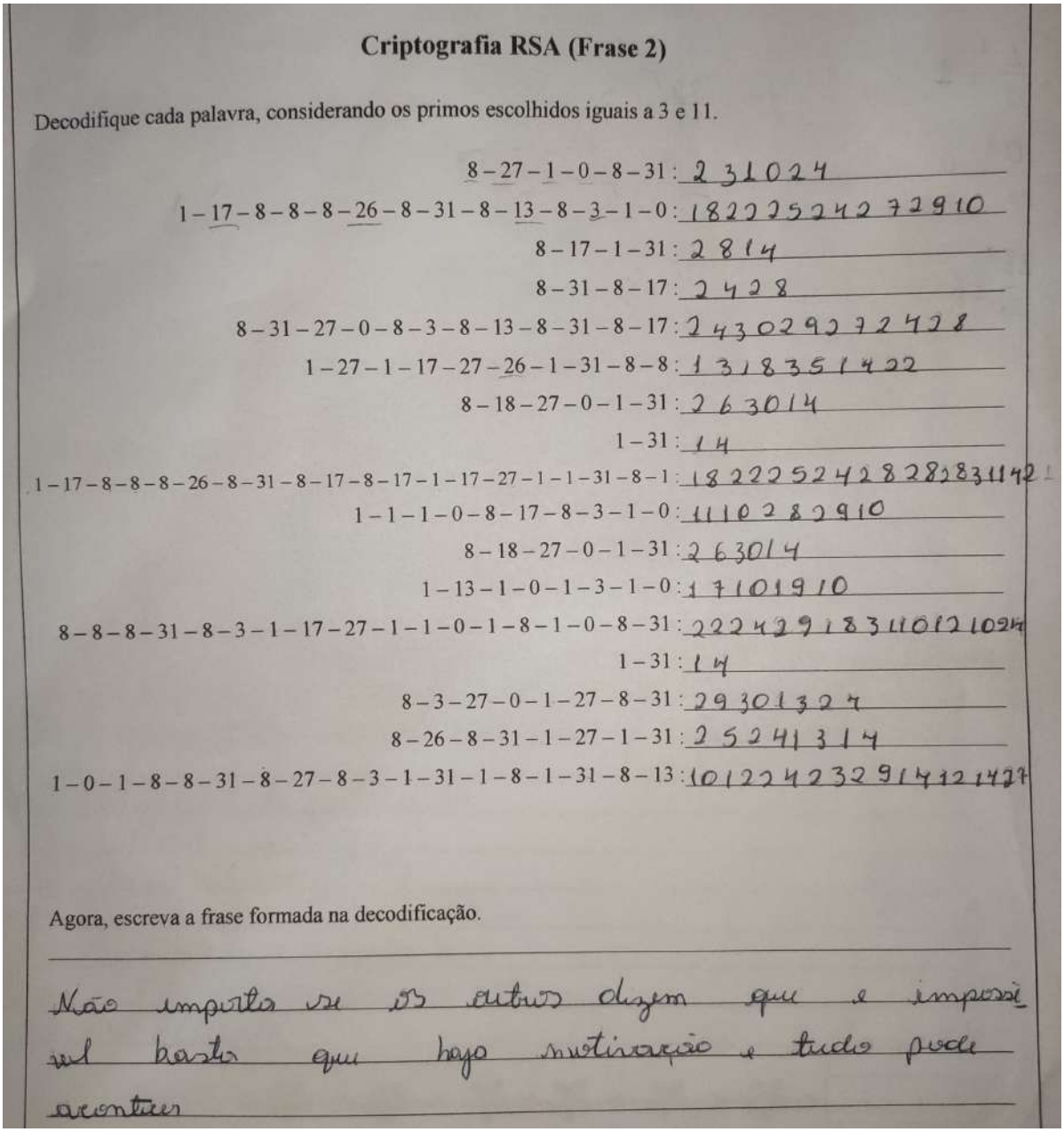


Fonte: Produzida pelo autor.

Podemos notar o que foi dito anteriormente, os educandos perceberam que os cálculos se repetem e então é necessário calcular uma única vez o resto da divisão da potência de cada bloco elevado ao expoente sete pela chave de decodificação, como explicado no algoritmo de decodificação da seção 3.2.

Na Figura 20 abaixo, observamos a atividade da folha da "Frase 2" de outro grupo que seguiram outra organização, mas chegaram ao mesmo objetivo que era de decodificar a frase.

Figura 20 – Folha da atividade 2 de um outro grupo de educandos.



Criptografia RSA (Frase 2)

Decodifique cada palavra, considerando os primos escolhidos iguais a 3 e 11.

8 – 27 – 1 – 0 – 8 – 31 : 2 31024

1 – 17 – 8 – 8 – 8 – 26 – 8 – 31 – 8 – 13 – 8 – 3 – 1 – 0 : 18222524272910

8 – 17 – 1 – 31 : 2814

8 – 31 – 8 – 17 : 2428

8 – 31 – 27 – 0 – 8 – 3 – 8 – 13 – 8 – 31 – 8 – 17 : 2430292724228

1 – 27 – 1 – 17 – 27 – 26 – 1 – 31 – 8 – 8 : 1318351422

8 – 18 – 27 – 0 – 1 – 31 : 263014

1 – 31 : 14

1 – 17 – 8 – 8 – 8 – 26 – 8 – 31 – 8 – 17 – 8 – 17 – 1 – 17 – 27 – 1 – 1 – 31 – 8 – 1 : 18222524282828311421

1 – 1 – 1 – 0 – 8 – 17 – 8 – 3 – 1 – 0 : 1110282910

8 – 18 – 27 – 0 – 1 – 31 : 263014

1 – 13 – 1 – 0 – 1 – 3 – 1 – 0 : 17101910

8 – 8 – 8 – 31 – 8 – 3 – 1 – 17 – 27 – 1 – 1 – 0 – 1 – 8 – 1 – 0 – 8 – 31 : 22242918311012102414

1 – 31 : 14

8 – 3 – 27 – 0 – 1 – 27 – 8 – 31 : 29301324

8 – 26 – 8 – 31 – 1 – 27 – 1 – 31 : 25241314

1 – 0 – 1 – 8 – 8 – 31 – 8 – 27 – 8 – 3 – 1 – 31 – 1 – 8 – 1 – 31 – 8 – 13 : 10122423291412141427

Agora, escreva a frase formada na decodificação.

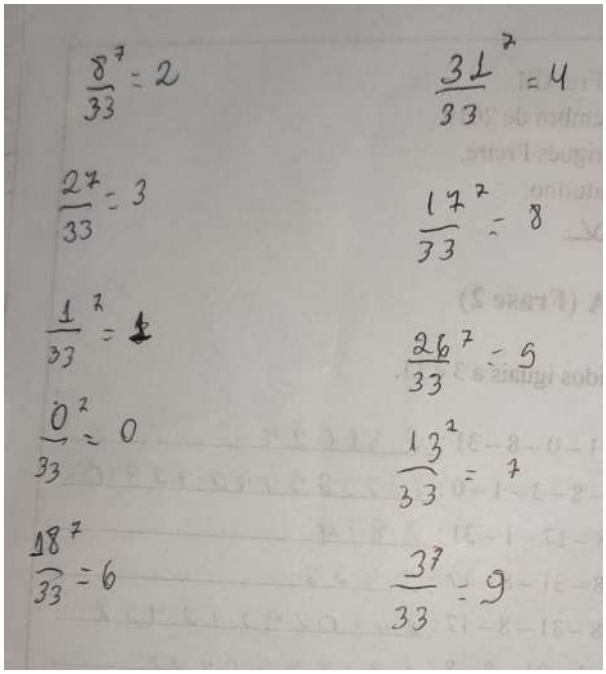
Não importa se os outros dizem que é impossível basta que haja motivação e tudo pode acontecer

Fonte: Produzida pelo autor.

Esse grupo anotou na linha de frente a cada código, o código encontrado após os cálculos matemáticos e que ainda precisam ser desvendados utilizando a tabela do alfabeto cifrado, que contém uma relação entre letras e números que são necessárias para a realização da pré-codificação inicial.

