UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL - UEMS
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO-PROPP
MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT
UNIDADE UNIVERSITÁRIA DE DOURADOS

Raissa Santos Rossetti Pereira

CRIPTOGRAFIA: PROPOSTA DE ATIVIDADES PARA O ENSINO BÁSICO

Dissertação de Mestrado

Dourados, MS

2020

UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL - UEMS
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO-PROPP
MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT
UNIDADE UNIVERSITÁRIA DE DOURADOS

CRIPTOGRAFIA: PROPOSTA DE ATIVIDADES PARA O ENSINO BÁSICO

Raissa Santos Rossetti Pereira

Dissertação submetida como requisito final para obtenção do grau de Mestre, pelo Curso de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT junto PRÓ-REITORIA DE PESQUISA E PÓS GRADUAÇÃO - PROPP da Universidade Estadual do Mato Grosso do Sul.

Orientador: Prof. Dr. Cosme E. Rubio Mercedes.

Dourados, MS
2020

P495c Pereira, Raissa Santos Rossetti
Criptografia : proposta de atividades para o ensino básico / Raissa Santos Rossetti Pereira. – Dourados, MS: UEMS, 2021.
75p.

Dissertação (Mestrado Profissional) – Matemática – Universidade Estadual de Mato Grosso do Sul, 2021.
Orientador: Prof. Dr. Cosme E. Rubio Mercedes.

1. Criptografia 2. Método RSA 3. Matemática I. Título

CDD 23. ed. – 652.8

Governo do Estado de Mato Grosso do Sul
Fundação Universidade Estadual de Mato Grosso do Sul
Divisão de Pós-Graduação (DPG/PROPP)

Ata de Defesa de Dissertação
Programa de Pós-Graduação em Matemática
Mestrado Profissional

Aos sete dias do mês de dezembro do ano de dois mil e vinte, às quinze horas, na defesa realizada por videoconferência síncrona (todos os participantes online), na Unidade Universitária de Dourados, da Fundação Universidade Estadual de Mato Grosso do Sul, realizou-se a sessão de defesa de Dissertação, intitulada: "Criptografia: proposta de atividades para o ensino básico" de autoria da aluna: **RAÍSSA SANTOS ROSSETTI PEREIRA**, CPF 047.360.971-16, sob a orientação de COSME EUSTAQUIO RUBIO MERCEDES do Programa de Pós-Graduação em Matemática, nível: Mestrado Profissional. Reuniu-se a Banca Examinadora composta pelos membros: COSME EUSTAQUIO RUBIO MERCEDES **(Presidente)**, José Angel Dávalos Chuquipoma (participação à distância por videoconferência) (UFSJ) e Otávio José Neto Tinoco Neves dos Santos (participação à distância por videoconferência). Concluída a apresentação e arguição, os membros da Banca Examinadora emitiram parecer expresso conforme segue:

☒ Aprovação ☐ Aprovação com revisão ☐ Reprovação

EXAMINADOR	**ASSINATURA**
Dr. COSME EUSTAQUIO RUBIO MERCEDES	
Dr. José Angel Dávalos Chuquipoma (participação à distância por videoconferência) (UFSJ)	
Dr. Otávio José Neto Tinoco Neves dos Santos (participação à distância por videoconferência)	

OBSERVAÇÕES:

Nada mais a ser tratado, o Presidente declarou a sessão encerrada e agradeceu a todos pela presença.

Assinaturas:

Presidente da Banca Examinadora

Aluna

UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

RAISSA SANTOS ROSSETTI PEREIRA

CRIPTOGRAFIA: PROPOSTA DE ATIVIDADES PARA O ENSINO BÁSICO

Produto Final do Curso de Mestrado Profissional apresentado ao Programa de Pós-Graduação *Stricto Sensu* em Matemática em Rede Nacional, da Universidade Estadual de Mato Grosso do Sul, como requisito final para a obtenção do Título de Mestre em Matemática.

Aprovado em: 07 de dezembro de 2020.

BANCA EXAMINADORA:

Prof. Dr. Cosme Eustaquio Rubio Mercedes (UEMS)
Universidade Estadual de Mato Grosso do Sul

Prof. Dr. Otávio José Neto Tinoco Neves dos Santos (UEMS)
Universidade Estadual de Mato Grosso do Sul
(participação realizada à distância por videoconferência)

Prof. Dr. José Angel Dávalos Chuquipoma (UFSJ)
Universidade Federal da Grande Dourados
(participação realizada à distância por videoconferência)

Dedico este trabalho a minha familia e amigas que ganhei no mestrado, que me apoiaram e incentivaram no decorrer de todo o curso.

Agradecimentos

Primeiramente agradeço a Deus por me dar sabedoria, paciência e força para concluir mais esse feito e a Nossa Senhora por me iluminar e não permitir desanimar ao longo do curso. Um muito obrigada a minha família pela força, em especial a minha mãe que sempre me incentivou e confiou na minha capacidade e meu esposo pelo apoio e compreensão. Agradeço também as minhas colegas de Mestrado, Brenda, Carolina e Idineia que estiveram comigo nesta jornada e meus professores do programa PROFMAT, em especial o meu orientador Prof. Dr. Cosme, que de alguma maneira contribuiram para o meu conhecimento durante esta trajetória.

" Há muito quem confunda tabuada com matemática.".

(Agostinho da Silva).

Resumo

A criptografia é um conjunto de técnicas utilizadas para codificar uma informação, protegê-la através da utilização de códigos e cifras, basicamente para garantir a autenticidade e privacidade de uma mensagem, de tal forma que somente o seu destinatário e o emissor da mensagem consigam acessá-la. Além de sua notória importância na segurança de informações, a criptografia está ligada a diferentes conteúdos da Matemática, assim, existem aplicações em diversas áreas e níveis do conhecimento, tornando-a, portanto, uma ferramenta motivadora para as aulas. Permitindo ao aluno visualizar situações reais do seu cotidiano, saindo de uma aula tradicional de conceitos e fórmulas apenas, solucionando assim um dos maiores desafios dos professores, ensinar matemática de maneira significativa. Sendo assim, o presente trabalho visa ampliar o conhecimento sobre a criptografia, sua importância e como pode ser útil para dar contexto a alguns conteúdos de matemática ensinados na educação básica, mas especificadamente no ensino médio. No decorrer do trabalho são apresentadas, com desenvolvimento, sugestões de atividades para serem aplicadas em sala de aula envolvendo conteúdo de matemática: funções, números primos, divisibilidade, e ainda atividades de aritmética modular e método RSA adaptadas para a educação básica.

Palavras-Chave

Criptografia, Método RSA, Matemática.

Abstract

Encryption is a set of techniques used to encode information, protect it through the use of codes and ciphers, basically to guarantee the authenticity and privacy of a message, in such a way that only its receptor and the transmitter of the message are able to access it. -over there. In addition to its notorious importance in information security, cryptography is linked to different mathematical content, thus, there are applications in different areas and levels of knowledge, making it, therefore, a motivating tool for classes. It allows the student to visualize real situations in their daily lives, leaving a traditional class of concepts and formulas only, thus solving one of the greatest challenges of teachers, teaching mathematics in a meaningful way. Thus, the present work aims to expand the knowledge about cryptography, its importance and how it can be useful to give context to some mathematics content taught in basic education, but specifically in high school. In this work, suggestions for activities to be applied in the classroom involving mathematical content are presented, with development: functions, prime numbers, divisibility, as well as modular arithmetic and RSA method activities adapted for basic education.

keywords

Encryption, RSA Method, Mathematics.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

A criptografia é um conjunto de técnicas utilizadas para codificar uma informação, protegê-la através da utilização de códigos e cifras, basicamente para garantir a autenticidade e privacidade de uma mensagem, de tal forma que somente o seu destinatário e o emissor da mensagem consigam acessá-la. Apesar da necessidade de manter segredo em certas situações do cotidiano, como em transações bancárias, senhas e até mesmo em mensagens trocadas em canais de internet, poucas são as pessoas que têm conhecimento de como essas informações são mantidas secretas.

Mas essa necessidade de se comunicar de maneira secreta sempre existiu e os métodos de criptografia utilizados foram diversos e vieram se aperfeiçoando e modernizando ao longo da história, eles eram utilizados principalmente por governantes em épocas de guerra. De acordo com PÓVOA[10]:

> *"A história da criptografia e seu desenvolvimento ao longo das gerações se da pela batalha intelectual entre aqueles que buscavam desenvolver métodos para manter secretas as mensagens, chamados criptógrafos, e aqueles que tinham o desafio de desvendar o segredo dos métodos utilizados, os criptoanalistas."*

Um exemplo antigo de criptografia é a Cétala ou Bastão de Licurgo, veja a figura 1.1, que de acordo com ARAÚJO[11] foi um dos primeiros métodos utilizados para fins militares. Consistia em um bastão com uma tira de couro enrolada no qual o emissor escrevia uma mensagem ao longo do seu bastão e depois desenrolava essa tira, que se transformava em uma tira de couro com uma sequência de letras sem sentido. Para a

mensagem chegar até o seu destino, o mensageiro usava a tira como cinto com as letras usadas para dentro, ao chegar ao destinatário, o mesmo enrolava a tira no seu bastão, cujo diâmetro era igual ao bastão do emissor, desta forma podia ler a mensagem.

Figura 1.1: Bastão de Licurgo

Outro código de criptografia bem conhecido é o da Cifra de César recebe esse nome, pois foi utilizado pelo ditador romano Júlio César em épocas de guerra é uma cifra de substituição, que consiste em trocar cada letra da mensagem original por outra letra do alfabeto, seguindo um padrão, que deve ser de conhecimento do destinatário, veremos este código com mais detalhes no capitulo 3. Mas esses métodos simples de criptografia são falhos, pois COUTINHO[6] afirma que, com uma simples análise de frequência das letras do idioma, uma pessoa consegue decifrar a mensagem mesmo não sendo seu destinatário legítimo.

Na Segunda Guerra Mundial surgiu uma das primeiras máquinas de codificação, a Enigma, desenvolvida pelo exército alemão, ela era capaz de bagunçar completamente o alfabeto a cada letra codificada, só quem soubesse quais rodas misturadoras foram utilizadas poderia decifrar a mensagem. Mas assim como outros métodos este também se tornou ineficaz, ODEMIR[12] diz que os codigos da Enigma foram quebrados por outra máquina, a Enigma Bomb, desenvolvida por Alan Turing.

Com a evolução dos computadores a criptografia passa a exercer não mais o papel de "arma de guerra", mas sim a tarefa de manter segura informações e dados que circulam pela internet. Hoje em dia, de acordo com COUTINHO[1]:

> "As técnicas de criptográfia mais utilizadas, envolvem o conceito das chaves criptográficas, que são formadas por um conjunto de bits basedo em um algoritmo capaz de interpretar as informações, ou seja, decodificá-las. A chave pública, fornecida ao emissor, deve ser compatível com a chave privada, de posse do receptor, para assim, as informações serem extraídas. A chave pública

é usada para codificar as informações e a privada para decodificá-las."

Em 1978, Ron Rivest, Adi Shamir e Leonard Adleman, apresentaram o que agora é conhecido como procedimento criptográfico RSA, um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para transmissão segura de dados. A segurança do método está relacionada a quantidade de bits, e quanto mais bits, mais segurança criptográfica, segundo COUTINHO[1], essa segurança está relacionada a dificuldade computacional de fatorar números inteiros muito grandes. ZOCON, CESPEDES, MERCEDES e QUIPUSCOA [2] dizem que:

> "Não é possível calcular em um tempo justificável sua decomposição em fatores primos, a fatoração de um número $n = p.q$, onde p e q são números primos e n tem um comprimento de 2048 bits, por exemplo, não é realizável em um tempo aceitável."

Além de sua notória importância na segurança de informações, a criptografia está ligada a diferentes conteúdos da Matemática, assim, existem aplicações em diversas áreas e níveis do conhecimento, tornando-a, portanto, uma ferramenta motivadora para as aulas, já que permite ao aluno vizualizar situações reais do seu cotidiado, saindo de uma aula tradicional de conceitos e fórmulas apenas, solucionando assim um dos maiores desafios dos professores, ensinar matemática de maneira significativa. Sendo assim, o presente trabalho visa ampliar o conhecimento sobre a criptografia, sua importância e como pode ser útil para dar contexto a alguns conteúdos de matemática ensinados na educação básica, mas especificadamente no ensino médio.

Para uma melhor apresentação, este estudo foi dividido em três capítulos mais a introdução e considerações finais. Primeiramente temos a introdução, aqui desenvolvida, onde apresentamos o objetivo e desenvolvimento do trabalho; em seguida, no segundo capítulo, apresentamos alguns conceitos preliminares e propriedades da aritmética modular, mas especificadamente sobre congruência, que é pré-requesito necessário para compreenção de cálculos utilizados no decorrer do capítulo 4; destacamos, na sequência, a importância, evolução e funcionalidade da criptofrafia e no quarto capítulo, apresentamos um passo a passo para a compreensão do método RSA. Tanto no terceiro como no quarto capítulo são apresentadas, com desenvolvimento, sugestões de atividades para

serem aplicadas em sala de aula envolvendo conteúdos de matemática como: funções, números primos, divisibilidade, e ainda atividades de aritmética modular e método RSA adaptadas para a educação básica, também no quarto capítulo é apresentado e proposto como ferramenta para atividade em grupo o aplicativo CodeClass, que tem como uma de suas funcionalidades, realizar de maneira simples, os processos necessários para implementação do método de criptografia RSA. Nas considerações finais temos as conclusões deste estudo. As atividades propostas no trabalho não foram possíveis de serem aplicadas em sala de aula, visto que devido a pandemia do novo coronavírus (Covid-19), e o consequente isolamento social, as escolas foram fechadas e tiveram que se adaptar a nova realidade.

