UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS BLUMENAU
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM MATEMÁTICA

Andresa Laurett da Silva

Criptografia e algumas aplicações em sala de aula

Blumenau - SC
2021

Andresa Laurett da Silva

Criptografia e algumas aplicações em sala de aula

Dissertação submetida ao Programa de Pós-Graduação Profissional em Matemática da Universidade Federal de Santa Catarina para a obtenção do título de Mestre Profissional em Matemática.
Orientador: Prof. Dr. Maicon José Benvenutti

Blumenau

2021

Ficha de identificação da obra

Silva, Andresa Laurett da
Criptografia e algumas aplicações em sala de aula / Andresa Laurett da Silva ; orientador, Maicon José Benvenutti, 2021.
121 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Campus Blumenau, Programa de Pós Graduação em Matemática, Blumenau, 2021.

Inclui referências.

1. Matemática. 2. Criptografia. 3. Sistemas criptográficos. 4. Chaves públicas e privadas. I. Benvenutti, Maicon José. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Matemática. III. Título.

Andresa Laurett da Silva

Criptografia e algumas aplicações em sala de aula

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Francis Felix Cordova Puma, Dr.
Universidade Federal de Santa Catarina – Campus Blumenau

Prof. Rafael dos Reis Abreu, Dr.
Universidade Federal de Santa Catarina – Campus Blumenau

Prof.(a) Débora Aparecida Francisco Albanez, Dr.(a)
Universidade Tecnológica Federal do Paraná – Campus Curitiba

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

Documento assinado digitalmente
Marcio de Jesus Soares
Data: 29/07/2021 09:37:55-0300
CPF: 270.670.858-10
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Márcio de Jesus Soares
Coordenador do Programa

Documento assinado digitalmente
Maicon Jose Benvenutti
Data: 29/07/2021 10:23:16-0300
CPF: 041.968.189-27
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Maicon José Benvenutti
Orientador

Blumenau, 2021.

Este trabalho é dedicado aos meus queridos pais e minha filha.

AGRADECIMENTOS

Agradeço a Deus pelas oportunidades que apareceram em minha vida, aos meus pais que através de suas atitudes ensinaram-me a ser honesta, dedicada e a não desistir dos objetivos. Às minhas irmãs e meu irmão que sempre acreditaram em mim. A meu esposo que precisou de muita paciência para escutar as lamentações, não me deixou desistir e ajudou no que foi possível.

Agradeço aos meus colegas de turma que foram parceiros em todos os momentos e fizeram com que as sextas-feiras fossem mais leves e alegres. Todos foram importantes nessa caminhada, mas serei eternamente grata pela amizade construída com a Nadir, uma pessoa de alegria contagiante, coração enorme e que trocamos inúmeras mensagens de resolução de atividades e desabafos também. Ao Luis e Dirceu, obrigada pelas horas de terapia coletiva durante nossas viagens.

Aos professores que nos ensinaram com maestria e, em especial, ao meu professor orientador que sempre se mostrou muito dedicado à sua missão de ensinar e orientar.

“A matemática é a rainha das ciências e a aritmética é a rainha da matemática.”

(Carl Friedrich Gauss)

RESUMO

Neste trabalho, estudamos alguns sistemas criptográficos e as teorias que dão suporte para estes métodos, tais como congruência linear, álgebra linear via congruências e elementos da teoria de grupos e de corpos finitos. Com base nos relatos históricos e na teoria apresentada, foram estruturadas atividades para alunos do ensino médio, inserindo a criptografia nos conteúdos que já são abordados regularmente na grade curricular. Isto proporciona uma contextualização da Matemática, pois trabalha-se com um tema que está presente nas operações eletrônicas que exigem proteção de dados e estas aparecem frequentemente em nosso cotidiano.

Palavras-chave: Criptografia. Sistema criptográficos. Chaves públicas e privadas.

ABSTRACT

In this work, we study some cryptographic systems and theories related with these methods, such as linear congruence, linear algebra via congruences, finite fiel theory and group theory. Based on the historical data and the theory presented, some activities were created for high school students. These activities allow the cryptography to be addressed in high school without changing the curriculum. This provides a contextualization of Mathematics, since we work with a theme that is present in electronic operations that require data protection and these appear frequently in our daily lives.

Keywords: Cryptography, Cryptographic system, Public and private keys.

LISTA DE FIGURAS

Figura 1 – Representação de um sistema criptográfico 59
Figura 2 – Representação de dígrafos com vetor no plano $(\boldsymbol{Z_n})^{\boldsymbol{2}}$ 69
Figura 3 – Representação de um sistema criptográfico simétrico 74
Figura 4 – Representação de um sistema criptográfico assimétrico 75
Figura 5 – Representação de um sistema criptográfico usando função unidimensional 76
Figura 6 – Representação de um sistema criptográfico usando função arapuca 77
Figura 7 - Tatuagens no corpo da personagem “Jane” 112

LISTA DE QUADROS

Quadro 1: Cifra de César 60
Quadro 2: Letras do alfabeto e seus números equivalentes 60
Quadro 3: Letras do alfabeto e caracteres com seus números equivalentes 63
Quadro 4: Dígrafos e seus números equivalentes 67
Quadro 5: Cifra de César. Na primeira linha o alfabeto normal, na segunda linha, o alfabeto deslocado em 3 casas 93
Quadro 6: Letras do alfabeto e seus números correspondentes 93
Quadro 7: Cifra ADFGVX 108
Quadro 8: Cifra ADFGVX escolhida 109
Quadro 9: Segunda etapa da Cifra ADFGVX 109
Quadro 10: Etapa da transposição da Cifra ADFGVX 109
Quadro 11: Grade da cifra ADFGVX resultado do desafio 112

SUMÁRIO

1 INTRODUÇÃO 27
2 NOÇÕES PRELIMINARES 31
2.1 ELEMENTOS DA TEORIA DOS NÚMEROS 31
2.1.1 Divisão de inteiros **31**
2.1.2 Congruência **34**
2.1.3 Congruência linear **38**
2.1.4 Função Φ de Euler **40**
2.1.5 Funções definidas via congruência **43**
2.1.6 Álgebra linear via congruência **45**
2.2 ELEMENTOS DE ÁLGEBRA ABSTRATA 49
2.2.1 Anel, corpo e grupo **50**
2.2.2 Grupos e corpos finitos **54**
3 MATEMÁTICA E CRIPTOGRAFIA **59**
3.1 SISTEMAS DE CRIPTOGRAFIA 59
3.2 UNIDADE DE MENSAGEM DE UMA LETRA: TRANSFORMAÇÕES LINEARES E AFINS 60
3.3 CRIPTOANÁLISE DAS CIFRAS DE SUBSTITUIÇÃO DE UNIDADE DE MENSAGEM DE UMA LETRA 64
3.4 UNIDADES DE MENSAGEM COM PAR DE LETRAS: TRANSFORMAÇÕES DE DÍGRAFOS 66
3.5 CRIPTOANÁLISE DAS CIFRAS DE UNIDADES DE MENSAGEM COM PAR DE LETRAS: TRANSFORMAÇÕES DE DÍGRAFOS 68
3.6 MATRIZES CODIFICADORAS 69
3.7 CRIPTOANÁLISE DAS CIFRAS ENVOLVENDO MATRIZES 71
3.8 SISTEMAS CRIPTOGRÁFICOS SIMÉTRICOS 73
3.9 CRIPTOGRAFIA ASSIMÉTRICA 75
3.10 FUNÇÕES UNIDIMENSIONAIS E FUNÇÕES ARAPUCAS 76
3.11 RSA 78
3.12 LOGARITMO DISCRETO 80
3.12.1 Método de troca de chaves Diffie-Hellman **82**
3.12.2 Protocolo de Massey-Omura para transmissão de mensagens **84**

3.12.3 Método de Elgamal para transmissão de mensagens 84
3.13 AUTENTICAÇÃO E ASSINATURA DIGITAL 87
3.13.1 Autenticação via métodos de criptografia de chave pública 88
3.13.2 Métodos de Elgamal para assinatura digital 89
4 PROPOSTAS DE APLICAÇÃO 91
4.1 PROPOSTA DE APLICAÇÃO PARA O 1º ANO DO ENSINO MÉDIO 91
4.1.1 Análise das atividades aplicadas no 1º ano do ensino médio 97
4.2 PROPOSTA DE APLICAÇÃO PARA O 2º ANO DO ENSINO MÉDIO 105
4.2.1 Análise das atividades aplicadas no 2º ano do ensino médio 115
5 CONCLUSÃO 119
REFERÊNCIAS 120

1 INTRODUÇÃO

A cada dia que passa percebemos a dependência que as pessoas possuem dos recursos tecnológicos, principalmente do uso da internet. São diversos serviços e possibilidades, tais como os aplicativos para conversas, que é febre entre a nova geração, redes sociais, que permitem interações entre pessoas de qualquer lugar do mundo, e operações bancárias, que dispensam a necessidade do deslocamento ao banco físico. Além disso, o comércio eletrônico é outro benefício para a população, que pode comparar preços e realizar a compra com apenas alguns cliques. Todas essas ferramentas, quase que indispensáveis na atualidade, requerem o uso da criptografia para garantir segurança e privacidade nas informações compartilhadas.

A necessidade de segurança no compartilhamento de informações é relatada desde os tempos remotos. De fato, no século V a.C Heródoto escreveu sobre este assunto ao narrar os conflitos entre a Grécia e a Pérsia (veja mais em [4]). Nesse período, a ocultação de mensagens, conhecida como esteganografia, era usada como meio de comunicação para instruir tropas através de um mensageiro. Embora tivesse uma certa segurança, os procedimentos adotados na época eram relativamente frágeis, bastando uma boa vigilância para identificar o mensageiro, e um certo tempo de exploração até desvendar a mensagem. Entre os meios de ocultar uma mensagem estavam métodos tais como raspar a cabeça do mensageiro, escrever a mensagem no couro cabeludo e esperar o cabelo crescer ou esconder a mensagem dentro de objetos, como um ovo cozido.

Em paralelo ao desenvolvimento da esteganografia, houve a evolução da criptografia (do grego *kriptós* = escondido, oculto; *grápho* = grafia), ciência que estuda as formas de escrever uma mensagem em cifras ou códigos utilizando técnicas matemáticas para torná-la incompreensível. Neste caso, apenas emissor e receptor, após um protocolo estabelecido previamente, saberão o conteúdo da mensagem. Sendo assim, a criptografia tem uma vantagem significativa em relação a esteganografia; se alguém interceptar uma mensagem criptografada, esta não será compreendida por terceiros, isto é, se o interceptador não conhece o protocolo utilizado para codificar a mensagem, ele achará difícil ou até mesmo impossível de chegar à mensagem original.

Há milhares de anos reis, imperadores, generais utilizaram da criptografia para uma comunicação secreta e segura com o seu exército durante as guerras. Uma das formas mais famosas de criptografar na antiguidade é a cifra de substituição, também chamada cifra monoalfabética, método em que cada letra é substituída por uma outra letra. Destas, a cifra de

Júlio César foi uma das primeiras a ser utilizada para fins militares. O sistema de Júlio César consiste em substituir cada letra na mensagem por outra que está três casas à frente no alfabeto.

Com a evolução dos métodos de quebra de códigos criptográficos, as cifras monoalfabéticas já não eram mais seguras a partir de um certo momento da história. Portanto, era necessário construir um novo método de cifragem, mais forte e poderoso. No século XVI, Leon Battista Alberti (1404 - 1472) propôs o uso de dois ou mais alfabetos cifrados, usados alternadamente. Porém, Alberti não conseguiu desenvolver completamente sua ideia. Ela foi aperfeiçoada por outros intelectuais como Johannes Trithemius (1462 - 1516), Giovanni Porta e o francês Blaise de Vigenère (1523 - 1596). Vigenère, baseando-se na ideia dos três intelectuais anteriores, foi responsável pela sistematização de uma cifra polialfabética, usando 26 alfabetos cifrados diferentes para construir uma mensagem cifrada. Para cifrar uma mensagem com base nesse método, é utilizado o quadrado de Vigenère, como segue abaixo:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

O quadrado de Vigenére é constituído de um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. Para cifrar uma mensagem, é utilizada uma palavra-chave, que é escrita acima da mensagem e repetida até que cada letra da mensagem fique associada com uma letra da palavra-chave. Por exemplo, para cifrar a mensagem HOJE À TARDE usando a palavra-chave RIMA, primeiro escreve-se a mensagem original e, acima dela, a palavra-chave como mostra o esquema abaixo:

Palavra-chave	R	I	M	A	R	I	M	A	R	I
Mensagem original	H	O	J	E	A	T	A	R	D	E

O próximo passo é fazer a cifragem. A letra H tem como letra chave R. A letra que criptografa H é a letra do quadrado de Vigenère que corresponde ao cruzamento da linha cuja primeira letra é R (linha 17) com a coluna cuja primeira letra é H. Neste caso, a letra H será substituída pela letra Y. Do mesmo modo, o cruzamento da linha I (linha 8) com a coluna O tem-se a cifragem de O, isto é, a letra O será substituída por W. Assim o processo é feito até que termine de cifrar a mensagem. No exemplo dado, HOJE À TARDE seria substituído por YWVE R BMUM.

A cifra polialfabética de Vigenére foi publicada em 1586 e era considerada indecifrável, até que em 1854 foi quebrada, (ver ref. [24]). Mais tarde, esse método foi substituído pela máquina Enigma, que utilizava o mesmo raciocínio, porém mais eficiente na codificação e decodificação de mensagens (ver ref. [9]). Inicialmente, para quebrar o código criado por esta máquina, só era possível se o interceptador possuísse uma máquina configurada de forma idêntica a máquina que efetuou a encriptação. Em 1940, Alan Turing e sua equipe de inteligência construíram o primeiro computador operacional com o objetivo de decifrar as mensagens alemãs cifradas pela máquina Enigma.

Com a evolução dos computadores, a criptografia foi ficando cada vez mais complexa. Em 1977, Rivest, Shamir e Adleman revolucionam esta área com o sistema RSA, criptografia assimétrica que é composta por duas chaves distintas, uma privada e outra pública. Esse sistema viabilizou a troca de informações, de forma segura, via internet. O método utiliza números primos e os criadores se basearam no fato de que é fácil obter o produto de dois primos, porém, é muito difícil determinar os primos a partir apenas do produto. Desse modo, a segurança desse sistema reside na dificuldade de fatoração em primos de números grandes. Atualmente, usuários

do sistema RSA utilizam primos com mais de 100 casas decimais para que a fatoração seja praticamente impossível, até mesmo com o uso de supercomputadores.

A criptografia utiliza vários ramos da Matemática e, dentre eles, a Teoria dos Números é um tópico fundamental. Neste trabalho, estudaremos alguns dos principais sistemas criptográficos, apresentando conceitos e definições indispensáveis para a sistematização do processo de cifrar e decifrar em cada um dos sistemas abordados.

No capítulo 2, introduzimos algumas propriedades elementares sobre divisão de números inteiros, o importante conceito de congruência que nos servirá como base para a compreensão dos sistemas criptográficos e, também, definições e proposições acerca de funções definidas via congruência e de elementos da Álgebra abstrata como anel, corpo e grupo.

No capítulo 3, apresentamos alguns sistemas criptográficos simétricos e assimétricos e como cada qual funciona, explorando exemplos que auxiliam na compreensão dos algoritmos. A cifra de César é o nosso ponto de partida para entendermos como codificar e decodificar uma mensagem utilizando uma função. Além disso, apresentamos o conceito de função unidimensional e função arapuca. Tais ideias são importantíssimas para a funcionalidade dos sistemas criptográficos assimétricos, como por exemplo, o RSA, o método de troca de chaves de Diffie-Hellman, o protocolo de Massey-Omura e o método de Elgamal para a transmissão de mensagens. Os três últimos são baseados na dificuldade de calcular o logaritmo discreto em grupos finitos grandes.

No capítulo 4, apresentamos duas aplicações para alunos do ensino médio. Tendo a criptografia como tema motivador, acreditamos que tais propostas constituam uma forma viável de contextualizar a Matemática, favorecendo uma reflexão crítica sobre as contribuições dos algoritmos para os avanços tecnológicos.

2 NOÇÕES PRELIMINARES

2.1 ELEMENTOS DA TEORIA DOS NÚMEROS

A criptografia utiliza vários ramos da Matemática, entre eles, a Teoria dos Números é um tópico fundamental. Nesta seção, são apresentados conceitos matemáticos indispensáveis para fundamentar as bases da criptografia, bem como para a compreensão de sua evolução. As definições e resultados aqui expostos podem ser encontrados nas referências como [2], [8], [12], [13], [14], [15], [16], [18], [19], [21], [22] e [23]. Escolhemos apresentar as demonstrações dos principais resultados.

2.1.1 DIVISÃO DE INTEIROS

Dentro da Teoria dos Números, a divisibilidade é um tópico relevante na aplicação da criptografia.

Definição 2.1.1.1 Sejam $a, b \in \mathbb{Z}$. Dizemos que a divide b, denotamos por $a|b$, se existir um inteiro k tal que $b = ak$. Nesse caso, dizemos que a é divisor de b ou que b é divisível por a. No caso em que a não divide b, escrevemos $a \nmid b$.

Proposição 2.1.1.2 Se a, b, c são números inteiros tais que $a|b$ e $b|c$, então $a|c$.
Demonstração:
Por definição de divisibilidade, existem inteiros k_1 e k_2 com $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$, temos $c = k_2 k_1 a$. Portanto, $a|c$. □

Proposição 2.1.1.3 Se a, b, c, m e n são inteiros, $c|a$ e $c|b$, então $c|(ma + nb)$.
Demonstração:
Desde que $c|a$ e $c|b$, existem inteiros k_1 e k_2 de modo que $a = k_1 c$ e $b = k_2 c$. Multiplicando as equações, respectivamente, por m e n, temos $ma = mk_1 c$ e $nb = nk_2 c$. Somando, obtemos $ma + nb = mk_1 c + nk_2 c = c.(mk_1 + nk_2)$. Isto significa que $c|(ma + nb)$.□

A seguir, apresentamos alguns outros resultados elementares relacionados com divisibilidade em $\mathbb{Z}$. A demonstração do resultado abaixo pode ser encontrada em [13], página 40.

Proposição 2.1.1.4 Sejam a, b, c números inteiros. Tem-se que:
$(i) a|a$;
$(ii) 1|a$;
$(iii) a|0$;
$(iv) 0|a \Leftrightarrow a = 0$;
$(v) a|b \Leftrightarrow |a|\ divide\ |b|$;
$(vi)\ Se\ a|b\ e\ b|c$, então $a|c$.

Teorema 2.1.1.5 – Divisão Euclidiana Sejam a e b números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$. Temos que q é chamado de quociente e r de resto da divisão de a por b.

Demonstração:

Considere o conjunto $S = \{x \in \mathbb{N} / \ x = a - by\ e\ y \in \mathbb{Z}\}$. Pela propriedade Arquimediana dos inteiros (veja página 11 de [13]), existe um $n \in \mathbb{Z}$ tal que $n.(-b) > -a$. Logo $a - nb > 0$. Desse modo, temos que S é um conjunto não vazio, sendo limitado inferiormente por 0. Pelo Princípio da Boa Ordenação (veja página 10 em [13]), temos que S possui um menor elemento r. Temos que $r = a - bq$, para algum inteiro q. Sabemos que $r \geq 0$. Vamos provar que $r < |b|$. Suponha, por absurdo, que $r \geq |b|$. Assim existe $s \in \mathbb{N}$ tal que $r = |b| + s$. Logo $0 \leq s < r$ e $s = r - |b| = a - bq - |b| = a - b(q + (|b|/b))$. Então s está em S e $0 \leq s < r$, o que é uma contradição. Portanto, $r < |b|$. Para provar a unicidade, suponha que $a = bq_1 + r_1 = bq_2 + r_2$, com $0 \leq r_1 < |b|$, $0 \leq r_2 < |b|$ e $r_2 \leq r_1$. Das desigualdades descritas, temos: $-|b| < -r_1$ e $-|b| < -r_2$. Assim, $-|b| < -r_1 \leq r_1 - r_2 < |b| - r_2 < |b|$ e, portanto, $-|b| < r_1 - r_2 < |b|$. Consequentemente, temos que $|r_1 - r_2| < |b|$. Da igualdade $bq_1 + r_1 = bq_2 + r_2$ temos $b(q_1 - q_2) = r_2 - r_1$. Então, $|b|.|q_1 - q_2| = |r_2 - r_1| < |b|$. Isso só é possível se $q_1 = q_2\ e\ r_1 = r_2$.□

Definição 2.1.1.6 Um número inteiro n, com $|n| > 1$, possuindo somente dois divisores positivos, $|n|$ e 1, é chamado de número primo.

Definição 2.1.1.7 Um número natural d é dito máximo divisor comum dos números inteiros a e b, e denotado por $d = mdc(a, b)$, se satisfaz as seguintes propriedades:

(i) d divide a e b;

(ii) Se c é inteiro e c divide a e b, então c divide d.

Observação 2.1.1.8:

1) Temos que $mdc(a, b)$ sempre existe e é único.

2) $mdc(a, b) = mdc(a, -b) = mdc(-a, b) = mdc(-a, -b)$

Teorema 2.1.1.9 (Identidade de Bezout) Seja $d \in \mathbb{N}$ o máximo divisor comum dos inteiros não nulos a e b. Então, existem inteiros m e n tais que $d = ma + nb$.

Demonstração:

Seja $S = \{ma + nb > 0;\ m, n \in \mathbb{Z}\}$. Considere m e n tais que $c = ma + nb$ seja o menor elemento pertencente a S. Vamos provar, por contradição, que $c|a$ e $c|b$. Suponha que $c \nmid a$. Nesse caso, pela divisão Euclidiana, existem inteiros q e r tais que $a = qc + r$, com $0 < r < c$. Portanto, $r = a - qc = a - q(ma + nb) = (1 - qm)a + (-qn)b$. Com isso, $r \in S$. Desde que $r < c$ e c é o menor elemento de S, temos uma contradição. Com isso, concluímos que $c|a$. Analogamente, $c|b$. Como d é divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1.d$ e $b = k_2.d$ e, portanto, $c = ma + nb = mk_1d + nk_2d = d(mk_1 + nk_2)$. Logo $d|c$, e portanto, $d \leq c$. Mas, $d < c$ não é possível, uma vez que d é o máximo divisor comum. Concluímos que $c = d$. Assim, $d = ma + nb$. □

Definição 2.1.1.10 Dois inteiros não nulos a e b, são ditos primos entre si, ou relativamente primos, quando m$dc(a, b) = 1$.

Lema 2.1.1.11 (Lema de Gauss) Sejam a, b e c números inteiros. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.

Demonstração:

Pelo Teorema 2.1.1.9, temos que existem inteiros m e n tais que 1$= ma + nb$. Multiplicando ambos os lados da equação por c, temos $cma + cnb = c$, o que implica em m$(ac) + n(bc) = c$. Como $a|ac$ e, por hipótese, $a|bc$, a Proposição 2.1.1.3 garante que $a|\big(m(ac) + n(bc)\big)$, ou seja, $a|c(ma + nb)$. Como $ma + nb = 1$, temos que $a|c$. □

Proposição 2.1.1.12 Sejam a, b, p números inteiros com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração:

Se $p|a$, a tese é imediata. Agora, se $p \nmid a$ então $mdc(a,p) = 1$. Pelo Lema de Gauss - 2.1.1.11, temos que $p|b$. □

Lema 2.1.1.13 Seja m e n naturais tais que $mdc(m,n) = 1$. Suponha que $m|a$ e $n|a$. Então, $mn|a$.

Demonstração:

Pela identidade de Bezout, existem k e l inteiros tais que $mk + nl = 1$. Logo $mka + nla = a$. Desde que $n|a$ temos que $nm|mka$. De forma similar, desde que $m|a$, temos que $mn|nla$. Logo $mn|a$. □

2.1.2 CONGRUÊNCIA

Congruência é conhecida como a aritmética dos restos. Em muitas situações, a criptografia faz uso dessa aritmética. Esse tema foi abordado pelo matemático Gauss, publicado por volta de 1801 e utilizado por diversos matemáticos da época, sendo útil até os dias atuais.

Definição 2.1.2.1 Seja m um número natural maior do que 1. Dois inteiros a e b são ditos *congruentes módulo* m, se os restos da divisão euclidiana de a e b por m forem iguais. Quando a e b são congruentes módulo m, escrevemos $a \equiv b \ mod\ (m)$.

Proposição 2.1.2.2 Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, tem-se que $a \equiv b \ mod\ (m)$ se, e somente se, $m|(a-b)$.

Demonstração:

Seja $a \equiv b \ mod\ (m)$, então, por definição, existem inteiros r, q e q' tais que $a = mq + r$ e $b = mq' + r$ com, $0 \leq r < m$. Subtraindo temos:

$$a - b = mq + r - (mq' + r)$$

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

Logo, $a - b$ é múltiplo de m e, portanto, $m|\ (a-b)$.

Reciprocamente, suponha que $m|(a-b)$. Pela divisão Euclidiana, temos que $a = mq + r$ e $b = mq' + r'$, com $0 \leq r < m$ e $0 \leq r' < m$. Fazendo novamente $a - b$, obtemos

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

Como $m|m(q - q')$, segue-se que $m|(r - r')$, mas isso só ocorre se $r = r'$, pois $|r - r'| < m$. Portanto, $a \equiv b\ mod\ (m)$.□

Exemplo 2.1.2.3: $41 \equiv 27\ mod\ (7)$, pois $41 - 27 = 14$ e $7|14$.

Proposição 2.1.2.4 Sejam a, b, c, d, m e n inteiros com $m > 1$ e $n \geq 1$. Então, as seguintes sentenças são verdadeiras:

i) (reflexiva) $a \equiv a\ mod\ (m)$;

ii) (simétrica) Se $a \equiv b\ mod\ (m)$, então $b \equiv a\ mod\ (m)$;

iii) (transitiva) Se $a \equiv b\ mod\ (m)$ e $b \equiv c\ mod\ (m)$, então $a \equiv c\ mod\ (m)$;

iv) (compatível com a adição) Se $a \equiv b\ mod\ (m)$ e $c \equiv d\ mod\ (m)$, então $a + c \equiv b + d\ mod\ (m)$;

v) (compatível com a multiplicação) Se $a \equiv b\ mod\ (m)$ e $c \equiv d\ mod\ (m)$, então $a.c \equiv b.d\ mod\ (m)$;

vi) Se $a \equiv b\ mod\ (m)$, então $a^n \equiv b^n\ mod\ (m)$.

Demonstração:

i) Sabemos que $m|0$ e que $a - a = 0$, logo $m|(a - a)$, o que implica que $a \equiv a\ mod\ (m)$.

ii) Se $a \equiv b\ mod\ (m)$, então $m|(a - b)$. Segue que $m| - (a - b)$, o que implica que $m|(b - a)$ e, portanto, $b \equiv a\ mod\ (m)$.

iii) Se $a \equiv b\ mod\ (m)$ e $b \equiv c\ mod\ (m)$, existem inteiros $k\ e\ k'$ de modo que, $a = mk + b$ e $b = mk' + c$. Então, $a - b = mk$ e $b - c = mk'$. Somando essas duas equações membro a membro, obtemos $(a - b) + (b - c) = m(k + k')$, isto é, $a - c = m(k + k')$ que, por definição, $a \equiv c\ mod\ (m)$.

iv) Seja $a \equiv b\ mod\ (m)$, logo $a = mk + b$ para algum $k \in \mathbb{Z}$. Então,

$$a - b = mk \qquad (2.1).$$

Do mesmo modo, se $c \equiv d\ mod\ (m)$, $c = mk' + d$, implicando que

$$c - d = mk' \qquad (2.2),$$

para algum $k' \in \mathbb{Z}$. Somando as equações (2.1) e (2.2), temos $(a - b) + (c - d) = m(k + k')$, resultando em $(a + c) - (b + d) = m(k + k')$. Portanto, $a + c \equiv b + d\ mod\ (m)$.

v) Multiplicando a equação (2.1) por c e a equação (2.2) por b, obtemos $ac - bc = mkc$ e $cb - bd = mk'b$. Somando membro a membro essas duas últimas equações, teremos $ac - bc + cb - bd = m(kc + k'b)$ o que implica que $ac \equiv bd\ mod\ (m)$.
vi) Segue diretamente do item v.

Com a demonstração das propriedades da Proposição 2.1.2.4, provamos que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência, pois ela satisfaz as propriedades reflexiva, simétrica e transitiva.

Teorema 2.1.2.5 Se a, b, c e m são números inteiros, com m>1, e $ac \equiv bc\ mod\ (m)$, então $a \equiv b\ mod\ \left(\frac{m}{d}\right)$, em que $d = mdc(c, m)$.
Demonstração:
Desde que $ac \equiv bc\ mod\ (m)$, por definição temos que $m|(ac - bc)$. Logo existe $k \in \mathbb{Z}$ tal que $k.m = (ac - bc) = c(a - b)$. Dividindo ambos os membros da equação por d, obtemos $\frac{km}{d} = \frac{c}{d}(a - b)$. Daí segue que $\left(\frac{m}{d}\right) | \frac{c}{d}(a - b)$. Mas, como $mdc\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, pelo Lema de Gauss 2.1.1.11, $\left(\frac{m}{d}\right) | (a - b)$, ou seja, $a \equiv b\ mod\ \left(\frac{m}{d}\right)$. □

Proposição 2.1.2.6 Sejam $a, b \in \mathbb{Z}$ e $m\ e\ n$ inteiros maiores do que 1. Temos que:
(i) Se $a \equiv b\ mod\ (m)$ e $n|m$, então $a \equiv b\ mod\ (n)$;
(ii) Se $a \equiv b\ mod\ (m)$, então $mdc(a, m) = mdc(b, m)$.
Demonstração:
(i) Se $a \equiv b\ mod\ (m)$, então $m|(a - b)$. Como $n|m$, pela Proposição 2.1.1.4, item (vi), temos que $n|(a - b)$. Portanto, $a \equiv b\ mod\ (n)$.
(iii) Desde que $a \equiv b\ mod\ (m)$, existe $k \in \mathbb{Z}$ tal que $k.m = a - b$, isto é, $a = b + km$. Considere $d = mdc(a, m) = mdc(b + km, m)$. Por definição, $d|b + km$ e $d|m$, o que implica $d|b$. Seja $c = mdc(b, m)$. Sendo d divisor de b e m, temos que $d|c$. Por outro lado, desde que $c = mdc(b, m) = mdc(a - km, m)$, também podemos concluir que $c|m\ e\ e\ c|a$. Como $d = mdc(a, m)$, temos que $c|d$. Acabamos de mostrar que $d|c$ e $c|d$. Como ambos são naturais, temos que $d = c$. □

Lema 2.1.2.7 Seja p um número primo e i um número inteiro positivo. Os números $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, tal que $0 < i < p$, são todos divisíveis por p.