Veja na Figura 21 as anotações que esse grupo fez no verso da folha. Elas nos remetem a compreensão de que eles também notaram que os cálculos se repetiam e esse grupo, assim como vários outros, anotavam os restos das divisões das potências pela chave de codificação com uma igualdade.

Figura 21 – Anotações da atividade 2 do grupo da figura anterior.



Fonte: Produzida pelo autor.

Podemos então considerar que o objetivo dessa aula foi alcançado, devido ao sucesso dos grupos em conseguirem decodificar as frases propostas.

Nesta aula houve poucas dúvidas por parte dos educandos. Eles apresentaram autonomia no desenvolvimento do algoritmo de decodificação. Julgamos que essa autonomia dos educandos se deu devido aos cálculos do algoritmo da decodificação serem semelhantes aos do algoritmo da codificação, já trabalhados nas aulas anteriores.

4.2.7 Sétima aula

Foi iniciada com uma discussão a respeito dos erros e das dúvidas apresentadas pelos educandos na última atividade. Na atividade da folha da "Frase 1" foi onde apareceram a maioria dos erros. Já na folha da "Frase 2" não apareceram erros, pois realizamos a correção dos erros junto aos educandos quando eles terminavam a primeira frase e nos entregavam. Mesmo havendo esse momento de correção com cada um dos grupos, foi importante iniciarmos essa sétima aula com essas discussões, para que os educandos relembrassem do desenvolvimento dos algoritmos da Criptografia RSA trabalhados nas últimas aulas, o de codificar e o de decodificar.

Após esse momento de discussões, propomos a atividade dessa aula, que consiste em todos os grupos criar uma frase e a codificar usando a chave de codificação do exemplo utilizado na terceira aula (lembrando que essa chave foi o número 33, formado pelos primos 3 e 11).

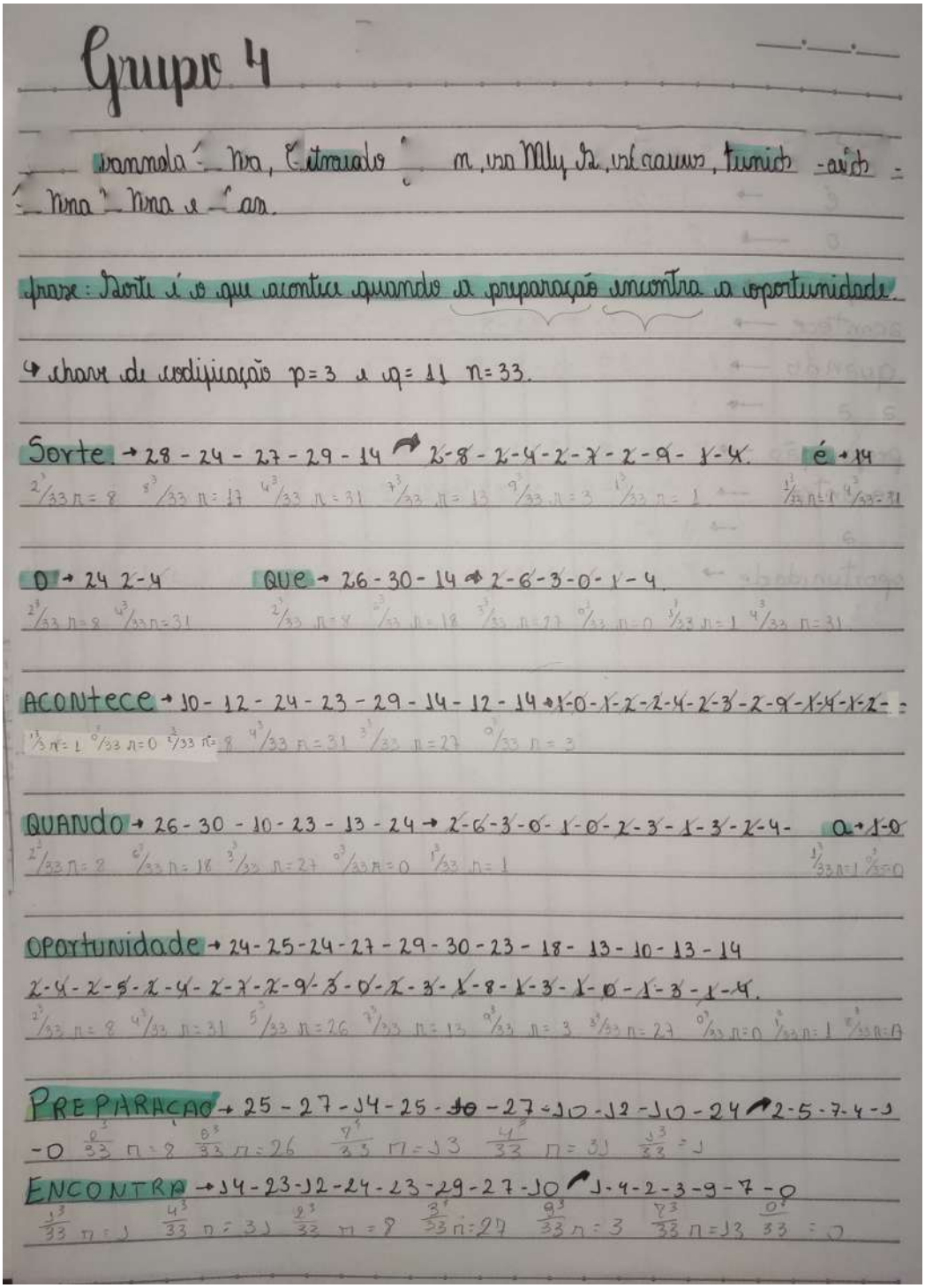
Passamos a instrução para que os grupos não trocassem informações a respeito da frase escolhida, pois na próxima aula o desafio seria de um grupo decodificar a mensagem de outro. Visando o tempo de aula, a criação da frase foi limitada em no mínimo dez e no máximo quinze palavras. Nessa atividade também foi autorizado a utilização de calculadoras e ficou liberada a consulta das atividades anteriores.

O objetivo dessa aula é, por meio do algoritmo de codificação, levar os educandos a praticarem os conceitos matemáticos básicos envolvidos e com isso firmar a compreensão dos mesmos.

Os educandos pouco solicitaram a ajuda do professor no desenvolvimento dessa atividade, isso se deu devido à consulta nas atividades já realizadas, pois conseguimos ouvir, nas discussões que ocorriam entre os integrantes dos grupos, frases como "Você não lembra que fazia assim?", "É assim, agora lembrei.", "Olha aqui no meu caderno. Está certo como estamos fazendo." entre outras.

Nas Figuras 22 e 23 a seguir, temos as fotos dessa atividade de um dos grupos para que o leitor possa observar a organização criada pelos educandos para realizarem a codificação. Os nomes dos integrantes dos grupos foram apagados para colocarmos a foto da folha completa.

Figura 22 – Anotações da codificação de uma frase criada pelo grupo.