Capítulo 2

Conceitos Preliminares

Neste capítulo apresentamos alguns conceitos como: função inversa, divisão euclidiana, congruência, inverso modular e função de Euler que serão utilizados nos capítulos adiante, para tal utilizamos as referências [1],[4], [6], [7], [8] e [9].

2.1 Função Inversa

Só existe função inversa de uma função bijetora, ou seja, injetora e ao mesmo tempo sobrejetora. Quando uma função f é invertível, o seu domínio será o contradomínio da função f^{-1}. Temos que:

$f^{-1}(y) = x \leftrightarrow f(x) = y$

Definição 2.1.1 *Uma função é INJETORA quando elementos diferentes no domínio(D) são transformados pela função em elementos diferentes no contradomínio(CD), ou seja, para todo $x_1, x_2 \in D$, com $x_1 \neq x_2$, tem-se $f(x_1) \neq f(x_2)$, ou ainda, se $f(x_1) = f(x_2)$, implica que $x_1 = x_2$.*

E uma função é SOBREJETIVA quando, para qualquer elemento y do contradomínio, pode-se encontrar, pelo menos, um elemento x no domínio da função, ou seja, a função é sobrejetiva se o conjunto imagem coincidir com o contradomínio. E para mostrar que f é sobrejetiva deve-se provar que a "equação"$f(x) = y$ possui uma solução $x \in D$, seja qual for o $y \in CD$ dado.

Exemplo 2.1.1 *Seja a função $f : R \to R$ com $f(x) = 2.x + 1$ vamos encontrar a sua*

função inversa.

Solução:

Primeiramente vamos analisar se a função é bijetora. Podemos observar que elementos diferentes no domínio possuem imagens diferentes no contradomínio. Além disso, o contradomínio é igual à imagem, pois qualquer elemento y que eu escolher no contradomínio terá uma solução x no domínio da função. Logo, essa função é bijetora.

Para obtermos a sua inversa devemos isolar a variável x:

$x = \frac{y-1}{2}$ *, assim obtemos a função inversa*

$$f^{-1}(y) = \frac{y-1}{2}$$

EXEMPLO 2.1.2 *Determine a inversa da função* $f(x)$*, de* $R - \{5\}$ *em* $R - \{2\}$*, definida por* $f(x) = \frac{2.x+3}{x-5}$.

Solução:

Primeiramente vamos analisar se a função é bijetora. Podemos observar pelo gráfico 2.1 da função que elementos diferentes do eixo x possuem correspondendes diferentes no eixo y. Além disso, o contradomínio, $R - \{2\}$*, é igual à imagem, pois qualquer elemento que eu escolher no contradomínio corresponde a algum elemento x no domínio. Logo, essa função é bijetora.*

Figura 2.1: Gráfico da Função: $f(x) = \frac{2.x+3}{x-5}$

Agora vamos obter a sua inversa.

$y = \frac{2.x+3}{x-5}$

$y.x - 5.y = 2.x + 3$

$y.x - 2.x = 5.y + 3$

$x.(y-2) = 5.y + 3$

$x = \frac{5.y+3}{y-2}$, *para efeito de notação vamos permutar as letras* x *e* y

$y = \frac{5.x+3}{x-2}$ *ou* $f^{-1}(x) = \frac{5.x+3}{x-2}$, *com* $x \neq 2$

2.2 Algoritmo de Euclides

Através da divisão com resto de um número natural por outro, Euclides criou um algoritmo para determinar o máximo divisor comum (MDC) de dois números. Tal resultado foi de grande importância para a aritmética modular, e consequente para os estudos de criptografia, já que a base dos métodos criptográficos são cálculos de congruência - restos da divisão euclidiana por um número fixado.

2.2.1 Divisão Euclidiana

Dados dois números inteiros a e b com $a \neq 0$, pela divisão Euclidiana temos que existem dois únicos números inteiros q e r, denominados, respectivamente, quociente e resto tais que

$$b = a.q + r, \text{ com } 0 \leq r < |a|$$

EXEMPLO 2.2.1 *O quociente e o resto da divisão de* 35 *por* 6 *são* $q = 5$ *e* $r = 5$, *pois* $35 = 6.5 + 5$. *E de* -35 *por* 6 *são* $q = -6$ *e* $r = 1$, *pois* $-35 = 6.(-6) + 1$.

Através desta divisão Euclides criou um algoritmo para o cálculo do máximo divisor comum de dois inteiros, que veremos a seguir.

2.2.2 Algoritmo de Euclides

O algoritmo de Euclides é um método utilizado para encontrar o máximo divisor comum entre dois números inteiros não nulos, vamos apresentar um passo a passo de como ele funciona.

Primeiramente, efetuamos a divisão euclidiana $b = a.q_1 + r_1$ e escrevemos os números no diagrama:

	q_1	
b	a	
r_1		

Fazemos novamente a divisão $a = r_1.q_2 + r_2$ e escrevemos os números no diagrama:

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Repetindo a divisão até quando for possível, teremos:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n		

EXEMPLO 2.2.2 *Vamos calcular pelo algoritmo de Euclides o mdc de* 648 *e* 1218.

	1	1	7	3	4
1218	648	570	78	24	6
570	78	24	6	0	

Assim, temos que o mdc$(648, 1218) = 6$.

2.3 Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética nos mostra que todo número natural maior do que 1 é primo ou se escreve como um produto de números primos.

Assim, podemos observar a importância dos números primos, já que todo número natural pode ser construído apartir do produto de dois primos.

A decomposição de um número em fatores primos é um dos segredos do método RSA que veremos com mais detalhes no capítulo 4.

2.4 Aritmética modular

Aritmética Modular ou Aritmética do Relógio, como também é conhecida, é a aritmética dos fenômenos periódicos, isto é, aqueles que se repetem a intervalos regulares. Ela é uma das ferramentas mais importantes na Teoria dos Números (área que estuda as propriedades dos números inteiros) e envolve o conceito de congruência que é a relação de dois números, que divididos por um terceiro, chamado de módulo, deixam o mesmo resto.

A criptografia é uma das aplicações da congruência, assim para compreendermos as regras e cálculos por trás do código RSA , iremos abordar de maneira sucinta, alguns resultados e propriedades de congruência.

Se dois números a e b, quando divididos por um mesmo número m deixam restos iguais, dizemos que eles são congruentes modulo m. Ou ainda, de maneira mais formal temos por [1]: diremos que dois números inteiros a e b são congruentes módulo m, se $a-b$ é um múltiplo de m. Assim podemos escrever:

$a \equiv b \, mod \, m$ quando $m|(a-b)$, ou seja, $(a-b) = k.m$, onde k é um número inteiro.

EXEMPLO 2.4.1 $75 \equiv 51 \mod 8$, *pois pela definição temos,* $8|(75-51) = 24$, *ou seja,* $(75-51) = 3.8$. *E ainda, ambos os números* 75 *e* 51, *deixam resto* 3 *quando divididos por* 8.

Temos que a congruência, módulo um inteiro fixado m, é uma relação de equivalência. Assim vale a proposição abaixo.

PROPOSIÇÃO 2.4.1 *Seja* $m \epsilon \mathbb{N}$. *Para todos* $a, b, c \epsilon \mathbb{Z}$. *Temos as propriedades:*

- ***Reflexiva:*** $a \equiv a \, mod \, m$;
- ***Simétrica:*** $a \equiv b \, mod \, m$ *e* $b \equiv a \, mod \, m$;
- ***Transitiva:*** *se* $a \equiv b \, mod \, m$ *e* $b \equiv c \, mod \, m$, *então* $a \equiv c \, mod \, m$.

EXEMPLO 2.4.2 *Temos que* $38 \equiv 26 \, mod \, 6$ *e* $26 \equiv 20 \, mod \, 6$, *então* $38 \equiv 20 \, mod \, 6$. *Ambos deixam os mesmos restos quando divididos por* 6.

Já vimos que as propriedades reflexiva, simétrica e transitiva valem para a congruência. Outras propriedades utilizadas nas operações de adição e multiplicação também são válidas e facilitam os cálculos de congruência. Como veremos abaixo.

PROPOSIÇÃO 2.4.2 *Seja* $a, b, c, d, m \in \mathbb{Z}$, *com* $m > 1$.

- *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$, *então* $a + c \equiv b + d \bmod m$;
- *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$, *então* $a.c \equiv b.d \bmod m$, *disso temos,* $a^k \equiv b^k \bmod m$.

EXEMPLO 2.4.3 *1. Efetue as divisões e descreva o resultado usando o algoritmo de Euclides:* $b = a.q + r$ *e também congruência:* $b \equiv r \bmod a$. *Obs: b=dividendo, a=divisor, q=quociente e r=resto.*

a) $89 : 6$

Solução: $89 = 6.14 + 5$ *ou* $89 \equiv 5 \bmod 6$.

b) $112 : 5$

Solução: $112 = 5.22 + 2$ *ou* $112 \equiv 2 \bmod 5$

c) $201 : 3$

Solução: $201 = 3.67 + 0$ *ou* $201 \equiv 0 \bmod 3$

2. Resolva as congruências, assim como no exemplo:

Exemplo: $(35 + 19) \equiv X \bmod 6$

Solução:

$35 \equiv X \bmod 6$ *e* $19 \equiv X \bmod 6$

$35 \equiv 5 \bmod 6$ *e* $19 \equiv 1 \bmod 6$

$(35 + 19) \equiv (5 + 1) \bmod 6$

$(35 + 19) \equiv 6 \bmod 6$ *, mas* $6 \equiv 0 \bmod 6$

Assim, $(35 + 19) \equiv 0 \bmod 6$.

a) $(51 + 13) \equiv X \bmod 7$

Solução:

$51 \equiv X \bmod 7$ *e* $13 \equiv X \bmod 7$

$51 \equiv 2 \bmod 7$ *e* $13 \equiv 6 \bmod 7$

$(51 + 13) \equiv (2 + 6)\ mod\, 7$

$(51 + 13) \equiv 8\ mod\, 7\ ,\ mas\ 8 \equiv 1\ mod\, 7$

Assim, $(51 + 13) \equiv 1\ mod\, 7.$

b) $(9.22) \equiv X\ mod\, 5$

Solução:

$9 \equiv X\ mod\, 5 \quad e \quad 22 \equiv X\ mod\, 5$

$9 \equiv 4\ mod\, 5 \quad e \quad 22 \equiv 2\ mod\, 5$

$(9.22) \equiv (4.2)\ mod\, 5$

$(9.22) \equiv 8\ mod\, 5\ ,\ mas\ 8 \equiv 3\ mod\, 5$

Assim, $(9.22) \equiv 3\ mod\, 5.$

c) $7^{26} \equiv X\ mod\, 12\ ,$ *obs.: use* $7^{26} = 7^2.(7^2)^{12}$

Solução:

$7^2 = 49 \equiv X\ mod\, 12$

$7^2 = 49 \equiv 1\ mod\, 12\ ,$ *elevando ambos os lados a* 12*, temos*

$(7^2)^{12} \equiv (1)^{12}\ mod\, 12$

$7^2.(7^2)^{12} \equiv 1.1^{12}\ mod\, 12$

Assim, $7^{26} \equiv 1\ mod\, 12.$

2.4.1 Classes residuais e Inverso modular

Todo número natural é congruente módulo m ao resto da sua divisão por m. Pois, dados $a, m \epsilon \mathbb{N}$, e $m > 0$, temos que $a = b.m + r$, onde $b, r \epsilon \mathbb{N}$ e $0 \leq r < m$, e ainda, $a - r = b.m$. Falamos que r, o resto da divisão, é um resíduo de a módulo m. E o conjunto de todos os resíduos de m, possui sempre m elementos $0, 1, 2, 3, ..., m - 1$.

Exemplo 2.4.4 *Os possíveis restos de uma divisão por* 8 *são* $0, 1, 2, 3, 4, 5, 6, 7$*, portanto esse é o conjunto dos resíduos do número* 8*.*

Definição 2.4.1 *Seja* $a, m \in \mathbb{Z}$*, com* $m > 1$*. O conjunto* $\bar{a} = \{x \in \mathbb{Z};\ x \equiv a\ mod\ m\}$*, é chamado de classe residual módulo* m*.*

Ou seja, $\bar{a}$ é o conjunto de todos os inteiros que deixam resto a quando divididos por m. Representamos por $\mathbb{Z}_m$ o conjunto de todas as classes residuais módulo m, logo $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \bar{m - 1}\}$

EXEMPLO 2.4.5 *Seja* $m = 5$. *Então*

$$\begin{aligned}
\bar{0} &= \{5.t; t \in \mathbb{Z}\} \\
\bar{1} &= \{5.t; t+1 \in \mathbb{Z}\} \\
\bar{2} &= \{5.t; t+2 \in \mathbb{Z}\} \\
\bar{3} &= \{5.t; t+3 \in \mathbb{Z}\} \\
\bar{4} &= \{5.t; t+4 \in \mathbb{Z}\}
\end{aligned}$$

Temos que

$$a \in \begin{cases} \bar{0}, & \textit{se } a \textit{ é múltiplo de } 5; \\ \bar{1}, & \textit{se } a \textit{ tem resto } 1 \textit{ quando dividido por } 5; \\ \bar{2}, & \textit{se } a \textit{ tem resto } 2 \textit{ quando dividido por } 5; \\ \bar{3}, & \textit{se } a \textit{ tem resto } 3 \textit{ quando dividido por } 5; \\ \bar{4}, & \textit{se } a \textit{ tem resto } 4 \textit{ quando dividido por } 5. \end{cases}$$

Um elemento $\bar{a} \in \mathbb{Z}_m$ será dito invertível, quando existir $\bar{b} \in \mathbb{Z}_m$ tal que $\bar{a}.\bar{b} = 1$. Assim, $\bar{b}$ será o inverso de $\bar{a}$.