Demonstração:

Se $i = 1$ o resultado é trivial. Suponha $1 < i < p$. Temos que $\binom{p}{i} = \frac{p!}{i!.(p-i)!} = \frac{p.(p-1)\ldots(p-i+1).(p-i)!}{i!\,(p-i)!} = p.\frac{(p-1)\ldots(p-i+1)}{i!}$ e este é um número natural. Temos que $mdc(i!, p) = 1$, pois p é primo e $i < p$. Desse modo, pela Proposição 2.1.1.11, temos que $i!\,|(p-1)\ldots.(p-i+1)$. Logo, $\frac{(p-1)\ldots(p-i+1)}{i!} \in \mathbb{Z}_+^*$ $e\ p|\binom{p}{i}$.□

Teorema 2.1.2.8 (Primeiro Teorema de Fermat) – Seja p primo. Tem-se que $a^p \equiv a\ mod\ (p), \forall\ a \in \mathbb{Z}$.

Demonstração:

Basta provarmos que $p|a^p - a$. Para isso, vamos fixar p e tratar primeiramente o caso a maior ou igual a zero. Nesse caso, vamos aplicar indução em a. Se $a = 0$ o resultado é elementar. Suponha $a > 0$ e $p|a^p - a$. Usando Binômio de Newton (veja [13] página 25),

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1 - (a+1) =$$

$$= (a^p - a) + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$$

Logo, pela hipótese de indução e usando o Lema 2.1.2.7, temos que $p|(a+1)^p - (a+1)$, ou seja, $(a+1)^p \equiv (a+1)\ mod(p)$. Concluímos, via indução, que $a^p \equiv a\ mod\ (p), \forall\ a \in N$. Vamos ao caso $a < 0$. Desde que $-a > 0$, temos $(-1)^p a^p \equiv -a\ mod(p)$. Se $p = 2$, da igualdade anterior, obtemos que 2 divide $a^2 + a$. Então, claramente 2 divide $a^2 + a - 2a = a^2 - a$. Isto mostra que $a^2 \equiv a\ mod(2)$. Finalmente vamos ao caso p primo diferente de 2. Então sabemos que p é ímpar. Segue de $(-1)^p a^p \equiv -a\ mod(p)$, que -$a^p \equiv -a\ mod(p)$. Como $-1 \equiv -1\ mod(p)$, utilizando a propriedade de compatibilidade da multiplicação (Proposição 2.1.2.4), temos que $a^p \equiv a\ mod(p)$.□

Teorema 2.1.2.9 (Pequeno Teorema de Fermat) Seja p primo. Se $p \nmid a$ então $a^{p-1} \equiv 1\ mod\ (p)$.

Demonstração:

Pelo Teorema 2.1.2.8 (Primeiro Teorema de Fermat), temos que $a^p \equiv a\ mod\ (p)$, isto é, $p|(a^p - a)$. Desde que $a^p - a = a(a^{p-1} - 1)$, então $p|\ a(a^{p-1} - 1)$. Como $p \nmid a$ e p é primo, então $mdc(a, p) = 1$. Então, o Lema de Gauss 2.1.1.11 garante que $p|(a^{p-1} - 1)$. Portanto, $a^{p-1} \equiv 1\ mod\ (p)$. □

Corolário 2.1.2.10 (Corolário do Pequeno Teorema de Fermat) Se p é um número primo, a um inteiro, m e n naturais positivos tais que $m \equiv n\ mod\ (p-1)$. Então $a^m \equiv a^n\ mod(p)$.
Demonstração:
Caso $p|a$, o resultado é elementar. Vamos ao caso $p \nmid a$. Suponha $m \geq n$ e seja l natural tal que $m - n = l(p-1)$. Então, usando o pequeno Teorema de Fermat, $a^m = a^{n+\ l(p-1)} = a^n.(a^{p-1})^l \equiv a^n\ mod\ (p)$. O caso m $< n$ é similar. □

2.1.3 CONGRUÊNCIA LINEAR

Chamamos de *congruência linear* em uma variável a congruência da forma $aX \equiv b\ mod\ (m)$, onde X é uma incógnita. Se $aX \equiv b\ mod\ (m)$ então $m|(aX - b)$ e, portanto, existe um inteiro c de modo que $mc = aX - b$. Logo, $b = aX - mc$. Tal equação é conhecida como equação diofantina linear, seu nome é em homenagem a Diofanto de Alexandria, matemático grego. Logo, resolver uma congruência linear $aX \equiv b\ mod\ (m)$ é equivalente a resolver a equação diofantina $b = aX - mc$.

Resolver congruências do tipo $aX \equiv b\ mod\ (m)$, onde $a, b, m \in \mathbb{Z}, m > 1$ significa determinar se existem $X \in \mathbb{Z}$ que satisfazem a congruência $aX \equiv b\ mod\ (m)$. Para isso, é necessário identificar se tal congruência admite solução.

Proposição 2.1.3.1 Sejam $a, b, c \in \mathbb{Z}$. A equação $aX + bY = c$ admite solução inteira se, e somente se, $mdc(a, b)|c$.
Demonstração:
Suponha que a equação $aX + bY = c$ admita uma solução $x_0\ e\ y_0$, isto é, $ax_0 + by_0 = c$. Seja $d = mdc(a, b)$, temos por definição que, $d|a$ e $d|b$, desse modo, a Proposição 2.1.1.3 garante que $d|\ ax_0 + by_0$, logo $d|c$. Portanto, $mdc(a, b)|c$.

Reciprocamente, suponha que $d|c$, onde $d = mdc(a, b)$. Então existe um inteiro k tal que

$$d.k = c \qquad (2.3).$$

Segue pelo Teorema 2.1.1.9 (Identidade de Bezout) que, existem inteiros m_0 *e* n_0 tais que

$$m_0a + n_0b = d \qquad (2.4).$$

Multiplicando por k e usando (2.3), temos $(m_0a + n_0b).k = c$, ou seja, $c = a(km_0) + b(kn_0)$. Com isso, $km_0 = x$ e $kn_0 = y$ são soluções inteiras da equação. □

Proposição 2.1.3.2 Seja x_0 e y_0 uma solução da equação $aX + bY = c$, e $mdc(a, b) = 1$. Então as soluções inteiras x e y da equação são $x = x_0 + tb$ e $y = y_0 - ta$, com $t \in \mathbb{Z}$.

Demonstração:

Seja x e y uma solução da equação $aX + bY = c$, logo $ax_0 + by_0 = ax + by = c$. Desenvolvendo a equação temos $a(x - x_0) = b(y_0 - y)$. Como $mdc(a, b) = 1$, segue que $b|(x - x_0)$. Logo, existe um inteiro t de modo que $tb = x - x_0$. Substituindo o valor de $(x - x_0)$ na equação $a(x - x_0) = b(y_0 - y)$ teremos $a.tb = b(y_0 - y)$ implicando em $ta = y_0 - y$, ou seja, $y = y_0 - ta$. Além disso, da igualdade $tb = x - x_0$, concluímos que $x = x_0 + tb$. Por outro lado, seja $x = x_0 + tb$ e $y = y_0 - ta$, com $t \in \mathbb{Z}$. Então, o par (x,y) é solução da equação, pois $ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + atb + by_o - atb = ax_0 + by_0 = c$. □

Proposição 2.1.3.3 Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência $aX \equiv b\ mod\ (m)$ possui solução se, e somente se, $mdc(a, m)|b$.

Demonstração:

Suponha que x seja uma solução da congruência $aX \equiv b\ mod\ (m)$. Logo, temos que $m|(ax - b)$. Então, existe $y \in \mathbb{Z}$ tal que $my = ax - b$, o que implica em $b = ax - my$. Essa equação admite solução quando $mdc(a, m)|b$, como garante a Proposição 2.1.3.1.

Reciprocamente, suponha que $mdc(a, m)|b$. Decorre da Proposição 2.1.3.1 que a equação $aX - mY = b$ admite uma solução x, y. Portanto, $ax = b + my$ e, consequentemente, x é solução da congruência, pois $ax \equiv b\ mod\ (m)$. □

Definição 2.1.3.4 Dado a inteiro, dizemos que um inteiro a' é um *inverso* de a módulo m se $a'.a \equiv 1\ mod\ (m)$.

Teorema 2.1.3.5 Seja $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$, então existe um inverso de a módulo m. Neste caso, podemos escolher a' tal que $0 < a' < m$.

Demonstração:

Seja $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$, então existem inteiros s e t tal que $sa + tm = 1$. Logo $tm = 1 - sa$ e, com isso, temos que m$|(1 - sa)$. Portanto, $sa \equiv 1\ mod\ (m)$ e, por definição, s é o inverso de a módulo m. Se $0 < s < m$, escolha $a' = s$. Caso contrário, pelo algoritmo da divisão de Euclides, seja $r\ e\ q$ tais que $s = q.m + r$, com r entre 1 e $m - 1$ (aqui r não pode ser 0, pois temos que $sa + tm = 1$) . De $sa \equiv 1\ mod(m)$, temos $(q.m + r)a \equiv 1\ mod\ (m)$. Desde que $q.m \equiv 0\ mod\ (m)$, usando a compatibilidade da soma, temos $ra \equiv 1\ mod\ (m)$. Logo, escolha $a' = r$. □

Observação 2.1.3.6: Uma forma de resolver a congruência linear $ax \equiv b\ mod\ (m)$, se $mdc(a, m) = 1$, seria multiplicar ambos os lados da congruência pelo o inverso de a módulo m, ou seja, $a'.ax \equiv b.a' mod\ (m)$, implicando em $x \equiv b.a' mod\ (m)$. Temos, neste caso, que a solução é única, a menos de congruência $mod(m)$.

Exemplo 2.1.3.7: Considere a congruência linear $5x \equiv 2\ mod\ (7)$. Note que $mdc(7,5) = 1$. Podemos inicialmente determinar um inverso de 5 módulo 7. Observe que $5.3 = 15 \equiv 1\ mod(7)$. Logo, $a' = 3$, para $a = 5$. Multiplicando ambos os lados da congruência por 3 teremos $3.5x \equiv 2.3\ mod\ (7)$, resultando em $15x \equiv 6\ mod\ (7)$. Como $15 \equiv 1\ mod\ (7)$, então $x \equiv 6\ mod\ (7)$. Note que qualquer inteiro congruente a 6 módulo 7 será uma solução.

Exemplo 2.1.3.8: Considere a congruência linear $2x \equiv 4\ mod\ (8)$. Note que $mdc(2,8) = 2 \neq 1$ e que $mdc(2,8)$ divide 4. Logo, pela Proposição 2.1.3.3, a congruência $2x \equiv 4\ mod\ (8)$ possui solução. Note que $x = 2$ e $x = 6$ são soluções, mas não são congruentes módulo 8.

2.1.4 FUNÇÃO Φ DE EULER

Definição 2.1.4.1 Seja m um inteiro positivo. A função Φ *de Euler*, denotada por $\Phi(m)$, é definida como sendo o número de inteiros positivos menores do que m e que são relativamente primos com m.

Exemplo 2.1.4.2: $\Phi(12) = 4$, pois no conjunto {1,2,3, ... 11}, formado pelos inteiros positivos menores do que 12, os números $1, 5, 7$ e 11 são primos relativos a 12.

Definição 2.1.4.3 Um *sistema reduzido de resíduos* módulo m é um conjunto de $\Phi(m)$ inteiros $\{r_1, r_2, \dots, r_{\Phi(m)}\}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \ mod(m)$.

Exemplo 2.1.4.4: Considere $m = 8$, temos que $\Phi(8) = 4$, pois no conjunto $\{0,1,2,3,4,5,6,7\}$ formado pelos inteiros positivos menores do que 8, apenas os números $1, 3, 5$ e 7 são primos relativos a 8. Desse modo, o conjunto $\{1,3,5,7\}$ é um sistema reduzido de resíduos módulo 8.

Proposição 2.1.4.5 Seja $\{r_1, r_2, \dots, r_{\Phi(m)}\}$ um sistema reduzido de resíduos módulo m. Seja $a \in \mathbb{Z}$ tal que $mdc(a, m) = 1$. Então, $\{ar_1, ar_2, \dots, ar_{\Phi(m)}\}$ é um sistema reduzido de resíduos módulo m.

Demonstração:

Como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, temos que $mdc\ (ar_i, m) = 1$. Logo, cada ar_i é primo relativo com m. Como $mdc(a, m) = 1$, existe a' tal que $aa' \equiv 1\ mod(m)$. Suponha, por contradição, que $ar_i \equiv ar_j\ mod(m)$. Então, $a'ar_i \equiv a'ar_j\ mod(m)$, isto é, $r_i \equiv r_j\ mod(m)$. Contradição. □

Proposição 2.1.4.6 Seja $n \in \mathbb{N}, n > 1$ e seja a um inteiro relativamente primo com n. Seja $S = \{r_1, \dots, r_{\Phi(n)}\}$ o conjunto dos inteiros positivos menores que n e relativamente primos com n e tais que $r_i < r_j$ se $i < j$. Tem-se que:

(a) $ar_i \equiv ar_j\ mod\ (n) \Rightarrow r_i = r_j$;

(b) Cada ar_i é congruente a exatamente um elemento r_j módulo m.

Demonstração:

Como $mdc(a, n) = 1$, existe a' tal que $aa' \equiv 1\ mod(n)$.

(a) Se $ar_i \equiv ar_j\ mod(n)$, então, $a'ar_i \equiv a'ar_j\ \ mod(n)$, isto é, que $r_i \equiv r_j\ \ mod(n)$. Logo $r_i = r_j$.

(b) Como já vimos na Proposição 2.1.4.5, $mdc(ar_i, n) = 1$. Pela divisão Euclidiana, existem q e r inteiros tais que $ar_i = q.n + r$, e $0 < r < n$. Como $mdc(ar_i, n) = 1$, temos $mdc(r, n) = 1$. Logo, existe j tal que $r = r_j$. Logo, $ar_i \equiv r_j\ \ mod(n)$.□

Teorema 2.1.4.7 (Teorema de Euler) Se m é um inteiro positivo e $a \in \mathbb{Z}$, com $mdc(a,m) = 1$, então $a^{\Phi(m)} \equiv 1\ mod\ (m)$.

Demonstração:

Seja $\{r_1, r_2, \dots, r_{\Phi(m)}\}$ um sistema reduzido de resíduos módulo m. Logo, pela Proposição 2.1.4.5 e 2.1.4.6, $\{ar_1, ar_2, \dots, ar_{\Phi(m)}\}$ é um sistema reduzido de resíduos módulo m e $ar_1.ar_2.\dots.ar_{\Phi(m)} \equiv r_1.r_2.\dots.r_{\Phi(m)}\ mod(m)$. Consequentemente,

$$a^{\Phi(m)} r_1.r_2.\dots.r_{\Phi(m)} = ar_1.ar_2.\dots.ar_{\Phi(m)} \equiv r_1.r_2.\dots.r_{\Phi(m)}\ mod(m).$$

Como $mdc(r_1.r_2.\dots.r_{\Phi(m),}m) = 1$, segue que $r_1.r_2.\dots.r_{\Phi(m)}\ mod(m)$ possui inverso. Logo, $a^{\Phi(m)} \equiv 1\ mod\ (m)$. □

Proposição 2.1.4.8 Seja p um número primo e α um número natural. Tem-se que $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Demonstração:

Sendo p um número primo, os números inteiros positivos menores ou iguais a p^α e que não são primos com p^α são aqueles múltiplos de p, ou seja, é o conjunto $\{p, 2p, 3p, \dots p^{\alpha-1}p\}$. Note que a quantidade de elementos desse conjunto é $p^{\alpha-1}$. Logo, $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

Corolário 2.1.4.9 Se p é um número primo, então $\Phi(p) = p - 1$.

Demonstração:

Da Proposição 2.1.4.8 temos que $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Fazendo $\alpha = 1$ obtemos que $\Phi(p^1) = p^1 - p^{1-1}$, isto é, $\Phi(p) = p - 1$. □

Proposição 2.1.4.10 Sejam m e n números naturais tais que $mdc(m,n) = 1$. Então, $\Phi(m.n) = \Phi(m).\Phi(n)$.

A demonstração do resultado acima pode ser encontrada em [14], página 124.

Exemplo 2.1.4.11: Seja $N = p.q$, com p e q primos distintos. Então $\Phi(N) = (p-1).(q-1)$.

Demonstração:

Sendo p e q números primos distintos, temos que $mdc(p,q) = 1$. Pela Proposição 2.1.4.10 temos que, $\Phi(N) = \Phi(p.q) = \Phi(p).\Phi(q) = (p-1).(q-1)$ de acordo com o Corolário 2.1.4.9. □

Teorema 2.1.4.12 Seja $m > 1$ e $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ a decomposição de m em fatores primos. Então, $\Phi(m) = p_1^{\alpha_1} \dots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right)$.

Demonstração:

$\Phi\left(p_1^{\alpha_1} \dots p_n^{\alpha_n}\right) = \Phi\left(p_1^{\alpha_1}\right) \dots \Phi\left(p_n^{\alpha_n}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \dots \left(p_n^{\alpha_n} - p_n^{\alpha_n - 1}\right)$

$= p_1^{\alpha_1} \dots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right)$.□

2.1.5 FUNÇÕES DEFINIDAS VIA CONGRUÊNCIA

Seja n um número natural. Vamos considerar o conjunto $\{0, 1, 2, \dots, n-1\}$ e, neste momento, vamos denotar esse conjunto por $\mathbb{Z}_n$. Adiante, definiremos em $\mathbb{Z}_n$ uma operação de adição e uma de multiplicação, e este denotará também o anel das classes de resíduos módulo n. Vamos considerar a função

$$f_n: \mathbb{Z} \to \mathbb{Z}_n;$$
$$x \to f_n(x),$$

em que $f_n(a)$ é o resto da divisão Euclidiana de a por n.

Exemplo 2.1.5.1: $f_9(22) = 4$, pois $22 = 9.2 + 4$.

Vamos denotar a função $f_n(a)$ por $a \ mod\ (n)$, isto é, $f_n(a) = a \ mod\ (n)$. Dada uma função $g: \mathbb{Z}_n \to \mathbb{Z}$, vamos considerar a composição

$$f_n \circ g: \mathbb{Z}_n \to \mathbb{Z}_n$$
$$x \to g(x) mod\ (n)$$

No estudo da Cifra de César (ver seção 3.2 do capítulo 3), estaremos interessados em tais funções compostas que são bijetoras. Abaixo, temos um resultado para $g(x)$ do tipo $g(x) = ax + b$, em que a e b estão em $\mathbb{Z}_n$.

Proposição 2.1.5.2 Seja $n \in \mathbb{N}, n > 1$, e $a, b \in \mathbb{Z}_n$. Considere a função $h: \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $h(x) = ax + b \ mod\ (n)$. Então, h é bijetora se, e somente se, $mdc(a, n) = 1$. Nesse caso, h^{-1} é dada por $h^{-1}(y) = a'y - b' \ mod\ (n)$, em que $a', b' \in \mathbb{Z}_n$ e $a'.a \equiv 1 \ mod\ (n)$ e $b' \equiv a'b \ mod\ (n)$.

Demonstração:

Suponha h bijetora. Suponha, por contradição, que $mdc(a,n) = m > 1$. Seja $m' = \frac{n}{m}$. Note que $m' \in \mathbb{Z}_n$ e m' é diferente de zero. Temos que $h(m') = a\left(\frac{n}{m}\right) + b\ mod(n) = b\ mod(n) = b$. Como $h(0) = a.0 + b\ mod(n) = b\ mod(n) = b$, temos uma contradição com a bijetividade.

Reciprocamente, suponha que $mdc(a,n) = 1$. Vamos mostrar que f é bijetora. Pelo Teorema 2.1.3.5, existe $a' \in \mathbb{Z}_n$ tal que $a'.a \equiv 1\ mod\ (n)$. Seja $b' \in \mathbb{Z}_n$ tal que $b' \equiv a'b\ mod\ (n)$. Considere a função $f(y) = a'y - b'\ mod\ (n)$. Então, utilizando propriedades de congruência (ver Proposição 2.1.2.4), se $x \in \mathbb{Z}_n, f\big(h(x)\big) = a'h(x) - b'\ mod\ (n) = a'(ax + b) - b'\ mod\ (n) = aa'x + a'b - b'\ mod\ (n) = x\ mod\ (n) = x$. Logo, $f\big(h(x)\big) = x, \forall x \in \mathbb{Z}_n$. De forma similar temos que $h\big(f(y)\big) = y,\ \forall\ y \in \mathbb{Z}_n$. Portanto, h é bijetora, sendo sua inversa dada por $f(y)$. □

No estudo da criptografia RSA (ver seção 3.11 do capítulo 3), estaremos interessados em funções compostas $f_n \circ g: \mathbb{Z}_n \to \mathbb{Z}_n$ que são bijetoras, para $g(x)$ do tipo $g(x) = x^e$, em que e está em $\mathbb{Z}_n$.

Proposição 2.1.5.3 Sejam p e q dois primos distintos e $N = p.q$. Seja e um número natural tal que $1 < e < \Phi(N)$ e $mdc(e, \Phi(N)) = 1$. Considere a função dada por $f(x) = x^e mod\ (N)$. Temos que esta função é bijetora em $\mathbb{Z}_N$ e sua inversa é dada por $f^{-1}(y) = y^{e'} mod\ (N)$, em que e' é o natural em $\mathbb{Z}_{\Phi(N)}$ tal que $e'.e \equiv 1\ mod\ (\Phi(N))$.

Demonstração:

Pelo Teorema 2.1.3.5, temos que e' existe. Logo, existe k natural tal que $ee' = 1 + k.\Phi(N)$. Seja $g(y) = y^{e'} mod\ (N)$. Vamos verificar que $g(f(x)) = x$, para todo x em $\mathbb{Z}_N$. De fato, vamos dividir a demonstração em 3 casos:

(i) Caso $x = 0$. Temos $g(f(0)) = g(0) = 0$;

(ii) Caso $0 < x < N$ e $mdc\ (x,N) = 1$. Então, $g(f(x)) = x^{ee'} mod(N) = x^{1\ +k.\Phi(N)} mod(N) = x(x^{.\Phi(N)})^k mod(N)$. Desde que $mdc\ (x,N) = 1$, pelo Teorema de Euler (Teorema 2.1.4.7), temos que $(x^{\Phi(N)})^k \equiv 1 mod(N)$. Logo $g(f(x)) = x\ mod(N) = x$.

(iii) Caso $0 < x < N$ e $mdc\ (x,N) \neq 1$. Então $mdc\ (x,N) = p$ ou $mdc\ (x,N) = q$. Suponha que a primeira situação seja verdadeira (se a segunda situação for verdadeira, a demonstração

é similar e, portanto, será omitida). Nesta situação, temos $x\,mod\,(p) \equiv 0$. Portanto, $x^{ee'}\,mod\,(p) \equiv 0 \equiv x\,mod\,(p)$. Logo, p divide $x^{ee'} - x$. Por outro lado, pelo Pequeno Teorema de Fermat (Teorema 2.1.2.10), temos que $x^{(q-1)} \equiv 1 mod(q)$. Logo, $x^{ee'}mod(q) = x^{1+k.\Phi(N)}mod(q) = x(x^{\Phi(N)})^k mod(q) = x(x^{(p-1)(q-1)})^k mod(q) = x(x^{(q-1)})^{k(p-1)} mod(q) = x\,mod\,(q)$. Logo q também divide $x^{ee'} - x$. Pelo Lema 2.1.1.13 acima, temos que $p.q$ divide $x^{ee'} - x$. Portanto, $g(f(x)) = x^{ee'}mod(N) = x^{ee'}mod(p.q) = x\,mod(p.q) = x$. Desse modo, verificamos que $g(f(x)) = x$, para todo x em $\mathbb{Z}_n$. De forma similar, verifica-se que $f(g(x)) = x$, para todo x em $\mathbb{Z}_n$. Então f é bijetora e sua inversa é g. □

2.1.6 Álgebra linear via congruência

Na seção 3.6 são abordados matrizes como forma de criptografar dígrafos. Nesse caso, cada dígrafo corresponde a um vetor $\begin{pmatrix} x \\ y \end{pmatrix}$, onde x e y são números inteiros equivalente a posição da letra no alfabeto.

Primeiramente vamos analisar como se trabalha com vetores no plano real xy e com matrizes 2×2 com entradas reais. Dada uma matriz 2×2 com entradas reais, denotada por $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, e um vetor do plano, representado por uma matriz coluna $\begin{pmatrix} x \\ y \end{pmatrix}$, podemos aplicar a matriz ao vetor e assim obter um novo vetor, como segue:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Além disso, fixado um vetor $\begin{pmatrix} u \\ v \end{pmatrix}$, denotado por B, podemos considerar a soma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} ax + by + u \\ cx + dy + v \end{pmatrix}$$

Vamos associar estas operações a uma transformação $f: R \times R \rightarrow R \times R$ dada por $f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix}$. Essa transformação é chamada afim. Se B é identicamente nulo,

então é dita linear, que significa que preserva somas e múltiplos constantes de vetores. Definimos o determinante da matriz A, denotado por $det(A)$, como $ad - bc$. O determinante está relacionado com a bijeção da função f. De fato, têm-se que f é bijetora se, e somente se, $det(A) \neq 0$ (veja [16] p.70). Neste caso, a função inversa é dada por

$$f^{-1}\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1}\begin{pmatrix} x \\ y \end{pmatrix} - A^{-1}B,$$

em que $A^{-1} = \frac{1}{det\ A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ e $A^{-1}B$ é obtida via multiplicação usual de matrizes.

Agora vamos adaptar os resultados acima para o caso em que é utilizada a álgebra modular. Para isto, fixamos um número natural n e novamente vamos considerar $\mathbb{Z}_n$ como o conjunto $\{0, 1, \ldots, n-1\}$.

Definição 2.1.6.1: Dados dois vetores com entradas inteiras $B = \begin{pmatrix} u \\ v \end{pmatrix}$ $e\ E = \begin{pmatrix} x \\ y \end{pmatrix}$, escrevemos $B \equiv E\ mod(n)$, se $u \equiv x\ mod(n)$ e $v \equiv y\ mod(n)$.

Definição 2.1.6.2: Dadas duas matrizes com entradas inteiras $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ $e\ E = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix}$, escrevemos $A \equiv E\ mod(n)$, se $a_i \equiv e_i\ mod(n)$, para $i = 1,2,3,4$.

Observação 2.1.6.3: Se A e E são matrizes com entradas inteiras tais que $A \equiv E\ mod(n)$ e $B = \begin{pmatrix} u \\ v \end{pmatrix}$ um vetor com entradas inteiras, então $A.B \equiv E.B\ mod(n)$. Além disso, se R é outra matriz com entradas inteiras, então $A.R \equiv E.R\ mod(n)$.

Consideramos a função

$$F_n: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_n;$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \to F_n\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} f_n(x) \\ f_n(y) \end{pmatrix},$$

em que $f_n(a)$ é o resto da divisão Euclidiana de a por n.

Exemplo 2.1.6.4: $F_7\begin{pmatrix} 14 \\ 25 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$, pois $14 = 7.2 + 0$ e $25 = 7.3 + 4$.

Vamos denotar a função $F_n\binom{x}{y}$ por $\binom{x}{y}\ mod\ (n)$, isto é, $F_n\binom{x}{y} = \binom{x}{y}\ mod\ (n)$. Dada uma função $g\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z} \times \mathbb{Z}$, podemos considerar a composição

$$F_n \circ g\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$$
$$\binom{x}{y} \to g\binom{x}{y}\ mod\ (n)$$

No estudo da cifra via matrizes codificadoras (ver seção 3.6 do capítulo 3), estaremos interessados em tais funções compostas que são bijetoras. Abaixo, obtemos um resultado para $g\binom{x}{y}$ do tipo $g\binom{x}{y} = A\binom{x}{y} + \mathrm{B}$, em que $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \binom{u}{v}$ possuem entradas inteiras. Neste caso, temos a função $F\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ dada por $F\binom{x}{y} = (A\binom{x}{y} + \mathrm{B})\ mod\ (n)$.

Aqui, como descrito acima, $mod(n)$ é considerado em cada linha de forma separada, isto é, temos

$$F\binom{x}{y} = \binom{(ax + by + u) mod(n)}{(cx + dy + v) mod(n)}.$$

Exemplo 2.1.6.5: Considere a função $f\binom{x}{y} = \left(A\binom{x}{y} + \mathrm{B}\right)\ mod\ (10)$, tal que $A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$ e $B = \binom{2}{1}$. Vamos determinar $f\binom{5}{7}$.

Temos que $f\binom{5}{7} = \left(\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}\binom{5}{7} + \binom{2}{1}\right) mod\ (10) = \binom{15 + 35}{5 + 14} + \binom{2}{1} mod\ (10) = \binom{52}{20} mod\ (10) = \binom{2}{0}$.

Proposição 2.1.6.6 Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ uma matriz de entradas $a, b, c, d \in \mathbb{Z}_n$, $B = \binom{u}{v}$ um vetor com entradas $u, v \in \mathbb{Z}_n$. Considere a função $f\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ dada por $f(X) = (AX + B)\ mod(n)$, em que $\mathrm{X} = \binom{x}{y}$. Tem-se que $f(X)$ é bijetora se, e somente se, $mdc\ (det(A), n) = 1$. Nesse caso, a inversa é dada por $f^{-1}(X) = A'X - B'\ mod\ (n)$, em que $A' = \begin{pmatrix} D'd & -D'b \\ -D'c & D'a \end{pmatrix}$, D' é tal que $D'.det(A) \equiv 1\ mod(n)$ e $B' \equiv A'B\ mod\ (n)$.

Demonstração:

Suponha f bijetora. Suponha, por contradição, que $mdc\,(det(A), n) = m > 1$. Considere $m' = \frac{n}{m}$ Vamos dividir em três casos:

Caso 1: $Se\ a, b, c, d$ são todos divisíveis por m. Seja $\mathrm{X} = \binom{m'}{m'}$. Então $f(X) = AX + B\ mod(n) = B\ mod(n) = B$. Como temos também $f\binom{0}{0} = B$, temos uma contradição com a bijetividade.

Caso 2: Se a, b, não são simultaneamente divisíveis por m. Seja $X = \binom{-bm'}{am'} mod(n) \neq \binom{0}{0}$. Então $f(X) = AX + B\ mod(n) = \binom{0}{det(A)m'} + B\ mod(n) = B$. Novamente temos uma contradição com a bijetividade.

Caso 3: Se c, d, não são simultaneamente divisíveis por m. Seja $X = \binom{dm'}{-cm'} mod(n) \neq \binom{0}{0}$. Então$f(X) = AX + B\ mod(n) = \binom{det(A)m'}{0} + B\ mod(n) = B$. Novamente temos uma contradição com a bijetividade.

