Universidade Federal do Maranhão
Mestrado Profissional em Matemática
Curso de Pós-graduação em Matemática

Luiz Alves de Souza Neto

Aritmética Modular e Criptografia no Ensino Básico

São Luís
2014

Luiz Alves de Souza Neto

Aritmética Modular e Criptografia no Ensino Básico

Dissertação apresentada ao Curso de Matemática da Ufma, como requisito para a obtenção parcial do grau de MESTRE em Matemática.

Orientador: João Coelho Silva Filho

Doutor em Matemática

São Luís

2014

Luiz Alves de Souza Neto

Aritmética Modular e Criptografia no Ensino Básico

Dissertação apresentada ao Curso de Matemática da Ufma, como requisito para a obtenção parcial do grau de MESTRE em Matemática.

Aprovado em 28 de Agosto de 2014

BANCA EXAMINADORA

João Coelho Silva Filho

Doutor em Matemática

José Cloves Verde Saraiva

Doutor em Matemática

Mário Tanaka Filho

Doutor em Matemática

FICHA CATALOGRÁFICA PREPARADA PELA BIBLIOTECA CENTRAL DA UFMA.

Souza Neto, Luiz Alves

Aritmética modular e Criptografia no ensino básico

Luiz Alves de Souza Neto - São Luís

UFMA, 2014.

64f. : il.

Impresso por computador (Fotocópia).

Dissertação (Mestrado em Matemática)

Universidade Federal do Maranhão, 2014.

Orientador: João Coelho Silva Filho.

1 - Criptografia 2 - Diffie-Hellman 3 - Aritmética Modular

4 - Chaves 5 - Simétrica 6 - Assimétrica 7- Matrizes

CDU 004.056.65:51

À minha família.

Dedico

"Se as leis da Matemática referem-se à realidade, elas não estão corretas; e, se estiverem corretas, não se referem à realidade.".

Albert Einstein

Agradecimentos

Agradeço a Deus, por sempre me acompanhar nos caminhos de minha vida, guiando e ajudando nos momentos difíceis.

Agradeço aos meus pais, pelo apoio dado e por todo o esforço para que eu pudesse atingir os meus objetivos.

Agradeço a minha esposa Sildenice, pela paciência que teve comigo nos momentos de maior stresse e por me apoiar sempre.

Agradeço aos meus irmãos, por estarem sempre por perto, em todos os momentos, ofereçendo apoio quando precisei.

Agradeço a meu orientador João Coelho, pelo seu apoio e compreensão. Por sugerir caminhos e me ajudar a conduzir este trabalho.

Agradeço a todos os professores do Mestrado Profissional em Matemática.

Agradeço à UFMA e ao IMPA a SBM, conjuntamente com a Capes, por viabilizarem a realização deste Mestrado Profissional em Matemática.

Agradeço a todos os meus amigos, por terem sempre uma expectativa de vitória com relação aos meus projetos.

Resumo

Neste trabalho, será apresentado o contexto histórico da criação e desenvolvimento da criptografia passando pelo Império Romano até os dias atuais com os seus poderosos algoritmos de encriptação utilizando chaves públicas e privadas em sistemas simétricos e assimétricos evidenciando procedimento do protocolo da troca de chaves de Diffie-Hellman com uma aplicação prática que poderá ser utilizado como propostas de atividades em sala de aula pelo professor para o ensino de Aritmética Modular, Matrizes e Funções. Dessa forma, a abordagem do tema Aritmética Modular e Criptografia na Educação Básica são formas motivadoras para o ensino de conteúdos relacionados como expressões numéricas, funções, funções inversas, matrizes, divisibilidade no intuito de motivar o aluno a comtemplar a matemática de forma prática e contextualizada.

Palavras-Chave: Criptografia, Diffie-Hellman, Aritmética Modular, Chaves, Siméticra, Assimétrica, Matrizes.

Abstract

In this work, the history of creation and development of encryption is presented through the Roman Empire to the present day with its powerful encryption algorithms using public and private keys in symmetric and asymmetric systems showing the protocol of exchange of keys procedure Diffie-Hellman with a practical application that can be used as proposals for activities in the classroom by the teacher for teaching modular arithmetic, arrays and functions. Thus, the approach to the subject and Modular Arithmetic Cryptography in Basic Education are motivating ways to teach content related to numerical expressions, functions, inverse functions, arrays, severability in order to motivate the student to contemplate the mathematics in a practical and contextualized .