Procurando Classes Inversas:

Quadro 2.1: Tabela Multiplicativa das classes *mod* 5

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Quadro 2.2: Tabela Multiplicativa das classes $mod\,8$

.	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Quadro 2.3: Tabela Multiplicativa das classes $mod\,10$

.	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Quadro 2.4: Tabela Multiplicativa das classes $mod\,11$

.	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{10}$	$\overline{2}$	$\overline{5}$	$\overline{8}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{5}$	$\overline{9}$	$\overline{2}$	$\overline{6}$	$\overline{10}$	$\overline{3}$	$\overline{7}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{4}$	$\overline{9}$	$\overline{3}$	$\overline{8}$	$\overline{2}$	$\overline{7}$	$\overline{1}$	$\overline{6}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{1}$	$\overline{7}$	$\overline{2}$	$\overline{8}$	$\overline{3}$	$\overline{9}$	$\overline{4}$	$\overline{10}$	$\overline{5}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{3}$	$\overline{10}$	$\overline{6}$	$\overline{2}$	$\overline{9}$	$\overline{5}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{10}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Analisando os resultados obtidos nas tabelas, podemos observar que: dois casos sempre tem inverso, a classe 1 cujo inverso é sempre ela mesma e o último elemento da tabela também será sempre inverso dela mesma; o inverso modular de $a\ mod\, m$ está sempre entre 0 e $(m-1)$; e ainda, nas tabelas 2.1 e 2.4, que apresentam as classes de equivalência módulo 5 e 11, respectivamente, todas as classes com excessão da classe zero, tem inverso; já nas tabelas 2.2 e 2.3, que apresentam as classes de equivalência módulo 8 e 10, nessa ordem, nem todas as classes possuem inverso modular. Das observações concluimos, portanto, que para existir um inverso modular, a e m devem ser primos entre si, ou seja, $mdc(a,m) = 1$.

Teorema 2.4.1 *A classe a tem classe inversa* $(mod\, b) \leftrightarrow mdc(a,b) = 1$

$(\rightarrow)$ *Vamos assumir que existe classe inversa de a, que vamos denominar por* a'*. Então,* $a.a' \equiv 1\, mod\, b$*, assim temos*

$a.a' - 1 = b.k$*, com* $k \in \mathbb{Z}$

$a.a' + b.(-k) = 1$*, daqui temos que* a' *e* $-k$ *são soluções da equação diofantina* $a.x + b.y = 1$ *e sabemos pelo teorema da equação diofantina [9] que "*$a.x + b.y = c$ *tem solução se* $mdc(a,b)$ *divide c".*

Já vimos acima que nossa equação $a.x + b.y = 1$ *tem solução, logo* $mdc(a,b)$ *divide* 1*,*

portando o $mdc(a, b) = 1$.

($\leftarrow$) *Vamos considerar a seguinte equação* $a.x + b.y = 1$.
Partindo do fato que $mdc(a, b) = 1$ *e sabendo pelo teorema da equação diofantina [9] que "se* $mdc(a, b)$ *divide c, então uma equação diofantina* $a.x + b.y = 1$ *tem solução", logo existem dois números* x_0 *e* y_0 *tais que,*
$a.x_0 + b.y_0 = 1$, *reescrevendo temos*
$a.x_0 = 1 - b.y_0$
$a.x_0 - 1 = b.(-y_0)$, *assim*
$a.x_0 \equiv 1 \, mod \, b$, *ou seja, a tem classe inversa* $(mod \, b)$.

2.5 Função fi de Euler

A função $\phi(n)$ corresponde a quantidade de números naturais entre 0 e $n - 1$ que são primos com n. Ou seja, dado um número n, a função fi representa a quantidade de números inteiros que são menores do que n, tal que esses números não podem compartilhar qualquer fator comum com n.

Por exemplo, vamos encontrar o $\phi(10)$, para isso olharemos todos os valores de 1 a 9 e então contamos quantos inteiros não compartilham fator maior do que 1 comum com o número 10; temos que os números $2, 4, 5, 6$ e 8 não são contados pois compartilham fator comum com o 10, enquanto que os números $1, 3, 7$ e 9 são todos contados, pois apenas partilham o fator 1, ou seja, o mdc entre eles e o número 10 é igual a 1. Portanto, $\phi(10) = 4$

O interessante é que o cálculo da função fi é dificil para números grandes, exceto no caso dos números primos. Já que os números primos não tem nenhum valor maior do que 1 como fator comum, o fi de qualquer primo p é simplesmente igual a $p - 1$. De maneira formal, temos que:

Definição 2.5.1 $\phi(p) \leq p - 1$, *para todo* $p \geq 2$. *E ainda, se* $p \geq 2$, *então* $\phi(p) = p - 1$ *se, e somente se, p é um número primo.*

Exemplo 2.5.1 $\phi(7) = 7 - 1 = 6$. *De fato, pois o número* 7 *não tem fator, além do número* 1, *comum com os núemros* $1, 2, 3, 4, 5, 6$, *que nos da uma quantidade de* 6 *números.*

Temos ainda que a função fi é multiplicativa, ou seja, dados $a, b \in \mathbb{N}$ tais que $(a, b) = 1$ temos, $\phi(a.b) = \phi(a).\phi(b)$. Se sabemos que o número n é o produto de dois números primos p e q, então $\phi(n)$ é apenas o valor de fi para cada número primo multiplicado um pelo outro, ou seja:

$$\phi(n) = \phi(p).\phi(q) = (p-1).(q-1)$$

Capítulo 3

Criptografia

3.1 Criptografia

Desde a antiguidade, sempre existiu a necessidade de se comunicar por mensagens e algumas vezes até de forma secreta. Nas guerras, por exemplo, o objetivo era que as mensagens fossem decifradas apenas pelo destinatário, ou seja, não poderiam ser lidas por inimigos, seu conteúdo só poderia ser compreendido por quem era de interesse. Assim, através desse fato de compartilhar uma mensagem de tal forma que ela não fosse lida pelas pessoas erradas, criou-se o desafio de desenvolver uma forma de escrever uma mensagem de maneira oculta, surgia assim a criptografia.

Em grego, *cryptos* significa secreto, oculto. Assim a criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la [1].

Existem dois métodos de criptografia, em um deles o emissor e o receptor possuem a mesma chave secreta, ou seja, a mesma chave utilizada pelo emissor para codificar a mensagem é também utilizada pelo receptor para decodificá-la, um exemplo deste método é a Cifra de César. Em termos matemáticos pode-se dizer que esse modelo de criptografia usa de uma função para criptografar uma mensagem e utiliza da função inversa para decodificá-la [3].

No segundo método, que veremos com mais detalhes no próximo capítulo, é o de criptografia de chave pública, que ao contrário do anterior não se tem uma regra secreta entre o emissor e o receptor da mensagem, pelo contrário há duas chaves, uma pública e

outra privada. O emissor codifica a mensagem, com a chave pública que está disponível para qualquer pessoa, e a envia para alguém que a decodifica através da chave privada de sua posse apenas. Logo, já que a chave privada não é transmitida a ninguém, caso alguém intercepte a mensagem, não conseguiria decifra-la [5].

Contextualizar conteúdos nas aulas de matemática muitas vezes não é tarefa fácil, o que causa desinteresse na aprendizagem por parte dos alunos. Assim, veremos no decorrer dessa seção, como a criptografia pode ser utilizada para dar significado ao estudo de função.

3.1.1 Cifra de César

Um dos códigos secretos mais simples é o de substituição, que consiste em trocar cada letra da mensagem original por outra letra do alfabeto, seguindo um padrão, que deve ser de conhecimento do destinatário. Esse método foi utilizado pelo ditador romano Júlio César em épocas de guerra, e ficou conhecido como *Cifra de César*, ele utilizava um deslocamento de 3 posições no alfabeto para cifrar suas mensagens, as letras A, B e C, por exemplo, correspondiam, respectivamente, as letras D, E e F, como pode ser visto no quadro 3.1.

Quadro 3.1: Tabela de referência para Cifra de César

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

Exemplo 3.1.1 *Codificando o texto* MENSAGEM CRIPTOGRAFADA*, utilizando a cifra de César obtemos a mensagem cifrada:*

$$PHQVDJHPFUMSXRJUDIDGD$$

Mas é fácil observarmos a falha neste método de criptografia ao qual o segredo é o deslocamento do alfabeto, pois já que temos 26 letras no alfabeto então temos 25 possibilidades de deslocamento do alfabeto cifrado, sendo simples testar cada uma das possibilidades. Assim POVOA[10] afirma que as cifras de deslocamento são bastante inseguras, não resistindo nem mesmo a um simples ataque por força bruta.

Além disso, com uma simples análise de frequência das letras do idioma, é possível decifrar a mensagem mesmo não sendo seu destinatário legítimo. Por exemplo, a frequência média de cada letra na língua portuguesa é dada pela tabela 3.2. Logo, obtendo a frequência de cada símbolo no texto, basta observarmos o que aparece em uma quantidade maior de vezes e cifrarmos por ele o alfabeto. Exemplo, se eu tenho um texto onde o símbolo "M" aparece com mais frequência, iremos cifrar o alfabeto iniciando pelo M, ou seja, a letra "a" do alfabeto correspondera ao símbolo "M", a letra "b" ao "N" e assim por diante.

Quadro 3.2: Frequência das letras na língua portuguesa [6]

Letra	A	B	C	D	E	F	G	H	I	J	L	M
%	14,4	1,04	3,88	4,10	12,57	1,02	1,30	1,28	6,18	0,40	2,78	4,75
Letra	N	O	P	Q	R	S	T	U	V	X	Z	
%	5,05	10,73	2,52	1,20	6,53	7,81	4,34	4,64	1,70	0,21	0,47	

De modo geral, quanto mais longo o texto, maior a probabilidade de apresentar a frequência padrão do idioma. Portanto, como afirma [9] para uma mensagem curta a análise de frequência é falha, pois se pode facilmente criar uma mensagem curta ao qual a contagem de frequência seja completamente diferente da tabela de frequência da lingua portuguesa, como pode ser verificado nos exemplos a seguir.

Exemplo 3.1.2 *Na mensagem "O rato roeu a roupa do rei de roma"podemos observar que a letra que aparece com maior frequência é a "R", logo se codificássemos este texto o símbolo mais frequente não representaria a letra "a", como afirma o método da tabela de referência já apresentada.*

Exemplo 3.1.3 *Vamos decifrar a mensagem abaixo utilizando a tabela de frequência da lingua portuguesa.*

LDPZMXRTZHPFRQIZQGDXDEZDGDFRPPDXHPDXMFDDERDPDXHPDXMF
DQDRVHGHIMQHSHODTZDQXMGDGHGHUHVSRVXDVTZHVHVDEHPDVSH
ODIRUPDFRPRUHDJMPRVTZDQGRQDRVDEHPRVDUHVSRV

Solução: *Analisando o texto podemos observar que o símbolo "D" é o que aparece com maior frequência, portanto ele irá corresponder a letra "a" do alfabeto.Assim, temos*

o alfabeto cifrado correspondente:

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

Substituindo temos o texto original:

"Há muito quem confunda tabuada com matemática. A boa matemática não se define pela quantidade de respostas que se sabe, mas pela forma como reagimos quando não sabemos a resposta."

3.1.2 Códigos de Chave Pública

Observamos que o método de criptografia anterior, é falho quando falamos em transações bancárias ou compras pela internet, por exemplo, já que qualquer pessoa com experiência na área, poderia interceptar a mensagem e decodificá-la. Pois, seja qual for o código utilizado, se sabemos como fazer a codificação, basta desfazê-la e deciframos a mensagem.

Mas e se tivéssemos um método de codificar fácil, porém muito difícil de ser decodificado? É essa a base do método de codificação de chave pública, por mais que a mensagem seja interceptada ou, como o próprio nome ja diz "pública"e a pessoa tenha conhecimento de como foi codificada, ela teria um trabalho enorme para conseguir decifrá-la.

Uma das aplicações mais notáveis dos números primos é na criptografia de chave pública. A segurança do método, que se usa para codificar uma mensagem está relacionada a quantidade de bits, e quanto mais bits são usados, mais segurança criptográfica. Pois, essa segurança está relacionada a dificuldade computacional de fatorar números inteiros muito grandes [1].

O mais conhecido dos métodos de criptografia de chave pública, e que veremos com detalhes no próximo capítulo, é o RSA.

3.2 Sugestões de atividades

Um dos desafios enfrentados nas aulas de matemática, é fazer com que os alunos além de compreenderem o conteúdo, também vejam significado e se interessem por ele.

Assim, a criptografia pode ser usada no ensino médio como ferramenta para contextualizar atividades envolendo funções, basta relacionarmos cada letra, símbolo a um número e codificarmos cada um desses caracteres através de uma função $f(x)$, e para decodificarmos a mensagem utilizamos a função inversa, substituindo o valor fornecido por $f(x)$ em $f^{-1}(x)$.