Reciprocamente, suponha que $mdc(det(A), n) = 1$. Vamos mostrar que f é bijetora. Pelo Teorema 2.1.3.5 existe $D' \in \mathbb{Z}_n$ tal que $D'.det(A) \equiv 1\ mod\ (n)$. Considere a função $h(Y) = A'Y - A'B\ mod\ (n)$, com A' conforme o enunciado. Note que,

$AA'\ mod(n) = \binom{D'det(A)}{0} \quad \binom{0}{D'det(A)} mod(n) = \binom{1}{0} \quad \binom{0}{1}$. Então, utilizando propriedades de congruência (ver Proposição 2.1.2.4), se $Y \in \mathbb{Z}_n x\, \mathbb{Z}_n, então\ f\big(h(Y)\big) = Ah(Y) + B\ mod\ (n) = A(A'Y - A'B) + B\ mod\ (n) = (AA'Y - AA'B + B) mod\ (n) =$

$Y\ mod\ (n) = Y$. Logo, $f\big(h(Y)\big) = Y, \forall Y \in \mathbb{Z}_n x\, \mathbb{Z}_n$. De forma similar temos que $h\big(f(X)\big) = X,\ \forall\ X \in \mathbb{Z}_n x\, \mathbb{Z}_n$. Portanto, f é bijetora, sendo sua inversa dada por h. □

Exemplo 2.1.6.7: Considere a função $f(X) = \binom{7}{3} \quad \binom{4}{5} X + \binom{1}{-3}\ mod(5)$. Vamos determinar sua inversa.

Temos que $\det A = 35 - 12 = 23$. Note $mdc(23,5) = 1$. Conforme a Proposição 2.1.6.6 e o fato que $mdc(\det(A), n) = 1$, a função é bijetora e, portanto, admite inversa. Para determina-la, precisamos calcular D', de modo que $D'.23 \equiv 1\ mod\ (5)$, Como $2.23 = 46 \equiv 1\ mod\ (5)$, segue que $D' = 2$. Assim, podemos obter $A' = \binom{D'a_{22}}{-D'a_{21}} \quad \binom{-D'a_{12}}{D'a_{11}} = \binom{2.5}{-2.3} \quad \binom{-2.4}{2.7} =$

$\begin{pmatrix} 10 & -8 \\ -6 & 14 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix} mod\ (5)$. Resta agora determinar $A'B = \begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix}.\begin{pmatrix} 1 \\ -3 \end{pmatrix} = \begin{pmatrix} 0-6 \\ 4-12 \end{pmatrix} = \begin{pmatrix} -6 \\ -8 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \end{pmatrix} mod\ (5)$. Assim, $f^{-1}(X) = \begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix} X - \begin{pmatrix} 4 \\ 2 \end{pmatrix}\ mod\ (5)$.

Exemplo 2.1.6.7: Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ uma matriz de entradas $a, b, c, d \in \mathbb{Z}_n$, $B = \begin{pmatrix} u \\ v \end{pmatrix}$ um vetor com entradas $u, v \in \mathbb{Z}_n$ e com $mdc(Det\ A, n) = 1$. Uma forma de resolver o sistema $AX \equiv B\ mod\ (n)$, seria multiplicar ambos os lados do sistema por A´, e obtemos $X = A'B\ mod(n)$. Neste caso, a solução é única, a menos de congruência. Além disso, A' é chamada a inversa de $A\ mod(n)$.

2.2 ELEMENTOS DE ÁLGEBRA ABSTRATA

Na seção 1 do capítulo 3 (criptografias simétricas), abordaremos técnicas criptográficas que estão baseadas na aritmética modular, vista anteriormente. De fato, veremos que o conjunto a ser considerado é $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$, em que n é o número de caracteres de um certo alfabeto fixado. Uma correspondência biunívoca entre $\mathbb{Z}_n$ e os caracteres deste alfabeto será estabelecida. Então, para criar um algoritmo de criptografia, utilizaremos funções bijetoras em $\mathbb{Z}_n$. Estas funções bijetoras são obtidas a partir da aritmética modular (veja subseções 2.1.5 e 2.1.6 acima).

Temos que é possível definir operações em $\mathbb{Z}_n$de que modo que este se torne um anel (veja abaixo). Então, é possível reescrever os resultados utilizando esta linguagem. No entanto, evitamos, num primeiro momento, esta abordagem por acreditar que isto pode dificultar a aplicação deste conteúdo no ensino médio. Portanto, escolhemos não utilizar a linguagem de anel na seção 1 deste capítulo nem na seção 1 do capítulo 3.

No entanto, utilizaremos a linguagem de álgebra abstrata a partir da seção 3.8 do capítulo 3. Ali, consideramos criptografias assimétricas e os conjuntos a serem considerados serão corpos e grupos finitos, cujo exemplos básicos são $\mathbb{Z}_p$ e $\mathbb{Z}_p^*$, com p um número primo.

Acreditamos que esta parte poderá ser aplicada para alunos do ensino médio que possuem interesse em iniciar o contato com conceitos matemáticos abstratos.

No que segue, apresentamos as definições e resultados que serão utilizados da seção 2 do capítulo 3. As demonstrações dos resultados podem ser encontradas em [12], [14], [15] e [18].

2.2.1 ANEL, CORPO E GRUPO

Definição 2.2.1.1 Seja A um conjunto, com $A \neq \emptyset$, e $(+)$ e $(\cdot)$ duas operações em A, chamadas de adição e multiplicação. A terna $(A, +, .)$ será chamada de *anel* se as operações satisfazem os seguintes axiomas:

(i) A adição é associativa: Quaisquer que sejam $a, b, c \in A$, tem-se que $(a + b) + c = a + (b + c)$.

(ii) A adição é comutativa: Quaisquer que sejam $a, b \in A$, tem-se que $a + b = b + a$.

(iii) Existe o elemento neutro para a adição: Existe $\alpha \in A$ tal que $\alpha + x = x, \forall\, x \in A$.

(iv) Todo elemento de A possui um simétrico: Para cada $a \in A$, existe $k \in A$ tal que $a + k = \alpha$.

(v) A multiplicação é associativa: Quaisquer que sejam $a, b, c \in A$, tem-se que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(vi) A multiplicação é distributiva com relação à adição: Quaisquer que sejam $a, b, c \in A$, tem-se que $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Observação 2.2.1.2:

1) No item (iii), o elemento neutro da adição será denotado por 0_A.

2) No item (iv), o elemento simétrico de a, será denotado por $-a$.

3) a diferença entre dois elementos é definida por $a - b = a + (-b)$.

4) Temos que $0 \cdot x = x \cdot 0 = 0, \forall\, x \in A$. De fato, $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$. Então $0 \cdot x = 0 \cdot x + 0 \cdot x$. Somando o simétrico de $0 \cdot x$ em ambos os lados, obtemos $0 \cdot x - 0 \cdot x = 0.x + (0 \cdot x - 0 \cdot x)$. Então $0 = 0 \cdot x + (0) = 0 \cdot x$.

De forma similar, obtém-se que $x \cdot 0 = 0$.

Definição 2.2.1.3: Denotamos A^* pelo conjunto dos elementos de A diferentes do elemento neutro da adição.

Exemplo 2.2.1.4: O conjunto $\mathbb{Z}$, com as operações usuais de soma e multiplicação, é um anel.

Exemplo 2.2.1.5: O conjunto A de todas as matrizes 2×2 com entradas reais, isto é, $A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a, b, c, d \in \mathbb{R} \right\}$, com as operações de soma e multiplicação definidas por

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}$ e $\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & bb'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}$, respectivamente, com $a', b', c', d' \in \mathbb{R}$, é um anel.

Exemplo 2.2.1.6: Seja n número um natural maior que 1 e $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Lembremos da função

$$f_n : \mathbb{Z} \to \mathbb{Z}_n;$$
$$x \to f_n(x),$$

em que $f_n(x)$ é o resto da divisão Euclidiana de x por n. Vamos definir duas operações, $\oplus$ e $\otimes$, em $\mathbb{Z}_n$ da seguinte forma:

$$\oplus : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(a, b) \mapsto f_n(a+b)$$

e

$$\otimes : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(a, b) \mapsto f_n(a \cdot b),$$

em que $+$ e $.$ são as operações usuais em $\mathbb{Z}$. Logo, temos as operações em $\mathbb{Z}_n$ dadas por

$$a \oplus b = f_n(a+b)$$

e

$$a \otimes b = f_n(a \cdot b).$$

Vamos verificar que $(\mathbb{Z}_n, \oplus, \otimes)$ é um anel. Este resultado segue a partir das propriedades da soma e da multiplicação usual em $\mathbb{Z}$ e das seguintes propriedades de f_n:

$$f_n(a+b) = f_n(f_n(a)+b), \forall a, b \in \mathbb{Z}.$$
$$f_n(a \cdot b) = f_n(f_n(a) \cdot b), \forall\, a, b \in \mathbb{Z}.$$

De fato, $\forall a, b \in \mathbb{Z}_n$, temos:

(i) <u>A adição é associativa</u>: $(a \oplus b) \oplus c = f_n(a+b) \oplus c = f_n(f_n(a+b)+c) = f_n((a+b)+c) = f_n(a+(b+c)) = f_n(a+f_n(b+c)) = a \oplus f_n(b+c) = a \oplus (b \oplus c)$.

(ii) <u>A adição é comutativa</u>: $a \oplus b = f_n(a+b) = f_n(b+a) = b \oplus a$.

(iii) <u>Existe o elemento neutro para a adição</u>: $0 \oplus a = f_n(0+a) = f_n(a) = a$

(iv) <u>Todo elemento de A possui um simétrico</u>: Seja $a \in \mathbb{Z}_n$. Se $a = 0$, então $-a = 0$.

Se $a \neq 0$, então $-a = n-a$. De fato temos que $a \oplus (n-a) = f_n(a+(n-a)) = f_n(n) = 0$.

(v) A multiplicação é associativa: $(a \otimes b) \otimes c = f_n(a \cdot b) \otimes c = f_n(f_n(a \cdot b) \cdot c) = f_n\big((a \cdot b) \cdot c\big) = f_n(a \cdot (b \cdot c)) = f_n(a \cdot f_n(b \cdot c)) = a \otimes f_n(b \cdot c) = a \otimes (b \otimes c)$.

(vi) A multiplicação é distributiva com relação à adição: $a \otimes (b \oplus c) = a \otimes f_n(b + c) = f_n(a \cdot f_n(b + c)) = f_n(a \cdot (b + c)) = f_n(a \cdot b + a \cdot c) = f_n(a \cdot b + f_n(a \cdot c)) = f_n(f_n(a \cdot b) + f_n(a \cdot c)) = f_n(a \cdot b) \oplus f_n(a \cdot c) = (a \otimes b) \oplus (a \otimes c)$

De forma similar,

$(b \oplus c) \otimes a = f_n(b + c) \otimes a = f_n(f_n(b + c) \cdot a) = f_n((b + c) \cdot a) = f_n(b \cdot a + c \cdot a) = f_n(b \cdot a + f_n(c \cdot a)) = f_n(f_n(b \cdot a) + f_n(c \cdot a)) = f_n(b \cdot a) \oplus f_n(c \cdot a) = (b \otimes a) \oplus (c \otimes a)$

Observação: Daqui em diante, iremos denotar a soma e multiplicação em $\mathbb{Z}_n$ por $+$ e $\cdot$, respectivamente.

Definição 2.2.1.7 Um anel A é dito c*omutativo* se $a \cdot b = b \cdot a \; \forall \; a, b \in A$.

Definição 2.2.1.8 Um anel A é dito *unitário,* ou com unidade, se existe um elemento $1_A \in A$ tal que $1_A \cdot a = a \cdot 1_A = a, \forall \; a \in A$. Neste caso, 1_A é dito unidade do anel A.

Exemplo 2.1.1.9: Seja n número um natural maior que 1. Então $\mathbb{Z}_n$ é um anel comutativo com unidade, sendo a unidade dada por 1.

De fato,

$$a \otimes b = f_n(a \cdot b) = f_n(b \cdot a) = b \otimes a,$$

e

$$1 \otimes a = f_n(1 \cdot a) = f_n(a) = a$$

Observação 2.2.1.10: Dizemos que um anel A é sem divisores de zero se $a, b \in A$ e $a \cdot b = 0 \Longrightarrow a = 0 \; ou \; b = 0$.

Definição 2.2.1.11 Um domínio de integridade é um anel unitário, comutativo e sem divisores de zero.

Definição 2.2.1.12 Um corpo é um anel unitário e comutativo K tal que se $a \in K$ e $a \neq 0$, então existe $a' \in K$ tal que $a \cdot a' = 1$. Neste caso, a' é dito inverso de $a\ em\ K,$ e é denotado por a^{-1}.

Observação 2.2.1.13: Um corpo é um anel unitário, comutativo em que todo elemento diferente de zero possui inverso.

Observação 2.2.1.14: Todo corpo é um domínio de integridade. De fato, se $a.b = 0$ e $a \neq 0$, então a possui inverso. Logo $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (0)$. Temos que $a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b$. Por outro lado, desde que $a^{-1} \cdot (0) = 0$, temos que $b = 0$.

Exemplo 2.2.1.15: Com as operações usuais de adição e multiplicação, $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade que não é corpo pelo fato de não admitir o inverso de alguns elementos. Por exemplo, $3 \in \mathbb{Z}$ e não existe $x \in \mathbb{Z}$ tal que $3 \cdot x = 1$.

Exemplo 2.2.1.16: O conjunto dos polinômios com coeficientes reais $R[X]$, com as operações usuais, é um domínio de integridade que não é corpo.

Exemplo 2.2.1.17: Com as operações usuais de adição e multiplicação, $(\mathbb{Q}, +, .)$ e $(\mathbb{R}, +, .)$ são corpos.

Proposição 2.2.1.18: Seja n um número natural maior que 1. Então, $\mathbb{Z}_n$ é corpo se, e somente se, n é primo. Se n não é primo, $\mathbb{Z}_n$ não é domínio de integridade, isto é, possui divisores de zero.

Demonstração:

Seja $n > 1,$ um número não primo. Então n pode ser decomposto da forma $n = ab$ com a e b naturais maiores que 1 e menores que n. Temos que a, b estão em $\mathbb{Z}_n$, são não nulos e $a.b = f_n(a \cdot b) = f_n(n) = 0$. Portanto $\mathbb{Z}_n$ não pode ser um domínio de integridade. Logo, não é corpo.

Agora suponha que n é primo. Seja r um número natural tal que $1 \leq r < n$. Assim, como n é primo, r e n são coprimos. Pelo teorema de Bezout, existem inteiros a e b tais que $ar + bn = 1$. Considere o número $f_n(a)$. Claramente este número está em $\mathbb{Z}_n$. Temos $r \cdot (a) = f_n(r \cdot$

$f_n(a)) = f_n(r \cdot a) = f_n(1 - bn) = 1$. Então temos que $f_n(a)$ é o inverso de r em $\mathbb{Z}_n$. Logo, temos que $\mathbb{Z}_n$ é corpo.□

Definição 2.2.1.19 Um conjunto não vazio G, munido com uma operação (.), forma um grupo, denotado por $(G,\cdot)$, se são válidas as seguintes propriedades:
(i) É associativo: $a, b, c \in G$ implica que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(ii) Existência do elemento unidade em G: Existe um elemento $e \in G$ tal que $e \cdot a = a = a \cdot e, \forall\, a \in G$.
(iii) Existência do elemento inverso em G: Para todo $a \in G$ existe um elemento $a' \in G$ tal que $a \cdot a' = e = a' \cdot a$.

Observação 2.2.1.20: O grupo é dito comutativo, ou abeliano, se $a \cdot b = b \cdot a, \forall\, a, b \in G$.

Exemplo 2.2.1.21: Seja $(A, +, \cdot)$ um anel. Então $(A, +)$ é um grupo comutativo.

Exemplo 2.2.1.22: Se $(K, +, \cdot)$ é um corpo, então $(K^*, \cdot)$ é um grupo comutativo, em que K^* é o conjunto dos elementos de K, exceto o elemento neutro da adição. Este é chamado grupo multiplicativo obtido a partir de corpo K.

2.2.2 Grupos e Corpos finitos

Definição 2.2.2.1 Dizemos que um grupo $(G, .)$ é finito se ele possui uma quantidade finita de elementos. Neste caso, denotamos esta quantidade por $|G|$, e esta é chamada ordem do grupo.

Definição 2.2.2.2 Dados x em $(G, .)$, n inteiro, e a unidade do grupo e x^{-1} o inverso de x. Definimos:

$$x^n = \begin{cases} e, \quad se\ n = 0 \\ x.x.\ldots.x\ (n\ vezes)\ se\ n > 0 \\ x^{-1}.x^{-1}.\ldots.x^{-1}\ (-n\ vezes)\ se\ n < 0 \end{cases}$$

Proposição 2.2.2.3 Seja $(G, .)$ um grupo finito com e a unidade. Dado $x \in G$, existe um número natural positivo n com $1 < n < |G|$ tal que $x^n = e$.

Demonstração:

Se x é a identidade, basta escolher $n = 1$. Suponha x diferente da identidade. Seja $|G|$ a ordem do grupo e considere os elementos $x, x^2, , x^3, \ldots , x^{|G|}, , x^{|G|+1}$. Então existem i e j, com $|G| + 1 \geq i > j \geq 1$ e tal que, $x^i = x^j$. Logo $x^{-j} x^i = x^{-i} \cdot x^j = e$. Seja $n = i - j$. Então $x^n = e$. □

Definição 2.2.2.4 Seja G um grupo finito e x um elemento de G. O menor natural positivo que satisfaz a proposição acima é chamado ordem do elemento x em G.

Proposição 2.2.2.5 Seja $(G,\cdot)$ um grupo finito. Dado $x \in G$, a ordem de x em G divide a ordem do grupo G. Além disso, se a ordem de x é n, então $x^i \neq x^j$, para todo $1 \leq i < j \leq n$.

Demonstração:

Se x for a identidade, o resultado é obvio. Suponha x diferente da identidade. Seja n a ordem do elemento x. Suponha, por contradição, que exista $1 \leq i < j \leq n$ tal que $x^i = x^j$. Logo $x^{j-i} = e$, e $1 < j - i < n$, contrariando a minimalidade de n. Logo, os elementos $x, x^2, \ldots x^{n-1}, x^n$ são todos distintos. Seja $|G|$ a ordem de G. Note devemos ter $n \leq |G|$, desde que os elementos $x, x^2, \ldots x^{n-1}, x^n$ são todos distintos. Considere o conjunto $H = \{ x, x^2, \ldots x^{n-1}, x^n \}$. Definimos a seguinte relação em G: $y \sim z$ se $y. z^{-1}$ está em H. Temos que esta é uma relação de equivalência em G, pois H é um subgrupo (isto é, é fechado por multiplicação e por inverso).

Sejam $A_{1,} \ldots A_{r,}$ as classes de equivalências. Note que cada classe A_j possui exatamente n elementos. De fato, dado z em A_j temos que $A_{j,} = \{x \cdot z, x^2 \cdot z, \ldots, x^{n-1} \cdot z, x^n \cdot z \}$. Então, desde que G é a união disjunta das classes, tendo r classes e cada classe possui n elementos, temos

$|G| = r \cdot n$. Portanto n divide $|G|$. □

Observação 2.2.2.6: Seja $(G,.)$ um grupo finito. Dado $x \in G$ então $x^{|G|} = e$.

Definição 2.2.2.7 Um grupo finito $(G,.)$ é dito cíclico se existe um elemento $x \in G$ tal que $G = \{x, x^2, \ldots, x^{n-1}, x^n\}$, em que n é a ordem de x. Neste caso, x é dito um gerador do grupo.

Observação 2.2.2.8:

1) Note que todo grupo finito cíclico é comutativo.

2) x é um gerador do grupo finito cíclico G se, e somente se, a ordem de x em G é igual a ordem do grupo G.

3) Seja $(G,\cdot)$ um grupo finito cuja ordem é um número primo. Então G é um grupo cíclico e qualquer elemento diferente da identidade é um gerador.

4) Considere o grupo $(\mathbb{Z}_p^*,\cdot)$, sendo p um número primo. Este é um grupo com $p-1$ elementos. Então, a ordem de qualquer elemento de $\mathbb{Z}_p^*$ divide $p-1$.

Exemplo 2.2.2.9: Considere o grupo $\mathbb{Z}_{29}^* = \{1,2,3,\dots,28\}$. Vamos verificar se 2 é um gerador de $\mathbb{Z}_{29}^*$. Considere as congruências abaixo:

$2^1 \equiv 2\ mod\ (29)$ $2^8 \equiv 24\ mod\ (29)$ $2^{15} \equiv 27\ mod\ (29)$ $2^{22} \equiv 5\ mod\ (29)$

$2^2 \equiv 4\ mod\ (29)$ $2^9 \equiv 19\ mod\ (29)$ $2^{16} \equiv 25\ mod\ (29)$ $2^{23} \equiv 10\ mod\ (29)$

$2^3 \equiv 8\ mod\ (29)$ $2^{10} \equiv 9\ mod\ (29)$ $2^{17} \equiv 21\ mod\ (29)$ $2^{24} \equiv 20\ mod\ (29)$

$2^4 \equiv 16\ mod\ (29)$ $2^{11} \equiv 18\ mod\ (29)$ $2^{18} \equiv 13\ mod\ (29)$ $2^{25} \equiv 11\ mod\ (29)$

$2^5 \equiv 3\ mod\ (29)$ $2^{12} \equiv 7\ mod\ (29)$ $2^{19} \equiv 26\ mod\ (29)$ $2^{26} \equiv 22\ mod\ (29)$

$2^6 \equiv 6\ mod\ (29)$ $2^{13} \equiv 14\ mod\ (29)$ $2^{20} \equiv 23\ mod\ (29)$ $2^{27} \equiv 15\ mod\ (29)$

$2^7 \equiv 12\ mod\ (29)$ $2^{14} \equiv 28\ mod\ (29)$ $2^{21} \equiv 17\ mod\ (29)$ $2^{28} \equiv 1\ mod\ (29)$

Temos que 28 é o menor natural positivo tal que $2^{28} \equiv 1\ mod\ (29)$. Desse modo, 28 é a ordem do elemento 2 em $\mathbb{Z}_{29}^*$. O item 2 da observação 2.2.2.8 nos garante que 2 é um gerador de $\mathbb{Z}_{29}^*$.

Exemplo 2.2.2.10: Considere o grupo $\mathbb{Z}_{11}^*$=$\{1,2,3,\dots,10\}$. Temos que 2 é um gerador de $\mathbb{Z}_{11}^*$, pois potências de 2 geram todos os elementos de $\mathbb{Z}_{11}^*$, conforme podemos verificar abaixo:

$2^1 \equiv 2\ mod\ (11)$ $2^6 \equiv 9\ mod\ (11)$

$2^2 \equiv 4\ mod\ (11)$ $2^7 \equiv 7\ mod\ (11)$

$2^3 \equiv 8\ mod\ (11)$ $2^8 \equiv 3\ mod\ (11)$

$2^4 \equiv 5\ mod\ (11)$ $2^9 \equiv 6\ mod\ (11)$

$2^5 \equiv 10\ mod\ (11)$ $2^{10} \equiv 1\ mod\ (11)$

Exemplo 2.2.2.11: Em $\mathbb{Z}_7^*$, temos que 2 não é gerador, pois

$$2 \equiv 2\ mod\ (7)$$

$$2^2 \equiv 4\ mod\ (7)$$

$$2^3 \equiv 1\ mod\ (7)$$

$$2^4 \equiv 2\ mod\ (7)$$
$$2^5 \equiv 4\ mod\ (7)$$
$$2^6 \equiv 1\ mod\ (7).$$

Definição 2.2.2.12 Considere um corpo $(K, +, \cdot)$. Dizemos que o corpo é finito se ele possui uma quantidade finita de elementos.

Teorema 2.2.2.13 Seja q um número natural. Então, existe um corpo finito F_q contendo q elementos se, e somente se, q é uma potência de primo, isto é, existe um primo p e um número natural n tal que $q = p^n$. Neste caso, o corpo finito é único a menos de isomorfismo (veja definição de isomorfismo em [15] p.153). Além disso, o grupo finito $(F_q^*, .)$ é cíclico.
A demonstração do resultado acima pode ser encontrada em [16], no capítulo 2.

Definição 2.2.2.14 Seja q um inteiro positivo que é a potência de um primo. Daqui em diante denotamos, a menos de isomorfismo, por F_q o corpo finito que tem q elementos, e F_q^* o grupo multiplicativo associado.

Observação 2.2.2.15: Note que a ordem de F_q^* é $q - 1$. A ordem de qualquer elemento $a \in F_q^*$ divide $(q - 1)$.

Exemplo. 2.2.2.16: Se q é primo, então, a menos de isomorfismo, $F_q = \mathbb{Z}_q$.

Proposição 2.2.2.17 Seja $(F_q, +, \cdot)$ um corpo finito. Se x é um gerador do grupo $(F_q^*, \cdot)$, então x^j também é gerador se, e somente se, $mdc(j, q-1) = 1$. Em particular, existe um total de $\Phi(q-1)$ geradores distintos em F_q^*, em que Φ é a função de Euler.
Demonstração:
Para o caso $q = 2$ o resultado é obvio. Suponha $q > 2$.
Se $j = 1$, o resultado também é óbvio. Suponha j maior que 1 e tal que $mdc(j, q-1) = 1$.
Então, existem inteiros não nulos r e s tais que $rj + s(q-1) = 1$. Considere k o resto da divisão de r por $(q-1)$, isto é, $r = n(q-1) + k$. com $0 \leq k < q-1$. Note que não é possível termos $k = 0$. Logo $1 \leq k < q-1$. Desde que a ordem de F_q^* é $q-1$, temos que $x^{q-1} = e$. Então

$(x^j)^k = (x^j)^{r-\mathrm{n}(\mathrm{q}-1)} = x^{jr}.(x^{q-1})^{-\mathrm{n}} = x^{jr}.e = x^{jr} = x^{1-s(q-1)} = x^1.(x^{q-1})^{-\mathrm{s}} =$ $x.e = x$. Acabamos de concluir que existe $1 \leq k < q$ tal que $(x^j)^k = x$. Desde que x é gerador, temos que x^j também é gerador.

Seja j inteiro maior que 1 tal que x^j é gerador. Logo, existe um n natural tal que $x^{jn} = x$. Então $x^{jn-1} = e$. Desde que x é gerador, $jn - 1$ deve ter múltiplo de $q - 1$, isto é, existe um inteiro m tal que $(jn - 1) = m(q - 1)$. Portanto, $jn - m(q - 1) = 1$. Desta igualdade, vemos que qualquer divisor comum de j e $q - 1$ deve também ser divisor de 1. Logo, $mdc(j, q - 1) = 1$. Temos que F_q^* = $\{ x, x^2, \ldots, x^{q-2}, x^{q-1} \}$. Logo, temos que $\Phi(q - 1)$ é o número geradores em F_q^*. □

Exemplo. 2.2.2.18: Considere o conjunto $F = \{ (a, b) \mid a, b \in \mathbb{Z}_2\}$. Note que este conjunto possui 4 elementos Vamos definir duas operações em F da seguinte forma $(a, b) \oplus (c, d) = (a + c, b + d)$ e $(a, b) \otimes (c, d) =$ $(a.c + b.d, ad + bc + bd)$, em que + e . são as operações usuais em $\mathbb{Z}_2$. Então temos que F é um corpo com $4 = 2^2$ elementos.

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

.	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(1,1)	(0,1)	(1,0)
(1,0)	(0,0)	(0,1)	(1,0)	(1,1)
(1,1)	(0,0)	(1,0)	(1,1)	(0,1)

3 MATEMÁTICA E CRIPTOGRAFIA

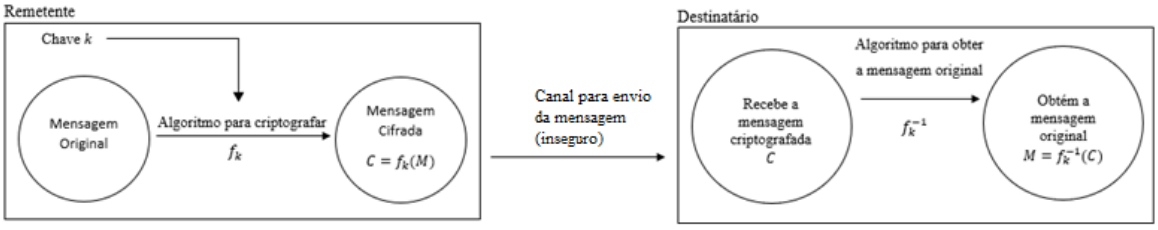
Neste capítulo será abordado alguns dos principais sistemas criptográficos e sistematização do processo de cifrar e decifrar em cada sistema abordado. Tais processos são baseados nas referências [3], [5], [6], [7], [10], [11], [17], [25] e [26].

3.1 SISTEMAS DE CRIPTOGRAFIA

Um sistema é considerado criptográfico quando, dada uma mensagem legível e uma chave, é gerada uma nova mensagem ilegível, sendo esta transferida a um certo destinatário. A transferência é feita por um canal considerado não seguro, isto é, passível de ser interceptado por terceiros. O sistema deve ser tal que os possíveis interceptadores não consigam decifrar a mensagem legível a partir da inelegível sem o conhecimento da chave. É necessário ainda que o destinatário consiga recuperar a mensagem original utilizando uma chave, seja a mesma utilizada pelo remetente ou outra.

Mais especificamente, dada uma mensagem legível (M), também chamada de mensagem original, utiliza-se uma chave k, que está associada a um algoritmo, aqui denotado por uma função f_k, que transforma a mensagem original (M) em uma mensagem cifrada (C). A esta etapa denominamos de cifragem. O destinatário recebe a mensagem cifrada e precisa fazer a decodificação, ou seja, faz a conversão da mensagem cifrada para a mensagem original utilizando f_k^{-1}. Podemos representar a situação através da figura 1:

Figura 1 – Representação de um sistema criptográfico



Fonte: Elaborada pela autora

A função f_k que transforma a mensagem de texto original na mensagem cifrada, deve ser injetora, isto é, dada uma mensagem cifrada, deve existir uma e apenas uma mensagem original associada a ela. Além disso, a mensagem original e a cifrada podem ser organizadas

em unidades de mensagens. A unidade de mensagem pode ser uma única letra, um par de letras (dígrafo), um triplo de letras (trígrafo) ou um bloco de n letras. Podemos ainda representar as unidades de mensagem como vetores ou pontos de uma curva.