Keywords: Encryption, Diffie-Hellman, Modular Arithmetic, Keys, Symmetric, Asymmetric, Arrays.

Sumário

Lista de Tabelas

Lista de Figuras

Introdução

A criptografia é um método de transpor dados de informações em outra de forma ilegível, de maneira que a mensagem enviada possa ser compreendida apenas pelo destinatário, ou seja, é a garantia do sigilo na comunicação entre o emissor e receptor através de um canal.

A criptografia é uma aplicação muito importante da Artimética Modular, essa teoria dos números é o estudo das propriedades dos números inteiros onde estão abordados grandes problemas matemáticos relacionados aos números primos de fundamental importância para o estudo de criptografia.

Deste a antiguidade houve a necessidade de manter em sigilo informações de mensagens enviadas, dessa forma foi preciso encontrar técnicas para codificar as informações sem que elas pudessem ser interceptadas e lidas por outra pessoa não autorizada. Dessa forma a criptografia tem por objetivo possibilitar que somente o emissor e receptor consigam interpretar as informações, dificultando que eventuais intrusos possam desvendar a mensagem transmitida.

Inicialmente seus procedimentos não exigiam grandes conhecimentos de matemática, sendo utilizados métodos simples, como por exemplo, a substituição de letras através de símbolos, por procedimentos de contagem, ou simplesmente por números, Oliveira[15].

A criptografia estava presente no sistema de escrita dos egípcios. Os romanos utilizaram um famoso sistema chamado código César ou cifra de César (50 A.C). É um tipo de técnica de substituição na qual cada letra do texto é substituída por outra. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim por diante. A cifra de César era utilizada para fins militares, onde a mensagem tinha que chegar aos comandantes da tropa e serem lidos para executarem uma ação, caso fosse interceptado pelo inimigo não poderiam ser entendidas. A cifra de César somente foi quebrada quase mil anos depois com os estudiosos Árabes com a técnica chamada análise

de frequência, onde se verifica qual a letra do alfabeto que mais aparece tanto em cifra como no alfabeto do idioma.

As transformações desenvolvidas pela criptografia foram acompanhadas pelo desenvolvimento da criptoanálise - a "quebra" de códigos e cifras. A descoberta e aplicação, desde cedo, de análise de frequência para a leitura de comunicações criptografadas, muitas vezes, alterou o curso da história. Conforme Coutinho: "A criptografia tem uma irmã gêmea na arte de decifrar códigos secretos, ou criptoanánalise.",Oliveira[15].

O singilo é uma preocupação histórica e, ao mesmo tempo, cotidiana. Os processos pelos quais informações enviadas eletronicamente são codificadas dependem, essencialmente, do uso da matemática mais utilizada nas aplicações à criptografia. Questão referente à aritmética modular, funções, matrizes, análise combinatória, são exemplos de assuntos do currículo básico da matemática que são aplicados na criptografia.

A utilização da criptografia em sala de aula pode motivar o aluno a se interessar pela matemática, ajudando o professor como uma proposta alternativa e dando suporte para apresentação de conceitos importantes dentro da teoria dos números.

As aplicações dos métodos matemáticos de criptografia podem levar em conta a utilização de recursos como o computador e implementação de algoritmos simples para descrever passos na resolução de problemas utilizando a aritmética modular.

A inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade, criando dessa forma, atividades lúdicas e diferenciadas.

"É importante destacar que a Matemática deverá ser vista pelo aluno como um conhecimento que pode favorecer o desenvolvimento do seu raciocínio, de sua sensibilidade expressiva, de sua sensibilidade estética e de sua imaginação", PCN[17].

Isso indica que o ensino da matemática deve ser tido como facilitador de concepções para aprimorar as formas de raciocínios, para resolver situações-problema, apresentar resultados em formas de argumentações em conjecturas.

O ensino da Matemática nas séries finais do ensino fundamental deve privilegiar as aplicações práticas pela exploração de situações-problema, o aluno reconhecerá diferentes padrões aritméticos, estabelecer relação entre duas grandezas, definir passos

para um algorito, e chegar a uma explicação dos procedimentos feitos no problema.

Assim, o aprendizado da matemática pode se tornar mais fácil e significativo, o que vem a contribuir não só com o desenvolvimento da vida escolar do aluno, mas também com seu crescimento pessoal.