As atividades apresentadas nessa seção foram elaboradas com o objetivo de facilitar e dar significado ao conteúdo de funções estudado no ensino médio. Vamos utilizar uma função como chave para codificar uma mensagem e sua função inversa para decifrá-la. Cada uma das questões estão resolvidas na sequência de maneira detalhada.

Nas atividades abaixo, estão propostas várias situações com o intuito de crifrar e também decifrar mensagens. Tais mensagens podem estar apresentadas com letras ou com números.

Para os enunciados propostos a seguir iremos utilizar a tabela de referência 3.3, porém pode-se utilizar uma tabela de sua preferência, que relacione outros valores para as letras ou símbolos.

Quadro 3.3: Tabela de referência para as atividades propostas

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Nº	1	2	3	4	5	6	7	8	9	10	11	12	13
Letra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nº	14	15	16	17	18	19	20	21	22	23	24	25	26

1. Já vimos como as mensagens criptografadas eram importantes em tempos de guerra, e um dos métodos que ficou muito conhecido foi a *Cifra de César*, ele utilizava um deslocamento de 3 posições no alfabeto para cifrar suas mensagens. Sabendo disso decifre uma mensagem famosa do Imperador: "HPHOKRUVRIUHURSLRUDJ-RUDGRTXHYLYHUQRHWHUQRPHGRGHOH".

   Desenvolvimento:Chamaremos de x o valor da letra na mensagem original e y o valor da letra correspondente na mensagem codificada. Sabendo que a regra utilizada pelo imperador era de deslocar 3 posições no alfabeto, então podemos definir uma lei matemática para conseguir decifrar a mensagem. O valor da letra

original, que estamos chamando de x, adicionado 3 unidades é igual ao valor da letra codificada:

$$x + 3 = y$$

Substituindo as letras da mensagem, criptografada pelo imperador, pelos números correspondentes de acordo com a tabela oferecida, temos a mensagem reescrita na forma númerica:

$$8, 16, 8, 15, 11, 18, 21, 22, 18, 9, 21, 8, 21, 18, 19, 12, 18, 21, 4, 10, 18, 21, 4, 7,$$

$$18, 20, 24, 8, 25, 12, 25, 8, 21, 17, 18, 8, 23, 8, 21, 17, 18, 16, 8, 7, 18, 7, 8, 15, 8.$$

Agora, basta que façamos a substituição de y pelos valores da mensagem codificada, e assim iremos chegar as letras da mensagem original.

- Para $y = 8$, temos: $x + 3 = 8 \Longrightarrow x = 5$, que corresponde a letra **E**
- Para $y = 16$, temos: $x + 3 = 16 \Longrightarrow x = 13$, que corresponde a letra **M**
- Para $y = 15$, temos: $x + 3 = 15 \Longrightarrow x = 12$, que corresponde a letra **L**
- Para $y = 11$, temos: $x + 3 = 11 \Longrightarrow x = 8$, que corresponde a letra **h**
- Para $y = 18$, temos: $x + 3 = 18 \Longrightarrow x = 15$, que corresponde a letra **O**
- Para $y = 21$, temos: $x + 3 = 21 \Longrightarrow x = 18$, que corresponde a letra **R**
- Para $y = 22$, temos: $x + 3 = 22 \Longrightarrow x = 19$, que corresponde a letra **S**
- Para $y = 9$, temos: $x + 3 = 9 \Longrightarrow x = 6$, que corresponde a letra **F**
- Para $y = 19$, temos: $x + 3 = 19 \Longrightarrow x = 16$, que corresponde a letra **P**
- Para $y = 12$, temos: $x + 3 = 12 \Longrightarrow x = 9$, que corresponde a letra **I**
- Para $y = 4$, temos: $x + 3 = 4 \Longrightarrow x = 1$, que corresponde a letra **A**
- Para $y = 10$, temos: $x + 3 = 10 \Longrightarrow x = 7$, que corresponde a letra **G**
- Para $y = 7$, temos: $x + 3 = 7 \Longrightarrow x = 4$, que corresponde a letra **D**
- Para $y = 20$, temos: $x + 3 = 20 \Longrightarrow x = 17$, que corresponde a letra **Q**
- Para $y = 17$, temos: $x + 3 = 17 \Longrightarrow x = 14$, que corresponde a letra **N**
- Para $y = 24$, temos: $x + 3 = 24 \Longrightarrow x = 21$, que corresponde a letra **U**

- Para $y = 25$, temos: $x + 3 = 25 \Longrightarrow x = 22$, que corresponde a letra **V**
- Para $y = 23$, temos: $x + 3 = 23 \Longrightarrow x = 20$, que corresponde a letra **T**

Reescrevendo, temos a mensagem original: **"É melhor sofrer o pior agora do que viver no eterno medo dele."**

2. Priscila estava organizando com seu pai uma festa surpresa para sua mãe que completaria cinquenta anos no final de semana. Assim os dois conversavam apenas por mensagens criptografadas, e utilizavam sempre a regra de deslocar 10 posições no alfabeto. No dia da festa ela precisava mandar a seguinte mensagem: "Os convidados chegaram ", como ficou a escrita depois de criptografar?

OBSERVAÇÃO 3.2.1 *Como a tabela de referência só vai até o número* 26*, ou seja* $Z = 26$*, para valores maiores deve-se reiniciar a contagem. O número* 30*, por exemplo, corresponde a letra D, pois* $30 - Z = 4$ *e pela tabela sabemos que a letra D corresponde ao número* 4*.*

Desenvolvimento: De acordo com a regra utilizada por eles, podemos escrever a seguinte função:

$$f(x) = x + 10,$$

sendo x o valor original da letra na tabela e y o valor da letra cifrada.

Substituindo as letras da mensagem original pelos números correspondentes, obtemos a seguinte mensagem na forma numérica:

$$15, 19, 3, 15, 14, 22, 9, 4, 1, 4, 15, 19, 3, 8, 5, 7, 1, 18, 1, 13$$

Vamos substituir na função para obtermos os valores das letras cifradas, e assim, consequentemente a mensagem criptografada.

- $f(15) = 15 + 10 = 25$, que corresponde a letra **Y**
- $f(19) = 19 + 10 = 29$, temos que $29 - 26 = 3$, que corresponde a letra **C**
- $f(3) = 3 + 10 = 13$, que corresponde a letra **M**
- $f(14) = 14 + 10 = 24$, que corresponde a letra **X**

- $f(22) = 22 + 10 = 32$, temos que $32 - 26 = 6$, que corresponde a letra **F**
- $f(9) = 9 + 10 = 19$, que corresponde a letra **S**
- $f(4) = 4 + 10 = 14$, que corresponde a letra **N**
- $f(1) = 1 + 10 = 11$, que corresponde a letra **K**
- $f(8) = 8 + 10 = 18$, que corresponde a letra **R**
- $f(5) = 5 + 10 = 15$, que corresponde a letra **O**
- $f(7) = 7 + 10 = 17$, que corresponde a letra **Q**
- $f(18) = 18 + 10 = 28$, temos que $28 - 26 = 2$, que corresponde a letra **B**
- $f(13) = 13 + 10 = 23$, que corresponde a letra **W**

Mensagem criptografada: **"YCMYXFSNKNYCMROQKBKW".**

3. A professora propôs um desafio em sala, cada aluno deveria criptografar uma frase de motivação e compartilhar com algum colega de sala, seguindo uma regra padrão de chave de criptação: o dobro do valor original da letra. Maria, uma das alunas, escolheu a seguinte frase: "Não pare até se orgulhar de você!", como ficou codificada a mensagem de Maria, na forma numérica?

   Desenvolvimento: Assim como nos exercícios anteriores, iremos chamar de x o valor original da letra na tabela e de y o valor da letra codificada. No enunciado foi apresentada a chave para codificar a mensagem: "o dobro do valor original da letra", assim, podemos escrever a função para criptografar a mensagem:

   $$f(x) = 2.x$$

   Utilizando a tabela de referência, vamos reescrever a frase de Maria na forma numérica, e depois substituir na função, para assim encontrarmos o valor de $f(x) = y$, que corresponde ao valor da letra codificada. Mensagem numérica:

   $$14, 1, 15, 16, 1, 18, 5, 1, 20, 5, 19, 5, 15, 18, 7, 21, 12, 8, 1, 18, 4, 5, 22, 15, 3, 5$$

   - $f(14) = 2.14 = 28$
   - $f(1) = 2.1 = 2$

- $f(15) = 2.15 = 30$
- $f(16) = 2.16 = 32$
- $f(18) = 2.18 = 36$
- $f(5) = 2.5 = 10$
- $f(20) = 2.20 = 40$
- $f(19) = 2.19 = 38$
- $f(7) = 2.7 = 14$
- $f(21) = 2.21 = 42$
- $f(12) = 2.12 = 24$
- $f(8) = 2.8 = 16$
- $f(4) = 2.4 = 8$
- $f(22) = 2.22 = 44$
- $f(3) = 2.3 = 6$

Então o código da frase motivacional escolhida por Maria ficou assim:"**28, 2, 30, 32, 2, 36, 10, 2, 40, 10, 38, 10, 30, 36, 14, 42, 24, 16, 2, 36, 8, 10, 44, 30, 6, 10**".

4. Ainda em relação a questão número 3. E se a regra dada pela professora agora fosse: o dobro do valor original da letra adicionado uma unidade, e Maria recebesse de seu colega a mensagem : "39, 31, 29, 17, 31, 39, 29, 3, 31, 41, 11, 27, 33, 11, 37, 29, 3, 39, 31, 33, 3, 33, 11, 25, 9, 11, 7, 31, 37,37, 11, 37, 3, 41, 37, 3, 39, 9, 11, 25, 11, 39, 11, 39,11, 43". Qual seria a frase motivacional recebida por ela?

   Desenvolvimento: Novamente, iremos denominar de x o valor original da letra na tabela e de y o valor da letra codificada. No enunciado foi apresentada a regra para codificar a mensagem: $f(x) = 2.x + 1$, assim vamos utilizar a função inversar para decodifica-la, lembrando que para achar a função inversa, basta isolarmos x na equação. Assim temos:

$$f^{-1}(y) = \frac{y-1}{2}$$

Vamos substituir y pelos valores da mensagem codificada e encontrar as letras da mensagem original.

- Para $y = 39$, temos: $\frac{39-1}{2} = x \Longrightarrow x = 19$, que corresponde a letra **S**
- Para $y = 31$, temos: $\frac{31-1}{2} = x \Longrightarrow x = 15$, que corresponde a letra **O**
- Para $y = 17$, temos: $\frac{17-1}{2} = x \Longrightarrow x = 8$, que corresponde a letra **H**
- Para $y = 3$, temos: $\frac{3-1}{2} = x \Longrightarrow x = 1$, que corresponde a letra **A**
- Para $y = 41$, temos: $\frac{41-1}{2} = x \Longrightarrow x = 20$, que corresponde a letra **T**
- Para $y = 11$, temos: $\frac{11-1}{2} = x \Longrightarrow x = 5$, que corresponde a letra **E**
- Para $y = 27$, temos: $\frac{27-1}{2} = x \Longrightarrow x = 13$, que corresponde a letra **M**
- Para $y = 33$, temos: $\frac{33-1}{2} = x \Longrightarrow x = 16$, que corresponde a letra **P**
- Para $y = 37$, temos: $\frac{37-1}{2} = x \Longrightarrow x = 18$, que corresponde a letra **R**
- Para $y = 25$, temos: $\frac{25-1}{2} = x \Longrightarrow x = 12$, que corresponde a letra **L**
- Para $y = 9$, temos: $\frac{9-1}{2} = x \Longrightarrow x = 4$, que corresponde a letra **D**
- Para $y = 7$, temos: $\frac{7-1}{2} = x \Longrightarrow x = 3$, que corresponde a letra **C**
- Para $y = 43$, temos: $\frac{43-1}{2} = x \Longrightarrow x = 21$, que corresponde a letra **U**

Substituindo os valores numéricos pelas letras encontradas temos a mensagem recebida por Maria: **"Sonhos não têm pernas. O papel de correr atrás deles é seu."**

5. Júlio gostou tanto da aula de matemática, em que o professor ensinou criptografar mensagens usando funções, que resolveu mandar no grupo de whatsapp da turma o seguinte recado criptografado: $-21, 15, -21, 18, 0, -21, 36, -9, 30, -9, 15, 21, 33, 36, 30, -9, 3, 18, 21, -12, -9, -18, -21, 33, 27, 39, -9, 36, -9$. Decifre o recado enviado por Júlio, sabendo que a chave que ele usou para codificar, foi a lei matemática: $y = 3.(x - 8)$.