3.2 UNIDADE DE MENSAGEM DE UMA LETRA: TRANSFORMAÇÕES LINEARES E AFINS

Nesta seção, abordaremos as chamadas cifras de substituição. Nessas, cada unidade de mensagem é substituída por um certo símbolo, sem alteração na ordem das unidades. Aqui, aplicaremos esta técnica às unidades de mensagem de uma letra. Esse tipo de cifra é conhecido desde a antiguidade, como indica o seguinte texto:

> O primeiro documento que usou cifras de substituição para propósitos militares aparece nas Guerras de Gália de Júlio César. César descreve como enviou uma mensagem para Cícero, que estava cercado e prestes a se render. Ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo. [...], graças a *As vidas dos Césares*, escrito no século II por Suetônio, nós temos uma descrição detalhada de um dos tipos de cifra de substituição usado por Júlio César. (SINGH, 2011, p.26)

Abordaremos um tipo específico de cifra de substituição chamada Cifra de César. Essa consiste em substituir cada letra de uma mensagem por outra, sempre avançando três casas no alfabeto, conforme o Quadro 1 a seguir:

Quadro 1: Cifra de César

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

Fonte: A autora.

Vamos associar cada letra do nosso alfabeto a um único número pertencente ao conjunto $\mathbb{Z}_{26} = \{0,1,2,\dots,25\}$, conforme o Quadro 2 abaixo:

Quadro 2: Letras do alfabeto e seus números equivalentes

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: A autora.

Neste caso, podemos, de forma inicial, relacionar a Cifra de César com a função $f(x) = x + 3$, em que x representa a posição da letra da mensagem original no alfabeto e $f(x)$

representa a posição da letra cifrada. Por exemplo, a palavra BELO é representada pela sequência $1-4-11-14$. Aplicando a função codificadora $f(x)=x+3$, temos que a palavra cifrada é representada por $4-7-14-17$. Por outro lado, se considerarmos a palavra AMIZADE, sua equivalência numérica é $0-12-8-25-0-3-4$. Novamente, aplicando a função $f(x)$ acima, obtemos os valores cifrados $3-15-11-28-3-6-7$. Aqui, se desejarmos visualizar a palavra cifrada ao invés de sua sequência numérica, temos que analisar o caso do valor 28. Desde que 28 é decorrente da cifragem da letra Z, pelo Quadro 1, 28 deve representar a letra C. Note que C também representado pelo número 2, conforme o Quadro 2. Portanto, para restringirmos o processo ao conjunto $\{0,1,2,\dots,25\}$, procedemos da seguinte forma: caso se obtenha um valor acima de 25, recomeçamos o alfabeto, no qual 26 é equivalente a 0, 27 a 1 e assim sucessivamente.

Pela análise acima, temos que a função codificadora fica melhor descrita se utilizarmos a aritmética modular (vista no capítulo 2). Neste caso, temos que a função codificadora é de fato $f(x)=x+3\ mod(26)$, sendo o domínio e contradomínio dados por $\mathbb{Z}_{26}=\{0,1,2,3,\dots,25\}$. Aqui, $x+3\ mod(26)$ representa o resto da divisão de $x+3$ por 26, seguindo o Teorema da divisão de Euclides (conforme visto no capítulo 2). Note que esta função é bijetora em $\mathbb{Z}_{26}$.

Para decifrar a mensagem devemos usar a função inversa, que neste caso é dada por $f^{-1}(C)=C-3\ mod(26)$, onde C é o valor da letra cifrada.

Podemos generalizar o método acima e considerar funções codificadoras do tipo $f(x)=ax+b\ mod\ (26)$, em que a,b são números naturais. Neste caso, devemos escolher o par (a,b) de forma que $f(x)$ seja injetora em $\mathbb{Z}_{26}$.

Exemplo 3.2.1: Considere, por exemplo $f(x)=2x+1\ mod\ (26)$ e vamos cifrar a palavra NADA. Temos que a palavra original é dada pela sequência $13-0-3-0$. Aplicando a função codificadora obtemos a sequência $27\ -1-7-1$. Desde que $27\equiv 1\ mod(26)$, a palavra cifrada é $1-1-7-1\rightarrow$ BBHB. Vemos que as letras N e A foram substituídas por B. Desse modo, ao tentar decifrar, há a dúvida se B representa a letra A ou a letra N, ou seja, uma cifra está associada a duas letras distintas da palavra original. Portanto, não temos uma função codificadora injetora. Conforme Proposição 2.1.5.2, devemos ter $mdc(a,26)=1$ para $f(x)=ax+b\ mod(26)$ ser bijetora em $\mathbb{Z}_{26}=\{0,1,2,\dots,25\}$.

Uma vez que a mensagem codificada esteja com o destinatário, ele precisa conhecer a função inversa para decifrar a mensagem.

Exemplo 3.2.2: Considere a função $f(x) = 5x + 3\ mod(26)$. Poderíamos ter a ilusão de sua inversa seria $f^{-1}(C) \equiv \frac{C-3}{5}\ mod(26)$. Note que isso está errado. De fato, para $x = 10$ temos $C = f(10) = 5.10 + 3\ mod(26) = 53\ mod(26) \equiv 1$. Neste caso, teríamos $f^{-1}(1) = \frac{1-3}{5}\ mod\ (26) = -\frac{2}{5}\ mod(26)$, o que não faz sentido na aritmética modular. Utilizando os resultados da Proposição 2.1.5.2 do capítulo 2, a inversa da função acima é de fato dada por $f^{-1}(\ C\ ) = a'.C - b'\ mod\ (26)$, em que a' e b' pertencem ao conjunto $\mathbb{Z}_{26}$ e são tais que $a'.5 \equiv 1\ mod(26)$ e $b' \equiv a'.3\ mod\ (26)$. Desde que $21.5 = 4.26 + 1$, temos que $a' = 21$. Então $b' = 21 \times 3\ mod\ (26) = 11$. Portanto, $f^{-1}(\ C\ ) = 21C - 11\ mod\ (26)$.

Em várias situações, é interessante incluir símbolos extras ao alfabeto utilizado, como, por exemplo, pontuação. Neste caso, podemos trabalhar com um alfabeto contendo N caracteres, sendo N um número natural, e funções bijetoras da forma $f(x) \equiv ax + b\ mod(N)$. Para $f(x) \equiv (ax + b)\ mod(N)$ ser bijetora no conjunto $\mathbb{Z}_N = \{1,2,3,..,N-1\}$, devemos ter $mdc(N,a) = 1$. Nessa situação, a função inversa é dada por $f^{-1}(C) = a'C - b'\ mod\ (N)$, em que $a', b' \in \mathbb{Z}_N$ são tais que $a'.a \equiv 1 mod(N)$ e $b' \equiv a'.b\ mod\ (N)$, conforme Proposição 2.1.5.2.

Para compreender melhor como obter a função decodificadora, acompanhe os exemplos abaixo.

Exemplo 3.2.3: Considere que para cifrar uma mensagem foi escolhida a função codificadora $f(x) \equiv 5x + 4\ mod\ (26)$. Para obter a função decodificadora, precisamos determinar em primeiro lugar o valor de a'que pertença ao conjunto $\mathbb{Z}_{26} = \{0,1,2,\ldots,25\}$ e tal que $5\ .a' \equiv 1\ mod\ (26)$. Note que $5 \times 21 = 105$ e que $104 = 4 \times 26$. Logo $5 \times 21 = 105 \equiv 1\ mod(26)$ e, portanto, $a' = 21$. Com isso, podemos obter $b' = a'b = 21 \times 4 = 84 \equiv 6\ mod\ (26)$. Segue que, a função decodificadora é dada por $f^{-1}(C) = 21C - 6\ mod(26)$.

Exemplo 3.2.4: Suponha que se deseja cifrar uma mensagem com as pontuações. Nesse caso teremos as 26 letras do alfabeto e o acréscimo de 4 caracteres. Logo nosso conjunto de caracteres tem 30 elementos, isto é, as funções de transformação afim será $mod\ (30)$. Considere que seja escolhida a função codificadora $f(x) = 7x - 5\ mod(30)$ para cifrar a

mensagem PAULA, PRECISAMOS CONVERSAR URGENTEMENTE! Para isso, vejamos o correspondente numérico para cada caractere segundo o quadro 3:

Quadro 3: Letras do alfabeto e caracteres com seus números equivalentes

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**.**	**,**	**?**	**!**
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Fonte: A autora.

Substituindo cada letra e pontuação da frase pelo correspondente numérico, temos a seguinte sequência:

$15-0-20-11-0-27-15-17-4-2-8-18-0-12-14-18-2-14$

$13-21-4-17-18-0-17-20-17-6-4-13-19-4-12-4-13-19$

$4-29$

Aplicando a função codificadora $f(x) = 7x - 5\ mod(30)$, a nova sequência é:

$10-25-15-12-25-4-10-24-23-9-21-1-25-19-3-1-9-3$

$26-22-23-24-1-25-24-15-24-7-23-26-8-23-19-23-26$

$8-23-18$

Desse modo, a frase cifrada ficará:

KZPMZEKYXJVBZTDBJD.WXYBZYPYHX.IXTX.IXS

Para obter a frase original, basta determinar a função decodificadora que é da forma $f^{-1}\ (C) = a'C - b'\ mod(30)$, em que $a', b' \in Z_{30}$, e $a'.7 \equiv 1\ mod(30)$ e $b' \equiv a'.(-5)\ mod\ (30)$. Observe que $7 \times 13 = 91 \equiv 1\ mod\ (30)$. Logo, $a' = 13$. Daí segue que, $b' = 13 \times (-5) = -65 \equiv -5\ mod\ (30)$. Portanto, $f^{-1}(C) = 13C + 5\ mod(30)$.

Uma função do tipo $f(x) \equiv ax + b\ mod(N)$ é dita uma transformação afim se b é não nulo, e linear se b é nulo. O par (a, b) é a chamado chave da encriptação, e denotado por k. Essa chave deve ser previamente compartilhada entre o remetente (para criptografar) e o destinatário (para descriptografar). Além disto, ela deve ser mantida em segredo de terceiros.

De forma geral, ao se considerar um alfabeto de N caracteres, pode-se escolher qualquer função bijetora em $\mathbb{Z}_N = \{0, 1, 3, \ldots N-1\}$ como uma função codificadora. Nesse caso, amplia-se o conjunto de funções codificadoras, desde que existem funções bijetoras de $\mathbb{Z}_N = \{0, 1, 3, \ldots N-1\}$ que não são da forma $ax + b\ mod\ (N)$. No entanto, há uma dificuldade em

se considerar uma classe muito geral de funções no sentido que o processo de determinação das chaves e dos algoritmos pode se tornar demasiadamente complexo.

3.3 CRIPTOANÁLISE DAS CIFRAS DE SUBSTITUIÇÃO DE UNIDADE DE MENSAGEM DE UMA LETRA.

Criptoanálise é a arte de tentar desvendar o algoritmo utilizado em uma encriptação, tendo acesso apenas a uma quantidade finita de textos criptografados e a estrutura geral do sistema, mas sem o conhecimento das chaves. Através de análises, podemos obter certas medidas relativas ao nível de segurança de um sistema criptográfico.

Dado um alfabeto com N caracteres, na subseção anterior utilizamos funções criptográficas da forma $f(x) = ax + b \; mod\; (N)$, com f sendo bijetora em $\mathbb{Z}_N$. Como vimos, o par (a, b) é chamado chave, denotado por k, e é utilizado tanto pelo remetente para criptografar a mensagem original, quanto pelo destinatário para calcular inversa $f^{-1}(C)$, e assim recuperar a mensagem original a partir da mensagem criptografada enviada pelo remetente. Portanto, para a devida segurança, essa chave deve ser mantida em segredo, sendo conhecida apenas pelo remetente e destinatário. Mesmo que terceiros consigam interceptar a mensagem criptografada, que é enviada por um canal considerado inseguro, conforme figura 1, esses, não tendo conhecimento da chave, a princípio não deveriam conseguir obter a mensagem original $f^{-1}(C)$. Porém, nessas situações, burladores podem tentar utilizar certos artifícios para quebrarem o código. Um método inicial, e bastante ingênuo para esse caso, seria tentar encontrar a chave por tentativa e erro, chamado também de ataque por força bruta.

Suponha que um invasor capture uma mensagem criptografada C e saiba que o sistema utilizado foi o anteriormente visto em um alfabeto de N caracteres. Portanto, ele sabe que, para recuperar a mensagem original, ele deve calcular$f^{-1}(C)$, que é da forma $a'C - b' \; mod\; (N)$, em que a' e b' estão em $\mathbb{Z}_N$ e são desconhecidos pelo burlador. Ele sabe também que f^{-1} é bijetora $\mathbb{Z}_N$, e, portanto, deve-se ter $mdc(a', N) = 1$. Logo, ele poderia testar todos os valores possível de a' e b' e ver para quais destes valores, $f^{-1}(C)$ produz uma mensagem coerente com uma possível mensagem original. O ponto central então é saber o quão computacionalmente viável é essa abordagem. Temos que existem $\Phi(N)$ possibilidades para a' (Φ é a função Totiente de Euler vista na seção 2.1.4) e N possibilidades para b'. Então, tem-se $\Phi(N) \times N$

testes a serem feitos. Essa quantidade pode ficar computacionalmente trabalhosa para N suficientemente grande, como vemos nos seguintes exemplos:

Exemplo 3.3.1: Suponha que um invasor saiba que para cifrar uma mensagem foi utilizado um alfabeto com $N = 26$ caracteres. O número de funções possíveis para ter sido utilizada como chave é dado por $\Phi(26) \times 26$. Conforme Proposição 2.1.4.10 do capítulo 2, $\Phi(26) = \Phi(2.13) = \Phi(2).\Phi(13) = (2-1).(13-1) = 1.12 = 12$. Logo, o número de chaves possíveis são $12 \times 26 = 312$.

Exemplo 3.3.2: Considerando uma situação similar abordada no exemplo 3.3.1, mas com um alfabeto com $N = 100$ caracteres. Nesse caso teríamos $\Phi(100) \times 100$ chaves possíveis. Como $\Phi(100) = \Phi(2^2.5^2)$, usando o Teorema 2.1.4.12 do capítulo 2, temos que $\Phi(100) = 2^2.5^2.\left(1-\frac{1}{2}\right).\left(1-\frac{1}{5}\right) = 40$. Portanto, há $40 \times 100 = 4000$ possibilidades de chaves.

Exemplo 3.3.3: Considerando agora um alfabeto com N caracteres, sendo N um número primo. Então, temos $\Phi(N) \times N = (N-1) \times N$ chaves.

No caso geral, em que consideramos o conjunto de todas as funções bijetoras em $\{0, 1, \ldots N-1\}$, a situação fica ainda mais segura, pois temos $N!$ possibilidades (número de permutações em $\{0, 1, 2, 3, \ldots N-1\}$). Note que, quanto maior o valor de N, mais possibilidades teremos. Usando um valor relativamente pequeno para N, por exemplo 26, serão $26! \cong 4\,.\,10^{26}$, o que representa muitas possibilidades, tornando o método de força bruta computacionalmente inviável.

Portanto, concluímos que o método apresentando é considerado relativamente seguro quando pensamos na tentativa de quebra de código por força bruta, caso a quantidade de recursos computacionais seja consideravelmente limitada. Porém, existem um outro ponto bastante fraco neste método se considerarmos uma análise de frequência de letras do alfabeto.

É conhecido que as letras em um determinado idioma possuem frequências distintas num texto. Por exemplo, no Português, para textos longos, a letra A é a mais utilizada, sendo sua frequência de 14.63%, seguidas por E, com 12.57% e O, com 10.73%. A menos frequentes são Y e W, com 0.01% conforme pode ser visto em [1].

Desde que as cifras de substituição apresentadas levam unidades de mensagem originais iguais em unidades de mensagens criptografadas iguais, esta frequência é transferida para a mensagem criptografada. A partir disto, tendo uma quantidade suficientemente grande de textos cifrados, um invasor pode quebrar o código de um sistema criptográfico baseado em substituição.

Exemplo 3.3.4: Suponha que tenhamos um texto grande o suficiente e codificado por uma função do tipo $f(x) = (ax + b) mod\ (26)$, em que a e b são números desconhecidos pelo invasor. Suponha que ele tenha obtido um texto codificado tal que a maior frequência são os números $6(F)$ e $10(J)$ respectivamente. Então, provavelmente $0(A)$ foi codificado em $6(F)$ e $5(E)$ em $10(J)$. Logo, tem-se o sistema

$$\begin{cases} a.0 + b \equiv 6\ mod\ (26) \\ a.5 + b \equiv 10\ mod\ (26) \end{cases}$$

Resolvendo, temos $b = 6$ e $a\ = 6$. Neste caso, o sistema ficou totalmente vulnerável.

3.4 UNIDADES DE MENSAGEM COM PAR DE LETRAS: TRANSFORMAÇÕES DE DÍGRAFOS

Transformações de dígrafos é quando a mensagem original e a cifrada são organizadas em bloco de duas letras. Nesta seção, veremos alguns métodos de substituição em dígrafos. No caso em que a mensagem original tenha um número ímpar de letras, é comum acrescentarmos uma letra no final de modo que não confunda a mensagem original.

Exemplo 3.4.1: Suponha que a palavra FELIZ será cifrada utilizando transformações de dígrafos. Inicialmente, organizamos a palavra em bloco de duas letras, como a palavra possui uma quantidade ímpar de letras, vamos acrescentar a letra X no final, de modo que não atrapalhe a compreensão da mensagem original. Logo temos a seguinte sequência de bloco: FE – LI – ZX.

Para cifrar a mensagem, cada bloco de letras é substituído por um novo bloco de letras, com exatamente a mesma quantidade de letras, nesse caso, duas. Note que, o número de combinações possíveis para uma sequência de duas letras é dado por $26 \times 26 = 676$.

De modo geral, para transformações de dígrafos em um alfabeto de n caracteres, podemos escolher uma função afim codificadora do tipo $C = f(x) = ax + b\ mod(n^2)$, tal que

a, b são inteiros, $a \neq 0$ e $mdc(a, n^2) = 1$. Neste caso, x representa o equivalente numérico do par de letras. Para $n = 26$, tendo o nosso alfabeto usual, temos o equivalente dado no quadro abaixo.

Quadro 4: Dígrafos e seus números equivalentes

AA	AB	AC	AD	...	AZ
0	1	2	3	...	25
BA	BB	BC	BD	...	BZ
26	27	28	28	...	50
...	...	...	...	...	...
ZA	ZB	ZC	ZD	...	ZZ
650	651	653	653		675

Fonte: A autora

Uma maneira prática de determinar o equivalente numérico do par de letras é dado por $pn + q$ onde p e q são as posições da primeira e segunda letra do dígrafo, respectivamente, no alfabeto.

Exemplo 3.4.2: Suponha que a mensagem FELIZ será cifrada utilizando a função $f(x) = 3x + 231\ mod(676)$ utilizando blocos de duas letras, conforme exemplo 3.4.1. Vamos determinar o equivalente numérico de cada dígrafo. Observe:

Dígrafo	Posição da 1ª letra no alfabeto (p)	Posição da 2ª letra no alfabeto (q)	Equivalente numérico
FE	5	4	$5 \times 26 + 4 = 134$
LI	11	8	$11 \times 26 + 8 = 294$
ZX	25	23	$25 \times 26 + 23 = 673$

Desse modo, a mensagem FELIZ é representada pela sequência numérica 134 – 294 – 673. Utilizando a função codificadora temos:

$$f(134) = 3.134 + 231 \equiv 633\ mod\ (676)$$

$$f(294) = 3.294 + 231 = 1113 \equiv 437\ mod\ (676)$$

$$f(673) = 3.673 + 231 = 2250 \equiv 222\ mod\ (676)$$

Logo, a sequência numérica da mensagem cifrada é 633 – 437 – 222.

Agora, é preciso determinar qual par de letras corresponde cada um desses números. Utilizando o algoritmo da divisão de Euclides, $633 = 24 \times 26 + 9$, daí segue que 24 é a posição da primeira letra do dígrafo e 9 é a posição da 2ª letra, portanto, 633 corresponde ao

dígrafo YJ, e $437 = 16 \times 26 + 21$, isto é, 437 representa o dígrafo QV. Por último, $222 = 8 \times 26 + 14$, logo esse representa o dígrafo IO. Portanto, a mensagem FELIZ cifrada é representada por YJQVIO.

Para determinar a função decodificadora, temos o processo semelhante ao caso já visto, ou seja, $f^{-1}(C) = a'C - b' \; mod\,(n^2)$, tal que $a'.a \equiv 1 \, mod(n^2)$ e $b' \equiv a'b \, mod(n^2)$. Importante ressaltar que C é o correspondente numérico do dígrafo, representado por $C = pn + q$, tal que p e q são equivalentes numéricos da 1ª e 2ª letra do dígrafo, respectivamente.

No caso da função codificadora $f(x) = 3x + 231 \; mod\,(676)$ para obter sua inversa devemos determinar a'. Temos que $3 \times 451 = 1353$ e que $676 \times 2 = 1352$, logo $3 \times 451 \equiv 1 \, mod(676)$, portanto, $a' = 451$. Desse modo, podemos obter $b' = a'b = 451 \times 231 = 104181 \equiv 77 \; mod\,(676)$. Daí segue que a função decodificadora é dada por $f^{-1}(C) = 451C - 77 \; mod(676)$.

Podemos generalizar o método acima e organizar a mensagem em blocos de k letras usando um sistema com n letras do alfabeto ou caracteres, nesse caso as funções codificadoras e decodificadoras serão em $mod(n^k)$.

3.5 CRIPTOANÁLISE DAS CIFRAS DE UNIDADES DE MENSAGEM COM PAR DE LETRAS: TRANSFORMAÇÕES DE DÍGRAFOS

Existem várias possibilidades de escolhas para a função codificadora do tipo $f(x) = ax + b \; mod\,(n^2)$. Temos a condição $mdc(a, n^2) = 1$ para que a função seja bijetora (veja Proposição 2.1.5.2). Logo o número de possibilidades para a é dado por $\Phi(n^2)$ (veja seção 2.1.4). Já para o valor de b teremos n^2 possibilidades. Portanto a quantidade de funções codificadoras, mais especificamente, a quantidade de chaves de encriptação, que corresponde ao par (a, b), é dado por $n^2.\Phi(n^2)$. Tal fato contribui para a dificuldade de decifrar uma mensagem utilizando o método da força bruta.

No caso em que se utiliza transformações dígrafas, também há vulnerabilidade baseada na frequência de letras. Note que, se considerado o alfabeto com 26 letras, teremos $26^2 = 676$ algarismos. Sabe-se que, na escrita em português, os dígrafos DE e RA, são os mais frequentes (veja em [1]) e, de modo semelhante na situação apresentada no parágrafo anterior, se num texto cifrado for observado, por exemplo, que o dígrafo TH e KX sejam os mais frequentes, nessa ordem, acredita-se num primeiro momento que TH e KX correspondem a DE e RA

respectivamente. A partir daí, determina-se a provável função codificadora e comprova se a mensagem faz ou não sentido, caso contrário, reinicia-se o processo. Agora, note que, se utilizarmos blocos de k letras, caracterizando uma cifra poligráfica, quanto maior o valor de k, maior a quantidade de polígrafos. Por exemplo, se $k = 10$, temos $26^{10} \cong 1{,}4 \,.\, 10^{14}$ polígrafos, dificultando consideravelmente a análise de frequência.

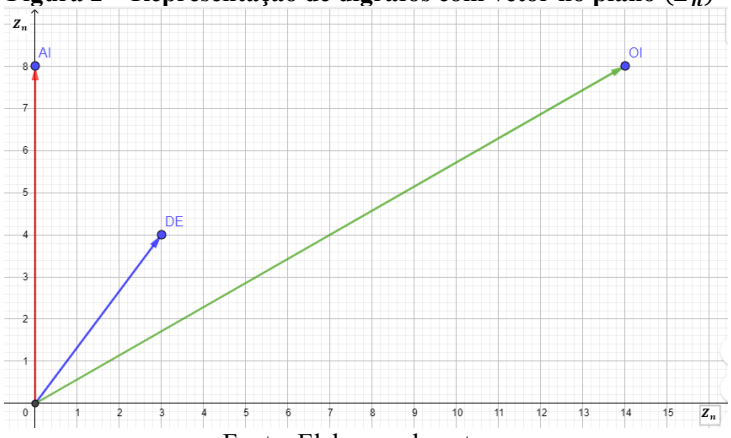
3.6 MATRIZES CODIFICADORAS

Uma outra forma de criptografarmos dígrafos é usando matrizes. Nesse caso, cada dígrafo corresponde a um vetor $\begin{pmatrix} x \\ y \end{pmatrix}$, em que x e y são números inteiros equivalente a posição dos caracteres no alfabeto.

Exemplo 3.6.1: Considere nosso alfabeto com 26 letras, numeradas de 0 a 25. Para cifrar a mensagem OI utilizando matrizes é possível considerar que OI forma um dígrafo. Como a letra O tem o valor 14 como equivalente numérico e I tem o valor 8, temos que a palavra OI corresponde ao vetor $\begin{pmatrix} 14 \\ 8 \end{pmatrix}$.

Considerando o plano cartesiano $\mathbb{Z}_n \times \mathbb{Z}_n$, temos abaixo um desenho com a interpretação dos vetores correspondentes a AI, DE, OL.

Figura 2 – Representação de dígrafos com vetor no plano $(Z_n)^2$



Fonte: Elabora pela autora.

Neste caso, uma função codificadora é uma função bijetora $f: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$, isto é, uma função rearranjo dos vetores que representam os dígrafos.

Vamos considerar funções do tipo $f(X) = AX + B\ mod(n),$ em que A é uma matriz $2x2$ com entradas inteiras e B, é um vetor $2x1$ com também entradas inteiras. Aqui mod é aplicado em cada linha. De forma mais precisa, se $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ e $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, então

$$f(X) = AX + B\ mod(n) = \begin{matrix} (a_{11}.x_1 + a_{12}.x_2 + b_1)\ mod\ (n) \\ (a_{21}.x_1 + a_{22}.x_2 + b_2) mod\ (n) \end{matrix}$$

Neste caso, para a função ser invertível em $\mathbb{Z}_n \times \mathbb{Z}_n$, devemos ter que $mdc\ (n, Det\ A) = 1$, em que Det é o determinante de A, isto, é $Det\ A = (a_{11}.a_{22} - a_{21}.a_{12})$, (veja Proposição 2.1.6.6). Neste método, o par (A, B) é a chave do processo de criptografia e é denotado por k.

Exemplo 3.6.2: Considere a mensagem ISOLAR. Para cifrar a mensagem com matrizes codificadoras vamos inicialmente organizar a mensagem em blocos com duas letras e obter seus equivalentes numéricos no alfabeto de A-Z. Desse modo teremos:

$$\begin{pmatrix} I \\ S \end{pmatrix}\begin{pmatrix} O \\ L \end{pmatrix}\begin{pmatrix} A \\ R \end{pmatrix} = \begin{pmatrix} 8 \\ 18 \end{pmatrix}\begin{pmatrix} 14 \\ 11 \end{pmatrix}\begin{pmatrix} 0 \\ 17 \end{pmatrix}$$

Agora, vamos escolher uma matriz-chave A tal que $mdc\ (det\ A, 26) = 1$. Uma possibilidade é:

$$A = \begin{pmatrix} 2 & 5 \\ 7 & 9 \end{pmatrix}$$

Em seguida, deve-se fazer $AX\ mod\ (26)$, isto é,

$$\begin{pmatrix} 2 & 5 \\ 7 & 9 \end{pmatrix}.\begin{pmatrix} 8 \\ 18 \end{pmatrix} = \begin{pmatrix} 106 \\ 218 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 10 \end{pmatrix}\ mod(26)$$

$$\begin{pmatrix} 2 & 5 \\ 7 & 9 \end{pmatrix}.\begin{pmatrix} 14 \\ 11 \end{pmatrix} = \begin{pmatrix} 83 \\ 197 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 15 \end{pmatrix}\ mod(26)$$

$$\begin{pmatrix} 2 & 5 \\ 7 & 9 \end{pmatrix}.\begin{pmatrix} 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 85 \\ 153 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 23 \end{pmatrix}\ mod(26)$$

Agora, podemos escolher uma matriz constante B para somar com cada matriz obtida. Considere que $B = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$. Com isso, teremos:

$$\begin{pmatrix} 2 \\ 10 \end{pmatrix} + \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 4 \\ 15 \end{pmatrix}\ mod(26)$$

$$\begin{pmatrix} 5 \\ 15 \end{pmatrix} + \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 7 \\ 20 \end{pmatrix}\ mod(26)$$

$$\begin{pmatrix} 7 \\ 23 \end{pmatrix} + \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 9 \\ 28 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 2 \end{pmatrix}\ mod(26)$$

Verificando as letras correspondentes a cada valor identificado na matriz, obtemos os dígrafos:

$$\binom{E}{P}; \binom{H}{U}; \binom{J}{C}$$

Com isso, a mensagem ISOLAR cifrada será EPHUJC.

Para voltar a mensagem original se faz necessário a função inversa. A função decodificadora obedece aos mesmos parâmetros que as transformações lineares e afins já vistos, isto é, a função inversa é dada por:

$$f(C) = A'C - B' \, mod(26),$$

dado que A' é a matriz tal que $A'.A \equiv I \, mod\,(26)$, sendo I a matriz identidade, isto é, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e $B' = A'B \, mod(26)$. Neste caso temos que $A' = \begin{pmatrix} D'a_{22} & -D'a_{12} \\ -D'a_{21} & D'a_{11} \end{pmatrix}$ e D' é tal que $D'.Det\ A \equiv 1\, mod(26)$.

Exemplo 3.6.3: Suponha que a mensagem EPHUJC tenha sido obtida através da cifragem com a função $C = f(X) \equiv \begin{pmatrix} 2 & 5 \\ 7 & 9 \end{pmatrix} X + \begin{pmatrix} 2 \\ 5 \end{pmatrix} \, mod(26)$.

Temos que $A = \begin{pmatrix} 2 & 5 \\ 7 & 9 \end{pmatrix}$. Com isso, devemos obter sua inversa A'. Temos:

$$\det A = 18 - 35 = -17 \equiv 9 \ \ mod(26)$$

$$\mathrm{D}' = 3, \text{ pois } 3.9 = 27 \equiv 1 \ mod(26)$$

$$A' = 3.\begin{pmatrix} 9 & -5 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 27 & -15 \\ -21 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 11 \\ 5 & 6 \end{pmatrix} \, mod(26)$$

$$B' = \begin{pmatrix} 1 & 11 \\ 5 & 6 \end{pmatrix}.\begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 57 \\ 40 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 14 \end{pmatrix} \, mod\ 26$$

Portanto, a função decodificadora é dada por:

$$f^{-1}(C) = \begin{pmatrix} 1 & 11 \\ 5 & 6 \end{pmatrix} C - \begin{pmatrix} 5 \\ 14 \end{pmatrix} \, mod\ 26.$$

3.7 CRIPTOANÁLISE DAS CIFRAS ENVOLVENDO MATRIZES

Assim como nos casos em que são utilizadas cifras de substituição de unidades de mensagens de uma letra ou de pares de letras, cifras utilizando matrizes como codificação também podem ser suscetíveis a ataques.