Será trabalhado o ensino da criptografia como auxiliadora em temas da aritimética levando em conta atividades didáticas que aliam conteúdos de matemática do ensino fundamental e médio a este tema, possibilitando ao professor um trabalho com temas atuais e aos alunos contato com um ramo novo, tendo como fonte motivadora a arte de cifrar, criptografar, esconder informações singilosas.

Assim o professor em sala de aula pode abordar propostas de atividades que contemple conteúdos como divisão euclidiana, algoritmo de Euclides estendido, equações do primeiro grau, teorema do resto, congruência modular e números primos, baseadas nas competências e habilidades constantes nos PNS.

Os procedimentos práticos levarão em conta situações onde se definirá conceitos de chaves públicas e privadas para decifrar as mensagens criptografadas, tipos de criptografias e algoritmos. Modos simples para exemplificar contextos empregados que possam trazer segurança na transmissão de informações, em situações de perigo, seja no serviço de atendimentos de bancos, ou na transmissão de segredos pessoais, comerciais, militares ou industriais.

No primeiro capítulo deste trabalho irá trazer o contexto histórico pelos quais passou a Criptografia como uma aplicação de um método muito importante no desenvolvimento da Aritmética Modular. O capítulo II desenvolverá os principais conceitos da Aritmética Modular e seus algoritmos nescessários para a compreensão de Criptografia, mostrando o processo da divisão de Euclides para encontrar o MDC e primos entre si. No capítulo III será mostrado a fundamentação da criptografia e seus principais sistemas aritméticos utilizado e o conceitos de chaves públicas e privadas e aplicações que podem ser utilizadas na sala de aula para melhor entendimento pelo aluno juntamente com a aplicação do algoritmo RSA utilizados nos computadores atuais e sua codificação com os símbolos. No capitulo IV será apresentado aplicações de criptosistemas envolvendo funções e matrizes como formas em que a Aritmética Modular pode ser envolvido com temas diversos dentro da Matemática.

Capítulo 1

História da Criptografia

Será mostrado neste capítulo contextos histórico em que a criptografia evoluiu em seus métodos de cifragem, fornecendo dados para que o Professor de Matemática possa ter ideias de como introduzir este assunto no ensino básico.

Um dos primeiros textos sobre códigos secretos foi escrito pelo geógrafo e historiador grego Heródoto (485 a.C. - 420 a.C.) na sua principal obra, conhecida por "as histórias de Heródoto", é retratada a história dos conflitos entre a Pérsia e a Grécia no início do século V a.C; atribuiu, pois, à habilidade da escrita secreta a causa de a Grécia não ter sido conquistada por Xerxes, cuja intenção, à época, era formar um grande exército para invadir a Grécia.

> O perigo de ser de scoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os gregos, SINGH[19]

Dessa forma os gregos puderam se antever e se preparar para uma batalha e formar um exercicito capaz de derrubar o inimigo na batalha portanto a arte de esconder menssagens foi descrita no ditos históricos de Herodoto.

1.1 Cifra de Cesar

Um exemplo histórico é uso do método de transposição, que está no primeiro aparelho criptográfico militar chamado de Bastão de Licurgo, que data de V a.C.

Por exemplo, MESTRADO PROFISSIONAL EM MATEMÁTICA, em uma tabela de 5 colunas, utilizando a letra H no lugar do espaço, teríamos o seguinte.

M	E	S	T	R
A	D	O	H	P
R	O	F	I	S
S	I	O	N	A
L	H	E	M	H
M	A	T	E	M
A	T	I	C	A

Tabela 1.1: Exemplo de Cifra

Que dá no seguinte texto tirando de cima para baixo:

MARSL MAEDO IHATS OFOET ITHIN MECRP SAHMA

É usual separar o texto inteligivel em blocos de 5. O exemplo mais clássico é a cifra de César. Adotada por César na época do Império Romano. Simples e relativamente eficiente.

A cifra de César utiliza tabela alfabética com números correspondentes e chave numérica. Chave: É uma informação utilizada em criptografia para codificar e decoficar a mensagem.

Algoritmo simples.

Algoritmo: C = (M + T)

Onde: C = Cifra

M = Mensagem

T = Chave

Caso a cifra C execeda em 26 devemos tirar a diferença entre $(C - 26)$ e encontrar a respectiva correspondência na tabela

Pelo nosso alfabeto podemos ter as correspondências:

O símbolo "!" representa o espaço entre duas frases da mensagem.