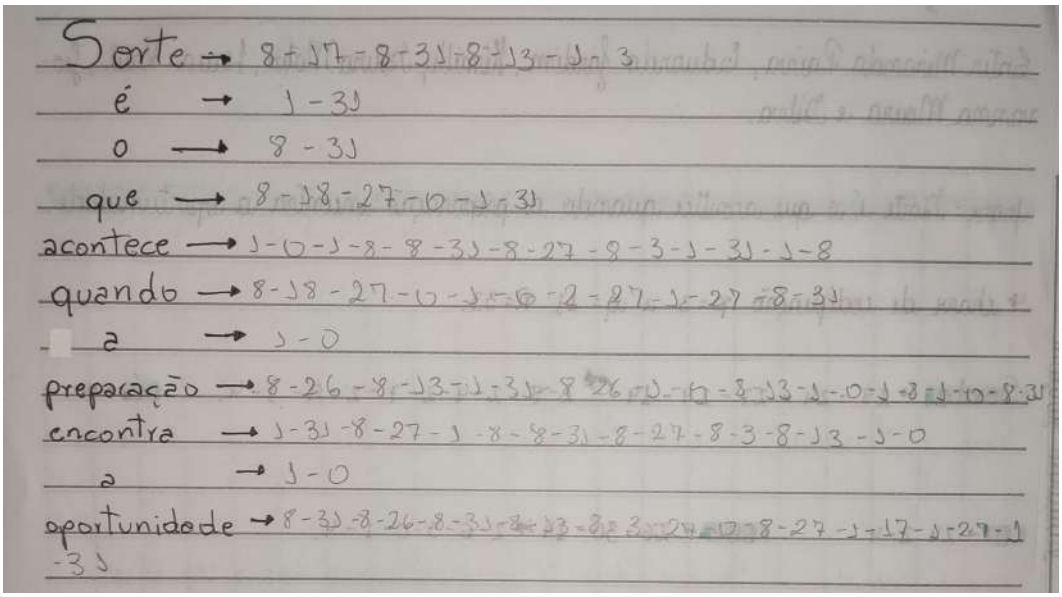
Fonte: Produzida pelo autor.

Podemos notar na Figura 22 que primeiro o grupo separou as palavras e realizou a pré-codificação, seguindo tabela do alfabeto cifrado. Feito isso eles escreveram para cada uma das palavras as razões das potências dos blocos unitários pela chave de codificação, sem repetir blocos da mesma palavra, e na frente os restos dessas razões, representando com a letra "r". Os cálculos do algoritmo da divisão não aparecem na folha, pois assim como vários outros grupos,

eles fizeram esses cálculos em folhas de rascunho e não entregaram ao professor junto com a atividade.

A Figura 23 abaixo é o verso da folha da Figura 22 e contém os códigos da codificação da frase proposta.

Figura 23 – Códigos criados na atividade da figura anterior.



Fonte: Produzida pelo autor.

Visto que todos os grupos conseguiram realizar a atividade no tempo da aula, sendo recolhidas as folhas com os códigos criados pelos grupos ao final da aula, podemos concluir que o objetivo dessa aula foi alcançado e que os educandos realmente compreenderam os processos matemáticos do algoritmo de codificação, pois corrigimos os códigos e não encontramos erros.

4.2.8 Oitava aula

Foi dedicada para que cada grupo decodificasse a mensagem criada por outro na atividade da aula anterior. Iniciamos distribuindo as folhas com os códigos, atentando-se para não entregar o código criado por um grupo para ele mesmo. As únicas instruções que foram passadas aos grupos é que deveriam decodificar a mensagem nessa aula, poderiam consultar as atividades anteriores, usar a calculadora para auxiliar nos cálculos e que não era permitido que os grupos se comunicassem a respeito da frase.

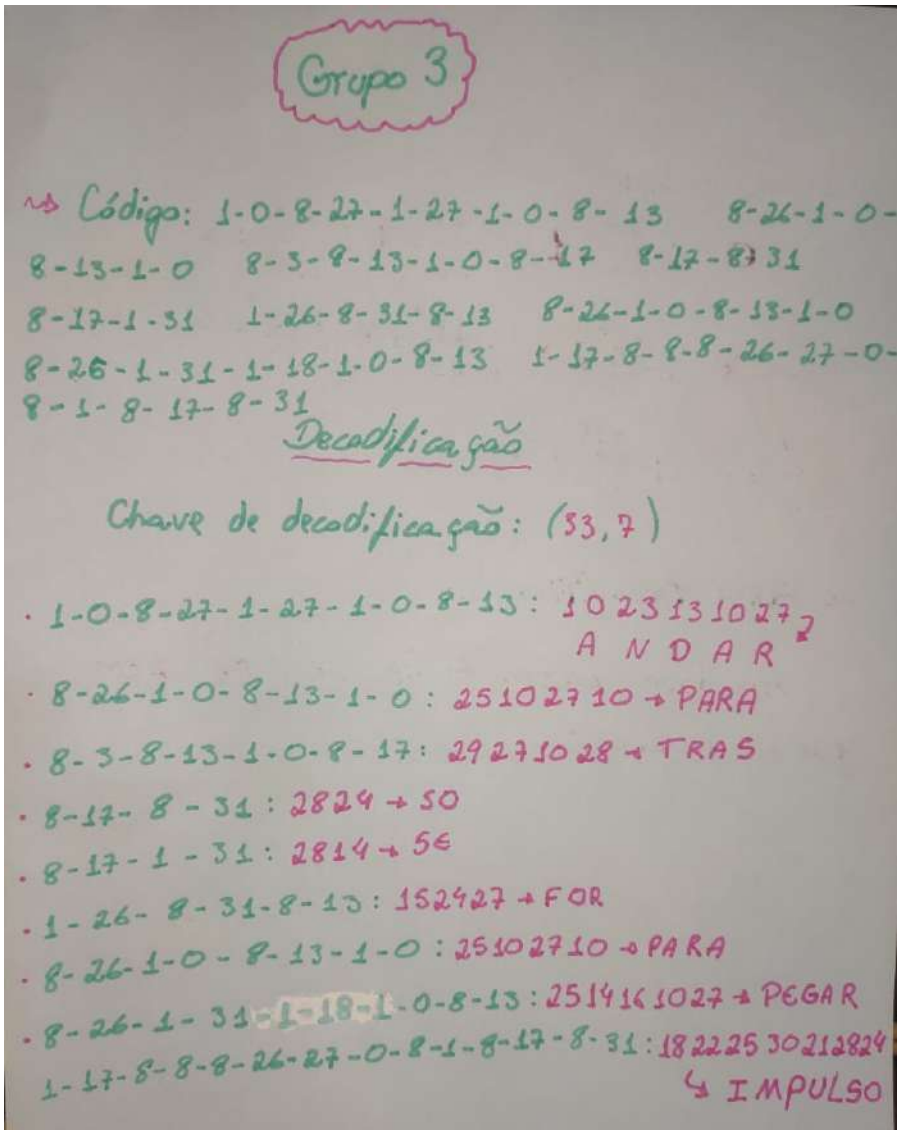
O objetivo dessa aula é, por meio do algoritmo de decodificação, fazer com que os educandos pratiquem os conceitos matemáticos básicos envolvidos nesse algoritmo e com isso potencializar a compreensão desses conceitos.

O desenvolvimento dessa atividade em sala de aula foi satisfatório, devido ao interesse demonstrado pelos educandos. Observamos que eles se focaram em realizarem os cálculos do algoritmo de decodificação e não buscaram comunicação entre os grupos visando obter informações a respeito da frase codificada.

Os educandos não apresentaram muitas dificuldades no desenvolvimento dessa atividade. Houve apenas alguns grupos que solicitaram a presença do professor, mas os erros que ainda apresentavam eram erros matemáticos, tinham errado cálculos no algoritmo da divisão.

Podemos observar a atividade desenvolvida por um dos grupos dos educandos na Figura 24 a seguir.

Figura 24 – Anotações da última atividade de um dos grupos de educandos.