Considere o caso que na troca de mensagens criptografadas entre duas pessoas, por um canal não seguro, terceiros interceptam tal mensagem e tentam decifrá-la. Suponha que esse

saiba que a mensagem foi cifrada utilizando um alfabeto com n caracteres e uma função linear do tipo $C = f(X) = AX\ mod\ (n)$. No entanto, o intruso desconhece a matriz-chave A e a matriz A' que seria a chave decodificadora. Mas, considere o fato de que o inimigo seja capaz de associar dois pares de dígrafos da mensagem original com a mensagem cifrada. Assim, é possível organizar os dígrafos em duas colunas em uma matriz de ordem 2, de modo que se obtém a equação matricial $C = A.X\ mod\ (n)$, sendo C a matriz com os dígrafos cifrados, X a matriz com os dígrafos da mensagem original e A é a matriz chave desconhecida. Suponha que C seja uma matriz invertível na álgebra $mod(n)$, com inversa C'. Neste caso, para determinar A', basta calcular $A' = X.C'\ mod\ (n)$.

Exemplo 3.7.1: Suponha que um intruso saiba que duas pessoas, ao trocar mensagens cifradas, estejam utilizando uma matriz de ordem 2 e uma função codificadora linear do tipo $C = f(X) = AX\ mod\ (n)$ e um alfabeto com 29 caracteres, dos quais do $0\ a\ 25$ são os correspondentes numéricos das letras de $A - Z$, espaço, hífen e ponto de exclamação têm, respectivamente, como correspondente numérico, $26, 27$ e 28. Ao interceptar a conversa, vê a seguinte mensagem:

SEMWWX! DFPCHBI!.XOJFPTE

Suponha ainda que o intruso saiba que as últimas cinco letras da mensagem correspondem a assinatura da remetente Carla. Com isso, os dígrafos FP e TE correspondem aos dígrafos AR e LA da mensagem original, isto é, $X = \begin{pmatrix} A & L \\ R & A \end{pmatrix}$, que é mensagem original, foi cifrada em $C = \begin{pmatrix} F & T \\ P & E \end{pmatrix}$. Como a função codificadora é do tipo $C = f(X) = A.X\ mod\ (n)$, temos:

$$\begin{pmatrix} 5 & 19 \\ 15 & 4 \end{pmatrix} = A.\begin{pmatrix} 0 & 12 \\ 17 & 0 \end{pmatrix} mod\ (n)$$

Nesse momento, o intruso tenta determinar a matriz decodificadora A' fazendo $X.C' mod\ (n)$, sendo C' a matriz inversa de C. Aplicando os passos demonstrados no Exemplo 3.6.3 para obter a inversa de uma matriz $mod\ (n)$, teremos que $C' = \begin{pmatrix} 28 & 12 \\ 11 & 6 \end{pmatrix}$. Assim,

$$A' = \begin{pmatrix} 0 & 12 \\ 17 & 0 \end{pmatrix}.\begin{pmatrix} 28 & 12 \\ 11 & 6 \end{pmatrix} mod\ (29) = \begin{pmatrix} 5 & 8 \\ 12 & 1 \end{pmatrix}.$$

Agora, é possível que o intruso descubra a mensagem fazendo

$$A'.(\text{matriz com os dígrafos cifrados}) =$$

$$\begin{pmatrix} 5 & 8 \\ 12 & 1 \end{pmatrix}.\begin{pmatrix} 18 & 12 & 22 & 28 & 3 & 15 & 7 & 8 & 27 & 14 & 5 & 19 \\ 4 & 22 & 23 & 26 & 5 & 2 & 1 & 28 & 23 & 9 & 15 & 4 \end{pmatrix},$$

Obtendo a mensagem: GREVE AO MEIO-DIA! CARLA.

Observe que acima a matriz C é invertível em $mod\ (n)$, caso contrário, o intruso deveria tentar associar outros dois pares de dígrafos da mensagem cifrada com a possível mensagem original, de modo que a nova matriz seja inversível e, seguir todos os passos descritos no exemplo acima.

Outra possibilidade de função codificadora usando matrizes é do tipo $f(X) = AX + B\ mod\ (n)$. Conforme visto no capítulo 2, seção 2.1.6, A deve ser invertível e, para que isso ocorra, é necessário que $mdc\ (n, Det\ A) = 1$, em que $Det\ A$ é o determinante de A. Para decifrar a mensagem cifrada com tal função é necessário possuir a função inversa dada por $f^{-1}(X) = A'X - B'\ mod(n)$, sendo A' a matriz tal que $A'.A \equiv I\ mod\ (n)$, sendo I a matriz identidade, e $B' = A'B\ mod(n)$.

Suponha que um intruso saiba que, na troca de mensagens entre duas pessoas e num canal não seguro, estejam usando matrizes codificadoras com um alfabeto com N caracteres. Para determinar A e B ou A' e B', será necessário associar pelo menos três pares de dígrafos. Suponha que saibamos que os dígrafos cifrados C_1, C_2, C_3 corresponde aos dígrafos da mensagem original X_1, X_2, X_3. Então temos o seguinte sistema de equações:

$$\begin{cases} X_1 = A'.C_1 + B'\ mod(n) \\ X_2 = A'.C_2 + B'\ mod(n) \\ X_3 = A'.C_3 + B'\ mod(n) \end{cases}$$

Resolvendo o sistema de equações é possível determinar A' e B'. Uma forma de resolver tal sistema seria subtrair a última equação das duas primeiras, com isso teríamos:

$$\begin{cases} X_1 - X_3 = A'.(C_1 - C_3) mod(n) \\ X_2 - X_3 = A'.(C_2 - C_3)\ mod(n) \end{cases}$$

Organizamos as duas equações em uma equação matriz da forma $(X_1 - X_3 \quad X_2 - X_3) = A'.(C_1 - C_3 \quad C_2 - C_3)\ mod\ (n)$. Supondo $(C_1 - C_3 \quad C_2 - C_3)$ inversível, é possível determinar A' fazendo o mesmo procedimento descrito no caso em que a função codificadora é linear. Por último, resta determinar B'. Para isso, basta substituir A' em qualquer uma das três equações do sistema e resolvê-la.

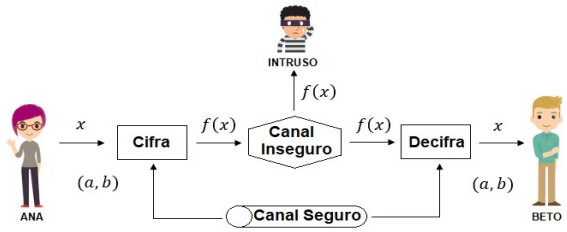
3.8 SISTEMAS CRIPTOGRÁFICOS SIMÉTRICOS

Nas seções 3.2, 3.4 e 3.6 foram apresentados alguns sistemas criptográficos, cada qual um modo particular de organizar a mensagem original, mas todos utilizam uma função codificadora $f(x)$ obtida a partir de uma chave. Esta chave é mantida em segredo, sendo conhecida apenas pelo emissor e pelo destinatário. Ela é utilizada pelo emissor para codificar a mensagem, isto é, para calcular $f(x)$, sendo x a mensagem original e $f(x)$ a mensagem criptografada. Já para o receptor, esta mesma chave é utilizada para descriptografar a mensagem, isto é, para calcular $f^{-1}(f(x)) = x$. Por exemplo, na transformação afim $f(x) = ax + b \ mod\ (26)$ utilizada na seção 3.1.1, a chave é o par (a, b).

Um sistema criptográfico em que o remetente e o destinatário utilizam a mesma chave (secreta) é chamado simétrico. As formas de criptografias visto até o momento são simétricas.

Um problema na implementação de um sistema simétrico é justamente no compartilhamento da chave secreta. Para iniciar uma troca de informação via o sistema criptográfico, é necessário que tanto o remetente quanto o destinatário já tenham previamente o conhecimento da chave a ser utilizada. Para fazer isto, eles precisam de um canal seguro (em que invasores não tenham acesso) para a determinação desta chave secreta. O mecanismo de troca de mensagens por ambos pode ser representado pelo esquema conforme figura 3:

Figura 3 – Representação de um sistema criptográfico simétrico



Fonte: Elaborada pela autora

Um outro problema associado ao sistema simétrico é o número elevado de chaves necessárias para um grupo de pessoas trocarem informações de forma protegida. Por exemplo, imagine que n pessoas queiram se comunicar entre si de maneira secreta e de forma que, quando duas se comuniquem entre si, as outras pessoas não consigam decifrar a conversa. Neste caso, cada par de pessoas deve ter uma chave secreta própria para se comunicarem. No total, teremos $C_{\mathrm{n}}^{2} = \frac{n.(n-1)}{2}$ chaves, e cada usuário deve ter $n - 1$ chaves armazenadas secretamente. Isto torna trabalhosa a administração destas chaves para n grande.

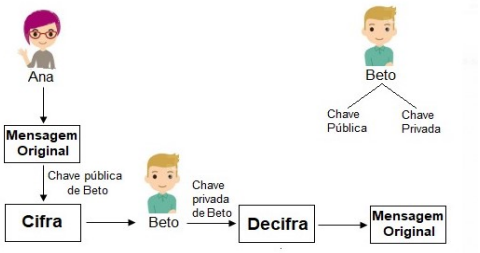
Uma terceira dificuldade dos sistemas simétricos é a impossibilidade de obter assinatura digital (veja seção 3.13), isto é, na troca de mensagens o destinatário ter a garantia de que a mensagem foi realmente escrita por certo emissor.

A seguir, será descrito o método conhecido como cifra assimétrica, nesse caso, a chave para cifrar é diferente da utilizada para decifrar e não se faz necessária a existência de um canal seguro (em que invasores não tenham acesso) para a troca de chaves.

3.9 CRIPTOGRAFIA ASSIMÉTRICA

Com a fragilidade no sistema simétrico, conforme mencionados anteriormente, criptográficos buscavam meios de corrigir essa falha. No final de 1976, os matemáticos Whitfield Diffie, Martin Hellman e Ralph Merkle revolucionaram a criptografia ao propor o conceito de cifra assimétrica. Neste método, temos duas chaves, uma pública e outra privada. A chave pública é disponibilizada publicamente pelo destinatário e deve ser utilizada por todos que queiram enviar uma mensagem criptografada para ele. Esta chave é utilizada para criptografar a mensagem. Uma vez criptografada a mensagem pelo emissor e enviada ao destinatário, ele utiliza a chave privada (diferente da pública e que apenas ele conhece) para descriptografar a mensagem, conforme mostra a figura 4:

Figura 4 – Representação de um sistema criptográfico assimétrico



Fonte: Elaborada pela autora

A figura mostra os personagens fictícios Ana e Beto. Ana deseja enviar uma mensagem a Beto de modo que somente ambos saibam o teor dela. Para isso, ela decide cifrar a mensagem utilizando o sistema assimétrico. Aqui ela, como qualquer outra pessoa, tem acesso a uma chave pública de Beto. De posse dessa chave, ela cifra a mensagem e então, envia a Beto. Ao recebê-la, ele utiliza sua chave privada, a qual seu próprio nome sugere, apenas ele a conhece, e decifra a mensagem. Se um terceiro receptar a mensagem, embora ele também tenha acesso a chave

pública de Beto usada para cifragem, ele não consegue decifrar, pois isto é possível somente com o uso da chave privada de Beto.

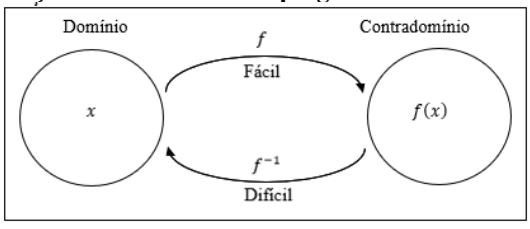
A situação representada pelos personagens Ana e Beto, descreve o método criado pelos matemáticos Diffie-Hellman-Merkle: o sistema assimétrico, que consiste em um par de chaves, uma pública e outra privada, no qual ambas são diferentes e a chave pública é usada para cifrar enquanto que a chave privada para decifrar.

O sistema assimétrico contribuiu para o aumento na transmissão de mensagens, desde que não há a necessidade da existência de um outro canal seguro para a transmissão das chaves, como no caso simétrico. Note também que o número de chaves necessárias para a transmissão de informações de um grupo de n pessoas reduz significativamente se comparado ao sistema simétrico. São necessárias duas chaves para cada pessoa (uma pública e uma privada), havendo, portanto, $2.n$ chaves. Além disto, cada pessoa deve armazenar secretamente apenas a sua própria chave privada. Todas as outras chaves que ele necessita são públicas.

3.10 FUNÇÕES UNIDIMENSIONAIS E FUNÇÕES ARAPUCAS

Para garantir a viabilidade e segurança do sistema assimétrico, a função codificadora f, obtida a partir de uma chave pública, deve satisfazer algumas propriedades. A primeira é que $f(x)$ deve ser fácil de calcular para todo x. Isto garante que o emissor não tenha dificuldade em criptografar a mensagem. A segunda é que, mesmo conhecendo f, a sua inversa f^{-1} seja computacionalmente inviável de ser calculada. Isto garante que o sistema seja seguro. Funções que satisfazem estas duas propriedades são chamadas funções unidimensionais.

Figura 5 – Representação de um sistema criptográfico usando função unidimensional

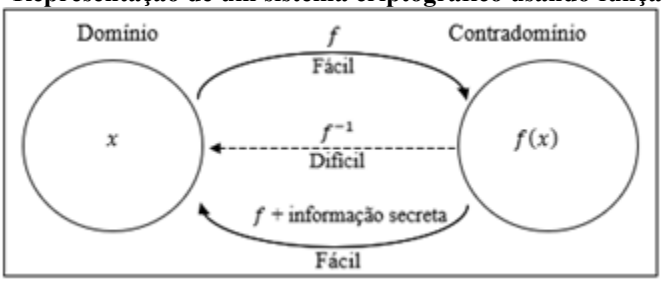


Fonte: Elaborada pela autora

Além disto, esta função unidimensional deve ser tal que, dado uma certa informação adicional (chave privada), $f^{-1}(f(x))$ seja fácil de ser calculada. Isto garante que, de fato, a

mensagem possa ser descriptografada pelo destinatário. Uma função que satisfaz estas propriedades é chamada função arapuca.

Figura 6 – Representação de um sistema criptográfico usando função arapuca



Fonte: Elaborada pela autora

Embora, Diffie-Hellman-Merkle tenham conseguido mostrar ao mundo uma solução para a distribuição de chaves, não conseguiram descobrir uma função arapuca que tornasse realidade o método apresentado. Um pouco mais tarde, por volta de 1977, o trio de matemáticos Ron Rivest, Adi Shamir e Leonard Adleman deram vida a criptografia RSA que utiliza funções cuja segurança está baseada na dificuldade computacional do cálculo da fatoração em primos de números naturais grandes. De fato, conjectura-se que $f(p,q) = p.q$, em que p e q são primos grandes, seja um exemplo de função unidimensional. Usando aritmética modular, e o fato acima, é possível criar funções arapucas.

Exemplo 3.10.1: Sejam p e q dois primos distintos grandes e $N = p.q$. Conforme Exemplo 2.1.4.12 do capítulo 2, temos que $\Phi(N) = (p-1).(q-1)$. Seja e um número natural tal que $1 < e < \Phi(N)$ e $mdc(e, \Phi(N)) = 1$. Considere a função dada por $f(x) = x^e \ mod\ (N)$. Temos que esta função é simples de ser calculada, bastando fazer a divisão Euclidiana de x^e por N e escolhendo $f(x)$ como o resto. Vimos na Proposição 2.1.5.3, que essa função é bijetora em $\mathbb{Z}_N$ e que sua inversa pode ser calculada da seguinte forma:
(1)Ache a inversa de e em $\mathbb{Z}_{\Phi(N)}$, isto é, calcule e' em $\mathbb{Z}_{\Phi(N)}$ tal que $e'.e \equiv 1\ mod\ (\Phi(N))$.
(2) A função inversa de f é dada por $f^{-1}(y) = y^{e'} mod\ (N)$.

Suponha conhecido apenas $f(x)$, então, para realizar o item (1) acima, precisamos calcular primeiramente $\Phi(N)$ a partir de N. Como, neste caso, temos as fórmulas

$$\begin{cases} p + q = N + 1 - (p-1)(q-1) \\ (p-q)^2 = (p+q)^2 - 4N \end{cases},$$

conhecer $\Phi(N) = (p-1).(q-1)$ a partir de N equivale a conhecer p e q a partir de N. Como o problema de fatoração é unidimensional, temos que a função $f(x)$ é também unidimensional.

No entanto, conhecendo adicionalmente a fatoração de N (aqui p e q serão as chaves secretas), calcula-se facilmente $\Phi(N)$ e, portanto, os passos (1) e (2) $p$odem ser calculados via algoritmo da divisão de Euclides. Logo, com as informações adicionais sobre a fatoração $N = p.q$, calcula-se a inversa de $f(x)$ sem dificuldades. Portanto, f é de fato uma função arapuca.

3.11 RSA

O sistema, o RSA, faz uso do exemplo 3.10.1 acima. Desse modo, a segurança desse sistema reside na dificuldade de fatoração de números grandes. Este é um dos sistemas criptográficos assimétricos mais influente da criptografia moderna. O nome é atribuído pela letra inicial do sobrenome de cada um dos criadores.

Vamos novamente usar os personagens fictícios Alice e Bob para descrever como seria trocar mensagens usando o sistema RSA. Considere que Alice deseja enviar uma mensagem a Bob usando o RSA, para isso Bob precisa de uma chave pública k_C e uma chave privada k_D. Para criar tais chaves, Bob segue os seguintes passos:

1. Escolhe dois números primos p e q;
2. Calcula $n = pq$;
3. Calcula $\Phi(n) = (p-1).(q-1)$;
4. Escolhe um inteiro e, tal que $1 < e < \Phi(n)$ de modo que $mdc\big(e, \Phi(n)\big) = 1$;
5. Determinar um número inteiro e', tal que $1 < e' < \Phi(n)$ e $ee' \equiv 1\ mod\ (\Phi(n))$.

Assim, a chave pública e privada de Bob é dado por $k_C = (n, e)$ e $k_D = (n, e')$ respectivamente.

Agora, para Alice cifrar uma mensagem que deseja enviar a Bob ela utiliza a chave pública dele (qualquer pessoa tem acesso) e calcula $c \equiv m^e\ mod\ (n)$, onde c é a cifra e m é a mensagem original, que está em $\mathbb{Z}_n$.

Bob ao receber a mensagem cifrada calcula $m \equiv c^{e'}\ mod\ (n)$ para decifrar a mensagem e assim chegar a original.

Exemplo 3.11.1: Vamos mostrar como construir a chave pública e privada de Bob. Suponha que Bob escolha os primos 7 e 11, logo $n = 7.11 = 77$. Em seguida calcula $\Phi(77) =$

$(7-1).(11-1) = 6.10 = 60$, que significa que há 60 números inteiros coprimo com 77. Agora, para compor a chave pública, Bob deve escolher um inteiro e , tal que $1 < e < \Phi(77)$ de modo que $mdc(e, 60) = 1$. Considere que ele escolha $e = 13$, portanto, a chave pública é o par $k_C = (77,13)$. Já para determinar sua chave privada k_D, Bob precisa determinar um número inteiro e', tal que $1 < e' < 60$ e $13.e' \equiv 1\ mod\ (60)$, ou seja, $60m = 13e' - 1$ com $m \in \mathbb{Z}$. Resolvendo pelo algoritmo de Euclides temos que $60 = 13.37 - 1$, teremos $e' = 37$. Portanto, a chave privada k_D é o par $(77,37)$.

Exemplo 3.11.2: Considere que Alice deseja enviar a mensagem FIQUE EM CASA para Bob utilizando o sistema RSA e sabendo que a chave pública dele é $k_C = (77,13)$. Primeiro Alice deve verificar o correspondente numérico de cada letra da mensagem conforme quadro 3 (veja seção 3.2, obtendo assim a sequência: $5 - 8 - 16 - 20 - 4 - 4 - 12 - 2 - 0 - 18 - 0$. Para cada um desses valores ela deve calcular $c \equiv m^{13}\ mod\ (77)$, onde c é o valor da cifra e m é o valor numérico da mensagem. Então, utilizando as propriedades de congruência citadas na seção 2.1.2.4 temos:

$$c \equiv 5^{13} \equiv 26\ mod\ (77)$$

$$c \equiv 8^{13} \equiv 8^{11}.8^2 \equiv 8.64 \equiv 50\ mod\ (77)$$

$$c \equiv 16^{13} \equiv 16^8.16^5 \equiv 4.67 \equiv 37\ mod\ (77)$$

$$c \equiv 20^{13} \equiv 20^7.20^6 \equiv 48.64 \equiv 69\ mod\ (77)$$

$$c \equiv 4^{13} \equiv 53\ mod\ (77)$$

$$c \equiv 12^{13} \equiv 12^9.12^3.12 \equiv 34.34.12 \equiv 12\ mod\ (77)$$

$$c \equiv 2^{13} \equiv 30\ mod\ (77)$$

$$c \equiv 0^{13} \equiv 0\ mod\ (77)$$

$$c \equiv 18^{13} \equiv 18^7.18^6 \equiv 39.15 \equiv 46\ mod\ (77)$$

Assim, a sequência da mensagem cifrada é $26 - 50 - 37 - 69 - 53 - 53 - 12 - 30 - 0 - 46 - 0$.

Exemplo 3.11.3: Suponha que Bob receba a mensagem cifrada de sequência $26 - 50 - 37 - 69 - 53 - 53 - 12 - 30 - 0 - 46 - 0$, calculada no exemplo anterior. De posse de sua chave privada $k_D = (77,37)$ ele deverá calcular $m \equiv c^{37}\ mod\ (77)$ e, aplicando as propriedades de congruência citadas na seção 2.1.2.4, temos que:

$$m \equiv 26^{37} \equiv (26^6)^6.26 \equiv 15^6.26 \equiv 15.26 \equiv 5\ mod\ (77)$$

$$m \equiv 50^{37} \equiv (50^5)^7 . 50^2 \equiv 43^7 . 36 \equiv 43.36 \equiv 8\, mod\ (77)$$
$$m \equiv 37^{37} \equiv (37^6)^6 . 37 \equiv 15^6 . 37 \equiv 15.37 \equiv 16\, mod\ (77)$$
$$m \equiv 69^{37} \equiv (69^5)^7 . 69^2 \equiv 34^7 . 64 \equiv 20\, mod\ (77)$$
$$m \equiv 53^{37} \equiv (53^5)^7 . 53^2 \equiv 23^7 . 37 \equiv 4 mod\ (77)$$
$$m \equiv 12^{37} \equiv (12^9)^4 . 12 \equiv 12\, mod\ (77)$$
$$m \equiv 30^{37} \equiv (30^6)^6 . 30 \equiv 36^6 . 30 \equiv 2\, mod\ (77)$$
$$m \equiv 0^{37} \equiv 0\, mod\ (77)$$
$$m \equiv 46^{37} \equiv (46^6)^6 . 46 \equiv 64^6 . 46 \equiv 18\, mod\ (77)$$

Obtendo assim a mensagem original.

Note que nos exemplos utilizados os números primos p e q são pequenos, se uma pessoa realmente tem uma chave pública onde $n = 77$ é muito rápido determinar os fatores utilizados, tornando o sistema muito vulnerável.

Note também que o protocolo acima nunca criptografa 0 nem 1, desde que $f(0) = 0$ e $f(1) = 1$, para $f(x) = x^e\ mod\ (N)$. Neste caso, para deixar o sistema mais seguro, é possível inutilizar o zero e o um fazendo uma associação do alfabeto com os números entre 2 e 27.

O sistema de chave pública RSA acabou com os problemas das cifras simétricas e com a troca de chaves. A sua existência foi anunciada pela primeira vez em 1977 por Martin Gardner no artigo “Um novo tipo de cifra que levará milhões de anos para ser decifrado”. Nele, Gardner explicou o sistema, apresentou um texto cifrado junto a chave pública utilizada com um valor n na ordem de 10^{129} e propôs o desafio aos seus leitores de decifrarem seu texto. Após 17 anos uma equipe de seiscentos voluntários com computadores de médio porte e supercomputadores trabalhando simultaneamente, conseguiram fatorar n e, assim, decifrar o texto. Atualmente, usuários do sistema RSA utilizam primos com mais de 100 casas decimais para que a fatoração de n seja praticamente impossível até mesmo com supercomputadores, e, segundo Singh, (2001, p.301) “talvez este seja o aspecto mais belo e elegante da cifra assimétrica RSA”.

3.12 LOGARITMO DISCRETO

A necessidade de buscar funções unidimensionais para viabilizar o método criptográfico de chave pública proporcionou um olhar especial por parte de Diffie-Hellman-Merkle em relação ao logaritmo discreto, pois eles tinham a percepção de que era computacionalmente difícil calcular o logaritmo em certos grupos finitos contendo grande quantidade de elementos. Tal suposição, após avanços na criptografia, verificou-se verdadeira.

Ao falar do logaritmo, nos remete como sendo a operação inversa da exponenciação. Por exemplo, dado um $x \in \mathbb{R}$, determinar x de modo que $3^x = 81$, é equivalente a calcular $\log_3 81 = x$, que nos diz $x = 4$. No conjunto dos números reais, o custo computacional do cálculo de exponenciais e logaritmos não são muito diferentes. Já em certos grupos finitos, tais como os grupos multiplicativos obtidos a partir de corpos finitos, existem algoritmos que tornam o cálculo da exponencial mais simples que o cálculo do logaritmo. Não iremos abordar esses algoritmos aqui, mais detalhes podem ser vistos em [19]. Portanto, exponenciais em corpos finitos grandes são consideradas funções unidimensionais.

Definição 3.12.1: Seja x um gerador de um grupo finito cíclico G, de ordem q. Dado $b \in G$, dizemos que o número natural n, com $1 \leq n \leq q$, é o logaritmo discreto de b na base x, e escrevemos $n = \log_x b$, se $b = x^n$.

Exemplo 3.12.2: Considere o grupo $\mathbb{Z}_{11}^*$ e o gerador 2 (conforme visto no Exemplo 2.2.2.10 do capítulo 2). Determine o logaritmo discreto de 10 na base 2.

Queremos determinar $n = \log_2 10$, isto é, determinar o número n tal que $2^n = 10$ no grupo $\mathbb{Z}_{11}^*$. Isso é equivalente achar n tal que $2^n \equiv 10\ mod\ 11$.

Podemos determinar n fazendo a sequência de potências de 2 até encontrar a potenciação que gera resto 10 ao dividir o resultado por 11. O que ocorre nos casos: $2^5, 2^{15}, 2^{25}, \ldots..$ Porém, por definição, $1 \leq n \leq 10$, logo, concluímos que $n = 5$, ou seja, o logaritmo discreto de 10 na base 2 é 5.

Podemos perceber que, quanto maior o valor de q, possivelmente mais difícil se torna o cálculo do logaritmo discreto.

Veremos que a segurança dos métodos apresentados abaixo está no seguinte princípio:

Suposição de Diffie-Hellman: Seja G um grupo finito cíclico de ordem q, com q grande. Dado x um gerador de G, m e n número naturais. Conhecendo-se apenas $x, x^n \, e \, x^m$, é computacionalmente inviável obter $x^{m.n}$ (desde que m, n sejam grandes também).

Note que este problema está relacionado com a dificuldade do cálculo do logaritmo discreto. De fato, seja G um grupo finito cíclico de ordem q, x um gerador em G e $1 \leq n, m < q$. Se conseguirmos calcular facilmente o logaritmo discreto, então facilmente obtemos m e n a partir de $x, x^n \, e \, x^m$, desde que $n = \log_x(x^n) \; e \; m = \log_x(x^m)$. Então $x^{n.m} = (x^n)^m$ pode ser facilmente calculado, desde que exponenciais são simples de serem calculadas.

3.12.1 Método de troca de chaves Diffie-Hellman

Conforme visto na seção 3.1, quando duas pessoas desejam ter uma comunicação em segredo utilizando a criptografia simétrica, é preciso que ambas definam uma chave. Sendo assim, antes de compartilhar uma conversa em segredo, é preciso compartilhar uma chave também em segredo. Porém, nem sempre é possível que os dois encontrem uma forma de trocar a chave de modo seguro, como por exemplo um encontro presencial. Tal situação ilustra uma fragilidade do sistema de chave simétrica, e é considerado um grande problema no pós-guerra, tanto para governos quanto para empresas.

Foi então que os matemáticos Diffie-Hellman-Merkle em 1976, propuseram um protocolo de troca de chaves, que permite determinar uma chave secreta mesmo utilizando canais de comunicação não seguros.

A lógica do pensamento que os fez chegar na proposta de tal sistema pode ser explicada usando uma analogia com cadeados envolvendo personagens clássicos da literatura sobre criptografia como Alice e Bob. Suponha que Alice deseja mandar uma mensagem secreta a Bob sem depender de uma terceira pessoa. Então, decide enviar uma carta pelo Correio a Bob, mas para garantir que ninguém a leia, coloca dentro de uma caixa fechada com um cadeado. A caixa chega até Bob e, como ele não tem a chave do cadeado, pois esta somente Alice possui, decide então colocar um cadeado seu na caixa e mandá-la de volta à Alice, que recebe a caixa com dois cadeados. Esperta, Alice retira o seu cadeado e envia novamente a caixa para Bob, que finalmente consegue abrir a caixa, pois restava apenas o seu cadeado.

Para descrever o protocolo, considere novamente os personagens Alice e Bob. Suponha que eles desejam definir uma chave secreta para posteriormente criptografar suas

mensagens via algum sistema simétrico. Para isso, suponha um grupo finito cíclico G de ordem q, g um gerador de G e que tais itens sejam de conhecimento público. Então, para definir uma chave secreta k, que será um elemento de G, Alice e Bob seguem os passos descritos abaixo:

Passo	Alice	Bob
1	Escolhe G e g e envia para Bob	Recebe G e g de Alice
2	Escolhe a, um número natural tal que a esteja entre 1 e $q-1$. Mantem a em segredo.	Escolhe b, um número natural tal que b esteja entre 1 e $q-1$. Mantem b em segredo.
3	Calcula $A = g^a$	Calcula $B = g^b$
4	Envia A para Bob	Recebe A de Alice
5	Recebe B de Bob	Envia B para Alice
6	Calcula $k = B^a$	Calcula $k = A^b$

Note que, $B^a = A^b$ pois, $B = g^b$ e $A = g^a$. Desse modo, k é uma chave secreta que Alice e Bob possuem em comum.

A troca de mensagens entre eles pode ser por meio de um canal não seguro, desse modo, qualquer outra pessoa pode ter acesso a algumas informações, como no caso aos valores transmitidos de $G, g, A = g^a e\ B = g^b$. Porém, uma terceira pessoa, apenas com essas informações, não consegue determinar a chave secreta em comum k. Isso se deve ao fato de que ela deverá calcular g^{ab} , tendo apenas g, g^a e g^b, que é inviável justamente pela suposição de Diffie-Hellman.