SOLUÇÃO = Os valores menores ou iguais a 26 que são considerados o próprio resto.

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

Tabela 1.2: Correspondência Letras e Números

MENSAGEM = ISTO É GREGO
CHAVE T = 15
CRIPTO = XHID!T!VGTVD

$$\boxed{I = (09 + 15) = 24 \longrightarrow X}$$
$$\boxed{S = (19 + 15) = 34 - 26 \longrightarrow 8 \longrightarrow H}$$
$$\boxed{T = (20 + 15) = 35 - 26 \longrightarrow 9 \longrightarrow I}$$
$$\boxed{O = (15 + 15) = 30 - 26 \longrightarrow 4 \longrightarrow D}$$
$$\boxed{E = (05 + 15) = 20 \longrightarrow 20 \longrightarrow T}$$
$$\boxed{G = (07 + 15) = 22 \longrightarrow 22 \longrightarrow V}$$
$$\boxed{R = (18 + 15) = 33 - 26 \longrightarrow 7 \longrightarrow G}$$
$$\boxed{E = (05 + 15) = 20 \longrightarrow 20 \longrightarrow T}$$
$$\boxed{G = (07 + 15) = 22 \longrightarrow 22 \longrightarrow V}$$
$$\boxed{O = (15 + 15) = 30 \longrightarrow 4 \longrightarrow D}$$

PORTANTO A FRASE CRIPTOGRAFADA É:

XHID!T!VGTVD

1.2 Análise de Frequência

Por volta de 750 d.C; apesar do grande desenvolvimento em ciências matemática, as suas grandes contribuições não foi na criptografia, e sim na criptoanálise, técnica que permite decifrar uma mensagem criptografada sem utilização de chaves, de onde surgiu o método de análise de frequência. Esse método consiste em verificar o aparecimento, a frequência de uma determinada letra do alfabeto, com a frequência de algumas letras no texto cifrado fazendo correspondência entre elas.

A Análise de Frequência foi descoberta pelo matemático Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi onde na década de 80 foi encontrado um arquivo em Istambu na Turquia com o título “Um manuscrito sobre a decifração de mensagens criptográficas”

de sua autoria.

A técnica de Al-Kindi basea-se em decifrar uma mensagem codificada, quando se domina o idioma. Para isso, deve-se encontrar um texto diferente, no mesmo código, suficiente longo para preencher uma página e fazer essa análise das frequências. Dessa forma, o símbolo que aparecer com maior frequência no texto é chamada de "primeira", a segunda mais frequente recebe o nomes e "segunda" e assim por diante, até todas as letras ou símbolo do texto serem contadas. Depois faz-se o exame do texto cujo deciframento se pretende elaborar e os símbolos e letras são classificados em relação à frequência. O símbolo que aparecer com maior frequência será substituído pela letra que foi denominada como "primeira", o símbolo seguinte mais frequênte é substituído pela "segunda", o terceiro símbolo é substituído pela "terceira" sucessivamente e até o último símbolo até todos serem transformados em uma frase legível.

Para aplicação da análise de frequência, precisamos conhecer qual é a tabela de porcentagem de aparição de cada letra nos textos de uma determinada língua ou código de símbolos. A frequência média de cada letra na Língua Portuguesa está apresentada na tabela 1.3.

Letra	Frequência(%)	Letra	Frequência(%)
a	14,60	n	5,00
b	1,00	o	10,70
c	3,80	p	2,50
d	4,90	q	1,20
e	12,50	r	6,50
f	1,00	s	7,80
g	1,30	t	4,30
h	1,20	u	4,60
i	6,10	v	1,60
j	0,40	w	0,01
k	0,02	x	0,20
l	2,70	y	0,01
m	4,70	z	0,40

Tabela 1.3: Tabela de Frequência

Sabendo a frequência de aparição das letras no alfabeto podemos fazer a correspondência entre os símbolos do texto em que queremos decoficar. Isto irá gerar equivalências que geralmente será suficiente para quebrar o código e ler toda a mensagem.

1.3 Máquinas de Cifragem.

De acordo com SINGH [19], a primeira máquina criptográfica que se tem registro foi inventada no século XV pelo arquiteto italiano Leon Alberti, um dos criadores da cifra polialfabética. A máquina do italiano era composta de dois discos de cobre. O maior era fixo e o outro, o menor, era móvel. Nos discos continham o alfabeto ao longo das bordas extremas, no disco maior, o alfabeto original em letras maiúsculas e, no disco menor, o alfabeto cifrado em letras minúsculas. Pode-se girar o disco menor para gerar uma mensagem utilizando a cifra de César. O disco de cifras foi utilizado por séculos.