   Desenvolvimento:Para decodificarmos a mensagem enviada por Júlio, basta fazermos o inverso do que ele fez para codificá-la, ou seja, basta utilizarmos a função inversa de $f(x) = 3.(x - 8)$:

$$f^{-1}(y) = \frac{y}{3} + 8,$$

sendo y o valor númerico da mensagem codificada e $f^{-1}(y) = x$ o valor numérico da mensagem original, temos:

- Para $y = -21$, temos: $\frac{-21}{3} + 8 = x \Longrightarrow x = 1$, que corresponde a letra **A**
- Para $y = 15$, temos: $\frac{15}{3} + 8 = x \Longrightarrow x = 13$, que corresponde a letra **M**
- Para $y = 18$, temos: $\frac{18}{3} + 8 = x \Longrightarrow x = 14$, que corresponde a letra **N**
- Para $y = 0$, temos: $\frac{0}{3} + 8 = x \Longrightarrow x = 8$, que corresponde a letra **H**
- Para $y = 36$, temos: $\frac{36}{3} + 8 = x \Longrightarrow x = 20$, que corresponde a letra **T**
- Para $y = -9$, temos: $\frac{-9}{3} + 8 = x \Longrightarrow x = 5$, que corresponde a letra **E**
- Para $y = 30$, temos: $\frac{30}{3} + 8 = x \Longrightarrow x = 18$, que corresponde a letra **R**
- Para $y = 21$, temos: $\frac{21}{3} + 8 = x \Longrightarrow x = 15$, que corresponde a letra **O**
- Para $y = 33$, temos: $\frac{33}{3} + 8 = x \Longrightarrow x = 19$, que corresponde a letra **S**
- Para $y = 3$, temos: $\frac{3}{3} + 8 = x \Longrightarrow x = 9$, que corresponde a letra **I**
- Para $y = -12$, temos: $\frac{-12}{3} + 8 = x \Longrightarrow x = 4$, que corresponde a letra **D**
- Para $y = -18$, temos: $\frac{-18}{3} + 8 = x \Longrightarrow x = 2$, que corresponde a letra **B**
- Para $y = 27$, temos: $\frac{27}{3} + 8 = x \Longrightarrow x = 17$, que corresponde a letra **Q**
- Para $y = 39$, temos: $\frac{39}{3} + 8 = x \Longrightarrow x = 21$, que corresponde a letra **U**

Substituindo os valores da mensagem codificada pelas letras correspondentes encontradas, temos a mensagem de Julio decifrada: **"Amanhã teremos treino de basquete".**

OBSERVAÇÃO 3.2.2 *Nesta atividade é importante os alunos perceberem que os números* -18 *e* 18 *;* -21 *e* 21*, correspondem a letras diferentes.*

6. Em uma gincana de circuito, feita na escola, para vencer o grupo deveria decifrar as mensagens para encontrar as bandeiras e marcar pontos. Foi informada a regra de criptação utilizada para manter em segredo o local onde estavão escondidas as bandeiras:

- Regra: $y = x^2$, com $x \epsilon \mathbb{N}$
- Dica:
  (a) Bandeira amarela: $4, 81, 4, 144, 81, 225, 400, 25, 9, 1$
  (b) Bandeira azul: $324, 25, 36, 25, 81, 400, 225, 324, 81, 225$
  (c) Bandeira vermelha: $289, 441, 1, 16, 324, 1$

Utilize as informações dadas e decifre o local onde estariam escondidas as bandeiras.

Desenvolvimento: Assim como nos exercícios anteriores, vamos utilizar a função inversa para decifrar as dicas dadas.

$$\text{Chave de decodificação: } f^{-1}(y) = \sqrt{y}$$

(a) Bandeira amarela: $4, 81, 4, 144, 81, 225, 400, 25, 9, 1$

- Para $y = 4$, temos: $\sqrt{4} = x \Longrightarrow x = 2$, que corresponde a letra **B**
- Para $y = 81$, temos: $\sqrt{81} = x \Longrightarrow x = 9$, que corresponde a letra **I**
- Para $y = 144$, temos: $\sqrt{144} = x \Longrightarrow x = 12$, que corresponde a letra **L**
- Para $y = 225$, temos: $\sqrt{225} = x \Longrightarrow x = 15$, que corresponde a letra **O**
- Para $y = 400$, temos: $\sqrt{400} = x \Longrightarrow x = 20$, que corresponde a letra **T**
- Para $y = 25$, temos: $\sqrt{25} = x \Longrightarrow x = 5$, que corresponde a letra **E**
- Para $y = 9$, temos: $\sqrt{9} = x \Longrightarrow x = 3$, que corresponde a letra **C**
- Para $y = 1$, temos: $\sqrt{1} = x \Longrightarrow x = 1$, que corresponde a letra **A**

Dica decifrada: **Biblioteca**

(b) Bandeira azul:$324, 25, 36, 25, 81, 400, 225, 324, 81, 225$

- Para $y = 324$, temos: $\sqrt{324} = x \Longrightarrow x = 18$, que corresponde a letra **R**
- Para $y = 25$, temos: $\sqrt{25} = x \Longrightarrow x = 5$, que corresponde a letra **E**
- Para $y = 36$, temos: $\sqrt{36} = x \Longrightarrow x = 6$, que corresponde a letra **F**
- Para $y = 81$, temos: $\sqrt{81} = x \Longrightarrow x = 9$, que corresponde a letra **I**
- Para $y = 400$, temos: $\sqrt{400} = x \Longrightarrow x = 20$, que corresponde a letra **T**
- Para $y = 225$, temos: $\sqrt{225} = x \Longrightarrow x = 15$, que corresponde a letra **O**

Dica decifrada: **Refeitório**

(c) Bandeira vermelha: $289, 441, 1, 16, 324, 1$

- Para $y = 289$, temos: $\sqrt{289} = x \Longrightarrow x = 17$, que corresponde a letra **Q**
- Para $y = 441$, temos: $\sqrt{441} = x \Longrightarrow x = 21$, que corresponde a letra **U**
- Para $y = 1$, temos: $\sqrt{1} = x \Longrightarrow x = 1$, que corresponde a letra **A**
- Para $y = 16$, temos: $\sqrt{16} = x \Longrightarrow x = 4$, que corresponde a letra **D**
- Para $y = 324$, temos: $\sqrt{324} = x \Longrightarrow x = 18$, que corresponde a letra **R**

Dica decifrada: **Quadra**

Capítulo 4

Método RSA

Neste capítulo iremos apresentar, sem muito aprofundamento, o passo a passo para implementação do método RSA, e ainda, apresentaremos aqui algumas sugestões de atividades para alunos do ensino médio. Todos os resultados aqui apresentados tiveram como base as referências [1], [4], [6], [13] e [14].

Entre os códigos de chave pública, o método RSA é, atualmente, o mais utilizado em transações comerciais. Ele 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. Nesta seção temos como objetivo apresentar, através de uma linguagem simples, o funcionamento do método RSA e porque ele é tão eficiente e seguro.

Para implantar esse método de criptografia de chave pública, veremos a seguir que é preciso escolher dois números primos muito grandes p e q, para assim criar a chave pública(n, α), onde n é produto dos números primos escolhidos e α será definido mais adiante, para decodificar é preciso conhecer tais números p e q. Assim, a segurança do método está na dificuldade de fatorar n para descobrir p e q. Veremos o passo a passo deste método com mais detalhes nas seções a seguir.

4.1 Codificando uma Mensagem

Sabemos que no método RSA os primos escolhidos são números muito grandes, porém para compreendermos como funciona este método iremos utilizar um exemplo com

valores pequenos, já que não estamos utilizando nenhum software para auxiliar nos calculos aqui desenvolvidos nessa seção. Traremos, através de etapas, um exemplo simples de mensagem codificada pelo método RSA com o objetivo de entendermos o seu mecanismo de codificação.

Vamos codificar a mensagem: Olá.

- 1ª Etapa: Pré-codificação.

  Neste método a mensagem deve estar na forma numérica, ou seja, deve ser uma sequência de números, assim utilizamos a tabela de conversão 4.1 para realizar uma pré-codificação da mensagem.

Quadro 4.1: Tabela de conversão para a pré-codificação

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

OBSERVAÇÃO 4.1.1 *Cada número da tabela corresponde a um número de dois algarismos. Pois, se caso as letras A e B correspondessem aos número* 1 *e* 2*, respectivamente, e continuássemos a sequencia da tabela, como a letra L seria a décima segunda letra do alfabeto, não saberiamos se o número* 12*, por exemplo, corresponderia a AB ou L.*

De acordo com a nossa tabela de conversão 4.1 a mensagem **OLÁ** pré-codificada corresponderia a sequência 242110**.**

A próxima fase do processo de pré-codificação consiste em escolhermos, de maneira aleatória, dois números primos p e q. O produto desses dois números iremos chamar de n.

Para finalizar essa etapa, iremos quebrar em blocos o número 242110 encontrado. Vamos chamar de $b_1, b_2, ..., b_n$ os blocos formados, cada bloco deve ser menor que o número n encontrado, os blocos não precisam necessariamente ter os mesmos

tamanhos e não podem começar pelo número 0, pois isso causaria problema na hora de decodificar, já que, um bloco 012 seria o mesmo que um bloco 12, por exemplo.

Assim realizando a substituição das letras por números, obtemos a mensagem **OLÁ** pré-codificada: **24-21-10**. E escolhendo $p = 5$ e $q = 7$, obtemos $n = 35$. Agora vamos a próxima etapada.

- 2ª Etapa: Codificação

  Para codificarmos cada bloco fazemos:

  $$C(b) = \text{resto da divisão de } b^{\alpha} \text{ por } n,$$

  onde $C(b)$ é o bloco codificado, b o bloco original e α calculamos através da função de Euler $\phi(n) = (p-1).(q-1)$, tal que $mdc(\alpha, \phi(n)) = 1$. Assim temos, $\phi(35) = (5-1).(7-1) = 24$, como α e $\phi(35) = 24$, devem ser primos entre si, escolhemos $\alpha = 5$.

  Assim, temos a nossa **chave pública**$(n, \alpha) = (35, 5)$**.**

  Agora vamos codificar cada bloco do nosso exemplo:

  Para $b_1 = 24$, temos: $24^5 = 24^2.24^2.24 \equiv 16.16.24 \equiv 11.24 \equiv 19 \mod 35$

  Para $b_2 = 21$, temos: $21^5 = 21^2.21^2.21 \equiv 21.21.21 \equiv 21.21 \equiv 21 \mod 35$

  Para $b_3 = 10$, temos: $10^5 = 10^2.10^2.10 \equiv (-5).(-5).10 \equiv 5 \mod 35$

  Assim, temos os blocos codificados: $C(24) = 19$, $C(21) = 21$ e $C(10) = 5$. E a mensagem codificada correspondente:

$Mensagem$	$Pre-codificada$	$Codificada$
OLA	$24-21-10$	$19-21-5$

4.2 Decodificando uma Mensagem

Já vimos como obter a chave pública(n, α) e quais são as etapas para codificar uma mensagem pelo método RSA, agora veremos como decifrá-la. Primeiramente precisamos de uma chave de decodificação, essa chave também é formada por um par de números, um desses números é o n que já utilizamos anteriormente na chave de codificação e o

outro é o d, que corresponde ao inverso de $\alpha \ mod\,(p-1).(q-1)$, ou seja, o número que multiplicado por α é congruente a 1 módulo $(p-1).(q-1)$.

$5.d \equiv 1\, mod(5-1).(7-1) = 24$, logo $24|5d-1$, assim temos que $d = 5$.

Assim, temos a nossa **chave privada**$(n, d) = (35, 5)$**.**E agora vamos decodificar cada bloco do nosso exemplo.

A regra para decodificar uma mensagem é semelhante a de codificação. Iremos considerar cada bloco $C(b)$ codificado e transformaremos novamente no bloco b original. A diferença é que anteriormente utilizamos o expoente α, e agora iremos utilizar como expoente o $d = 5$ que acabamos de encontar.

Assim, para decodificarmos cada bloco calculamos o seguinte:

$$b = \text{resto da divisão de } D(C(b))^d \text{ por } n \ ,$$

Vamos codificar cada bloco do nosso exemplo:

Para $D(19)$, temos: $19^5 = 19^2.19^2.19 \equiv 11.11.19 \equiv 16.19 \equiv 24 \quad mod\, 35$

Para $D(21)$, temos: $21^5 = 21^2.21^2.21 \equiv 21.21.21 \equiv 21.21 \equiv 21 \quad mod\, 35$

Para $D(5)$, temos: $5^5 = 5^3.5^2 \equiv 20.25 \equiv 10 \quad mod\, 35$

Assim, temos os blocos decodificados: $D(19) = 24$, $D(21) = 21$ e $D(5) = 10$, que correspondem as letras OLA, de acordo com a tabela de conversão 4.1.

Uma das razões para a eficiência do método RSA é a inexistência de uma ferramenta que consiga rapidamente fatorar números muito grandes. Segundo Coutinho[6], "... não existem computadores rápidos o suficiente, nem algoritmos bons o suficiente, que nos permitam fatorar um número inteiro muito grande que não tenha fatores relativamente pequenos."Logo, se os primos p e q escolhidos forem muito grandes o valor de n fica maior ainda, dificultando a fatoração. E se não consegue fatorar n, não descobre os números primos p e q, que precisamos para calcular $\phi(n)$ e consequentemente o d, não obtendo assim o par (n, d), que é a nossa chave de decodificação.

4.3 Sugestões de Atividades

Como já foi citado anteriormente, o fato de alguns conteúdos serem apresentados apenas como regras a serem decoradas e reproduzidas sem ligação com o dia-a-dia do aluno, ou seja, sem conhecimento de algumas de suas aplicações, provoca o desinteresse

dos estudantes pelas aulas. Em relação aos conteúdos de aritmética modular, como divisibilidade, números primos, entre outros, podemos apresentar os cálculos de maneira diferente, utilizando novamente a criptografia para contextualizar e dar significado aos conceitos matemáticos. As aplicações podem ser difíceis de serem compreendidas com conhecimentos do ensino médio apenas, porém podemos adaptá-las de tal forma que fiquem acessíveis para os alunos, sem a necessidade de aprofundamentos.