Exemplo 3.12.1.1: Considere que Alice e Bob decidam combinar uma chave em segredo, Alice escolhe o grupo $\mathbb{Z}_{13}^*$ e o gerador $g = 2$. Bob, assim como qualquer outra pessoa, tem acesso a esses valores. Alice então escolhe um valor $a = 4$. Calcula $A = 2^4$ em $\mathbb{Z}_{13}^*$ que é o mesmo que $A = 3$. Alice envia a Bob esse valor 3. Bob, por sua vez, escolhe um número natural $b = 7$, calcula $B = 2^7\ mod\ 13 \rightarrow B = 11$ e, envia esse valor a Alice. Então, Alice calcula $11^4\ mod\ 13$ e Bob, $3^7\ mod\ 13$. Ambos chegam no resultado igual a 3, isto é, a chave secreta é $k = 3$. Um invasor terá acesso aos valores $\mathbb{Z}_{13}^*$, $g = 2, g^a = 3\ e\ g^b = 11$ mas, terá dificuldade em determinar, por exemplo, o valor de a tal que $2^a = 3\ mod\ 11$. Claro que, nesse exemplo utilizando do método de força bruta seria possível desvendar a chave. Mas na medida

que se escolhe um grupo suficientemente grande, o cálculo se torna inviável computacionalmente.

3.12.2 Protocolo de Massey-Omura para transmissão de mensagens

Na década de 1980, James L. Massey e Jimmy K. Omura patentearam um protocolo de troca de mensagens sigilosas sobre um canal de comunicação de domínio público. Tal método é conhecido como "protocolo de três passos", que consiste em uma sequência de troca de três mensagens criptografadas, sem o compartilhamento de chaves privadas. Para que protocolos desse tipo funcionem, é necessário um esquema de criptografia comutativo.

Um esquema de criptografia comutativo é aquele que, a ordem de cifrar e decifrar é permutável. A analogia da caixa com cadeados envolvendo Alice e Bob tratada na seção 3.12.1, é um exemplo de cifra comutativa.

O protocolo de Massey-Omura usa a comutatividade de funções do tipo exponencial. Para que dois usuários troquem mensagens secretas utilizando tal protocolo, é necessário que ambos definam um grupo finito G de ordem q, que é fixo e publicamente conhecido. Cada usuário escolhe um número inteiro aleatório entre 1 e $q-1$, com a condição de que o número escolhido e q sejam coprimos e, determinam seu inverso em $\mathbb{Z}_q$ (veja Teorema 2.1.3.5). Neste caso, a mensagem deve ser um elemento M do grupo G. Suponha que Alice deseja enviar uma mensagem M para Bob utilizando do protocolo citado. A sequência de troca de mensagens acontece da seguinte forma:

1) Alice envia para Bob o elemento M^a, em que a é o inteiro entre 1 e $q-1$, escolhido por Alice, tal que $mdc\ (a,q)=1$. O Número a é mantido em segredo.

2) Bob recebe a mensagem, que nada significa a ele, e eleva M^a a b, em que b é o seu inteiro escolhido entre 1 e $q-1$ e com $mdc(b,q)=1$. O número b também é mantido em segredo. Então, Bob calcula $(M^a)^b$ e envia o resultado para Alice.

3) Alice recebe $((M^a)^b)$ e eleva a a', sendo a' o inverso de a em $\mathbb{Z}_q$, isto é, a' é o elemento de $\mathbb{Z}_q$ tal que $a'.a=1\ mod(q)$. Com isso, obtêm $((M^a)^b)^{a'}=M^b$ e envia novamente a Bob que, por sua vez, consegue ler a mensagem elevando (M^b) a b'. Sendo b' o inverso b em $\mathbb{Z}_q$, isto é $b.b'=1\ mod\ (q)$.

Vamos justificar o passo 3 acima. De fato, observe que $((M^a)^b)^{a'} = M^{aba'} = (M^{a.a'})^b$. Como $a.a' = 1\ mod\ (q)$, temos que $a.a' - 1 = nq$, para algum n natural. Logo, $a.a' = 1 + n(q)$. Então $M^{a.a'} = M^{1+n(q)} = M.(M^q)^n$. Sabemos que em G, que possui ordem q, qualquer elemento elevado a q é a identidade. Logo, $(M^q)^n$, é a identidade. Portanto $M^{a.a'} = M$. Então, $((M^a)^b)^{a'} = M^{a.b.a'} = \left(M^{aa'}\right)^b = M^b$. Elevando esta expressão a b', obtém-se M.

O protocolo é bastante simples, mas é necessário que os usuários tenham um esquema de assinatura (veja seção 3.13) para que um intruso não finja ser um dos usuários. Caso a troca de mensagens seja através de um canal inseguro, um terceiro poderia ter acesso as seguintes informações: G, M^a, M^b, M^{ab}, mas isto não é suficiente para calcular M.

Note que o protocolo acima não criptografa o elemento neutro do grupo G, pois $e = e^a = e^b = e^{ab}$. Caso o grupo considerado seja o grupo multiplicativo de um corpo finito F_q, o elemento neutro da adição em F_q também pode ser considerado. No entanto, ele igualmente não será criptografado pelo protocolo, pois $0 = 0^a = 0^b = 0^{ab}$. Neste caso, para deixar o sistema mais seguro, é possível inutilizar o elemento neutro e a unidade um fazendo uma associação do alfabeto apenas com os outros elementos do grupo.

Exemplo 3.12.2.1: Considere que Alice e Bob decidem trocar mensagens usando o Protocolo de Massey-Omura. Suponha que ambos escolham o grupo $\mathbb{Z}_{29}^*$, que possui ordem 28. Suponha que Alice escolha um valor $a = 3$ e Bob escolha $b = 5$, de modo que esses valores ficam mantidos em segredo. Então, cada um determina o inverso do seu número escolhido em $\mathbb{Z}_{28}$, sendo assim, Alice conclui que $a' = 19$, pois $3.19 = 57 \equiv 1\ mod\ 28$, e Bob encontra $b' = 17$, visto que $5.17 = 85 \equiv 1\ mod\ 28$. Se Alice decide enviar para Bob a mensagem SORRIA, ela procede da seguinte forma:

1°passo: Alice identifica o equivalente numérico de cada letra da mensagem conforme o quadro abaixo:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
2	3	4	5	6	7	8	9	10	11	12	13	14	15
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**.**	
16	17	18	19	20	21	22	23	24	25	26	27	28	

Desse modo, a mensagem SORRIA tem como equivalente numérico a sequência $20 - 16 - 19 - 19 - 10 - 2$. Em seguida, calcula M^a , isto é, $20^3 - 16^3 - 19^3 - 19^3 - 10^3 - 2^3$ que, em $mod\ (29)$ corresponde a $25 - 7 - 15 - 15 - 14 - 8$. E, envia está última para Bob.

2º passo: Bob recebe a sequência $25-7-15-15-14-8$ e eleva cada termo a b, ou seja, $25^5-7^5-15^5-15^5-14^5-8^5$ que em $mod\,(29)$ corresponde a $20-16-10-10-19-27$ que será a sequência enviada para Alice.

3º passo: Alice recebe a sequência de Bob e eleva cada número a $a'=19$, obtendo assim a sequência $20^{19}-16^{19}-10^{19}-10^{19}-19^{19}-27^{19}$ que é equivalente a $24-23-21-21-8-3$. Novamente, envia está última a Bob.

4º passo: Bob recebe uma nova sequência de Alice e aplica $M^{b'}$:$24^{17}-23^{17}-21^{17}-21^{17}-8^{17}-3^{17}$ que é congruente $mod\,29$ a $20-16-19-19-10-2$. E finalmente, Bob consegue ler a mensagem original analisando a letra correspondente a cada valor obtido.

3.12.3 Método de Elgamal para transmissão de mensagens

Em 1984, Taher Elgamal descreveu um sistema criptográfico de chave pública baseado na troca de troca de chaves de Diffie-Hellman. O sistema é composto por três componentes: o gerador de chave, o algoritmo de criptografia e o algoritmo de descriptografia.

O sistema é descrito da seguinte maneira: define-se um grupo finito cíclico G de ordem q muito grande e um elemento $g \in G$ (preferencialmente um gerador). Suponha que Alice e Bob queiram trocar uma mensagem que é um elemento M em G. Cada usuário escolhe um número inteiro maior que 0 e menor que q. Vamos considerar que Alice escolha a. Esse valor corresponde a chave de decodificação secreta de Alice. A chave de codificação pública de Alice é $(g, g^a) \in G$. Com isso, para Bob enviar uma mensagem para Alice, ele procede da seguinte forma:

1) Bob escolhe um inteiro k aleatoriamente. Bob mantem k em segredo.
2) Bob calcula o elemento Mg^{ak},
3) Bob envia para Alice o par de elementos de G: (g^k, Mg^{ak}).

Desde que apenas Alice conhece a, ela, e apenas ela, pode recuperar a mensagem M da seguinte maneira:

4) Alice calcula $(g^k)^a$,
5) Alice multiplica o inverso de g^{ak} em G pelo elemento Mg^{ak}, obtendo assim a mensagem M.

Através de um canal não seguro, um intruso consegue obter os valores de G, g, g^a, g^k, Mg^{ak}, mas isto não é suficiente para calcular M, pois é necessário conhecer a, que é a chave secreta de Alice.

Note que o protocolo acima criptografa o elemento neutro do grupo G. Assim como no caso anterior, se o grupo considerado for o grupo multiplicativo de um corpo finito F_q, o elemento neutro da adição em F_q também pode ser considerado. No entanto, ele não será criptografado pelo protocolo, pois $0 = \ 0g^{ak}$.

Exemplo 3.12.3.1: Considere que Alice e Bob decidam trocar mensagens considerando o grupo $\mathbb{Z}_{29}^*$, que é de ordem 28. Suponha que Bob deseja enviar a mensagem VENHA LOGO! para Alice. Suponha que ambos decidam utilizar o método Elgamal. Vamos considerar que os dados da Alice são, $g = 2$ e $a = 3$. Portanto a chave pública de Alice é $(2, 2^3)$ e a privada é 3. A partir dessa informação, Bob efetua as seguintes operações para cifrar a mensagem:

1º passo: Bob transforma a mensagem em uma sequência numérica de acordo com o quadro usado no exemplo 3.12.2.1**.** Assim, a mensagem VENHA LOGO é representada pela sequência $22 - 6 - 15 - 9 - 2 - 13 - 16 - 8 - 16$. Em seguida, escolhe $k = 8$.

2º passo: Bob então, calcula $M(g^a)^k$, ou seja, efetua $22.8^8 - 6.8^8 - 15.8^8 - 9.8^8 - 2.8^8 - 13.8^8 - 16.8^8 - 8.8^8 - 16.8^8$ o que, em $mod\ 29$ é congruente a: $5 - 4 - 10 - 6 - 11 - 28 - 1 - 15 - 1$.

3º passo: Bob envia a sequência da mensagem cifrada junto com a informação $g^k = 256\ mod\ (29) = 24$.

Alice por sua vez, para decifrar a mensagem efetua $(g^k)^a = 24^3 \equiv 20\ mod\ (29)$. Além disso, precisa determinar seu inverso $mod\ (29)$, isto é, identificar o inteiro que multiplicado por 20 seja congruente a $1\ mod\ (29)$. Logo, conclui que 16 é o inverso de 20 pois, $16.20 = 320 \equiv 1\ mod\ (29)$. Por último, Alice multiplica o inverso de 20 por cada termo da sequência recebida de Bob, ou seja, calcula: $16.5 - 16.4 - 16.10 - 16.6 - 16.11 - 16.28 - 16.1 - 16.15 - 16.1$, obtendo como resultado $22 - 6 - 15 - 9 - 2 - 13 - 16 - 8 - 16$ que corresponde a mensagem original.

3.13 AUTENTICAÇÃO E ASSINATURA DIGITAL

Em certas situações de troca de mensagens, uma das partes mais importantes é a assinatura. Em casos de operações financeiras com cheques ou contratos, a assinatura é uma prova até mesmo jurídica. Portanto, quando a troca de mensagens ocorre por meio eletrônico e não é possível ter a assinatura física, existe a necessidade de ter-se algum dispositivo que sirva como um selo digital, e que não possa ser reproduzido por terceiros. Além disto, é igualmente importante que haja mecanismos que garantam que o texto original não tenha sido adulterado.

Para compreender a importância destes instrumentos, vamos supor a seguinte situação: Alice é proprietária de uma loja virtual de auto peças para carros, Bob é um cliente que deseja uma peça para seu carro antigo — peça muito rara de ser comercializada. Por algum motivo, ele desiste da compra e Alice tem uma política de "não retorno". Além disso, ela sabe que não será fácil vender esta peça. Porém, Bob argumenta que nunca pediu e Alice decide processá-lo. Em frente ao juiz, o advogado de Alice apresenta a ordem do pedido digital de Bob. Obviamente, o advogado argumenta que Bob deve ter gerado a ordem. Já o advogado de Bob argumenta que Alice pode ter feito uma encomenda falsa. Para o juiz, ao que parece, não tem como saber se o pedido foi gerado por Bob ou Alice!

Esse caso, embora fictício, mostra a importância de se provar a um terceiro neutro (no caso o juiz) o emissor da mensagem e a sua autenticidade.

3.13.1 Autenticação via métodos de criptografia de chave pública

Existe um protocolo simples que pode ser aplicado nos sistemas de chaves públicas que resolve o problema acima. Suponha que Alice queira mandar para Bob uma mensagem codificada e de forma que fique demonstrado que foi ela quem enviou esta mensagem. Seja P a mensagem original. Ao invés de enviar para Bob $f_{kb}(P)$, sendo kb a chave pública de Bob, ela envia $f_{kb}(f_{ka}^{-1}(P))$, sendo ka a chave pública de Alice. Veremos que isto é suficiente para garantir que a mensagem foi enviada por Alice, e ninguém mais, nem mesmo Bob. De fato, ao receber a mensagem criptografada $f_{kb}(f_{ka}^{-1}(P))$, Bob aplica a função inversa f_{kb}^{-1} (que somente ele conhece), na mensagem recebida, obtendo $f_{ka}^{-1}(P)$. Esta última continua sendo uma mensagem criptografada. No entanto, Bob tem acesso a chave pública de Alice (todos têm). Logo ele conhece f_{ka}. Ele aplica esta função em $f_{ka}^{-1}(P)$, obtendo assim a mensagem original P. Além disto, o procedimento garante que o emissor foi Alice, desde que a única pessoa capaz de criar $f_{ka}^{-1}(P)$ é a própria Alice, dado que ela é a única que conhece f_{ka}^{-1}.

3.13.2 Métodos de Elgamal para assinatura digital

Anteriormente foi apresentado o método Elgamal de transmissão de mensagens. A seguir, apresentamos um método, denominado esquema de assinatura de Elgamal, para a transmissão de uma mensagem contendo uma assinatura do emissor, sendo que esta assinatura pode ser conferida pelo destinatário. Assim como no método de Elgamal de transmissão de mensagens, a segurança deste esquema está baseada na suposição de Diffie-Hellman.

Suponha que Bob queira enviar uma mensagem M para Alice com uma assinatura. Vamos considerar que M seja um número natural. Neste protocolo, Bob deve primeiramente gerar uma chave pública para a verificação de sua assinatura. Para isto, ele procede da seguinte forma:

1) Escolhe um número primo p grande.

2) Escolhe um gerador $\alpha \in \mathbb{Z}_p^*$.

3) Escolhe um número inteiro $d \in \{2, 3, \dots, p-2\}$.

4) Calcula $\beta \in \mathbb{Z}_p$ tal que $\beta \equiv \alpha^d \bmod (p)$.

A tripla $k_{pub} = (p, \alpha, \beta)$ é a chave pública para a conferência da assinatura de Bob, enquanto d é mantido em segredo por ele. Note que para achar d a partir de $k_{pub,}$ é preciso resolver um problema de logaritmo discreto. Para gerar a assinatura associada à mensagem M, Bob procede como a seguir:

1) Escolhe um número inteiro $k_E \in \{1,2, \dots, p-2\}$ tal que $mdc(k_E, p-1) = 1$

2) Calcula o inverso de k_E em $\mathbb{Z}_{p-1}$, isto é, $k'_E \in \mathbb{Z}_{p-1}$ tal que $k_E . k'_E \equiv 1\ mod\ (p-1)$.

3) Calcula $r \in \mathbb{Z}_p$ tal que $r \equiv \alpha^{k_E}\ mod(p)$ e $s \in \mathbb{Z}_{p-1}$ tal que $s \equiv (M - dr)k'_E \ \ mod(p-1)$.

Bob envia para Alice os elementos (M, r, s), sendo M a mensagem e o par (r, s) a sua assinatura. Ele guarda $k_E\ e\ k'_E$ em segredo. Note novamente que, para achar $k_E\ e\ k'_E$ a partir dos dados enviados, é preciso resolver um problema de logaritmo discreto.

Para Alice conferir que a assinatura da mensagem (M, r, s) é de Bob, ela procede da seguinte forma:

1) Calcula $t \in \mathbb{Z}_p$ tal $que\ \ t \equiv \beta^r . r^s\ mod\ (p)$.

2) Compara t com α^{M}. Se $t \equiv \alpha^{\mathrm{M}} mod(p)$, então a assinatura de Bob é validada. Caso contrário, a assinatura não é validada.

Vamos demonstrar a veracidade do algoritmo acima. Devemos verificar que $t \equiv \alpha^{\mathrm{M}} mod(p)$. Note que,$t \equiv \beta^r . r^s \, mod\,(p) = (\alpha^d)^r . (\alpha^{k_E})^s \, mod\,(p)(\alpha)^{dr + k_E s} \, mod\,(p)$. Logo, devemos verificar que $(\alpha)^{dr + k_E s} \equiv \alpha^{\mathrm{M}} \mathrm{mod(p)}$. De acordo com o corolário 2.1.2.10 (corolário do Pequeno Teorema de Fermat), esta igualdade é válida se M$\equiv$ $(dr + k_E s) \, mod\,(p-1)$. Vamos verificar que isto é verdadeiro. De fato, desde que $\boldsymbol{s} \equiv (M - dr)k'_E \, mod(p-1)$, temos $(dr + k_E s) \, mod\,(p-1) = (dr + k_E (M - dr)k'_E) \, mod\,(p-1). = (dr + (M - dr)) \, mod\,(p-1). = M \, mod\,(p-1)$. Portanto o algoritmo está correto.

Note que, desde que apenas Bob conhece a chave secreta d, somente ele pode ter gerado o valor s, garantindo que foi ele o autor da mensagem M.

Um invasor pode ter acesso aos seguintes dados: $p,\ \alpha, \beta, M\ r, s$. Para encontrar d ele precisa resolver $\log_\alpha \beta$ em $\mathbb{Z}_p$, que é um problema de logaritmo discreto em grupo finito grande, e, portanto, computacionalmente inviável.

Exemplo 3.13.2.1: Considere que Bob deseja enviar uma mensagem para Alice utilizando o sistema de assinatura digital Elgamal. Para isso, Bob faz escolhas para gerar suas chaves. Suponha que ele escolha $p = 29$, $\alpha = 2$ e $d = 10$, com isso determina o valor de β, isto é, $\beta = 2^{10} = 1024 \equiv 9 \, mod\ 29$. Ele deixa público a tripla $k_{pub} = (\mathrm{p}, \alpha, \beta) = (29, 2, 9)$.

Suponha que a mensagem que Bob queira enviar a Alice seja $M = 18$, então ele precisa calcular a assinatura para essa mensagem. Desse modo escolhe uma raiz $k_E = 9$, respeitando a condição de que $mdc(k_E, 28) = 1$. Tem-se que $k'_E = 25, pois\ 9.25 \equiv 1 \, mod\ 28$. Em seguida, calcula os parâmetros r e s da assinatura, sendo $r = \alpha^{k_E} = 2^9 \equiv 19 \, mod\ 29$ e $s = (M - dr)k'_E = (18 - 10.19).25 = (-172).25 \equiv 12 \, mod\ (28)$. Alice, que já tem acesso a chave pública de Bob $k_{pub} = (\mathrm{p}, \alpha, \beta) = (29, 2, 9)$, recebe a mensagem junto com os parâmetros r e s, ou seja, $(M, (r, s)) = (18, (19, 12))$. Para verificar se a mensagem é mesmo de Bob, Alice calcula $t = \beta^r . r^s = 9^{19} . 19^{12} \equiv 5.20 \equiv 13$. Como $13 \equiv 2^{18} \, mod\ 29$, isto é, $t \equiv \alpha^{\mathrm{M}} mod(p)$, ela tem certeza de que a mensagem enviada foi escrita por Bob.

4 PROPOSTAS DE APLICAÇÃO

As propostas de aplicação foram pensadas de acordo com o perfil dos alunos de uma escola da rede privada, da cidade de Rio do Sul (SC). As questões e desafios propostos foram elaborados da forma mais contextualizada, utilizando contexto de séries e livros já vistos por uma grande parte dos alunos, e até mesmo abordando situações que remetem ao cotidiano. Fatos históricos também foram utilizados com o intuito de motivar um olhar mais crítico e reflexivo sobre a importância da Matemática através do tema criptografia.

4.1 PROPOSTA DE APLICAÇÃO PARA O 1º ANO DO ENSINO MÉDIO

Um dos assuntos mais abordados no 1º ano do Ensino Médio é o estudo das funções. De modo tradicional, segue-se a ordem:

- Introdução às funções: domínio, contradomínio, imagem, função injetora, sobrejetora, bijetora, função inversa, função composta.
- Função afim;
- Função quadrática;
- Função exponencial;
- Função logarítmica;
- Função modular.

É possível utilizar a Criptografia como tema motivador para a introdução do conceito de função, dos tipos de funções e a importância da função inversa. Desse modo, é proposta uma aplicação em sala de aula utilizando-se da criptografia para alcançar os seguintes objetivos:

- compreender o conceito de função;
- compreender os conceitos de domínio, contradomínio e imagem;
- determinar a função inversa;
- associar a função inversa com a propriedade de bijeção;
- verificar que há funções que precisam de restrição no seu domínio para que exista sua inversa;
- abordar, intuitivamente, a aritmética modular;
- estimular a curiosidade e reflexão sobre o tema Criptografia nos dias atuais.

Para que sejam alcançados os objetivos, foi elaborada a sequência didática abaixo, que está dividida em cinco momentos, sendo necessário aproximadamente 5 aulas com duração de 50 minutos.

1º momento: O professor deve iniciar a aula com uma conversa sobre o tema escolhido, como por exemplo, projetar a seguinte notícia extraída do site UOL:

> Criptografia garante a segurança do seu Whatsapp; sabe como ela funciona?
> Rodrigo Lara
> Colaboração para o UOL, em São Paulo
> 12/05/2019 04h00
>
> Com mais de um bilhão de usuários no mundo, o WhatsApp, sabemos, é campeão de popularidade. É provável, por exemplo, que você já tenha enviado mensagens pelo app diversas vezes somente hoje. Mas você já parou para pensar se suas mensagens estão realmente seguras? Qual o nível de privacidade? Há risco de as mensagens serem interceptadas? A base da segurança na troca de mensagens pelo WhatsApp é a chamada "criptografia de ponta a ponta". Em termos práticos, a tecnologia é uma forma de garantir que a mensagem só possa ser vista por quem enviou ou pelo destinatário. Fazendo um paralelo, é como se a mensagem fosse enviada dentro de um cofre, cuja combinação para a abertura só você e a pessoa do outro lado sabem. Assim, mesmo que a mensagem pudesse ser interceptada no meio do caminho, ela não poderia ser decodificada. Segundo o próprio WhatsApp, isso se aplica a todo tipo de conteúdo enviado: mensagem escrita, áudio, fotos, vídeos, etc. (....) O WhatsApp diz garantir que a barreira configurada pela criptografia é inquebrável. Essa, aliás, é uma das razões pelas quais o app é alvo de juízes por não colaborar com investigações --o que já fez com que ele fosse bloqueado algumas vezes no país.
>
> Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/05/12/criptografia-garante-a-seguranca-do-seu-whatsapp-sabe-como-ela-funciona.htm> Acesso em: 18/12/2019.

Após a leitura, propor o desafio aos alunos de decifrar a seguinte mensagem:

H SUHFLVR ROKDU D PDWHPDWLFD FRP RXWURV ROKRV, UHFRQKHFHU VXD SUHVHQFD QD QDWXUHCD, VXD EHOHCD H VHXV EHQHILFLRV.

Disponibilizar um tempo para que os alunos decifrem. Pode ser em dupla, trios. Após o tempo estipulado, verificar se conseguiram decifrar a mensagem que diz:

É preciso olhar a Matemática com outros olhos, reconhecer sua presença na natureza, sua beleza e seus benefícios.

Discutir sobre as tentativas feitas pelos alunos e conduzir a conversa de tal modo que contextualize a história da criptografia e apresente a cifra de César.

O método é bem simples; cada letra do alfabeto é substituída pela letra que está três casas a frente, isto é, a letra A é substituída pela letra D, a letra B é substituída pela letra E, e assim sucessivamente como mostra o Quadro 5:

Quadro 5: Cifra de César. Na primeira linha o alfabeto normal, na segunda linha, o alfabeto deslocado em 3 casas.

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

Fonte: A autora.

Com o quadro 5 apresentado aos alunos, pedir que eles decifrem a mensagem inicial.

2º momento: associar o método com uma função afim do tipo $f(x) = x + 3$, onde cada letra do alfabeto estará associada com um número de 1 a 26, conforme o Quadro 6 abaixo.

Quadro 6: Letras do alfabeto e seus números correspondentes

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: A autora.

Concluir que é possível usar outras funções afim como chaves para cifrar uma mensagem. Por exemplo, utilizando a função $f(x) = 3x + 1$ como chave, de forma coletiva, cifrar a palavra SAUDADE. Aqui, primeiramente, é necessário concluir que a palavra sugerida é representada pela seguinte sequência numérica: 19 – 1 - 21 – 4 – 1 – 4 – 5. Então, utilizando a função chave, tem-se que esta sequência é transformada em 58 – 4 – 64 – 13 – 4 – 13 - 16, pois:

$$f(19) = 3.19 + 1 = 58,$$
$$f(1) = 3.1 + 1 = 4,$$
$$f(21) = 3.21 + 1 = 64,$$
$$f(4) = 3.4 + 1 = 13,$$
$$f(5) = 3.5 + 1 = 16.$$

Nesse momento, é intuitivamente trabalhado o conceito de aritmética modular, onde os alunos devem perceber que 58 é congruente a 6, que representa a letra F. Do mesmo modo, que 64 é congruente a 12, que representa a letra L. Então, a palavra SAUDADE é cifrada e substituída por FDLMDMP.

É interessante abordar com os alunos o caso, por exemplo, da palavra ESTAR e da função chave $f(x) = 2x + 1$. Tem-se que 5 – 19 – 20 – 1 - 18 é a sequência numérica da

palavra original. Logo, a mensagem cifrada possui a seguinte sequência numérica: 11 – 39 – 41 – 3 – 37. Se a aritmética modular for utilizada, pode-se representar esta sequência pela palavra KMOCK. Notar que S e E são criptografados em K. Isto ocorre devido ao fato de $f(x) = (2x + 1)\ mod\ (26)$ não ser bijetora em $\mathbb{Z}_{26} = \{0,1,2\ldots,25\}$. Ademais, usando $f^{-1}(y) = \frac{y-1}{2}$, que é a função inversa de $f(x)$, mas não de $F(x)$, e y sendo o valor numérico de cada letra da palavra cifrada conforme Quadro 6, chega-se à sequência 5 – 6 – 7 -1 -5, que representa a palavra EFGAE, que obviamente é diferente da palavra original. Sendo assim, para evitar uma mistura equivocada entre a aritmética dos reais e a modular, escolhe-se trabalhar somente com funções reais, isto é, as mensagens criptografadas são representadas apenas numericamente (em $\mathbb{Z}$) e não se faz uso da aritmética modular neste ponto. Neste caso, qualquer função afim, exceto a nula, pode ser usada para efetuar uma criptografia.

Após essa sequência de atividade, é explorado o conceito de domínio, contradomínio, imagem da função e função inversa. Propor que os alunos determinem a operação necessária com a sequência numérica da palavra cifrada para chegar a original. Num primeiro momento é usado a ideia intuitiva de operação inversa e, posteriormente utiliza-se diferentes funções afins para abordar o processo algébrico da determinação da função inversa de uma função afim.

3º momento: Dinâmica em duplas

Organizar a sala em três filas de duplas com intenções distintas, na qual uma irá emitir a mensagem, outra tentará interceptar e a última receberá a mensagem cifrada.

A dinâmica terá três rodadas, conforme descrito abaixo:

1ª rodada:

- A dupla da primeira e terceira fila se unem para decidir uma função chave, sem que a segunda fila descubra.
- A dupla da primeira fila escreve uma mensagem cifrada, em sequência numérica, usando uma função chave escolhida. A dupla joga uma mensagem para a terceira fila.
- A dupla da segunda fila tenta interceptar a mensagem. Se conseguir pegar, vai tentar descobrir a mensagem original. Enquanto isso, uma pessoa da dupla da primeira fila entrega a mensagem cifrada (escrita na segunda folha) para a dupla da terceira fila. Sendo assim, a dupla que recebe a mensagem tem a função chave, e com ela deverá decifrar a mensagem.

2ª rodada:

Repete-se o procedimento, invertendo as funções das filas, isto é, a terceira fila irá cifrar e a primeira fila decifra.

3ª rodada:

Repete-se o procedimento, invertendo as funções das filas novamente, agora, a segunda fila irá cifrar, a primeira fila decifra e a terceira fila tentará interceptar.

Ao término da dinâmica, verificar se alguma dupla interceptadora descobriu a mensagem original. Discutir sobre o quanto isso é difícil, mas não impossível. Pode-se também na dinâmica propor uma pontuação para a dupla que conseguir decifrar a mensagem mais rápido, mas neste caso o professor deverá criar a mensagem para que seja do mesmo tamanho para todos.

4º momento: Utilizar como função chave uma função quadrática, por exemplo $f(x) = x^2$,para cifrar uma palavra que a turma escolha, apresentado apenas a sequência numérica.

Em seguida, propor a seguinte atividade para que seja resolvida em duplas:

1) Considere que a sequência 12 – 20 – 156 – 6 – 90 representa uma palavra cifrada e que para a cifragem foi utilizada a função chave $f(x) = x^2 - 11x + 30$.

a) De que forma é possível descobrir a palavra original usando a função chave?

Resposta possível: Para cada número da sequência, determinar x de modo que $f(x)$ =número da sequência. Por exemplo, determinar x de modo que $f(x) = 12$. Outra possibilidade seria obter a função inversa de $f(x)$.

b) Qual a palavra original?