Em 1918, os inventores alemães Arthur Scherbius e Richard Ritter fundaram uma empresa, a Scherbius&Ritter. Dentre os seus projetos era substituir os sistemas de criptografia, que eram muito básicos, utilizados na Primeira Guerra Mundial. Patentearam uma invenção de uma máquina de cifra mecânica, onde foi batizada popularmente como máquina Enigma.

A Sherbius produziu e vendeu a Enigma em grande escala em 1925, pelo fato das autoridades alemãs acreditavam na segurança absoluta que ela proporcionava. Trinta mil máquinas foram vendidas e utilizadas, nas duas décadas posteriores, pelo exército alemão. A Enigma era extremamente forte e, por treze anos, os criptoanalistas franceses e britânicos acreditaram que mensagens cifradas por ela eram impossíveis de serem acessadas sem o conhecimento da chave. Mas um matemático chamado Alan Turing em um trabalho árduo conseguiu quebra-la na primeira metade da década de 40. O fato ocorreu na sede da Escola de Cifras e Códigos do Governo da Inglaterra, o aparelho de quebra da criptografia da Enigma era chamado de Bombas. A quebra da criptografia utilizada pelos nazistas deu aos Aliados uma vantagem fundamental, que, de acordo com historiadores, encurtou a guerra por mais de dois anos, salvando muitas vidas.

Com base nas ideias de Alan Turing em criptoanálise, foi fundamental para o desenvolvimento de diversos outros equipamentos computacionais, um desses aparelhos que desempenha a função de decifrar mensagens foi criada na inglaterrar denominada de Colossus, foi utilizado para decifrar as codificações feitas pela máquina Lorenz, empregada nas comunicações de Hitler e seus generais. O Colossus era constituído de válvulas eletrônicas bem mais rápidas do que os antigos eletromecânicos utilizados nas bombas e podia ser programado. Dessa forma ele é considerado o primeiro computador moderno que surgiu pela necessidade militar de se saber o significado dos códigos secretos dos inimigos.

Figura 1.1: Máquina Inigma

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos, SINGH[19]

A partir da década de 70 a criptografia assumiu um importante papel na segurança nos tráfegos de dados pela internet como a criação de algoritmos eficientes onde temos como destaque o RSA.

Capítulo 2

Aritmética Modular

2.1 Algoritmos

Algoritmos é uma sequência de procedimentos e instruções finitas e ordenadas, com um esquema de processamento que permite a resolução de problemas, cálculos etc. Derivada do nome de Al Khowarizmi, matemático árabe do século 19. Ele surgiu da necessidade de fazer cálculos sem o auxílio de ábacos, dedos e outros recursos.

Pode-se exemplificar a noção dessa estrutura da seguinte forma: um algoritmo para se vestir pode especificar que você vista primeiro as meias e os sapatos antes de vestir a calça enquanto outro algoritmo especifica que você deve primeiro vestir a calça e depois as meias e os sapatos. Fica claro que o primeiro algoritmo é mais difícil de executar que o segundo apesar de ambos levarem ao mesmo resultado.

Algoritmo ensina a ordenar o pensamento lógico em diversas situações do cotidiano principalmente em se tratando de conteúdo matemático levando ao aluno o desenvolvimento de método que traduza uma sequência lógica de passos. Segundo Valéria[13], podemos ter o seguinte:

1. Ler atentamente o enunciado - para resolver um problema é necessária sua compreensão;
2. Retirar do enunciado os dados.
3. Determinar as ações para atingir o resultado.
4. Desenvolver o algoritmo e solucionar o problema.

Sem os algoritmos não seria possível desenvolver sistemas de criptografia seguros e capazes

de assegurar que a informação entre emissor e receptor não tenha interferência e não seja extraviada.

2.2 Teorema Fundamental da Aritmética

Teorema 2.2.1. Todo inteiro $a \geq 2$ pode ser escrito como produto de números primos. Esta decomposição é única exceto pela ordem dos fatores primos.

O método do Crivo de Eratóstenes nos mostra que dado um número natural a, existe um número primo p_0 tal que ou $a = p_0$, ou a é um múltiplo não trivial de p_0; isto é, $a = p_0a_1$, com $1<a_1< a$.