As atividades foram elaboradas relacionando criptografia a conteúdos de aritmética modular, tendo o cuidado de utilizar uma linguagem simples para serem acessíveis a alunos da educação básica. Cada uma das questões estão resolvidas de maneira detalhada e com a sugestão de desenvolvimento, a segunda questão é uma proposta de dinâmica de sala utilizando o aplicativo(app) CodeClass, assim antes das atividades propostas faremos uma breve apresentação do app.

4.3.1 Aplicativo CodeClass

O CodeClass é um aplicativo que apresenta de maneira simples, os processos necessários para implementação do método de criptografia RSA. Para ter acesso ao aplicativo, basta acessar do celular o link disponível em [15], entrar na pasta do drive e fazer o download. O aplicativo possui três funções: Criptografia Linear, Criptografia RSA e um módulo gerador de números primos, como pode ser observado na figura 4.1 que apresenta a tela inicial do aplicativo .

Figura 4.1: Tela inicial do aplicativo CodeClass

Após entrarmos na opção CRIPTOGRAFIA RSA, temos uma nova tela, como mostra a figura 4.2, onde temos acesso a três módulos para operar: Gerar Chaves, Criptografar Mensagem e Decifrar Mensagem. As opções são completamente independentes, não sendo necessário preencher informações em uma opção para utilização da outra.

Figura 4.2: Tela Criptografia RSA, opções: Gerar chaves, Criptografar Mensagem, Decifrar Mensagem e Voltar

O que faz cada uma das opções descritas na figura 4.2 :

- **Gerar Chaves:** Para gerar chaves, basta inserir dois números primos distintos, de no máximo 3 dígitos, para um melhor funcionamento do programa, e precionar o botão VERIFICAR PRIMALIDADE. O programa então irá verificar a primalidade dos números e posteriormente irá liberar a opção para geração das chaves. Exemplo, na figura 4.3, de geração de chaves com os números primos $p = 137$ e $q = 113$.

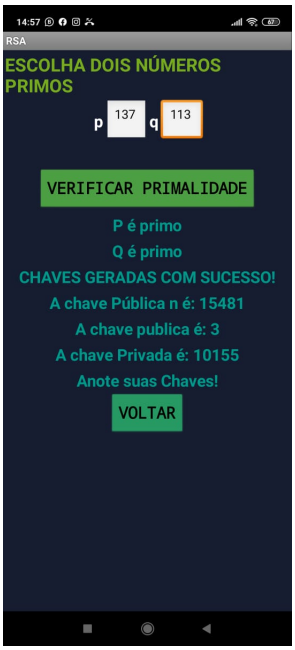

Figura 4.3: Tela do app CodeClass: Gerar Chaves

Na figura 4.3 acima, podemos observar que ao inserir dois números primos o aplicativo gera três números e os denomina como: chave pública n, chave pública e chave privada. Mas como são calculados esses valores?

Vimos anteriormente neste mesmo capítulo, como são geradas as chaves públicas e privadas no método RSA, e no aplicativo não é diferente, ele apenas utiliza outras notações, n, $Cpub$ e $Cpriv$, como veremos mais adiante.

A chave pública n, por exemplo, nada mais é do que o produto dos números primos preenchidos no app. A chave pública igual a 3 que aparece na figura 4.3 é o α, que como já vimos é calculado sabendo que o $mdc(\alpha, \phi(n)) = 1$. Verificando temos, $\phi(15481) = (137 - 1).(113 - 1) = 15232$ e como α e $\phi(15481) = 15232$, devem ser primos entre si, concluímos que o número 3 que no app aparece como chave pública

realmente corresponde ao valor de α. A outra informação que o app gera é a chave privada igual a 10155, este valor corresponde ao d, que já mostramos ao longo deste capítulo, é o inverso de $\alpha \ mod\,(p-1).(q-1)$, ou seja, o número que multiplicado por α é congruente a 1 módulo $(p-1).(q-1)$. De fato, pois $d = 10155$ é o inverso de $\alpha = 3$ módulo 15232, como mostra o app.

Quando o usúario abrir a tela de Criptografar ou Decifrar mensagem no app, ele irá se deparar com as notações: n, $Cpublica$ ou $Cpub$ e $Cprivada$ ou $Cpriv$, elas correspondem as chaves públicas e privadas. Assim, após gerar as chaves anote-as da seguinte maneira, como no exemplo 4.3.1 abaixo, para facilitar no momento de utilizá-las.

EXEMPLO 4.3.1 *Chaves geradas com os números primos $p = 137$ e $q = 113$.*

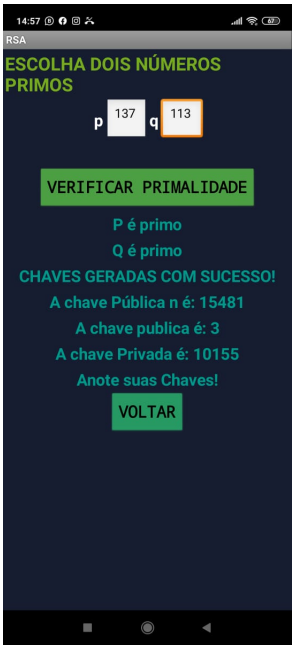

Figura 4.4: Gerar Chaves com os números primos $p = 137$ e $q = 113$

Chave pública$(n, Cpub) = (15481, 3)$ ***Chave privada***$(n, Cpriv) = (15481, 10155)$**.**

- **Criptografar Mensagem:** Nesta opção o usuário já de posse da chave pública:$(n, Cpub)$, pode iniciar o processo de codificação.

EXEMPLO 4.3.2 *Simulação de envio de Mensagem entre dois usuários Clara(receptora) e Marcos (rementente).*

Clara: *Pública:*$(n, Cpub) = (15481\,,\,3)$ *Privada:*$(n, Cpriv) = (15481\,,\,10155)$.

Marcos: *Pública:*$(n, Cpub) = (13483\,,\,5)$ *Privada:*$(n, Cpriv) = (13483\,,\,7949)$.

Para que Marcos consiga enviar uma mensagem para Clara, ele precisa ter conhecimento da chave pública dela e assim, preencher no aplicativo, na tela de criptografar mensagem, os campos n e Cpub com a chave pública de Clara, que é a destinatária. O próximo passo é escrever a sua mensagem, sempre respeitando um caractere por caixa e utilizando sempre letras maiúsculas.

O usuário pode ainda enviar a mensagem assinada ou não, para assinar basta marcar a opção Assinar Mensagem *e em seguida preencher nos espaços indicados com sua chave privada.*

Preenchido todos os campos, agora para enviar a mensagem criptografada basta apertar o botão COMPARTILHAR.

Na figura 4.5, podemos ver com mais detalhes o passo a passo realizado por Marcos para codificar a mensagem - BOA TARDE - que quer enviar a Clara e ainda como ficou a mensagem na forma codificada.

Figura 4.5: Mensagem criptografada por Marcos, o emissor

Observação 4.3.1 *A assinatura é sempre realizada com a chave privada do autor da mensagem, ou seja, o remetente que neste caso é Marcos. Caso haja uma in-*

versão destas chaves, será impossível para o receptor, no caso, Clara decodificar a informação.

- **Decifrar Mensagem:** Nesta opção, para decodificar a mensagem o receptor deve inserir em cada quadradinho os números que foram recebidos sem alterar a ordem e depois preencher os campos n e $Cpriv$ com a sua chave privada e então pressionar o botão DECODIFICAR MENSAGEM. Assim, para finalizar o usuário pode pressionar o botão CONVERTER PARA TEXTO, para que seja modificado o conteúdo para caracteres alfabéticos.

  Observação 4.3.2 *Caso a mensagem tenha sido assinada, deve ser marcado o campo* Mensagem Assinada *e entrar com as chaves públicas do remetente, e assim pressionar o botão DECODIFICAR MENSAGEM, que o sistema irá proceder da mesma forma que a decodificação sem assinatura, além de ter a certeza sobre a autoria do conteúdo.*

  Na sequência, na figura 4.6, temos a tela do app na opção decifrar mensagem, com o passo a passo realizado por Clara. E para decifrar o recado de Marcos, ela preencheu os quadradinhos com os números recebidos, respeitando a ordem dos blocos e inseriu sua chave privada$(n, Cpriv)$. Como Marcos assinou a mensagem, Clara selecionou a caixa *"mensagem assinada"* e inseriu a chave pública$(n, Cpub)$ dele.

Figura 4.6: Mensagem Decifrada pela destinatária Clara

O aplicativo tem também a opção GERADOR DE PRIMOS , nessa tela o usuário tem as opções de verificar a primalidade de um certo número ou gerar uma lista de números primos, exemplo na figura 4.7. Para apenas verificar se o número é primo, basta digitá-lo no campo específico e clicar em VERIFICAR PRIMALIDADE. No caso de gerar números primos, basta clicar na opção GERAR PRIMOS, o programa iniciará uma lista de números e só irá parar até que o usuário interrompa, clicando na opção PARAR.

Figura 4.7: Tela: verificar a primalidade e gerar números primos

4.3.2 Atividades

Lista - Implementação do método RSA.

1. As transações de compras pela internet utilizam o método de criptografia RSA para manter dados bancários em sigílo. Por exemplo, o site da loja gera uma chave pública, disponível para qualquer pessoa que queira realizar uma compra. Assim que o comprador insere os dados do seu cartão de crédito, esses dados são codificados utilizando essa chave e enviados para a loja, que de posse da chave privada decodifica e decifra os dados do cartão. Em grupos iremos realizar uma brincadeira de troca de informações, com base no código RSA. Para facilitar teremos um passo a passo a ser seguido. O grupo I será a loja e irá criar a sua chave pública e privada, já o grupo II representara o comprador e ira criar uma sequência de seis dígitos que simulará o número de um cartão de crédito. O grupo I, por exemplo, enviará a sua chave publica para o grupo II que irá codificar um número de seis dígitos, escolhidos aleoatoriamente, e devolverá a mensagem numérica ao grupo I que irá decifrá-la, através de sua chave privada.

Passo a passo.

Atividade do Grupo I.(Parte I)

A loja: Criando a Chave Pública (n, α) e a Chave Privada (n, d)

I. Escolha dois números primos maiores que 2 **e chame-os de primo** p **e primo** q**: (para facilitar os cálculos, limite sua escolha aos primos menores ou igual a** 11**).**

$p : 3 \qquad q : 5$

II. Calcule $n = p.q$

$n = 3.5 = 15$

III. Calcule $\phi(n) = (p-1).(q-1)$

$\phi(15) = (3-1).(5-1) = 8$

IV. Escolher o menor número (α) **possível maior que** 2 **para que o** $mdc(\alpha, \phi(n)) = 1$**. Esta escolha se dará através de tentativa e erro, iniciando pelo número** 3**.**

$mdc(\alpha, 8) = 1$, temos $\alpha = 3$.

V. Assim temos a **Chave pública:**$(15, 3)$.

VI. Agora vamos calcular o valor d**, que multiplicado pelo valor de** α **tenha resto** 1 **quando dividido por** $\phi(n)$**, ou seja,** $\{\alpha.d \equiv 1 \; mod \phi(n)\}$ **ou** $\{\phi(n).b + 1 = \alpha.d\}$**.**

$3.d \equiv 1 \quad mod 8$, temos que $d = 3$.

VII. Assim temos a **Chave privada:**$(15, 3)$.

VIII. Agora o grupo deve manter secreta a chave privada e fornecer ao grupo II**, o comprador, a chave pública.**

Observação 4.3.3 *Vamos aguardar o grupo II (comprador), codificar o número do seu cartão de crédito e retornar a mensagem para decifrarmos).*

Atividade do Grupo II.

Comprador: Codificando o número do cartão.

I. Número do meu cartão: 123456 e **Chave Pública fornecida pelo grupo I, receptor da mensagem:** $(15, 3)$.

II. Quebre a mensagem em blocos para serem menores de n e que não iniciem com 0**. (Escolha aleatória).**

$12 - 3 - 4 - 5 - 6$

III. Eleve cada bloco ao expoente α**.**

$12^3 = 1728$

$3^3 = 27$

$4^3 = 64$

$5^3 = 125$

$6^3 = 216$

IV. Obtenha o resto r **do resultado do passo** III **dividido por** n**.** $\{b^\alpha \equiv r\ modn\}$ **ou** $\{b^\alpha = x.n + r\}$

$12^3 \equiv r\ mod\ 15$

$1728 \equiv 3\ mod\ 15$

$3^3 \equiv r\ mod\ 15$

$27 \equiv 12\ mod\ 15$

$4^3 \equiv r\ mod\ 15$

$64 \equiv 4\ mod\ 15$

$5^3 \equiv r\ mod\ 15$

$125 \equiv 5\ mod\ 15$

$6^3 \equiv r\ mod\ 15$

$216 \equiv 6\ mod\ 15$

V. Anote em sequência os blocos. Essa sequência é a mensagem criptografada, ou seja, o número do cartão de crédito na forma codificada, que deve ser enviado a loja(grupo I).

Número codificado do cartão: 312456.

Atividade do Grupo I.(Parte II)

A loja: Decodificando o número do cartão de crétido recebido.