Resposta: BARCO

c) Qual a principal dificuldade no processo de decifrar nessa situação proposta?

Resposta: No caso $f(x) = 12$, obtemos $x = 9\ ou\ x = 2$, causando dúvidas se a letra original será I ou B. O mesmo ocorre com $f(x) = 20\ e\ f(x) = 6$.

d) É possível dizer que essa função chave possui inversa? Justifique.

Resposta possível: Depende, se for considerado que o domínio da função é o conjunto dos números reais, a função não possui inversa, pois a função quadrática não é injetora. Agora se, restringir o domínio de tal forma que a função seja bijetora, a função terá inversa.

e) Usando essa mesma função chave, cifre a palavra SELFIE.

Resposta: 182 – 0 – 42 – 0 – 12 - 0

f) Que problema vocês encontraram no processo de cifrar a palavra pedida no item anterior? Caso tenha identificado um problema, proponha uma solução para que seja possível cifrar a palavra pedida com a função chave atribuída.

Resposta possível: Usando a função $f(x) = x^2 - 11x + 30$, temos que 5 e 6 são os zeros da função, isto é, $f(5) = f(6) = 0$ e, de acordo com o quadro 6, que apresenta o alfabeto e o número correspondente de cada letra, foi utilizado números de 1 a 26, gerando o problema ao usar funções que cheguem no valor zero. Para corrigir esse problema, basta usar números de 6 a 31, para a função ser bijetora.

g) Cifre a palavra DEGUSTAR. Depois, analise qual seria o problema que uma pessoa teria na hora de decifrar a palavra, mesmo sabendo da função chave. Proponha alguma solução para esse problema.

Resposta possível: A palavra cifrada seria representada pela sequência 2 – 0 – 2 – 240 – 182 – 210 – 20 – 156. Ao decifrar, temos que $f(x) = 2 \rightarrow x = 4 \; ou \; x = 7$, gerando dúvidas qual será a letra correta. Isso ocorre porque, $x = 4$ e $x = 7$ são valores equidistantes do vértice da parábola. Uma solução para o problema seria usar uma função quadrática onde o vértice da parábola seja tal que $x \leq 0$.

h) Verifique se a função $f(x) = \frac{11 \pm \sqrt{1+4x}}{2}$ pode ser utilizada como uma função inversa de $f(x) = x^2 - 11x + 30$, sendo que $D = \{x \in \mathbb{N}; x > 6\}$.

Resposta: Sim.

i) Vocês consideram que uma função quadrática seja adequada para ser utilizada como chave? Justifique.

Resposta pessoal. Espera-se que o aluno perceba que ela exige restrições enquanto função afim não.

Após os alunos responderem as questões propostas, discutir junto a eles as respostas, principalmente sobre a questão do item h. Verificar se os alunos conseguem criar ou perceber o algoritmo que determina a inversa da função quadrática. Caso não consigam, retomar o processo de obter a inversa da função afim, de modo a induzir que é um processo semelhante. Também discutir com os alunos como identificar o domínio da função quadrática para que ela possua inversa. Nesse caso, a construção do gráfico da função pode ajudar os alunos a visualizarem a importância do vértice da parábola. Para a construção, o uso do Geogebra permite uma visualização mais rápida e interativa, possibilitando analisar mais exemplos em um intervalo de tempo menor do que se construído manualmente.

5º momento: Será realizada uma avaliação individual, com as questões abaixo, para verificar se os objetivos foram alcançados.

A avaliação será da seguinte forma:

Decifre a pergunta sabendo que a chave é a mesma que foi utilizada pelo Imperador Júlio César e, responda-a na forma original, isto é, não codifique a resposta.

1) Frpr ixqflrqd d fliud gh fhvdu?

Resposta: Como funciona a cifra de César?

2) Txdo vxd fru suhihulgd?

Resposta: Qual sua cor favorita?

3) Sru txh d fulswrjudild h lpsruwdqwh?

Resposta: Por que a criptografia é importante?

4) Suponha que Fernanda mande uma mensagem para sua amiga Paula, e que foi combinado entre elas que a chave utilizada seria a função $f(x) = 3x + 4$. Sabendo que a mensagem enviada por Fernanda foi 25 – 67 – 7 – 58 – 16 – 19 – 49 – 61 – 19 – 25 – 58 – 19 −16 – 49. Responda:

a) Qual a função inversa para determinar a mensagem original?

Resposta: $f(x)^{-1} = \frac{x-4}{3}$.

b) Qual a mensagem original?

Resposta: Guarde o segredo.

c) Que tipo de função chave as amigas deveriam tomar cuidado para não haver confusão na hora de decifrar a mensagem?

Resposta: Função quadrática

5) Qual a condição necessária para que uma função possa ser escolhida como chave para cifrar uma mensagem? Justifique sua resposta.

Resposta: Que seja uma função bijetora, para que exista a função inversa.

4.1.1 Análise das atividades aplicadas no 1º ano do Ensino Médio

As atividades propostas para o 1º ano do Ensino Médio foram aplicadas do dia 07/07/2020 a 21/07/2020, numa escola da rede privada na cidade de Rio do Sul (SC), com duração de 11 aulas de 50 minutos cada.

Participaram das atividades toda a turma, que é composta por 41 alunos, dos quais 5 possuem problemas neurológicos que interferem significativamente no processo de aprendizagem.

Em virtude da COVID-19, caracterizada pandemia pela Organização Mundial da Saúde em 11/03/2020 e, pelo Decreto nº 509 de 17/038/2020, o governador do estado de Santa Catarina suspendeu a partir de 19 de março de 2020, inclusive, as aulas nas unidades das redes pública e privada de ensino, municipal, estadual e federal, incluindo educação infantil, ensino fundamental, nível médio, educação de jovens e adultos (EJA), ensino técnico e ensino superior. Desde então, as aulas presencias passaram a acontecer de forma remota e exigiu adaptações no currículo escolar. Na escola em que foi pensada a proposta de aplicação, as aulas aconteceram de forma ao vivo pelo aplicativo Google-Meet, além de serem gravadas e disponibilizados os links da gravação no sistema de gestão escolar para que os alunos pudessem rever as aulas caso tenham ficado com dúvidas ou até para os casos em que eventualmente tiveram problemas com a conexão da internet.

Portanto, a proposta apresentada na seção 4.1 precisou ser adaptada à nova realidade escolar. A quantidade prevista inicialmente de 5 aulas estendeu-se para 11, pois, com as aulas online, o ritmo de aula é menor devido a vários fatores, tais como: conexão com internet; verificação de presença; análise do porquê certas tarefas não foram enviadas etc. Além disso, devido a curiosidades dos alunos, alguns tópicos, como a aritmética modular, necessitaram de um tempo maior de explicação e mais exemplos para compreensão. Também houve a participação muito efetiva de um grupo de alunos durante as discussões das resoluções, fazendo com que a atividade prevista para uma aula se ampliasse para duas.

A aplicação da proposta foi iniciada após os alunos terem estudado o capítulo 4 do seu material didático que trata sobre introdução às funções, no qual é abordado o que é função, domínio, contradomínio, imagem, função injetora, sobrejetora, bijetora, função inversa e composta. Após a introdução desses conceitos, realização de atividades e avaliação, foi apresentado aos alunos a proposta de estudar a criptografia como forma de compreender uma das aplicações das funções, bem como a necessidade de reconhecer se uma função possui inversa ou não. Assim, o que foi previsto para o 1º momento ocorreu quase em sua totalidade.

Discutimos sobre a notícia envolvendo criptografia e Whatsapp, o conceito de criptografia e foi compartilhada uma mensagem cifrada e dada como tarefa o desafio de decifrá-la.

Num segundo momento, com duração de duas aulas (50 min cada), realizamos a discussão sobre qual seria a mensagem e como conseguiram decifrar. Vários alunos lembraram que, no ano anterior, uma professora, ao se apresentar no primeiro dia de aula, contou um pouco de si através de um texto cifrado. Devido a esse fato, os alunos conseguiram associar rapidamente que havia uma troca de letras. A partir daí, foi apresentado um breve contexto histórico da cifra de César, lendo trechos do livro O livro dos códigos de Simon Singh [24] e relacionado a cifra com a função afim $f(x) = x + 3$. A sequência de atividades planejadas para esse 2º momento, ocorreu em sua totalidade. A respeito da aritmética modular, uma parte da turma já foi bem intuitiva em perceber que o valor 39 corresponde a letra de posição 13 do alfabeto. Foi associado a congruência como a aritmética do relógio, desse modo, os alunos conseguiram compreender de forma mais rápida a simbologia utilizada $(13 \equiv 1\ mod\ 12)$. Devido a curiosidade de alguns alunos em mais aplicações sobre congruências, foi dado o desafio de determinarem qual seria o resto da divisão de 3^{2020} por 5.

O que havia sido planejado para o 3º momento, uma atividade dinâmica de interação entre grupos, foi a atividade que precisou ser totalmente adaptada. Esse momento também ocupou duas aulas, no qual a primeira revimos os conceitos de criptografia, função-chave, como cifrar e decifrar e foram propostas atividades para praticarem o processo de cifrar. A atividade foi: Cifrem as palavras abaixo utilizando a função-chave dada.

a) BENEFÍCIO; $f(x) = 2x - 3$

b) HONESTIDADE; $f(x) = x^2$

c) BELEZA; $f(x) = 3x - 4$

Durante a discussão dos resultados, os alunos ficaram em dúvida no caso da palavra BELEZA, pois ao cifrar a letra A, obtiveram como resultado o número -1. Alguns alunos pensaram que então, deveríamos voltar uma casa na sequência do alfabeto, fazendo com que -1 correspondesse a letra Z. Assim, foi retomado o significado de congruência, apresentado mais exemplos numéricos para que os alunos concluíssem então que seria a letra Y, conforme quadro 6. Após a discussão, iniciamos a seguinte dinâmica: cada aluno escolheu uma palavra para cifrar e uma função chave. Em seguida, foram escolhidos 10 alunos, no qual cada um, na sua vez, escreveu a sequência numérica da palavra cifrada e a função utilizada no chat do Meet. Os demais alunos tinham a missão de decifrar a mensagem com a informação dada. O primeiro

aluno que escrevia no chat a palavra original corretamente, ganhava um ponto. Vencia o jogo aquele que conseguisse decifrar mais palavras. Os alunos adoraram a dinâmica, houve uma competição bem acirrada entre duas alunas que costumam ter excelentes notas. Elas argumentaram que em alguns momentos não foi preciso decifrar letra por letra para conseguir chegar à palavra original.

Para o 4º momento, ocupamos uma aula, mas com adaptações. Voltamos a discutir sobre a função chave, qual sua importância e poque ela deve ser bijetora. Para isso, foi retomado as funções utilizadas na atividade da aula anterior, $f(x) = x^2$ e $f(x) = 3x - 4$, para abordar se é possível ou não utilizar qualquer tipo de função, analisando seu domínio e contradomínio. Foi proposto ainda analisar o caso em que a função seja $f(x) = x^2 - 11x + 30$ e que tipo de problema teríamos ao cifrar a palavra AMAR. Nesse momento, os alunos perceberam que no caso da função quadrática, uma imagem está associada a dois valores de x diferentes, causando assim, problemas na decifragem. Foi apresentado uma visualização dessa situação através do gráfico da função construído no Geogebra. Alguns alunos apresentaram dificuldades na compreensão da importância que o x_v tem para restringir o domínio da função, fazendo com que ela possua inversa. As questões descritas na seção 4.1 ficaram de tarefa.

As duas aulas seguintes foram utilizadas para discussão das questões de tarefa. A participação mais efetiva ocorreu por parte das meninas e as respostas obtidas foram de acordo com o esperado. Apesar de não ter sido abordado ainda como determinar a inversa de uma função quadrática (com restrição no domínio para que isso aconteça), os alunos conseguiram determinar a mensagem original obtendo os valores de x que geravam $f(x)$. Na situação em que $f(x)$ era o mesmo para dois valores diferentes de x, por eliminatória, escolheram os valores de x que permitiam que a mensagem original fizesse sentido. Após a discussão das atividades, foi abordado como restringir o domínio para que uma função quadrática possua inversa, bem como determinar qual é a função inversa. Nesse momento vários alunos tiveram muita dificuldade e demonstraram preocupação em não conseguir acompanhar a explicação. Com isso, foi planejado mais uma aula para que os alunos pudessem praticar o método de cifrar, decifrar e determinar sua inversa. Foi proposto então, as seguintes atividades:

1) Cifre a palavra SALESIANO usando a função $f(x) = 2x + 3$.

2) Patrícia enviou a seguinte mensagem para Pedro: $14 - 56 - 59 - 44 - 62 - 8 - 44 - 38 - 56 - 2 - 62 - 11 - 2 - 11 - 14 - 56$. Pedro sabe que ela usou a função $f(x) = 3x -$

1 para a cifragem. Qual deve ser a função usada por Pedro para que consiga decifrar a mensagem? Qual é a mensagem?

3) Carla pretende cifrar uma mensagem para sua amiga e deseja usar como função chave $f(x) = x^2 + 2x + 1$. Será que é possível que ela escolha essa função?

4) Henry recebeu a seguinte mensagem: $361 - 16 - 16 - 324 - 225 - 16 - 289 - 196 - 81 - 16$. Ele consegue descobrir qual a mensagem original apenas sabendo a sequência numérica da mensagem cifrada? Que opções ele teria para descobrir a mensagem original?

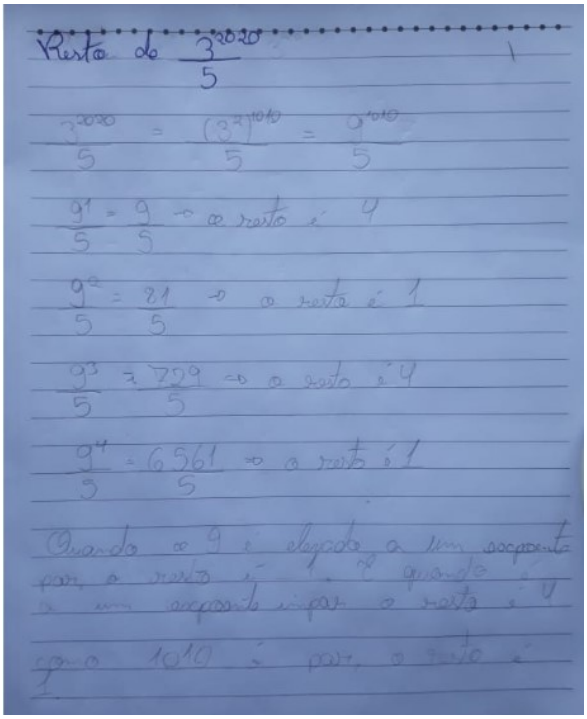
5) Se Henry tiver a informação de que a função codificadora foi $f(x) = x^2 - 2x + 1$, qual a função que ele deverá usar para decifrar a mensagem? Qual é a mensagem?

6) Carlos quer usar a função $f(x) = x^2 - 6x + 5$ para cifrar uma mensagem e sabe que ela não é bijetora quando seu domínio é o conjunto dos números reais. De que forma ele pode proceder para cifrar uma mensagem de modo que essa função seja bijetora.

Durante a correção, foi nítida a dificuldade maior em resolver as questões 5 e 6, necessitando maior detalhamento na resolução e ajuda da professora.

Ainda nessa aula, uma aluna se propôs a responder o desafio dado no 2º momento, aquele em que era preciso determinar o resto da divisão de 3^{2020} por 5. A aluna surpreendeu a todos com seu raciocínio, que foi pedido para que ela descrevesse e enviasse a foto do seu caderno para o Whatsapp da professora, conforme imagem abaixo:

Foto do caderno de uma aluna



Durante a explicação da aluna para a turma, ela cita que tentou identificar um padrão na divisão das potências de 3 por 5. Como não conseguiu encontrá-lo, ao aplicar a propriedade da potenciação, se deparou com o 9 e tentou analisar o padrão a partir desse valor. Chamou atenção também que ela relatou que até seu pai tentou resolver o desafio. Quando perguntado se ele teve sucesso, ela diz que não, porque inclusive ela teve que explicar o que era potenciação para o pai.

Finalizando a aplicação da proposta, nosso último momento, foi aplicada a atividade avaliativa descrita no momento 5. A atividade foi disponibilizada em arquivo pdf via Google Classroom, e tiveram o tempo de 40 minutos para a realização da atividade. Sendo que os alunos precisaram fotografar seus cadernos com a resolução das atividades e fazer a postagem na mesma plataforma disponibilizada para a atividade.

Em relação as notas, apenas dois alunos obtiveram notas abaixo da média 7,0, sendo estes alunos que possuem problemas neurológicos que interferem diretamente na aprendizagem. Um deles conseguiu decifrar a primeira pergunta, mas não a respondeu e, resolveu boa parte da questão 3. Porém, o outro obteve nota zero e, nitidamente, não compreendeu o conteúdo, pois suas respostas foram totalmente fora do contexto. Já os demais alunos obtiveram notas melhores, conforme tabela abaixo:

Tabela 1: Notas obtidas na avaliação sobre criptografia – 1º ano do Ensino Médio – Instituto Maria Auxiliadora – Rio do Sul (SC) – 21/07/2020.

Nota obtida	Quantidade de alunos
Zero	1
5,0 a 7,0	2
7,5 a 8,5	6
9,0 a 9,5	16
10,0	16
Total	41

Fonte: Elaborada pela autora.

Dos alunos que obtiveram notas abaixo de 10, a maioria, ao responder sobre como funciona a cifra de César, disseram que era andar algumas casas para a esquerda no alfabeto. Talvez o fato de a questão pedir para decifrar a pergunta, induziu o aluno a responder como decifrar a mensagem. Poucos foram os alunos que não justificaram o porquê a função chave deve ser bijetora. Alguns conseguiram descrever de forma bem objetiva, como, por exemplo, dizendo ser necessário a função ser bijetora para que ela seja invertível e, outros citaram que, caso a função não seja bijetora, pode-se fazer alguma restrição no domínio para que exista a

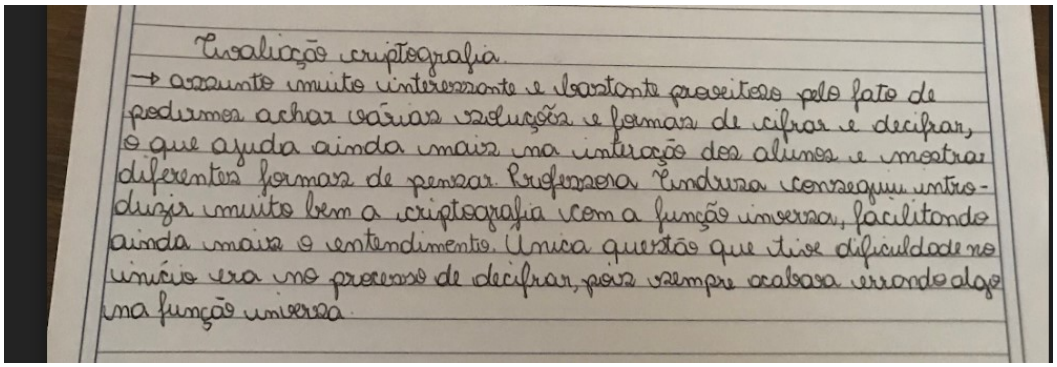
inversa. A questão 4 item a, mostrou claramente a dificuldade em usar a notação de função inversa; ao invés de $f^{-1}(x)$, eles escreveram $f(x)^{-1}$. Outro problema foi a representação correta da função inversa. Para muitos, $x - 4/3$ é o mesmo que $\frac{x-4}{3}$.

Durante as discussões sobre as atividades, foi percebido que a maioria dos alunos não tiveram muitas dificuldades em compreender o que é função injetora, sobrejetora e bijetora. Tal dificuldade sempre foi percebida em anos anteriores quando se abordava o tópico sem mostrar nenhuma aplicação desses conceitos.

Excluindo o aluno que obteve zero, todos os demais conseguiram relacionar a criptografia como importante para a segurança de nossos dados, desde conversas por aplicativos até dados bancários.

Após concluídas as atividades, foi requisitado dos alunos um retorno contendo comentários sobre a sequência didática aplicada. Como opção, eles podiam postar na página de rede, escrever no caderno e enviar por fotografia ou ainda anexar no mural de atividades no Classroom. De modo geral, os comentários foram positivos tanto ao tema quanto a forma de aplicação. Houve relatos de que as atividades ajudaram a solidificar o conteúdo de funções, especialmente na parte de funções inversas. Citaram que houveram dificuldades nas questões sobre bijetividade das funções quadráticas e a relação desta com as funções chaves. Perceberam que esta parte exigiu bastante explicação do professor, mas que também permitiu uma maior discussão sobre o assunto. Comentou-se também que, através das correções feitas em sala e das discussões promovidas, foi possível uma melhorar compreensão da matéria. Logo abaixo, temos as fotos extraídas do Classroom dos relatos de alguns alunos:

Comentário Aluno A:


Avaliação criptografia.
→ assunto muito interessante e bastante proveitoso pelo fato de podermos achar várias soluções e formas de cifrar e decifrar, o que ajuda ainda mais na interação dos alunos e mostrar diferentes formas de pensar. Professora Cindura conseguiu introduzir muito bem a criptografia com a função inversa, facilitando ainda mais o entendimento. Única questão que tive dificuldade no início era no processo de decifrar, pois sempre acabava errando algo na função inversa.

Comentário Aluno B:

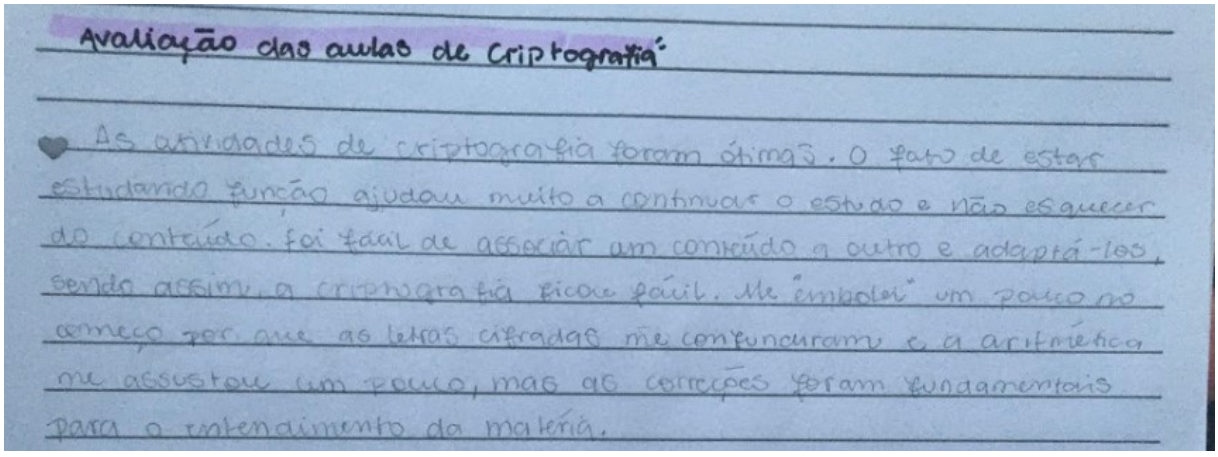
Comentário das aulas de Matemática sobre Criptografia:
Achei as aulas bem produtivas e o assunto muito interessante, gostei muito de aprender a cifrar palavras e decifrar, quando utilizamos as funções facilitou na compreensão do conteúdo que estávamos estudando. Acho que aprender sobre Criptografia foi diferente, divertido e muito interessante, eu pelo menos gostei muito. E além disso as explicações foram bem boas e de fácil compreensão. Só quando utilizamos as funções quadráticas que foi mais complicado mas a professora explicou bem e eu entendi.

Comentário Aluno C:

[redacted]
23 de jul., 13:25

Eu achei que foram aulas muito boas, por mais que é um assunto um pouco difícil, consegui entender bem. Eu acho as explicações muito boas também e quando eu n entendia algo, a professora voltava e revisava, fazendo a gente entender tudo.

Comentário Aluno D:

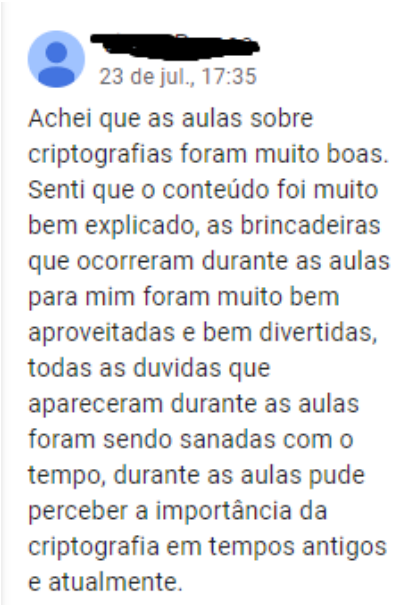

Avaliação das aulas de Criptografia:

As atividades de criptografia foram ótimas. O fato de estar estudando função ajudou muito a continuar o estudo e não esquecer do conteúdo. Foi fácil de associar um conteúdo a outro e adaptá-los, sendo assim, a criptografia ficou fácil. Me "embolei" um pouco no começo por que as letras cifradas me confundiram e a aritmética me assustou um pouco, mas as correções foram fundamentais para o entendimento da matéria.

Comentário Aluno E:

Confesso que não foi o conteúdo mais fácil de entender para mim, mas depois que peguei o jeito ficou muito mais fácil. Eu gostei bastante de termos recebido vários exercícios sobre, pois acho que é o melhor método de descobrirmos as dúvidas que temos, quando realizamos um exercício e encontramos um problema dentro da resolução, aprendemos muito mais tirando essa dúvida do que apenas lendo a teoria. Achei a criptografia algo necessário, pois reforçou muito bem o conteúdo de função que tínhamos estudado anteriormente, principalmente de função inversa, que era algo mais recente. Realmente encontrei bastante dificuldade para decifrar as criptografias que possuíam como chave uma função quadrática, mas aprendi uma forma de conseguir decifrar.

Comentário Aluno F:


[redacted]
23 de jul., 17:35

Achei que as aulas sobre criptografias foram muito boas. Senti que o conteúdo foi muito bem explicado, as brincadeiras que ocorreram durante as aulas para mim foram muito bem aproveitadas e bem divertidas, todas as duvidas que apareceram durante as aulas foram sendo sanadas com o tempo, durante as aulas pude perceber a importância da criptografia em tempos antigos e atualmente.

4.2 PROPOSTA DE APLICAÇÃO PARA O 2º ANO DO ENSINO MÉDIO

O tema criptografia pode ser utilizado como motivação para introduzir o estudo da permutação e fazer a retomada do conceito de probabilidade. Nesse sentido, sugere-se a abordagem didática abaixo, organizada em 5 momentos, cada um representando uma aula com 50 minutos de duração.

A sequência didática proposta tem como objetivos:

- Despertar a curiosidade sobre a criptografia;
- Analisar a importância da criptografia no mundo atual;
- Compreender o que é permutação;
- Perceber o princípio multiplicativo como método de contagem para analisar a quantidade de possibilidades distintas de escrever uma mensagem;
- Compreender a definição de fatorial;
- Intuitivamente, comprovar a fórmula da permutação com repetição;
- Utilizar-se da ideia de permutação para cifrar e decifrar mensagens.

1º momento: Iniciar a aula com a seguinte mensagem no quadro:

MU MBO AID AARP PEDERANR UPREMTRA!

Propor que os alunos tentem decifrar a mensagem. Participar junto com os alunos, mediando as estratégias. Espera-se que os alunos concluam que a mensagem escrita seja: UM BOM DIA PARA APRENDER PERMUTAR!

Decifrada a frase, indagar aos alunos o que eles compreendem por permutar. Desse modo, é possível introduzir a ideia de anagramas. Explicar que este processo de embaralhar as letras de tal forma que oculte a palavra original é conhecido na criptografia como cifra de transposição.

A partir desse momento, apresentar um breve contexto histórico sobre a criptografia. Pode-se também citar os filmes O jogo da imitação e O código da Vinci, que abordam o assunto, ou as séries de streaming Ponto cego e The Bletchley Circle, que também tratam desse tema. Então, abre-se uma discussão sobre a importância do tema no contexto atual. Nisto, pode-se questionar se o método utilizado na mensagem inicial na aula seria seguro para os dias atuais. Conforme conclusões e indagações dos alunos, o professor pode explorar os anagramas possíveis para cada uma das palavras. Por exemplo, a palavra UM permite apenas dois anagramas, sendo a própria palavra UM ou a palavra MU. Já a palavra DIA nos permite criar 6 anagramas, como: DIA, DAI, ADI, AID, IAD, IDA. Através dessas atividades, explorar, junto com os alunos, métodos de calcular a quantidade de anagramas de uma palavra, introduzindo o conceito de fatorial.

2º momento: Iniciar a aula com a mensagem:

O SEGREDO DEVE SER GUARDADO

Desafiar os alunos para que determinem de quantos modos podemos cifrar a mensagem, sendo que é permitido embaralhar todas as letras da frase. Propor também que cada aluno crie sua própria cifra da mensagem. Deixar que os alunos citem seus resultados. Aqui, pode-se registrar os resultados para posteriormente analisar se eles obtiveram, ou não, o número correto. O número de maneiras possíveis de cifrar a mensagem é dado por $P_{23}^{3,2,5,2,3,4,2} = \frac{23!}{3!2!5!2!3!4!2!} = \frac{23!}{829440}$, isto é, maior do que 30 000 000 000 000 000. Concluir que um interceptador teria sérias dificuldades para decifrar a mensagem.

A partir da atividade acima, discutir a segurança da cifra de transposição. Além disso, concluir a importância de se estabelecer previamente e de forma secreta, entre remetente e destinatário, um método de transposição.