Se a segunda possibilidade é verificada, segue que existe um número primo p_1, tal que ou $a_1 = p_1$, ou $a_1 = p_1a_2$, onde $1 < a_2< a_1< a$. Assim,

$a = p_0p_1$; ou $a = p_0p_1a_2$.

Continuando a argumentação para a_2, temos $a = p_0p_1p_2$, ou, $a = p_0p_1p_2a_3$, para algum primo p_2 e $1 < a_3<a_2<a_1<a$.

Note que desigualdades como a acima não podem continuar indefinidamente. Logo, para algum r, o número a_r é um primo p_r, obtendo desse modo uma decomposição de a em fatores primos:

$$a = p_1p_2 \dots p_r.$$

Proposição 2.2.1. (Euclides) Todo número natural $a \in \mathbb{N}$, $a > 1$, ou é primo, ou se escreve como produto de números primos.

Prova da existência de infinitos número primos. Os números $a \in \mathbb{N}$ que têm mais de dois divisores são chamados números compostos. Suponha por absurdo que os números primos sejam em número finito e seja a o produto de todos eles. O número $a + 1$ não seria primo pois ele seria maior do que qualquer número primo. Logo, $a + 1$ sendo composto, ele seria múltiplo de algum número primo q. Mas sendo a também múltiplo de q, teríamos, que 1 seria múltiplo do número primo q, o que é um absurdo.

O método utilizado é chamado de redução ao absurdo sustentado em negar a afirmação que se quer provar levando-o a uma contradição.

2.3 Algoritmo de Euclides da Divisão

O algoritmo de Euclides, também conhecido como procedimento das divisões sucessivas, é um método simples e eficiente de encontrar o máximo divisor comum entre dois números inteiros diferentes de zero. É um dos algoritmos mais antigos, conhecido desde que surgiu nos Livros VII e X da obra Elementos de Euclides por volta de 300 a.C.

Existem dois números naturais q e r, unicamente determinados, tais que:

$b = aq + r$; com $0 \leq r < a$

O número b é chamado dividendo, o número a divisor, os números q e r são chamados, respectivamente, quociente e resto da divisão de b por a. Se $r = 0$, b é multiplo de a.

2.3.1 Algoritmo de Euclides Estendido

O Algoritmo de Euclides é um a das formas de se encontrar o MDC - máximo divisor comum de dois números inteiros. O MDC é um a combinação linear destes dois números. O Algoritmo de Euclides estendido, ao invés de retornar um valor único, fornece a combinação linear , muito útil quando os inteiros são primos entre si.

O algoritmo de Euclides pode ser estendido para provar que existem inteiros x e y tais que $mdc(a, b) = ax + by$.

Teorema 2.3.1. Se $d = mdc(a, b)$ então existem x e y inteiros, de maneira que $ax + by = d$.

Exemplo 2.3.1. O $mdc(120, 23) = 1$. 120 e 23 são números inteiros, primos entre si porque não existe um divisor maior do que 1 que divida ambos.

O Algoritmo de Euclides estendido retorna $ax + by = mdc(a,b)$, ou seja, $120.(-9) + (23).(47) = mdc(120, 23)$. Para encontrar o $mdc(120, 23)$ usando o Algoritmo de Euclides, coloca-se da seguinte forma:

(1)	120/23 =	5 resta 5
(2)	23/5=	4 resta 3
(3)	5/3 =	1 resta 2
(4)	3/2 =	1 resta 1
(5)	2/1 =	2 resta 0

$mdc(120, 23) = 1$. Para encontrar-mos os valores de x e y podemos proceder da seguinte forma.

5 = 1.120 - 5.23
3 = 1.23 - 4.5 Substituindo o 5 temos
3 = 1.23 - 4.(1.120 - 5.23)
3 = -4.120 + 21.23
2 = 1.5 - 1.3 Substituindo o valor de 5 e 3 temos
2 = 1(1.120 - 5.23) - 1(-4.120 + 21.23)
2 = 5.120 - 26.23
1 = 1.3 - (1).(2). Novamente substituindo 3 e 2
1 = 1(-4.120 + 21.23) - 1(5.120 - 26.23)
1 = -9.120 + 47.23

portanto, $x = -9$ e $y = 47$ e temos: $mdc(120, 23) = 120.(-9) + 47.23$.