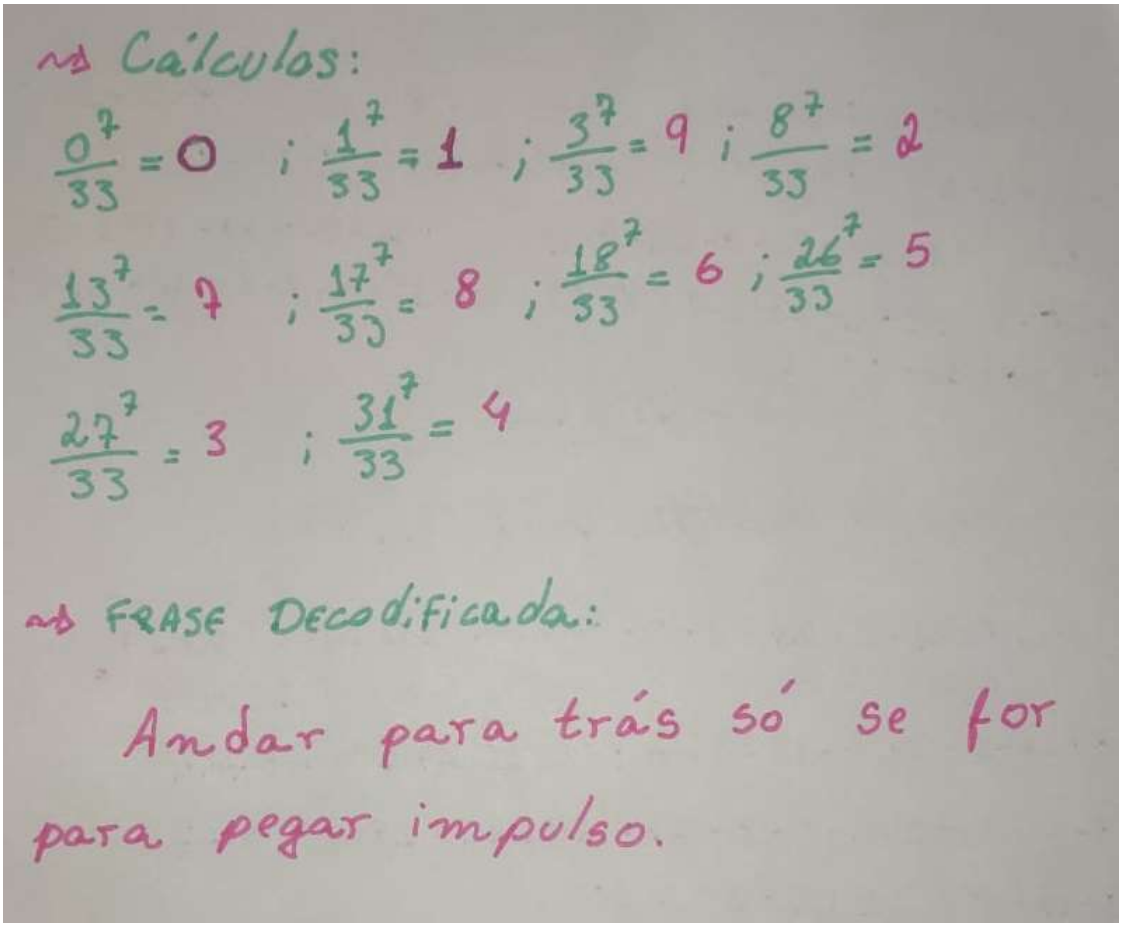
Fonte: Produzida pelo autor.

Na Figura 24, note que o grupo separou cada um dos códigos em uma linha, anotou na

frente de cada código a sua decodificação e por fim desfez a pré-codificação obedecendo a tabela do alfabeto cifrado.

A frase decodificada e os resultados dos cálculos da decodificação eles escreveram no verso da folha, como é possível ver na Figura 25 a seguir.

Figura 25 – Cálculos e frase decodificada do grupo da figura anterior.



Fonte: Produzida pelo autor.

Visto que todos os grupos conseguiram decodificar o código proposto a eles, podemos deduzir que o objetivo dessa aula, que era fazer com que os educandos praticassem os conceitos básicos da matemática envolvidos no algoritmo de decodificação, foi alcançado. E assim, ao final da aula, foi indagado aos educandos a respeito da segurança que a Criptografia RSA proporciona aos seus usuários e a respeito do aprendizado matemático que eles obtiveram após essas oito aulas.

5 CONSIDERAÇÕES FINAIS

Nesse capítulo serão apresentadas as considerações a respeito da criação e do desenvolvimento da Sequência Didática, voltada para educandos do 3º ano do Ensino Médio e que tem como tema central a Criptografia RSA.

Este trabalho teve como objetivo apresentar os conceitos matemáticos básicos de forma mais agradável, para instigar o interesse e a curiosidade por parte dos educandos. Para isso, optamos pelo uso da Criptografia RSA como uma ferramenta para viabilizar aos educandos uma melhor compreensão e fixação de conceitos matemáticos importantes e presentes nas matrizes curriculares.

O tema Criptografia RSA, além de contribuir para a fixação de conteúdos básicos da Matemática, possibilitou o desenvolvimento de importantes competências nos educandos, tais como: autonomia nas resoluções, raciocínio lógico e cooperativismo em trabalhos em grupo.

No planejamento da Sequência Didática nos deparamos com o seguinte problema: o tempo de aula seria curto para a realização de codificação e decodificação de frases longas. Percebemos que mesmo o algoritmo necessitando de apenas conceitos matemáticos básicos, os educandos levariam muito tempo para codificar ou decodificar uma mensagem grande, por exemplo, codificar um parágrafo de cinco linhas. Então, nesse momento, decidimos que proporíamos aos educandos a codificação e decodificação de frases curtas, com no máximo uma linha.

No entanto sentimos a necessidade de planejar aulas de codificação e decodificação de palavras antes de propor as frases aos educandos, pois eles precisariam compreender os algoritmos antes de utilizá-lo em uma frase.

O planejamento da Sequência Didática buscou assessorar os educandos na compreensão e execução dos algoritmos da Criptografia RSA e com isso potencializando o ensino, principalmente do conceito do algoritmo da divisão, pois esse conceito é de essencial importância a sua compreensão para a codificação e decodificação com os algoritmos da Criptografia RSA. Além da contribuição no ensino dos educandos, essa Sequência Didática conseguiu instigar e estimular os educandos no desenvolvimento da aula de Matemática.

O que nos dá força para chegarmos a esse entendimento é a análise das atividades desenvolvidas pelos educandos e suas falas e atitudes durante as aulas. Assim pudemos observar

que a grande maioria dos educandos se interessou pelo tema e sentiram desafiados a realizarem as codificações e decodificações, ou seja, com essa Sequência Didática conseguimos instigar a curiosidade e o interesse dos educandos em estudar Matemática.

Durante o desenvolvimento das atividades propostas em sala de aula, pudemos notar o aprendizado falho, de grande parte dos educandos, a respeito dos conteúdos matemáticos básicos abordados nessa Sequência Didática, principalmente do algoritmo da divisão, pois uma parte dos educandos apresentaram dificuldades nas codificações iniciais. No entanto essas dificuldades foram sendo sanadas e nas atividades finais foram poucos educandos que ainda apresentavam dificuldades. Visto que a procura pelo auxilio do professor foi pouca durante as últimas aulas de codificação e decodificação.

Assim sendo, a Sequência Didática elaborada demonstrou ter potencial para contribuir com o desenvolvimento de conceitos matemáticos básicos, como números primos, potenciação e algoritmo da divisão, e estimular a curiosidade e o interesse dos educandos pela disciplina de Matemática, pois conseguimos mostrar a eles que os conteúdos matemáticos, mesmo considerados básicos, são sim de extrema importância no cotidiano em que vivemos.

REFERÊNCIAS

APLICADA, I. de Matemática Pura e. **Descoberto número primo com quase 25 milhões de dígitos**. 2019. Disponível em: <https://impa.br/noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/>. Acesso em: 23 out. 2019.

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

BONFIM, D. H. **Criptografia RSA**. 91 p. Dissertação (Programa de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional) — Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2017.

CAVALCANTE, A. L. B. Teoria dos números e criptografia. **Revista de Informática**, n. 01, p. 1–7, 2005.

CHANNEL, H. **Luta contra os hackers**. 18 ago. 2014. Disponível em: <https://blog.corujadeti.com.br/>. Acesso em: 07 out. 2019.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2014.

____. **Criptografia**. 1. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2015.

FREITAS, O. **Equipamentos e materiais didáticos**. Brasília: Universidade de Brasília, 2009.

HEFEZ, A. **Aritmética**. 2. ed. Rio de Janeiro: SBM, 2016.

KAHN, D. **The Codebreakers**: The comprehensive history os secret. E.U.A.: Editora Scribner Book Company, 1996.