I. Mensagem numérica recebida do grupo II: 312456.

II. Quebre a mensagem em blocos para serem menores de n e que não iniciem com 0. (Escolha aleatória).

$3 - 12 - 4 - 5 - 6$

III. Eleve cada bloco codificado ao expoente d.

$3^3 = 27$

$12^3 = 1728$

$4^3 = 64$

$5^3 = 125$

$6^3 = 216$

IV. Obtenha o resto do resultado do passo III dividido por n. $\{a^d \equiv r\ modn\}$ ou $\{a^d = x.n + r\}$.

$3^3 \equiv r\ mod\ 15$

$27 \equiv 12\ mod\ 15$

$12^3 \equiv r\ mod\ 15$

$1728 \equiv 3\ mod\ 15$

$4^3 \equiv r\ mod\ 15$

$64 \equiv 4\ mod\ 15$

$5^3 \equiv r\ mod\ 15$

$125 \equiv 5\ mod\ 15$

$6^3 \equiv r\ mod\ 15$

$216 \equiv 6\ mod\ 15$

V. Anote em sequência os blocos. Essa sequência é a mensagem decodificada.

Número do cartão de crédito : 123456.

VI. A mensagem está correta? (Conferir com o grupo II).

SIM.

A seguir apresentamos outra sugestão de resolução agora com o grupo I como comprador e o grupo II como sendo o site da loja onde será realizada a compra.

Passo a passo.

Atividade do Grupo II.(Parte I)

A loja: Criando a Chave Pública (n, α) e a Chave Privada (n, d)

I. Escolha dois números primos maiores que 2 **e chame-os de primo** p **e primo** q**: (para facilitar os cálculos, limite sua escolha aos primos menores ou igual a** 11**).**

$p : 5 \qquad q : 7$

II. Calcule $n = p.q$

$n = 5.7 = 35$

III. Calcule $\phi(n) = (p-1).(q-1)$

$\phi(35) = (5-1).(7-1) = 24$

IV. Escolher o menor número (α) **possível maior que** 2 **para que o** $mdc(\alpha, \phi(n)) = 1$**. Esta escolha se dará através de tentativa e erro, iniciando pelo número** 3**.**

$mdc(\alpha, 24) = 1$, temos $\alpha = 5$.

V. Assim temos a **Chave pública:**$(35, 5)$.

VI. Agora vamos calcular o valor d**, que multiplicado pelo valor de** α **tenha resto** 1 **quando dividido por** $\phi(n)$**, ou seja,** $\{\alpha.d \equiv 1 \; mod \phi(n)\}$ **ou** $\{\phi(n).b + 1 = \alpha.d\}$**.**

$5.d \equiv 1 \quad mod 24$, temos que $d = 5$.

VII. Assim temos a **Chave privada:**$(35, 5)$.

VIII. Agora o grupo deve manter secreta a chave privada e fornecer ao grupo I, o comprador, a chave pública.

OBSERVAÇÃO 4.3.4 *Vamos aguardar o grupo I (comprador), codificar o número do seu cartão de crédito e retornar a mensagem para decifrarmos.*

Atividade do Grupo I.

Comprador: Codificando o número do cartão.

I. Número do meu cartão: 411253 e **Chave Pública fornecida pelo grupo II, receptor da mensagem:** $(35, 5)$.

II. Quebre a mensagem em blocos para serem menores de n e que não iniciem com 0**. (Escolha aleatória).**

$4 - 11 - 25 - 3$

III. Eleve cada bloco ao expoente α**.**

$4^5 = 1024$

$11^5 = 161.051$

$25^5 = 9.765.625$

$3^5 = 243$

IV. Obtenha o resto r **do resultado do passo** III **dividido por** n**.** $\{b^\alpha \equiv r\ mod n\}$ **ou** $\{b^\alpha = x.n + r\}$

$4^5 \equiv r\ mod\ 35$

$10241 \equiv 9\ mod\ 35$

$11^5 \equiv r\ mod\ 35$

$161.051 \equiv 16\ mod\ 35$

$25^5 \equiv r\ mod\ 35$

$9.765.625 \equiv 30\ mod\ 35$

$3^5 \equiv r\ mod\ 35$

$243 \equiv 33\ mod\ 35$

V. Anote em sequência os blocos. Essa sequência é a mensagem criptografada, ou seja, o número do cartão de crédito na forma codificada, que deve ser enviado a loja(grupo II).

Número codificado do cartão: 9163033.

Atividade do Grupo II.(Parte II)

A loja: Decodificando o número do cartão de crétido recebido.

I. Mensagem numérica recebida do grupo II: 9163033.

II. Quebre a mensagem em blocos para serem menores de n e que não iniciem com 0. (Escolha aleatória).

$9 - 16 - 30 - 33$

III. Eleve cada bloco codificado ao expoente d.

$9^5 = 59.049$

$16^5 = 1.048.576$

$30^5 = 24.300.000$

$33^5 = 39.135.393$

IV. Obtenha o resto do resultado do passo III dividido por n. $\{a^d \equiv r\ mod n\}$ ou $\{a^d = x.n + r\}$.

$9^5 \equiv r\ mod\ 35$

$59.049 \equiv 4\ mod\ 35$

$16^5 \equiv r\ mod\ 35$

$1.048.576 \equiv 11\ mod\ 35$

$30^5 \equiv r\ mod\ 35$

$24.300.000 \equiv 25\ mod\ 35$

$33^5 \equiv r\ mod\ 35$

$39.135.393 \equiv 3\ mod\ 35$

V. Anote em sequência os blocos. Essa sequência é a mensagem decodificada.

Número do cartão de crédito : 411253.

VI. A mensagem está correta? (Conferir com o grupo I).

SIM.

Questionamentos para refletir com os alunos na aula:

- Se um terceiro grupo interceptar a mensagem e tiver acesso a chave pública da loja, ele conseguirá decifrar o número do cartão de crédito utilizado no momento da compra?
- O que precisamos saber para decifrar uma mensagem codificada?
- Conseguimos encontrar p e q através da chave pública?
- Mas e se a chave pública fosse um número grande de 10 dígitos ou mais por exemplo, iriamos conseguir fatorar sem auxílio de alguma tecnologia para descobrir p e q?

CONCLUSÕES E/OU RESPOSTAS ESPERADAS, APARTIR DOS QUESTIONAMENTOS:

Se um terceiro grupo interceptar a mensagem e tiver acesso apenas a chave pública da loja, ele não conseguirá decifrar o número do cartão de crédito utilizado no momento da compra, isso porque para decodificar os blocos ele precisaria do número d, que pertence a chave privada. Como vimos acima para calcular este valor de d é necessário ter conhecimento dos números primos p e q , no caso destes exemplos como $n = p.q$ é um número pequeno é fácil decifrarmos os primos escolhidos, apenas fatorando. Porém se tivessemos n grande, não conseguiriamos fatorar para achar p e q e assim conseguimos perceber o segredo deste método de criptografia, uma operção fácil de realizar $(n = p.q)$, mas muito díficil de decodificar se não for o destinatário legitimo da mensagem.

2. Vamos realizar uma brincadeira de troca de mensagens, utilizando o aplicativo CodeClass. Para isso organize a sala em trios, dois alunos do trio formado irão trocar

mensagens, um como emissor e outro como destinatário, enquanto que o terceiro irá interceptar a mensagem do emissor e também assim como o receptor irá tentar decifrá-la.

O passo a passo para gerar chaves, codificar e decodificar uma mensagem, assim como outros detalhes estão disponiveis na seção 4.3.1. Abaixo dois exemplos de solução para esta atividade, uma com a mensagem enviada de maneira assinada e outra não.

Emissor: Beatriz, **Destinatário:** Maria e **Terceiro Aluno:** Paulo.

Primeiro Exemplo: Mensagem não assinada.

- Os alunos do trio devem gerar suas chaves pública e privada. Lembrando que devem fornecer a chave pública, ou seja, essa chave deve ser de conhecimento de qualquer um do grupo, já a chave privada deve anotar e manter em segredo.

  As chaves públicas, devem estar disponíveis para qualquer um do grupo, assim uma sugestão é anotar em uma folha e deixar sobre a mesa para que os três (Beatriz, Maria e Paulo) possam ver, ou que a professora anote no quadro o nome de cada um dos alunos da turma e suas respectivas chaves públicas. Caso os alunos encontrem dificuldade em achar números primos, podem utilizar a opção *Gerador de primos* do aplicativo, mais detalhes sobre o gerador de números primos na seção 4.3.1.

  Beatriz:(Chaves geradas por Beatriz na figura 4.8)
  Chave pública $(n, cpub) = (7099, 7)$ e
  Chave privada $(n, cpriv) = (7099, 5863)$

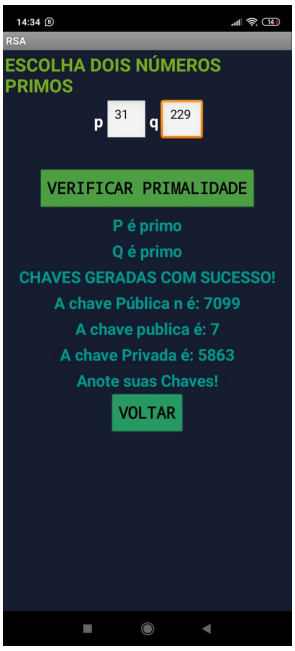

Figura 4.8: Chaves geradas por Beatriz

Maria:(Chaves geradas por Maria na figura 4.9)

Chave pública $(n, cpub) = (2921, 5)$ e

Chave privada $(n, cpriv) = (2921, 1109)$

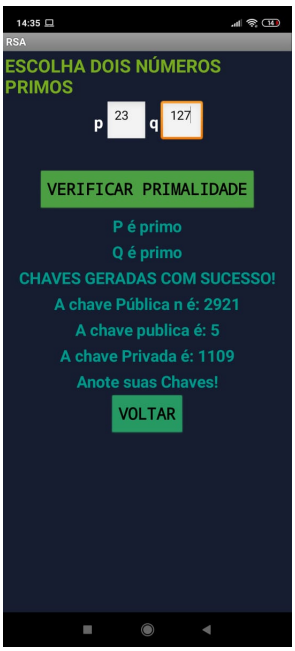

Figura 4.9: Chaves geradas por Maria

Paulo:(Chaves geradas por Paulo na figura 4.10)

Chave pública $(n, cpub) = (721, 5)$ e

Chave privada $(n, cpriv) = (721, 245)$

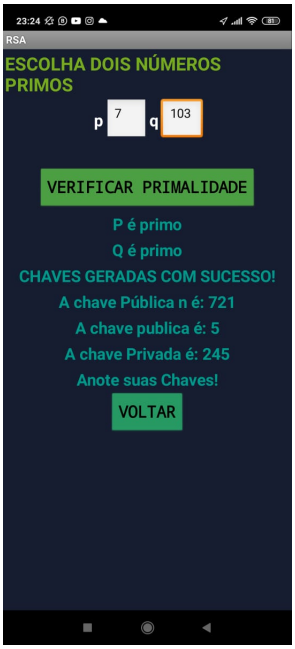

Figura 4.10: Chaves geradas por Paulo

- Beatriz, com a chave pública da destinatária original - Maria, codifica a mensagem - FEZ A TAREFA, sem assiná-la, compartilha com Maria e também envia a mesma mensagem codificada a Paulo, para ele tentar decifrá-la, assim como Maria. Na figura 4.11 podemos observar a chave pública de Maria,utilizada po Beatriz para codificar a mensagem, além do texto original e a mensagem criptografada: $1934 - 204 - 1669 - 1 - 1505 - 1 - 2602 - 204 - 1934 - 1$.

Figura 4.11: Tela com passo a passo realizado por Beatiz

Observação 4.3.5 *Lembrando que para criptografar uma mensagem no aplicativo basta inserir a chave pública da pessoa ao qual você deseja enviar a mensagem, em seguida, escrever o texto colocando uma letra em cada caixa, usando sempre letras maiúsculas. Pronto agora é só clicar em CRIPTOGRAFAR MENSAGEM e depois COMPARTILHAR. Ao clicar em COMPARTILHAR o aluno têm a opção de encaminhar a mensagem pelo whatsapp, mas caso o professor não queira utilizar está opção pode ser anotada a mensagem em um papel e entregue aos colegas do grupo.*

- Assim que recebe a mensagem criptografada, Maria deve copiá-la nos espaços indicados no aplicativo, respeitando a quantidade de números de cada bloco e sem misturá-los. Na figura 4.12, podemos observar com detalhes o passo a passo realizado por ela.

Figura 4.12: Tela com passo a passo realizado por Maria

Paulo, o terceiro aluno, também teve acesso a mesma mensagem recebida por Maria, e deve tentar decifrá-la com auxilio do aplicativo e discutir com o grupo a dificuldade enfrentada.

Observação 4.3.6 *Lembrando que para decodificar a mensagem, utilize o campo* decifrar mensagem*, digíte os blocos de números recebidos, insira sua chave privada, em seguida, clique em DECODIFICAR MENSAGEM e depois em MENSAGEM ALFABÉTICA.*

Logo, assim que Paulo inserir sua chave privada e tentar decodificar a mensagem o aplicativo apresentará uma tela de erro, como mostra a figura 4.13 abaixo. Isso acontece, pois para decifrar a mensagem a chave privada deve ser compatível com a pública utilizada no momento de codificar, portanto somente Maria, a destinatária legítima, com sua chave privada irá conseguir decodificar a mensagem.