2.4 Congruência

A aritmética modular envolve o conceito de congruência. Congruência é a relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto, SÁ[20]. Por exemplo, o número 10 é congruente ao número 3 módulo 7, pois ambos deixam resto 3, ao serem divididos por 7. Representamos essa congruência do exemplo por $10 \equiv 3 \ mod \ 7$. Foi Gauss que observou que usávamos com muita frequência frases do tipo "a dá o mesmo resto que b quando divididos por m" e que essa relação tinha um comportamento semelhante à igualdade. Gauss introduziu uma notação específica para este fato e que denominou de congruência.

Muito se tem escrito sobre esse tema, principalmente nos livros sobre teoria dos números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

O estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas ainda não é muito comum. Diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, criptografia, calendários e diversos fenômenos periódicos estão diretamente ligados ao tema, conforme mostraremos em nosso estudo.

É um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental e Médio, é gerador de excelentes oportunidades de contextualização no processo de ensino aprendizagem de matemática.

Devemos trabalhar com alguns aspectos teóricos sobre a aritmética modular e mostrar exemplos de aplicação desse importante e interessante tema da área de teoria dos números.

Propriedades relacionadas à congruência mostram que as definições vem através de alguns exemplos que podem ser desenvolvidos e colocados a alunos da Educação Básica e Médio, ainda não familiarizados com o tema, como introdução ao assunto específico.

Antes de avançarmos nos próximos capítulos deveremos definir alguns teoremas em Congruência Modular.

Definição 2.4.1. Sejam a, b e $n \in \mathbb{Z}$. Diz-se que a e b são congruentes módulos n se os restos de a e b quando dividido por $n$forem iguais. Se a e b são congruentes módulo n, escreve-se: $\boxed{a \equiv b \ mod \ n}$

Uma maneira equivalente de dizer isso, segundo SÁ[20], é afirmar que a diferença (a - b) ou (b - a) é divisível por n, ou que n é divisor dessa diferença. Veja um exemplo: $47 \equiv 43 \ mod \ 4$, logo $(47 - 43)$ é divisível por 4.

Exemplo 2.4.1. $12 \equiv 37 \ mod \ 5$. Pois, $12 = 2.5 + 2$ e $37 = 7.5 + 2$.

Exemplo 2.4.2. $15 \equiv -1 \ mod \ 4$. Pois, $15 = 3.4 + 3$ e $-1 = -1.4 + 3$.

Teorema 2.4.1. Sejam a, b, c, d, k, $n \in \mathbb{Z}$ com $n > 1$ e $k \geq 1$. Então as conduções seguintes são satisfeitas:

1º) $a \equiv a \ mod \ n$;
2º) $a \equiv b \ mod \ n \Longrightarrow b \equiv a \ mod \ n$;
3º) $a \equiv b \ mod \ n$ e $b \equiv c \ mod \ n \Longrightarrow a \equiv c \ mod \ n$;
4º) $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n \Longrightarrow a.c \equiv b.d \ mod \ n$;
5º) $a \equiv b \ mod \ n \Longrightarrow a^k \equiv b^k \ mod \ n$

Exemplo 2.4.3. Podemos notar que $9^4 \equiv 1 \ mod \ 5$. Pois, se $a \equiv 0 \ mod \ n$, estão $a = n.k$ e 9^4 - $1 = (9^2$ - $1)(9^2 + 1) = (80).(82) = (5).(16).(82)$.

Exemplo 2.4.4. Determinar o resto da divisão de 2^{30} por 17 utilizando as propriedades de congruência. Observe que:

$2^4 \equiv -1 \ mod \ 17$

Elevando ambos os membros da igualdade a 7, fica: $2^{28} \equiv -1 \ mod \ 17$ e multiplicando por 4, obtém-se:

$2^{30} \equiv -4 \ mod \ 17.$

Como $-4 \equiv 13 \ mod \ 17$, tem-se pelo teorema 2.4.2 :

$2^{30} \equiv 13 \ mod \ 17.$

Logo, o resto da divisão de 2^{30} por 17 é 13.

Exemplo 2.4.5. Calcular o resto da divisão de $(2006^{2006} + 2004^{2004})^{2005}$ por 5.

$(2006^{2006} + 2004^{2004})^{2005} \equiv (1^{2006} + (-1)^{2004})^{2005} \equiv 2^{2005}$. Como $16 = 2^4 \equiv 1$ mod 5. Podemos escrever $2^{2005} = (2^4)^{501}.2 \equiv (1)^{501}.(2) = 2$. Logo $(2006^{2006} + 2004^{2004})^{2005}$ deixa resto 2 quando na divisão por 5.