LIMA, E. L. **Análise Real**. 12. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2016. v. 1.

LOPES, A. O. Aula expositiva: superando o tradicional. in: Feltran, a. et al. **Técnicas de ensino: Por que não?**, Papirus Editora, v. 19, p. 37–50, 2013.

MACHADO, A. P. **Teoria dos números e Criptografia RSA**: uma proposta de ensino para alunos de matemática olímpica. 93 p. Dissertação (Programa de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal de Santa Maria, Santa Maria, 2018.

MIGUEL, J. C. Alfabetização matemática: implicações pedagógicas. In: **VIII Congresso estadual paulista sobre formação de educadores**. Águas de Lindóia, SP: [s.n.], 2005. p. 414–429.

MOURA, M. de O. **Criptografia motivando o estudo das funções no 9º ano do Ensino Fundamental**. 93 p. Dissertação (Programa de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal do Tocantins, Arraias, 2019.

OLGIN, C. de A. **Currículo no Ensino Médio**: uma experiência com o tema criptografia. 136 p. Dissertação (Programa de Pós - Graduação em Ensino de Ciências e Matemática) — Universidade Luterana do Brasil, Canoas, 2011.

OLIVEIRA, M. M. **Sequência didática interativa no processo de formação de professores**. Petrópolis, RJ: Vozes, 2013.

RIBENBOIM, P. **Números Primos**: mistérios e recordes. 1. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2001.

SILVA, E. G. da. **Criptografia RSA**: da teoria à aplicação em sala de aula. 68 p. Dissertação (Programa de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional) — Universidade de São Paulo, São Carlos, 2019.

SILVA, M. A. dos S. **Frações Contínuas**: uma aplicação em criptografia rsa. 90 p. Dissertação (Programa de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal de Sergipe, Itabaiana, 2019.

SILVA, M. R. G. da. Considerações sobre o trabalho em grupo na aula de matemática. In: **Mimesis**. Bauru: [s.n.], 1998. v. 19, n. 2, p. 135–145.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

ZABALA, A. **A prática educativa**: como ensinar. Porto Alegre: Artmed, 1998.

APÊNDICE A – PLANOS DE AULAS

1ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Criptografia

Objetivos

Levar o educando a:

- Compreender o que é Criptografia;
- Identificar algum tipo de Criptografia usado por eles em brincadeiras;
- Conhecer a importância atualmente da Criptografia RSA.

Procedimentos

A aula inicia com a apresentação de slides (Apêndice B1) a respeito do conteúdo abordado. O primeiro slide mostra com três perguntas: “Você já ouviu falar sobre Criptografia?”, “Sabe para que serve?” e “Conhece alguma forma de Criptografia?”. Essas perguntas tem o intuito de identificar os conhecimentos prévios dos educandos a respeito do tema. Nesse momento procuraremos identificar alguma brincadeira vivenciada por eles que se utiliza de códigos criptográficos, como por exemplo, a língua do P (consiste na introdução da consoante P seguida pela vogal prévia). Feito isso, apresentaremos um pouco da história da Criptografia, desde seu surgimento até os dias atuais, mostrando dois métodos criptográficos (Cítala Espartana e Cifra de César). Explanaremos, a partir dos métodos mostrados, a evolução das técnicas de criptografar até chegarmos às máquinas criptográficas. Falaremos de duas (Enigma e Colossus), mostrando suas importâncias históricas e influencias nos códigos atuais. Agora apresentaremos um vídeo de 5 minutos e 11 segundos que discorre a respeito da Criptografia RSA. Após o vídeo faremos um momento de discussão, abrindo espaço para que os educandos façam perguntas a respeito do

que acabaram de assistir. E então o slide apresentará quais conteúdos matemáticos básicos que são essenciais para o desenvolvimento dos algoritmos da Criptografia RSA. E no momento final dessa aula, serão expostas informações a respeito da sequência didática que está sendo proposta a eles.

Recursos

- Notebook;
- Televisão;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões a respeito do tema.

Referências Bibliográficas

BONFIM, D. H. **Criptografia RSA**. 91 p. Dissertação (Programa de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional) — Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2017.

OLGIN, C. de A. **Currículo no Ensino Médio**: uma experiência com o tema criptografia. 136 p. Dissertação (Programa de Pós - Graduação em Ensino de Ciências e Matemática) - Universidade Luterana do Brasil, Canoas, 2011.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

2ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Números primos;
- Potenciação;
- Divisão de números naturais.

Objetivos

Levar o educando a:

- Relembrar o conceito de números primos;
- Relembrar as propriedades de potenciação;
- Relembrar o algoritmo da divisão, encontrando quociente e restos.

Procedimentos

No primeiro momento abordaremos o conteúdo de números primos. Discorreremos sobre suas características e explanaremos a respeito da dificuldade de se encontrar um número primo muito grande. E então discutiremos a respeito de potências e suas propriedades, mostrando exemplos e propondo alguns exercícios de cálculos rápidos utilizando as propriedades de multiplicação de potências de mesma base e potência de potência. Por fim, explanaremos a respeito do algoritmo da divisão de dois números naturais, com o intuito encontrarmos o quociente e o resto nessas divisões. Proporemos ao final alguns exercícios que envolvam divisão de potencias por números inteiros, com o objetivo de calcular os restos das divisões, pois no desenvolvimento dos algoritmos da Criptografia RSA, nas próximas aulas, os educandos precisaram saber calcular os restos em divisões de potencias por números naturais.

Recursos

- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e suas resoluções dos exercícios propostos durante a aula.

Referências Bibliográficas

HEFEZ, A. **Aritmética**. 2. ed. Rio de Janeiro: SBM, 2016.

RIBENBOIM, P. **Números Primos**: mistérios e recordes. 1. ed. Rio de Janeiro: IMPA, 2001.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

3ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Algoritmo de codificação da Criptografia RSA.

Objetivos

Levar o educando a:

- Identificar a dificuldade na fatoração de números semiprimos;
- Conhecer melhor a Criptografia RSA;
- Utilizar o algoritmo para codificar uma palavra;
- Praticar conceitos básicos da matemática.

Procedimentos

No primeiro momento relembraremos o vídeo apresentado na primeira intervenção, relembrando a importância dos números primos para o desenvolvimento e segurança da Criptografia RSA. Em seguida mostraremos os seguintes números semiprimos: 119, 391 e 2257. E assim desafiaremos os educandos a encontrarem quais foram os primos multiplicados que resultaram nele. Após apresentarmos esse desafio, discorreremos a respeito do algoritmo de codificar da Criptografia RSA. Apresentaremos, através de um exemplo, o desenvolvimento do algoritmo passo a passo para codificar uma palavra. O exemplo apresentado é a codificação da palavra: Frei. Será usado os números primos 3 e 11 que formam a chave de codificação 33. O expoente da codificação será o número 3, devido a comum utilização desse número para codificar com esse algoritmo. Feito isso, será proposto aos educandos que formem grupos, de no máximo quatro pessoas, e sortearemos palavras selecionadas pelo educador para os grupos codificarem. O objetivo dessa primeira atividade é fazer com que os educandos entendam os processos do algoritmo da codificação, para assim conseguirem codificar frases completas, que será o objetivo da próxima intervenção.

Recursos

- Folhas de papel A4;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e se conseguiram codificar a palavra proposta durante a aula, buscando identificar suas possíveis dificuldades nos cálculos matemáticos.

Referências Bibliográficas

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

4ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Algoritmo de codificação da Criptografia RSA.

Objetivos

Levar o educando a:

- Utilizar o algoritmo para codificar uma frase;
- Praticar conceitos básicos da matemática.

Procedimentos

No primeiro momento relembraremos os passos do algoritmo da codificação utilizado na aula anterior. Em seguida proporemos que os educandos formem os mesmos grupos formados na ultima aula e distribuiremos frases, previamente selecionadas pelo educador, para cada um dos grupos. O intuito dessa atividade é que os educandos dividam a frase e cada integrante codifique algumas palavras, para assim formarem a frase e entregarem em uma folha ao final da aula. Para isso não fixamos a chave de codificação, ficou livre para cada grupo escolher os dois números primos e montarem sua chave de codificação. No momento final da aula, iremos recolher as folhas com os códigos e a identificação de cada grupo e será exposta a frente da turma cada um dos códigos.