Para um outro exemplo, foi pensado numa situação envolvendo personagens da série Grey's Anatomy, série estadunidense que é assistida pela maioria dos alunos em que a atividade será aplicada. Diante do exposto, propor aos alunos a seguinte situação problema: Meredith envia a seguinte mensagem a Alex: PSLUEE AVSA EEDLO TN!. Porém, Shonda consegue interceptar a mensagem e, para decifra-la, pretende embaralhar as letras até encontrar a forma que produz a frase original. Shonda cronometrou sua primeira tentativa e levou um minuto para conseguir uma frase, mas que não fez sentido. Supondo que para cada tentativa, Shonda leva esse mesmo tempo para recriar uma nova frase, qual seria o tempo máximo que ela levaria para descobrir a mensagem original (Please don't leave us!)? Nesta atividade, permitir o uso de calculadora científica. Espera-se que os alunos concluam que serão necessários mais de um 690 milhões de dias, algo em torno de um 1,8 milhão de anos, visto que há mais de 10^{12} combinações de frases, com ou sem significado algum e, num dia têm 1440 minutos. Com isso, relacionar a expectativa de vida das pessoas, a segurança de uma criptografia e a probabilidade dela ser quebrada. Aproveitar o momento e lançar um recorte da seguinte notícia (veja mais em [20]):

> Se a sua senha tem 9 caracteres e usa apenas letras minúsculas, ela levaria 14 anos para ser quebrada por um sistema que realiza 10 mil tentativas por segundo, mas só uma hora e doze minutos em um sistema que faz um bilhão de tentativas por segundo. Especialistas demonstraram em 2012 um sistema que consegue testar 350 bilhões de senhas por segundo usando 25 placas de vídeo. [...] Qualquer senha com menos de 10 caracteres corre o risco de ser quebrada em até uma semana em sistemas não muito caros de serem construídos. Por outro lado, se você usar uma senha de 13 caracteres que combine letras maiúsculas, minúsculas e números, o mesmo sistema, com um bilhão de tentativas por segundo, levaria 9,6 milhões de anos para quebrar a senha. Mesmo um supercomputador testando 100 milhões de senhas por segundo levaria 96 anos!
> Disponível em: <http://twixar.me/tgST>. Acesso em: 14/01/2020.

Discutir sobre a reportagem e analisar como, usando um supercomputador, pode-se diminuir consideravelmente o tempo para quebrar uma senha utilizando o método de força bruta. É válido ressaltar a importância de sistemas bancários restringirem o número de tentativas para digitar a senha. Concluir também que, conforme métodos de criptografia são quebrados, novas técnicas surgem para aumentar a segurança de informações.

Propor que os alunos desafiem uma pessoa (amigo de outra turma, familiar, professor) a descobrir uma mensagem criptografada via cifra de transposição. Caso as pessoas escolhidas por eles não consigam decifrar, tais alunos devem explicar o método de cifra de transposição, e então, sugerir que as pessoas desafiadas tentem novamente descobrir a mensagem.

3º momento: Iniciar a aula com um contexto histórico (descrito abaixo) para abordar a cifra ADFGVX.

A invenção do rádio no final do século XIX trouxe grandes contribuições aos militares da época, sendo que uma delas foi permitir melhores condições para que generais tivessem contato constante com seus batalhões. Por outro lado, essa vantagem inicial se revelou como um ponto fraco e de investidas de inimigos durante a Primeira Guerra Mundial, pois, do mesmo modo que a mensagem chegava ao destinatário, também chegava ao inimigo. Tal situação permitiu a evolução da criptografia, visto que 'todos os lados estavam ávidos por explorar o poder do rádio, mas não tinham certeza de como garantir a segurança" (SINGH, 2001).

A cifra ADFGVX, foi uma das cifras utilizadas na Primeira Guerra Mundial em 1918. Essa cifra utiliza ao mesmo tempo o método de substituição e transposição. Tal processo fez com que ela fosse classificada na época como uma cifra altamente segura.

Após a contextualização histórica, apresentar como funciona a cifra em questão; para cifrar uma palavra ou frase, constrói-se uma grade 7 x 7, totalizando 49 espaços, dos quais 48 serão preenchidos, sendo que o primeiro espaço ficará em branco e a primeira linha e coluna serão ocupadas pelas letras ADFGVX, como mostra o Quadro 7.

Quadro 7: Cifra ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A						
D						
F						
G						
V						
X						

Fonte: A autora.

Os 36 espaços restantes, serão preenchidos com as 26 letras do alfabeto e com os numerais 0 a 9. A distribuição desses elementos pode ser de forma aleatória.

Nesse momento, propor que os alunos determinem a quantidade de maneiras distintas de se montar a cifra ADFGVX. Espera-se que os alunos concluam que seja 36!. Após, análise

desse resultado, escolher uma ordem proposta por algum aluno. Em seguida pedir para que um aluno escolha uma palavra ou frase curta que se deseja cifrar e outro aluno escolha uma palavra-chave (esta não deve conter letras repetidas). Por exemplo, vamos considerar que a palavra a ser cifrada seja DESAFIO e que a cifra ADFGVX escolhida pelos alunos seja:

Quadro 8: Cifra ADFGVX escolhida

	A	**D**	**F**	**G**	**V**	**X**
A	1	D	3	E	5	F
D	A	2	B	4	C	6
F	G	N	O	J	P	Q
G	R	H	8	T	X	W
V	S	U	I	Y	K	Z
X	L	7	L	C	9	0

Fonte: A autora.

Para a cifragem, inicialmente cada letra da palavra DESAFIO será substituída por duas letras dentre ADFGVX, sendo estas as que estão, respectivamente, na linha e na coluna da letra que está sendo considerada. Por exemplo, a letra D será substituída por AD, a letra S será substituída por VA. Sendo assim, a palavra DESAFIO será substituída por ADAGVADAAXVFFF.

No próximo passo, faremos uma transposição. Para isso, será utilizada a palavra-chave, que por sua vez, não deve conter letras repetidas. Vamos supor que a palavra escolhida seja FÁCIL. Então, uma nova tabela é construída, de modo que as letras da palavra FÁCIL preencham os espaços da primeira linha. Nas linhas abaixo, deve ser escrito a palavra cifrada, conforme mostra o Quadro 9:

Quadro 9: Segunda etapa da Cifra ADFGVX

F	**Á**	**C**	**I**	**L**
A	D	A	G	V
A	D	A	A	X
V	F	F	F	

Fonte: A autora.

Organizado o novo quadro, devemos trocar a ordem das colunas, de forma que as letras da palavra-chave fiquem em ordem alfabética. Desse modo, obtemos o Quadro 10:

Quadro 10: Etapa da transposição da Cifra ADFGVX

Á	**C**	**F**	**I**	**L**
D	A	A	G	V
D	A	A	A	X
F	F	V	F	

Fonte: A autora.

Finalmente, ao ler cada coluna de cima para baixo, teremos a cifragem final, isto é, a palavra DESAFIO, usando a cifra ADFGVX, fica DDFAAFAAVGAFVX.

Deve-se ressaltar, que no período da guerra, a mensagem cifrada era transmitida em código Morse. Nesse momento é interessante lançar como uma tarefa aos alunos a pesquisa sobre o porquê a cifra em questão utiliza apenas as letras ADFGVX ao invés de qualquer outra sequência de letras. Na aula seguinte, verificar os resultados da pesquisa dos alunos. Espera-se no mínimo que tenham identificado que as letras ADFGVX não causavam confusão ao transcrevê-las em código Morse.

4º momento: Atividade em grupos aplicando a cifra ADFGVX.

Iniciar a aula propondo uma atividade em grupo, sendo dupla contra dupla. Cada dupla terá uma função; uma dupla será a remetente e a outra o destinatário. A sequência da atividade pode seguir os seguintes passos:

1. A dupla remetente fica sentada em frente a dupla destinatário.
2. Ambas as duplas devem combinar a palavra-chave e a distribuição dos 36 caracteres na grade ADFGVX.
3. A dupla remetente escolhe uma mensagem que deseja enviar a dupla destinatário e faz a cifragem de acordo com as regras da cifra em estudo.
4. Após cifrada a mensagem, a dupla remetente entrega a mensagem a dupla destinatário.
5. A dupla destinatário deve decifrar a mensagem recebida.
6. Após a decifragem, a dupla destinatário deve elaborar uma resposta a mensagem recebida e, deve cifrá-la utilizando a mesma grade ADFGVX e mesma palavra-chave combinadas entre as duplas.
7. A dupla destinatário envia a resposta para a dupla remetente.
8. A dupla remetente deve decifrar a resposta.

Esta sequência de atividades pode ser realizada com lápis e papel. Caso a turma em que a atividade será realizada possui computadores e internet disponível, pode-se fazer o uso de mensagens via e-mail. Porém, deve-se ressaltar que a grade e palavra-chave não deve ser compartilhada de forma que algum interceptador possa ter conhecimento.

A atividade também pode ser enviada ao professor, seja em papel ou e-mail, para acompanhamento do mesmo no processo de aprendizagem. Sugere-se ainda, lançar um desafio para as duplas, de forma que a dupla que conseguir resolver ganha algum bônus. Segue uma sugestão para o desafio, composto por um texto introdutório, um texto chave e o desafio:

Texto introdutório: Durante o século XIX, a criptografia não era apenas um recurso para os militares, mas também, uma forma de jovens apaixonados da Inglaterra vitoriana, proibidos de expressar seus sentimentos publicamente, conseguirem enviar mensagens a sua pessoa amada sem correr o risco de seus pais interceptar correspondências. As mensagens cifradas eram publicadas em colunas de jornais dedicadas as mensagens dos leitores, essas eram famosas "colunas de óbitos".

Texto chave: Vamos supor que uma das mensagens publicadas seja:

"Amor, palavra tão importante, carinhosamente é assim que te chamo! Guardo nas grades do meu coração números e fatos que fazem minha frequência cardíaca ser de 180 pbm. Sétimo dia do mês de fevereiro, às 9 horas da manhã tive a sensação maravilhosa de nosso primeiro beijo e que após esse, no mesmo dia foram mais de seis. Pena, que só quatro dias depois, tivemos a oportunidade de ficar com mãos unidas por quase 25 minutos até que chegou dona Katharyna toda veloz para nos separar. Mas estávamos em êxtase por esse momento digno de memória. Após 36 horas, William trouxe a garantia de que você me correspondia. Diante disso posso lhe dizer com certeza que AVFFXGGDVDGAFDGFAFDFDVX XAFADAGFAXDXAVDGVAXFFADDADDDDFDXDFDAFAFDXAGXFFFXXVFFADX VAV XAFFVAXAXGF!

Desafio: Um analista ao ler a mensagem, percebe rapidamente que a mensagem criptografada utiliza a cifra ADFGVX e, tem a intuição de que consta na mensagem dados necessários para saber a grade utilizada e a palavra-chave. Com essas dicas, determine a mensagem final deixada pela pessoa apaixonada.

A mensagem que os alunos devem obter é: MEU MAIOR DESEJO É FUGIR COM VOCÊ NA PRÓXIMA SEGUNDA! Obtida através da palavra-chave AMOR e da grade conforme o Quadro 11:

Quadro 11: Grade da cifra ADFGVX resultado do desafio

	A	**D**	**F**	**G**	**V**	**X**
A	1	8	0	B	P	M
D	7	F	E	V	R	I
F	O	9	A	N	H	T
G	S	C	L	J	6	4
V	U	2	5	K	Y	Z
X	X	D	3	6	W	G

Fonte: A autora.

5º momento: Atividade avaliativa.

Aplicar uma avaliação individual sobre permutação com temas sobre criptografia. Sendo as questões abaixo como sugestão:

1) BLINDSPOT (Ponto Cego) é uma série norte-americana, que apresenta a história de uma mulher misteriosa que aparece nua em plena Times Square, completamente coberta por misteriosas e complexas tatuagens, sem memória de quem é e de como chegou ali. Porém, um nome se destaca em meio a todos os desenhos: o do agente do FBI Kurt Weller. Logo, eles descobrem que cada marca no corpo de "Jane" é um crime a se resolver, o que os levará para mais perto da resolução dos mistérios, incluindo a identidade da desconhecida. Na primeira temporada episódio 2, uma das agentes percebe que o número 399 e o 7 que aparecem na tatuagem era um endereço já descoberto antes por eles, que significa rua White, 399, apartamento 7. E as letras entre os numerais, usando a cifra de Vigenère (como visto na introdução) com a palavra chave WHITE STREET APARTMENT, obtêm-se a frase MAJARTHURGIBSON, indicando um possível crime a acontecer relacionado com major Arthur Gibson, um piloto da força aérea com um passado doloroso e um agente letal.

Disponível em: https://www.minhaserie.com.br/serie/1078-blindspot. Acesso: 15/01/2020.

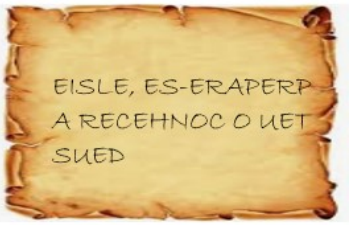
Figura 7 - Tatuagens no corpo da personagem "Jane"

Fonte: < https://starcasm.net/all-the-jane-doe-blindspot-tattoo-photos-we-could-find/ >. Acesso em 15/01/2020.

Assim como a mensagem criptografada leva ao Major Gibson, se o nome do agente do FBI Kurt Weller tatuado nas costas de “Jane”, conforme figura 7, fosse criptografado permutando as letras do nome completo do agente, quantas possibilidades o tatuador teria disponível?

Resposta: $P_{10}^{2,2,2} = \frac{10!}{2!2!2!} = \frac{10!}{8} = 453\,600$ possibilidades.,

2) Em um de seus casos, Sherlock Holmes foi confrontado com uma mensagem enviada pelo sr. Cubitt através do correio. A mensagem era:



Embora Watson estivesse confuso, Holmes mediatamente deduziu que foi utilizada uma cifra de transposição, e que pareceu muito fácil o tipo de permutação utilizada. Sherlock estava esperando uma mensagem bem mais desafiadora.

De acordo com o problema responda:

a) O que seria permutação?

Resposta possível: Uma forma de ordenar de diferentes maneiras distintas, objetos, pessoas, números, letras.

b) Qual o segredo da cifra que Sherlock percebeu imediatamente?

Resposta possível: uma permutação de tal forma que cada palavra foi ordenada de trás para frente tendo como referência a palavra original.

c) Qual a mensagem original?

Resposta: Elsie, prepare-se a conhecer o teu Deus.

3) Camila deseja enviar uma mensagem para sua amiga Ana pelo whatsapp, mas sabe que o irmão de Ana é muito metido e sabe a senha de bloqueio do celular de sua irmã. As duas já haviam combinado de que caso a mensagem fosse comprometedora, a mensagem seria criptografa para dar a impressão de que digitou letras aleatórias no teclado, parecendo estar rindo de algo e, claro, sem ser o tradicional kkkkkk. A criptografia escolhida por elas seria a cifra de transposição, mas que a mensagem deveria começar com a letra P para que fosse entendido que havia sido feito uma permutação. Sabendo que Camila deseja enviar a mensagem: ELE ESTÁ ESPERANDO POR VC, VENHA LOGO., de quantas maneiras

possíveis a mensagem pode ser permutada? Obs: pode-se deixar o resultado na forma fracionária.

Resposta: $P_{29}^{6,2,2,3,2,2,4,2} = \frac{29!}{6!2!2!3!2!2!4!2!} = \frac{29!}{3317760}$

4) Quantos anagramas são possíveis de se formar com seu nome?

Resposta pessoal

5) Dois jovens ingleses apaixonado decidem se corresponder por mensagens criptografadas usando a cifra ADFGVX, combinam secretamente que a grade será:

	A	**D**	**F**	**G**	**V**	**X**
A	1	6	0	C	P	M
D	7	F	E	V	R	I
F	O	9	B	N	H	W
G	S	A	L	J	9	4
V	X	2	5	K	Y	Z
X	U	D	3	8	G	T

E que, a palavra-chave é LOVE. Cifre a mensagem enviada por um deles: O MELHOR LUGAR É AO TEU LADO.

Resposta: Fazendo cifra de substituição -1ª etapa obtemos: FA AXDFGFFVFADV GFXAXVGDDV DF GD FA XXDFXA GFGDXDFA. Para a 2ª etapa, utilizando a tabela com a palavra chave LOVE, obtemos:

L	O	V	E
F	A	A	X
D	F	G	F
F	V	F	A
D	V	G	F
X	A	X	V
G	D	D	V
D	F	G	D
F	A	X	X
D	F	X	A
G	F	G	D
X	D	F	A

Para a 3ª etapa – organizar a palavra-chave em ordem alfabética:

E	L	O	V
X	F	A	A
F	D	F	G
A	F	V	F
F	D	V	G
V	X	A	X
V	G	D	D
D	D	F	G
X	F	A	X
A	D	F	X
D	G	F	G
A	X	D	F

Logo, a mensagem cifrada é:
XFAFVVDXADAFDFDXGDFDGXAFVVADFAFFDAGFGXDGXXGF

4.2.1 Análise das atividades aplicadas no 2º ano do Ensino Médio

As atividades propostas para o 2º ano do Ensino Médio foram aplicadas do dia 13/02/2020 a 20/02/2020, numa escola de rede privada da cidade de Rio do Sul (SC), com duração de 5 aulas de 50 minutos cada.

A turma é composta por 35 alunos, mas participaram 34 alunos, pois uma aluna estava de atestado médico durante o período de aulas que foram desenvolvidas as atividades propostas.

O ano letivo foi iniciado pelo capítulo 3 – Análise combinatória, do livro didático adotado pela escola, tendo como primeiro tópico o princípio fundamental da contagem. Realizamos atividades do livro e de plataformas com banco de questões. Após esse tópico é comum os livros didáticos trazerem o tema sobre permutação. A partir daí foi introduzida as atividades propostas para explorar o tema aliado a criptografia.

A primeira impressão durante a aplicação é de que vários alunos estavam curiosos em relação ao tema e sentiam-se desafiados em cada pergunta. Em relação as questões e séries comentadas, ficaram animados e abriu-se margem para mais conversas. Alguns reclamaram por

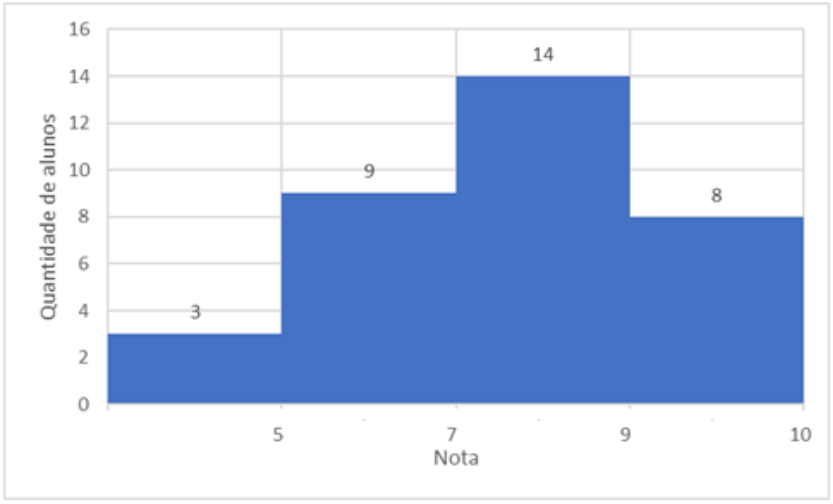
ter sido apresentado alguns spoilers. Em todas as situações, ficaram espantados com a quantidade de combinações possíveis, e que é possível tentar quebrar um código pela análise de frequência das letras.

O desafio proposto no 4º momento, que ocorreu na 4ª aula, intrigou bastante os alunos. Nenhuma dupla conseguiu decifrar a mensagem, mas conseguiram perceber que a palavra-chave era amor, bem como datas e palavras na sequência do texto seria a pista para a distribuição das letras e números no quadro ADFGVX. Todos os alunos relataram ser muito difícil descobrir. Alguns sentiram-se curiosos porque um método com tantas combinações não seria ainda o mais seguro. Também foi percebido uma falta de persistência dos alunos. O fato de precisar de várias tentativas, fez com que muitos desistissem, mesmo que durante a atividade dicas tenham sido dadas

O fechamento das atividades foi através da atividade descrita no momento 5, com o objetivo de identificar se os alunos compreenderam o que é permutação e fatorial, além de saber aplicar os conceitos na resolução de problemas.

Em relação aos resultados da avaliação, é possível observar a distribuição de notas com o gráfico abaixo:

Gráfico 1: Notas obtidas pelos alunos do 2º ano 1 – Rio do Sul (SC) – 20/02/2020.



Fonte: Elaborado pela autora

É costume da escola que, em cada avaliação, seja analisado o percentual dos alunos que atingem nota igual ou superior a 5,0. O ideal é que seja no mínimo 70% da turma. Compreende-se que nas notas entre 5,0 e 7,0, há maior facilidade de recuperação. Além disso, nesta faixa, é maior a possibilidade do aluno ter apenas uma dificuldade específica do conteúdo. Notas abaixo de 5,0 geram preocupações maiores em relação a reprovação. Levando em

consideração os parâmetros da escola, podemos observar que, nessa avaliação, aproximadamente 91% da turma está dentro do esperado.

Na aula seguinte, foi apresentado um panorama geral das notas obtidas e foi discutido os principais erros cometidos, tais como simplificar expressões com fatorial de forma equivocada. Além disso, na questão 3, muitos não observaram a condição de que a mensagem deveria iniciar com a letra P. Na questão 5, boa parte dos alunos não cifraram a frase corretamente, pois a palavra chave não foi escrita em ordem alfabética na última etapa do método de cifragem. A palavra-chave era LOVE e vários organizaram da forma EVOL ou VLOE. Uma parte dos alunos fizeram apenas a primeira etapa do método, que é o passo da substituição. Uma situação engraçada, foi que uma aluna estava tão relacionada com o desafio proposto na aula anterior cuja palavra-chave era AMOR, que nessa questão envolvendo a palavra LOVE, ela usou a palavra AMOR. Como realizou todo o processo da cifra ADFGVX corretamente, foi perdoado o equívoco com a palavra-chave.

Após a discussão em sala sobre os resultados, foi pedido aos alunos que escrevessem em um papel uma avaliação em relação a sequência didática utilizada. De modo geral, os alunos classificaram as aulas como bem organizadas, com boa explicação, bons exemplos, apresentação de fatos históricos interessantes, desafio estimulante e prova com questões adequadas. Porém, vários gostariam que houvesse mais aulas sobre o assunto, com mais atividades, para que se pudesse treinar mais e melhorar as habilidades antes da avaliação.

Seguem alguns relatos escritos pelos alunos:

Aluno A: *As aulas experimentais forma muito criativas, sendo elas de fácil entendimento e também muito produtiva. O tema foi bem elaborado para a devida atividade, sendo ele um tema amplo e muito utilizado. Os exercícios foram feitos com clareza, sendo um método de ensino bom, elaborado com muita atenção.*

Aluno B: *Em minha opinião foi muito bom termos juntado os dois assuntos, vejo que contribuiu muito a compreensão de ambos. Porém, infelizmente, por vezes podemos confundir os conceitos. As atividades foram ótimas, adorei estudar criptoanálise, envolver a história, o português e o amor (um assunto que, por muitas vezes conversamos) foi excelente, pois assim conseguimos nos "identificar" no assunto. Vejo que o nível de dificuldade nas questões era o ideal, pois nos tirava da zona de conforto e nos instigava.*

Aluno C: *Eu tive muita dificuldade em criptografia, não pelo o tema não ser interessante, mas sim porque não conseguia decifrar as frases usando a "cifra ADFGVC" nem o quadradinho não consegui entender. Consegui entender bem a fórmula de permutação, mas depois disso tive muita dificuldade. Gostei muito do tema criptografia pois adoro enigmas e para mim esse assunto é interessantíssimo.*

Aluno D: *Aprender sobre permutação foi muito legal, saber que que usavam muito isso nas épocas de guerras, juntando a história com a matemática. Na minha opinião a professora soube explicar muito bem sobre isso, usando exemplos de séries e livros que nós conhecemos, ajudou muito. Muitas das coisas que aprendemos nunca tínhamos visto antes, mas c=acredito que a professora soube explicar e apresentar o assunto muito bem. A prova que fizemos sobre estava muito bem estruturada, pois nos fazia pensar, mas nada estava tão na cara. Adorei os desafios que foram propostos em aula, tentavam descobrir os segredos das palavras ou frases.*

Aluno E: *Aprendemos sobre criptografia e análise combinatória, no início para mim era muito complexo, mas por um lado estimulante, pois mesmo sendo difícil, é gratificante descobrir a resposta de uma questão. Para mim, se tivesse mais prática de exercícios teríamos melhores resultados, teve partes que entendi de fato o conteúdo na execução do trabalho. Mas foi válido e suficiente com a explicação que tivemos mesmo com um assunto tão complicado.*

Considerando a postura dos alunos diante das atividades propostas, seus resultados na avaliação e seus pareceres sobre a sequência didática, percebe-se que as aulas foram bem sucedidas. Contudo, é interessante que, em outras oportunidades de aplicação, mais atividades sejam agregadas para que os alunos tenham maior segurança e domínio do conteúdo.

É válido destacar que a maior riqueza na aplicação dessa proposta foi trabalhar a matemática dentro de um contexto histórico e sua relação com a atualidade. Desse modo, os alunos refletiram mais sobre a importância da disciplina, não classificando o assunto como algo que "nunca vou usar isso", frase típica para assuntos complexos ou nada atraentes para os alunos.

5 CONCLUSÃO

Nos últimos anos a criptografia vem ganhando um grande destaque entre a população devido a aplicativos, como o Whatsapp, que garantem que as conversas são criptografadas de ponta-a-ponta. Além disso, o uso de aplicativos bancários e de rede sociais, compras via internet, entre outros, exigem que se tenha segurança nas informações compartilhadas. Todos estes fatos vem sendo fatores determinantes para o entendimento da necessidade de haver sistemas criptográficos cada vez mais eficientes e seguros. Portanto, diferentemente dos séculos passados, em que a criptografia costumava ter aplicações restritas aos círculos militares, atualmente este é um tema que aparece no nosso cotidiano.

Vários matemáticos foram primordiais para a evolução da criptografia, seja das cifras simétricas ou assimétricas. Percebe-se que, graças a Teoria dos Números e a Álgebra, pôde-se construir métodos de cifragem adequados para os dias atuais.

Ao abordar os sistemas criptográficos, constata-se que a criptografia é um ramo não estático, isto é, a cada momento é descoberto uma fragilidade de um determinado método existente, e outros métodos mais complexos e seguros são desenvolvidos.

A escolha desse tema para elaborar e aplicar atividades para alunos do ensino médio mostrou-se proveitosa, visto que é um tema atual e importante. A sequência de atividade propostas foi bem aceita pelos alunos que participaram das aulas. Entretanto, acrescentar mais atividades pode contribuir para uma melhor compreensão dos algoritmos. De forma a enriquecer a aplicação do conteúdo, o contexto histórico da criptografia é um importante ponto para fazer a ligação entre a Matemática e a realidade, bem como permitir que os alunos percebam a importância da mesma para a evolução da tecnologia, compreender o mundo atual e fornecer subsídios para que sejam pessoas mais críticas e atuantes na sociedade.

REFERÊNCIAS

[1] ALMEIDA, Pedro Quaresma de. Página sobre Criptologia (Criptografia e Criptoanálise). Disponível em: < http://www.mat.uc.pt/~pedro/cientificos/Cripto/ >. Acesso em: 04/06/2020.

[2] ÂNGULO, Rigo Julian Osorio. **Criptografia de curvas elípticas**. Goiânia. 2017. 100 f. Dissertação (Mestrado em Matemática) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), Programa de Pós-Graduação em Matemática.

[3] ANTON, Howard; RORRES, Chris. **Álgebra linear com aplicações**. 10 ed. Porto Alegre: Bookman, 2012.

[4] ARINOS, Edgard José dos Santos. **Criptografia: aplicações no ensino fundamental e médio.** Campo Grande. 2014. 97 f. Dissertação (Mestrado) – Universidade Federal de Mato Grosso do Sul.

[5] BEHRENS, Fabiele. **Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira**. Curitiba. 2005. 134 f. Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Departamento de Direito.

[6] BONFIM, Daniele Helena. **Criptografia RSA**. São Carlos. 2017. 91 f. Dissertação (Mestrado) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

[7] DEUSAJUTE, Alexandre Machado. **Proposta de um mecanismo de segurança alternativo para o SIP utilizando o protocolo Massey-Omura aperfeiçoado com o uso de emparelhamentos bilineares**. São Paulo, 2010. 165 f. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo.

[8] DOMINGUES, Hygino H. **Fundamentos de aritmética**. São Paulo: Atual, 1991.

[9] FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**. Belas. 2010. 144 f. Dissertação (Mestrado) – Universidade de Lisboa, Faculdade de Ciências, Departamento de Matemática.

[10] FILHO, José E. R. V.; AZEREDO, Paula Prestes. Tecnologia, criptografia e matemática: da troca de mensagens ao suporte em transações econômicas. **Revista desenvolvimento socioeconômico em debate**. [S.I], v. 2, n. 2, p. 22-31. Jan, 2016. Disponível em: < https://www.researchgate.net/publication/314352364_Tecnologia_criptografia_e_matematica_da_troca_de_mensagens_ao_suporte_em_transacoes_economicas>. Acesso em: 17/12/19.

[11] GOLDWASSER, Shafi.; BELLARE, Mihir. **Lecture notes on cryptography**. Summer course “Cryptography and computer security” at MIT, 1999:1999, 1996.

[12] GONÇALVES, Adilson. **Introdução à álgebra**. 6 ed. Rio de Janeiro: IMPA, 2017.

[13] HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2016.

[14] HEFEZ, Abramo. **Curso de álgebra**, volume 1. 5 ed. Rio de Janeiro: IMPA, 2016.

[15] JANESCH, Oscar Ricardo; TANEJA, Inder Jeet. **Álgebra I**. 2 ed. Florianópolis: UFSC/EAD/CED/CFM, 2011.

[16] KOBLITZ, Neal. **A course in number theory and cryptography**. 2 ed. Springer Science & Business Media, 1994.

[17] MARQUES, Thiago Valentim. **Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula**. João Pessoa. 2013. 82 f. Dissertação (Mestrado) – UFPB|CCEN.

[18] NASCIMENTO, Mauri Cunha do; FEITOSA, Hércules de Araujo. **Elementos da teoria dos números**. São Paulo. 2013. Disponível em: < http://wwwp.fc.unesp.br/~mauri/TN/TN.pdf>. Acesso em: 25/11/ 2020.

[19] PAAR, Christof ; PELZL, Jan. **Understanding Cryptography**. Springer Science & Business Media, 2010.

[20] ROHR, Altieres. Quanto tempo um computador precisa para quebrar sua senha?. G1, 2015. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/quanto-tempo-um-computador-precisa-para-quebrar-sua-senha.html> Acesso em: 14/01/2020.

[21] ROSEN, Kenneth H. **Elementary number theory and its applications.** Addison-wesley Publishing Company, 1986.

[22] SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 3 ed. Rio de Janeiro: IMPA, 2018.

[23] SARTORI, Karina Kfouri. **Curvas elípticas:** algumas aplicações em criptografia e em teoria dos números. Campinas. 2006. 65 f. Dissertação (mestrado em Matemática) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

[24] SINGH, Simon. **O livro dos códigos**. Rio de Janeiro: Record, 2001.

[25] SOUSA, Antonio Nilson Laurindo. **Criptografia de chave pública, criptografia RSA**. Rio Claro. 2013. 57 f. Dissertação (Mestrado) – Universidade Estadual Paulista Júlio de Mesquita Filho, Instituto de Geociências e Ciências Exatas.

[26] STALLINGS, William. **Criptografia de redes: princípios e práticas**. 6 ed. São Paulo: Pearson Education do Brasil, 2015.