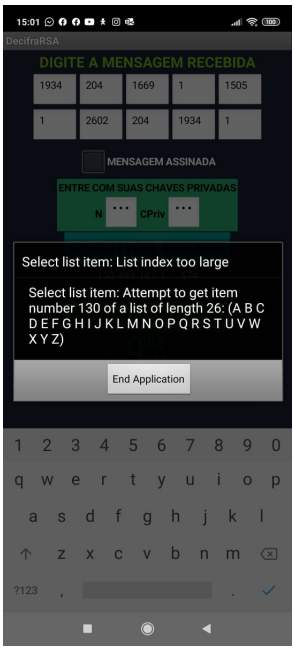

Figura 4.13: Erro ao tentar decifrar Mensagem

Segundo exemplo: Mensagem Assinada pela Remetente - Beatriz.

- Aqui também os alunos, Beatriz, Maria e Paulo devem gerar suas chaves públicas e privadas. Lembrando, novamente, que devem fornecer apenas a chave pública, ou seja, essa chave deve ser de conhecimento de qualquer um do grupo, já a chave privada deve anotar e manter em segredo.

  As chaves públicas, devem estar disponíveis para qualquer um do grupo, assim uma sugestão é anotar em uma folha e deixar sobre a mesa para que os três (Beatriz, Maria e Paulo) possam ver, ou que a professora anote no quadro o nome de cada um dos alunos da turma e suas respectivas chaves públicas. Caso os alunos encontrem dificuldade em achar números primos, podem utilizar a opção *Gerador de primos* do aplicativo, mais detalhes sobre o gerador de números primos na seção 4.3.1.

  Beatriz:(Chaves geradas por Betriz na figura **??**)

  Chave pública $(n, cpub) = (7099, 7)$ e

  Chave privada $(n, cpriv) = (7099, 5863)$

  Maria:(Chaves geradas por Maria na figura **??**)

  Chave pública $(n, cpub) = (2921, 5)$ e

Chave privada $(n, cpriv) = (2921, 1109)$

Paulo:(Chaves geradas por Paulo na figura 4.10)

Chave pública $(n, cpub) = (721, 5)$ e

Chave privada $(n, cpriv) = (721, 245)$

- Beatriz, com a chave pública da destinatária original - Maria, codifica a mensagem - FEZ A TAREFA, assina, compartilha com Maria e também envia a mesma mensagem codificada a Paulo, para ele tentar decifrá-la, assim como Maria. Na figura 4.14 podemos observar a chave pública de Maria, utilizada por Beatriz para codificar a mensagem, além do texto original, o campo para preencher a chave privada e a mensagem criptografada: $5194 - 3926 - 7001 - 1 - 5490 - 1 - 5851 - 3926 - 5194 - 1$.

Figura 4.14: Tela com mensagem codificada e assinada por Beatriz

Lembrando que para criptografar uma mensagem no aplicativo basta inserir a chave pública da pessoa ao qual você deseja enviar a mensagem, em seguida, escrever o texto colocando uma letra em cada caixa, usando sempre letras maiúsculas. Para assinar a mensagem basta selecionar a caixa *assinar mensagem*, inserir sua chave privada e escrever seu nome no local indicado, como ilustrado na figura 4.14, acima. Pronto agora é só clicar em CRIPTOGRAFAR

E ASSINAR e depois COMPARTILHAR. Ao clicar em COMPARTILHAR o aluno têm a opção de encaminhar a mensagem pelo whatsapp, mas caso o professor não queira utilizar está opção pode ser anotada a mensagem em um papel e entregue aos colegas do grupo.

- Assim que recebe a mensagem criptografada, Maria deve copiá-la nos espaços indicados no aplicativo, respeitando a quantidade de números de cada bloco e sem misturá-los. Na figura 4.15, podemos observar com detalhes o passo a passo realizado por ela.

Figura 4.15: Tela com mensagem decifrada por Maria

Paulo, o terceiro aluno, também teve acesso a mesma mensagem recebida por Maria, e deve tentar decifrá-la com auxílio do aplicativo e discutir com o grupo a dificuldade enfrentada.

Observação 4.3.7 *Lembrando que para decodificar a mensagem, o aluno deve utilizar o campo* decifrar mensagem*, digítar os blocos de números recebidos e insir a sua chave privada. No caso da mensagem assinada pela remetente, o destinatário deve selecionar a opção* mensagem assinada *e insir a chave pública do autor da mensagem, em seguida, clicar em DECODIFICAR MENSAGEM e depois em MENSAGEM ALFABÉTICA.*

Logo, assim que Paulo inserir sua chave privada e tentar decodificar a mensagem o aplicativo apresentará uma tela de erro, como mostra a figura 4.16 abaixo. Isso acontece, pois para decifrar a mensagem a chave privada deve ser compatível com a pública utilizada no momento de codificar, portanto somente Maria, a destinatária legítima, com sua chave privada irá conseguir decodificar a mensagem.

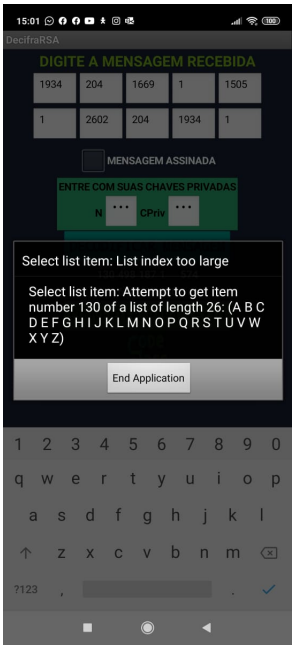

Figura 4.16: Erro ao tentar decifrar Mensagem

- Questionamentos para realizar em sala com os alunos:
  - Maria, conseguiu decifrar a mensagem recebida de Beatriz, nos dois casos, mensagem assinada e não assinada?
  - O que Maria utilizou para decifrar a mensagem codificada recebida?
  - A mesma mensagem com as mesmas chaves quando codificada, na opção assinada, ficou diferente? Por que você acha que isso acontece?
  - O que muda no momento de decifrar, quando a mensagem é assinada?
  - E Paulo conseguiu decifrar a mensagem? Por que?
  - A mensagem assinada, se torna mais segura? Por que?

CONCLUSÕES E/OU RESPOSTAS ESPERADAS, APARTIR DOS QUESTIONAMENTOS PROPOSTOS: Nos dois casos Maria irá conseguir decifrar a mensagem enviada por

Beatriz, já que para isso precisa no primeiro caso (mensagem não assinada), apenas de sua chave privada e no segundo caso (mensagem assinada), além de sua chave privada precisa também da chave pública de Beatriz, que como o próprio nome propõe é de conhecimento de qualquer pessoa. As mensagem codificadas quando assinadas mudam seus caracteres, pois o rementente utiliza, no momento de codificar, a sua chave privada. Quando recebe uma mensagem assinada, não basta somente o destinatário inserir a sua chave privada, como a mensagem foi assinada ele precisa inserir a chave pública do remetente para assim conseguir decifrá-la. O terceiro aluno, Paulo não conseguirá decifrar a mensagem que Beatriz enviou para Maria, isso porque ele não possui a chave privada de Maria. A mensagem assinada se torna mais segura, pois se tem certeza da autoria. Por exemplo, se caso Paulo enviasse a mesma mensagem para Maria e colocasse como remetente, não o seu nome, mas o nome de Beatriz, para tentar enganá-la. Quando ela tentasse decifrar a mensagem no aplicativo e inserisse a chave pública de Beatriz, o aplicativo daria erro. E isso acontece, pois Pedro para assinar a mensagem utilizou a sua chave privada e não a de Beatriz. Enfim, o intuito desta atividade é que os alunos cheguem a conclusão que Paulo, o terceiro aluno, não irá conseguir decifrar a mensagem já que não possui a chave privada de Maria, e com isso perceberem a importância e o segredo de termos uma chave pública e outra privada neste método, além da segurança e legitimidade na informação quando se tem uma mensagem assinada.

No geral, objetivo das atividades e dos questionamentos aqui propostos, nesta seção, é que os alunos percebam a importância dos números primos, como eles influenciam para esse método ser eficiente e seguro. Perceberem ainda que o segredo da criptografia RSA é a fatoração de números primos grandes, já que temos uma opereração fácil de realizar para codificar ($n = p.q$), porém muito difícil de decodificar, já que precisamos fatorar n para conhecer p e q. E ainda, que até mesmo utilizando um recurso tecnológico, se você não é a pessoa ao qual a mensagem fora destinada, não conseguirá decifrá-la. Podendo assim, perceber a eficiência do método e como ele influência de modo significativo em nosso cotidiano, protegendo informações e permitindo o avanço da troca de mensagens de modo a aumentar a praticidade e a comunicação no dia-a-dia.

Capítulo 5

Considerações Finais

Visto que, não é de hoje a necessidade de se manter sígilo em certas informações, conseguimos observar que a criptografia está presente a muito tempo no nosso meio, desde meios de codficação simples até métodos mais atuais e eficientes como o RSA.

Apesar da sua notária importância no que se refere a segurança de informações poucas são as pessoas que têm conhecimento de como seus dados são mantidos secretos e protegidos. Por ser este um tema tão atual e estar ligado a diferentes conteúdos da matemática, a criptografia, de modo especial o método RSA, se torna uma ferramenta motivadora que permite ao aluno vizualizar situações reais do seu cotidiado, saindo de uma aula tradicional de conceitos e fórmulas apenas, solucionando assim um dos maiores desafios dos professores, ensinar matemática de maneira significativa.

O objetivo principal desde trabalho foi ampliar o conhecimento sobre a criptografia, mostrar maneiras de utilizá-la para beneficiar as aulas, buscando dar significado a conteúdos da grade curricular de matemática, de modo especial aos números primos. Para isso foram elaboradas e apresentadas atividades para serem discutidas e realizadas em conjunto na sala de aula, para interação entre professor e aluno. As atividades propostas no trabalho não foram possíveis de serem aplicadas em sala de aula, visto que devido a pandemia do novo coronavírus (Covid-19), e o consequente isolamento social, as escolas foram fechadas e tiveram que se adaptar a nova realidade.

O estudo aqui concluído, contribuiu significativamente na formação de uma base conceitual sólida tanto para minha atuação como professora de matemática no ensino

básico como pode também ajudar outros professores que tenham o interesse e motivação de proporcionar aulas com mais significado e focadas para o contidiano do aluno, buscando mostrar a beleza da matemática que esta escondida por trás de fórmulas e exercícios repetitivos sem significado para os estudantes. É importante que o professor aprofunde seus conhecimentos para conseguir ministrar as aulas tendo conciência que tanto a aula como o conteúdo dado são relevantes não apenas para cumprir a grade curricular, mas para que o aluno perceba a importância de aprender a matemática para ser usado para além da sala de aula.

Referências Bibliográficas

[1] COUTINHO, S. C.**Números Inteiros e Criptografia RSA**. IMPA, Série de Computação e Matemática, Rio de Janeiro, 2005.

[2] ZOCON, R. M.; CESPEDES, L. O.; MERCEDES, J. H.; QUIPUSCOA, A. Z. **Algoritmos para pruebas de primalidad**. Departamento de Matemáticas, Universidad Nacional de Trujillo.

[3] TEREZA, D. M. **A matemática dos testes de primalidade**. Departamento de Matemática, Instituto de Ciências Exatas, Universidade Federal de Juiz de Fora. Disponível em: `https://impa.br/wp-content/uploads/2017/07/31CBM-P_DMTereza.pdf`

[4] GANASSOLI, A. P.; SCHANKOSKI F. R. **Criptografia e Matemática**. Departamento de Matemática, Universidade Federal do Paraná. Disponível via internet: http://www.mat.ufpr.br

[5] SOARES, V. C. **Números Primos: aplicações e primalidade**. Dissertação (Mestrado),Dourados: UEMS, 2015.

[6] COUTINHO, S. C. **Criptografia**. IMPA/OBMEP, Rio de Janeiro, 2015.

[7] **Função totiente de Euler.**Disponível em: `https://pt.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function`. Acesso em: 14/07/2020.

[8] **Função Inversa.**Disponível em: `https://www.todamateria.com.br/funcao-inversa/`. Acesso em: 14/07/2020.

[9] HEFEZ, A. **Aritmética**. Coleção Profmat, Sociedade Brasileira de Matemática, 2016.

[10] PÓVOA, T. M. E. **Estudo sobre os Principais Aspectos da Criptografia Simétrica e Assimétrica ao longo da História**. Dissertação de Mestrado, Universidade de Brasília (UnB), Departamento de Matemática (MAT), PROFMAT/SBM, 2019.

[11] ARAÚJO, P. F. de.**Aplicações de criptografia no ensino médio**. Dissertação (Mestrado), Viçosa, MG, 2017.

[12] ODEMIR M. B.**Criptografia: de arma de guerra a pilar da sociedade moderna.**Jornal USP, disponível em: `jornal.usp.br/?p=63370`. Acesso em: 30/07/2020.

[13] SANTOS B.**Introdução ao software MAXIMA.**Trabalho de Conclusão de Curso, Centro de Matemática da Universidade do Porto, 2009.

[14] ALVES E. A. W.**CodeClass: o uso da tecnologia como recurso metodológico no ensino da criptografia.**Dissertação (Mestrado - PROFMAT), Universidade Estadual do Sudeste da Bahia, 2019.

[15] ALVES E. A. W. **Aplicativo CodeClasspara andriod. CodeClass.apk**. Disponível em: ¡https://drive.google.com/open?id=1ZIGebePmMCXP6gXMrBTfBFWfoQGQXaj¿ ou Disponível em: ¡https://is.gd/lniSDC¿ (encurtador de url). Acessado em: 27/09/2020.