Recursos

- Folhas de papel A4;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e se os grupos conseguiram codificar as frases propostas, buscando identificar suas possíveis dificuldades nos cálculos matemáticos apresentadas nas folhas que foram recolhidas.

Referências Bibliográficas

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

5ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Algoritmo de decodificação da Criptografia RSA.

Objetivos

Levar o educando a:

- Utilizar o algoritmo para decodificar um código;
- Praticar conceitos básicos da matemática.

Procedimentos

No primeiro momento será apresentado o código da Criptografia RSA formado no exemplo apresentado na terceira intervenção (que é o código: 1 – 26 – 8 – 13 – 1 – 31 – 1 – 17) e será perguntado aos educandos se eles conseguiriam supor que palavra esse código significa, com o intuito de demonstrar que um código não deixa pista de seu significado. Assim, apresentaremos o algoritmo de decodificação, realizando a decodificação do código previamente apresentado. Neste momento é importante lembrar-se de falar a respeito da escolha dos primos para a criação da chave de codificação, pois não é todos os primos que são possíveis calcular a chave de decodificação. Faremos os processos passo a passo. Inicialmente calcularemos a chave de decodificação, deixando claro que para isso é preciso saber os números primos escolhidos para a formação da chave de codificação. Feito isso mostraremos que o processo da decodificação é semelhante ao processo de codificação, realizando as mesmas operações, mas agora com outros números. E por fim, na parte final do algoritmo, encontraremos a palavra na linguagem formal, que é desfazer a pré-codificação dos blocos com dois algarismos. Após a execução do algoritmo de decodificação com o exemplo citado e esclarecimento das dúvidas que tenham surgido, proporemos aos educandos que formem os mesmo grupos das aulas anteriores e sortearemos alguns códigos para que os mesmos realizem as decodificações. Esses códigos representam palavras e pediremos que os grupos anotem os códigos, cálculos e a palavra decodificada em

uma folha, identificando o grupo, para que possa ser entregue ao final dessa aula para a correção e avaliação.

Recursos

- Folhas de papel A4;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e se os grupos conseguiram decodificar os códigos propostos, buscando identificar suas possíveis dificuldades nos cálculos matemáticos apresentadas nas folhas que foram recolhidas.

Referências Bibliográficas

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

6ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Algoritmo de decodificação da Criptografia RSA.

Objetivos

Levar o educando a:

- Utilizar o algoritmo para decodificar vários códigos;
- Praticar conceitos básicos da matemática.

Procedimentos

No primeiro momento relembraremos oralmente os processos do algoritmo da decodificação da Criptografia RSA utilizado a aula anterior. Feito isso proporemos que os educandos formem os grupos das ultimas aulas e distribuiremos uma folha (Apêndices B2 e B3) com vários códigos a cada grupo, objetivando novamente que cada grupo repartam esses códigos com o intuito de que cada educando do grupo decodifique ao menos um código. Falaremos qual foi os números primos escolhidos para a criação da chave de codificação para que cada grupo calcule a chave de decodificação, seguindo o raciocínio da aula anterior. Pediremos que cada grupo anote em uma folha os cálculos realizados na decodificação assim como a frase formada ao final. Essa folha será recolhida ao final da aula para ser corrigida e analisada.

Recursos

- Folhas de papel A4;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e se os grupos conseguiram decodificar os códigos propostos, buscando identificar suas possíveis dificuldades nos cálculos matemáticos apresentadas nas folhas que foram recolhidas.

Referências Bibliográficas

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

7ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Algoritmo de codificação da Criptografia RSA.

Objetivos

Levar o educando a:

- Utilizar o algoritmo para codificar uma frase;
- Praticar conceitos básicos da matemática.

Procedimentos

No primeiro momento discutiremos a respeito dos resultados da correção da atividade realizada na aula anterior, com o objetivo de sanar as dúvidas e eliminar os erros nas próximas atividades. Em seguida, proporemos que juntem os mesmos grupos das aulas anteriores, e proporemos que cada grupo crie uma mensagem e a codifiquem utilizando a chave de codificação que preferirem. Relembraremos da explicação da aula cinco do que se deve evitar na escolha dos números primos na codificação, para que seja possível decodificar a mensagem criada. O objetivo dessa atividade é verificar a compreensão do algoritmo de codificação. Ao final dessa aula será recolhida a folha com o código criado por cada grupo.

Recursos

- Folhas de papel A4;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e se os grupos realizaram a codificação da uma frase.

Referências Bibliográficas

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

8ª Intervenção

Turma: 3º ano do Ensino Médio.

Duração: uma aula de 45 minutos.

Conteúdo

- Algoritmo de decodificação da Criptografia RSA.

Objetivos

Levar o educando a:

- Utilizar o algoritmo para decodificar um código que representa uma frase;
- Praticar conceitos básicos da matemática.

Procedimentos

No primeiro momento pediremos aos educandos que formem os mesmos grupos das aulas anteriores. Distribuiremos para cada grupo um dos códigos criados na ultima aula, de modo que cada grupo pegue um código criado por outro grupo e pediremos sigilo aos grupos a respeito da frase inicial criada, informando apenas quais foram os números primos inicialmente escolhidos para a formação da chave de codificação. O objetivo dessa última atividade é verificar a compreensão do algoritmo de decodificação. Ao final dessa aula, recolheremos a folha da atividade proposta a cada grupo, contendo os cálculos realizados e a frase decodificada escrita na linguagem formal.

Recursos

- Folhas de papel A4;
- Quadro branco e pincel.

Avaliação

Será avaliada a participação e o interesse dos educandos durante as discussões e se os grupos realizaram a decodificação correta do código proposto.

Referências Bibliográficas

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida**. 1. ed. Rio de Janeiro: Record, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005.

APÊNDICE B – SLIDES

Criptografia

Professor: Tércio Rodrigues Freire

Criptografia

* Você já ouviu falar sobre Criptografia?

* Sabe para que serve?

* Conhece alguma forma de criptografar?

Criptografia na história

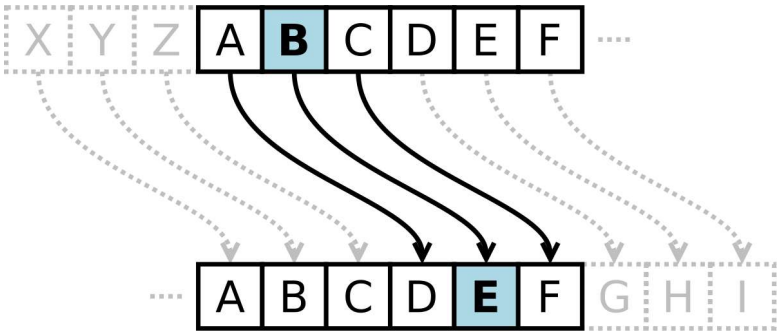
* Na evolução humana, sempre houve uma busca por meios eficazes para se comunicar.
* Os indícios são que a criptografia começou a ser usada no antigo Egito quando o faraó Amenemhet II governava, por volta de 1900 a.C.
* A Criptografia teria sido usada pelo arquiteto Khnumhotep II, com o intuito de dificultar que ladrões encontrassem os tesouros do faraó, realizando trocas de palavras importantes por símbolos nos documentos que indicavam a localização de tesouros.

Scytale ou Cítala Espartana

* Considerado por alguns historiadores como o primeiro aparelho criptográfico militar.

Cifra de César

* Utilizada pelo ditador da República Romana (de 49 a.C. a 44 a.C.) ***Caio Júlio César***.
* Essa cifra consiste em trocar cada letra da mensagem original pela terceira letra que a segue no alfabeto.



* Vamos criptografar um pouco?
* Utilizando a Cifra de César, como fica o código da mensagem:
  * **"Frei Gil é escola de vencedores!"**

Texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Texto simples	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

A mensagem criptografada é:

IUHL JLO H HVFROD GH YHQFHGRUHV

Outras cifras

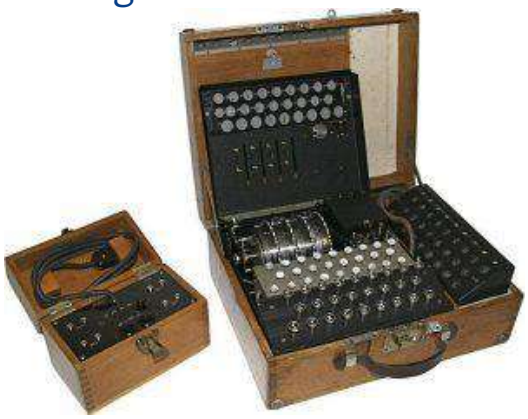
* Ao passar dos anos, obviamente houve diversas outras cifras utilizadas. Muitas se basearam na Cifra de César mas adicionaram alguma particularidade para dificultar sua descoberta.
* No entanto, houve também avanço no desvendar de tais cifras, como por exemplo, pesquisadores estudavam a frequência das letras em cada língua e assim descobriam o que cada código significava.

Frequência das letras

Letra	Francês	Espanhol	Italiano	Português
A	7.636%	12.53%	11.74%	14.63%
B	0.901%	1.42%	0.92%	1.04%
C	3.260%	4.68%	4.5%	3.88%
D	3.669%	5.86%	3.73%	4.99%
E	14.715%	13.68%	11.79%	12.57%
F	1.066%	0.69%	0.95%	1.02%
G	0.866%	1.01%	1.64%	1.30%
H	0.737%	0.70%	1.54%	1.28%
I	7.529%	6.25%	11.28%	6.18%
J	0.545%	0.44%	0.00%	0.40%
K	0.049%	0.01%	0.00%	0.02%
L	5.456%	4.97%	6.51%	2.78%
M	2.968%	3.15%	2.51%	4.74%
N	7.095%	6.71%	6.88%	5.05%
O	5.378%	8.68%	9.83%	10.73%
P	3.021%	2.51%	3.05%	2.52%
Q	1.362%	0.88%	0.51%	1.20%
R	6.553%	6.87%	6.37%	6.53%
S	7.948%	7.98%	4.98%	7.81%
T	7.244%	4.63%	5.62%	4.34%
U	6.311%	3.93%	3.01%	4.63%
V	1.628%	0.90%	2.10%	1.67%
W	0.114%	0.02%	0.00%	0.01%
X	0.387%	0.22%	0.00%	0.21%
Y	0.308%	0.90%	0.00%	0.01%
Z	0.136%	0.52%	0.49%	0.47%

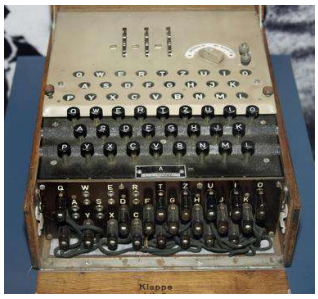
Máquina criptográfica

* Dando um pulo na história, vamos direto para o século XIX, por volta de 1918.
* É criada a ***ENIGMA***, considerada a primeira máquina eletromecânica de criptográfica.
* Foi elaborada pelo engenheiro alemão Arthur Scherbius, por volta de 1918.



Enigma

* Os militares alemães foram aperfeiçoando a Enigma, usando uma combinação maior de rotores e ligações elétricas.
* Isso fez com que as mensagens do exercito alemão, apesar de serem facilmente interceptadas, fossem indecifráveis e assim proporcionando vantagens táticas aos alemães durante a Segunda Guerra Mundial (1939 – 1949).



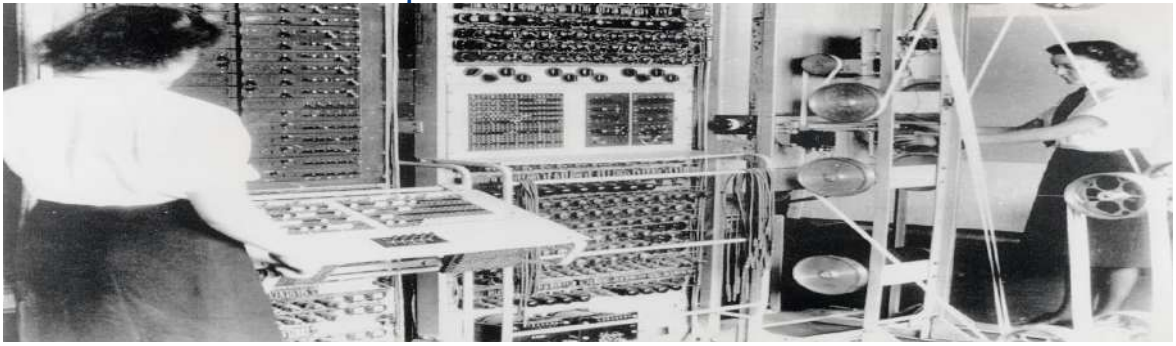

Klappe

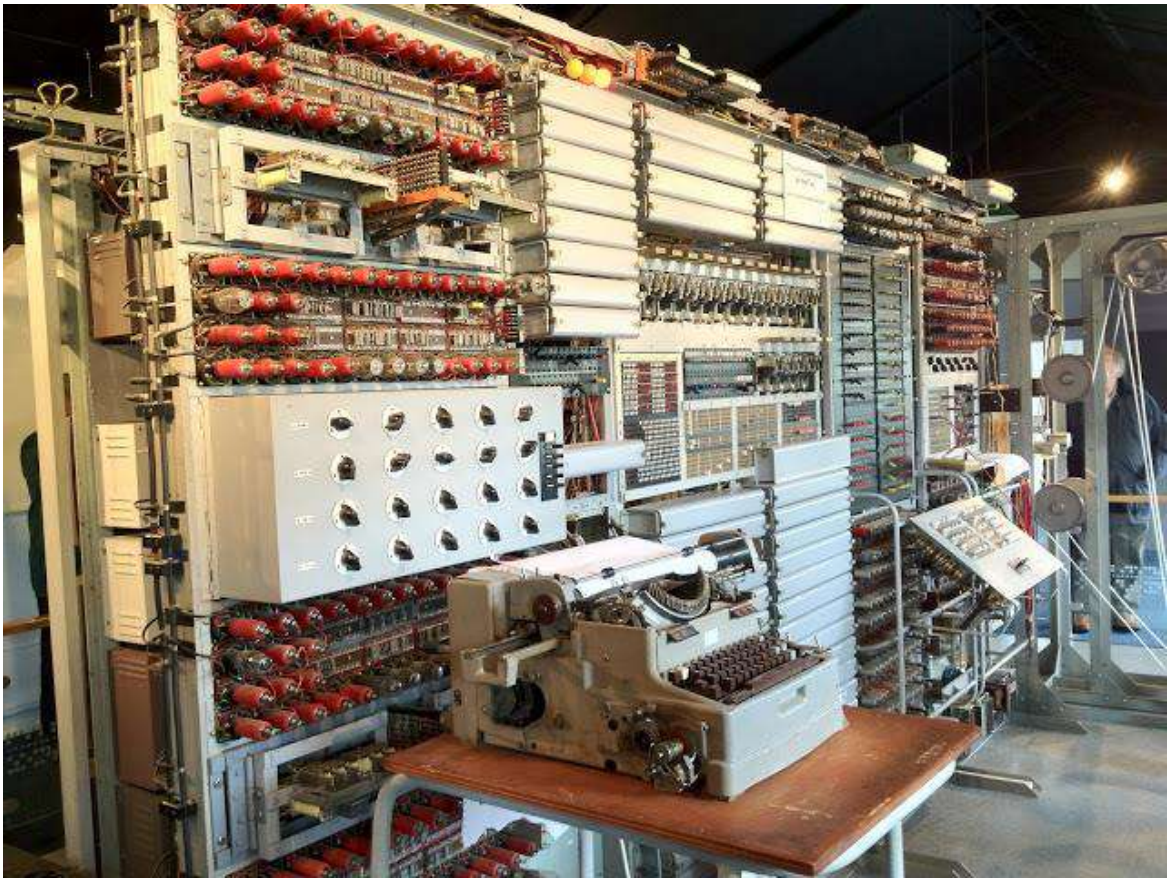

Zur Beachtung!

Colossus

* No ano de 1943, foi projetada a máquina ***Colossus***, pela equipe do engenheiro elétrico inglês Tommy Flowers.
* A Colossus possuía mais de 1700 válvulas e é conhecida como o primeiro computador eletrônico programável da história.
* E graças a Colossus os ingleses conseguiram decifrar os códigos ultrassecretos utilizados pelos nazistas.

* A máquina Colossus deu início a era moderna da criptografia, onde os computadores começam a ser programados com chaves de codificação muito mais complexas do que as utilizada pelas máquinas existentes na época.





E na atualidade?

* Você acredita que a criptografia é importante na sua vida?

* Vamos assistir um vídeo, que é uma parte de um documentário a respeito de Hackers.

* Nesse vídeo podemos entender melhor sobre a ***Criptografia RSA***, que é muito utilizada nos dias atuais.

Criptografia RSA

* Esse método de criptografar utiliza conhecimentos matemáticos como:

- ✓ Multiplicação;
- ✓ Divisão;
- ✓ Números primos;
- ✓ Potenciação;
- ✓ Entre outros.

Trabalho

* Serão esses conteúdos que revisaremos nas próximas aulas com o intuito de conseguirmos codificar e descodificar mensagens simples com a ***Criptografia RSA***.

* Vale lembrar que esse trabalho que estou propondo, faremos em sala de aula e valerá uma nota das três do 4° Bimestre.
* Para mais informações, aguardem as próximas aulas!

APÊNDICE C – ATIVIDADE DE DECODIFICAÇÃO DE UMA PALAVRA

Códigos para serem cortados e sorteados um para cada grupo:

A. 1-8-8-31-8-13-1-0-1-18-1-31-8-8
B. 1-31-8-17-1-26-8-31-8-13-1-8-8-31
C. 8-17-27-0-1-1-8-1-1-17-8-8-1-31
D. 1-8-8-31-8-13-1-27-1-17-1-0-8-1
E. 1-0-27-27-1-17-8-31-8-8-1-0
F. 1-0-1-8-1-31-8-27-8-3-8-31
G. 1-0-8-17-8-26-1-31-1-8-8-3-8-31
H. 8-1-1-31-1-18-1-0-1-27-8-31
I. 1-0-8-1-8-8-1-31-1-3-1-0-8-13
J. 1-31-27-27-1-8-1-31-8-3-8-31

Para o professor, código com seus significados:

A. 1-8-8-31-8-13-1-0-1-18-1-31-8-8 = Coragem
B. 1-31-8-17-1-26-8-31-8-13-1-8-8-31 = Esforço
C. 8-17-27-0-1-1-8-1-1-17-8-8-1-31 = Sublime
D. 1-8-8-31-8-13-1-27-1-17-1-0-8-1 = Cordial
E. 1-0-27-27-1-17-8-31-8-8-1-0 = Axioma
F. 1-0-1-8-1-31-8-27-8-3-8-31 = Acento
G. 1-0-8-17-8-26-1-31-1-8-8-3-8-31 = Aspecto
H. 8-1-1-31-1-18-1-0-1-27-8-31 = Legado
I. 1-0-8-1-8-8-1-31-1-3-1-0-8-13 = Almejar
J. 1-31-27-27-1-8-1-31-8-3-8-31 = Exceto

APÊNDICE D – ATIVIDADES DE DECODIFICAÇÃO DE FRASE

Centro de Ensino Frei Gil.
Estreito, _____ de Novembro de 2019.
Professor: Tércio Rodrigues Freire.
Série: 3º ano Matutino.
Grupo: _____

Criptografia RSA (Frase 1)

Decodifique cada palavra, considerando os primos escolhidos iguais a 3 e 11.

1 – 0 – 1 – 8 – 8 – 13 – 1 – 31 – 1 – 27 – 1 – 17 – 8 – 3 – 1 – 31 :_____

1 – 31 – 8 – 8 :_____

8 – 17 – 1 – 17 :_____

8 – 26 – 8 – 13 – 8 – 31 – 8 – 26 – 8 – 13 – 1 – 17 – 8 – 31 :_____

1 – 31 :_____

1 – 8 – 1 – 13 – 1 – 31 – 1 – 18 – 1 – 0 – 8 – 13 – 1 – 0 :_____

27 – 0 – 8 – 8 :_____

1 – 27 – 1 – 17 – 1 – 0 :_____

1 – 31 – 8 – 8 :_____

8 – 18 – 27 – 0 – 1 – 31 :_____

8 – 31 – 8 – 17 :_____

8 – 31 – 27 – 0 – 8 – 3 – 8 – 13 – 8 – 31 – 8 – 17 :_____

8 – 27 – 1 – 0 – 8 – 31 :_____

8 – 3 – 1 – 31 – 8 – 13 – 1 – 0 – 8 – 31 :_____

8 – 31 – 27 – 0 – 8 – 3 – 8 – 13 – 1 – 0 :_____

1 – 31 – 8 – 17 – 1 – 8 – 8 – 31 – 8 – 1 – 1 – 13 – 1 – 0 :_____

8 – 17 – 1 – 31 – 8 – 27 – 1 – 0 – 8 – 31 :_____

1 – 0 – 1 – 8 – 8 – 13 – 1 – 31 – 1 – 27 – 1 – 17 – 8 – 3 – 1 – 0 – 8 – 13 :_____

1 – 8 – 8 – 31 – 8 – 8 :_____

27 – 1 – 8 – 31 – 1 – 8 – 1 – 31 :_____

Agora, escreva a frase formada na decodificação.

_____

_____

_____

_____

Centro de Ensino Frei Gil.
Estreito, _____ de Novembro de 2019.
Professor: Tércio Rodrigues Freire.
Série: 3º ano Matutino.
Grupo: _____

Criptografia RSA (Frase 2)

Decodifique cada palavra, considerando os primos escolhidos iguais a 3 e 11.

8 – 27 – 1 – 0 – 8 – 31 :_____

1 – 17 – 8 – 8 – 8 – 26 – 8 – 31 – 8 – 13 – 8 – 3 – 1 – 0 :_____

8 – 17 – 1 – 31 :_____

8 – 31 – 8 – 17 :_____

8 – 31 – 27 – 0 – 8 – 3 – 8 – 13 – 8 – 31 – 8 – 17 :_____

1 – 27 – 1 – 17 – 27 – 26 – 1 – 31 – 8 – 8 :_____

8 – 18 – 27 – 0 – 1 – 31 :_____

1 – 31 :_____

1 – 17 – 8 – 8 – 8 – 26 – 8 – 31 – 8 – 17 – 8 – 17 – 1 – 17 – 27 – 1 – 1 – 31 – 8 – 1 :_____

1 – 1 – 1 – 0 – 8 – 17 – 8 – 3 – 1 – 0 :_____

8 – 18 – 27 – 0 – 1 – 31 :_____

1 – 13 – 1 – 0 – 1 – 3 – 1 – 0 :_____

8 – 8 – 8 – 31 – 8 – 3 – 1 – 17 – 27 – 1 – 1 – 0 – 1 – 8 – 1 – 0 – 8 – 31 :_____

1 – 31 :_____

8 – 3 – 27 – 0 – 1 – 27 – 8 – 31 :_____

8 – 26 – 8 – 31 – 1 – 27 – 1 – 31 :_____

1 – 0 – 1 – 8 – 8 – 31 – 8 – 27 – 8 – 3 – 1 – 31 – 1 – 8 – 1 – 31 – 8 – 13 :_____

Agora, escreva a frase formada na decodificação.

_____

_____

_____

_____