Exemplo 2.4.6. Questão pertencente ao banco de questões do site da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas). A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

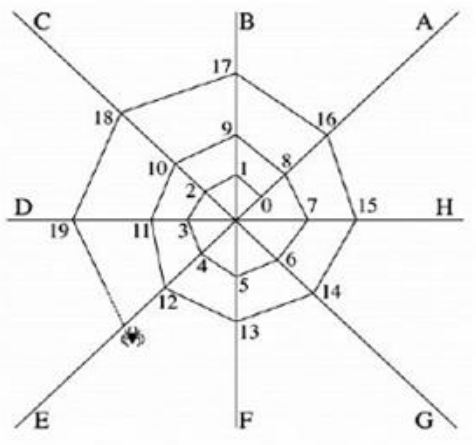

Figura 2.1: Exemplo da Telha de Aranha

Vejamos o que está acontecendo?

Cada fio forma uma progressão aritmética de razão igual a 8, pois os fios se repetem numa periodicidade a cada oito números, portanto um fio vem depois do outro de oito em oito. Dessa forma podemos observar uma correspondência em que cada fio é representado como múltiplos de 8. Os fios em A são números que divididos por 8 deixam

resto *zero* ($8.n$, com $n \in \mathbb{N}$). O fio B são os números onde a correspondência é ($8.n + 1$, com $n \in \mathbb{N}$), ou seja, são os que são múltiplos de 8 mais 1. O fio C representa os números que divididos por 8 deixam resto 2 ($8n + 2$, $n \in \mathbb{N}$), ou seja, múltiplos de 8 mais 2. Assim podemos inferir que a cada fio posterior até o fio H se matem com uma relação de formação semelhante, onde o fio H é definido pelos números que divididos por oito deixam resto 7. Então para sabermos em qual fio se encontra o número 118 temos que dividi-lo por 8. Vejamos o que está acontecendo?

Cada fio forma uma progressão aritmética de razão igual a 8, pois os fios se repetem numa periodicidade a cada oito números, portanto um fio vem depois do outro de oito em oito. Dessa forma podemos observar uma correspondência em que cada fio é representado como múltiplos de 8. Os fios em A são números que divididos por 8 deixam resto zero ($8.n$, com $n \in \mathbb{N}$). O fio B são os números onde a correspondência é ($8.n + 1$, com $n \in \mathbb{N}$), ou seja, são os que são múltiplos de 8 mais 1. O fio C representa os números que divididos por 8 deixam resto 2 ($8n + 2$, com $n \in \mathbb{N}$), ou seja, múltiplos de 8 mais 2. Assim podemos inferir que a cada fio posterior até o fio H se matem com uma relação de formação semelhante, onde o fio H é definido pelos números que divididos por oito deixam resto 7. Então para sabermos em qual fio se encontra o número 118 temos que dividi-lo por 8.

$$\boxed{\frac{118}{8} = 8.14 + 6}$$

Fazendo a divisão 118 por 8 verificamos que o resultado é $8.14 + 6$, ou seja, o resto 6 indica que o fio está simbolizado com o grupo de fios do G.

Os exemplos nos mostram que podemos encontrar qualquer fio através de um padrão quando divididos por 8 deixam o mesmo resto, portanto encontrar uma lógica para aplicar na resolução desse problema deixa claro que os fios forma uma congruência entre si no módulo 8. O número 15, por exemplo, é congruente ao número 23, no módulo 8, e isso significa que esses dois números deixam o mesmo resto quando divididos por 8.

$$\boxed{14 = 8.1 + 6} \text{ e } \boxed{22 = 8.2 + 6}$$

Simbolicamente, poderemos escrever: $14 \equiv 22 \ mod \ 8$.

Exemplo 2.4.7. Aritmética do relógio

O relógio analógico mostra um tipo bem comum de congruência onde temos o módulo 12. Fazendo alguns exemplos temos que o número 13 é congruente a 1 hora no

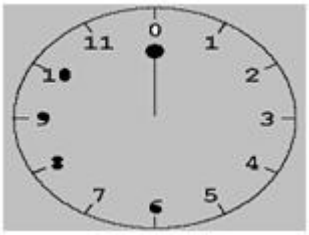

Figura 2.2: Congruencia no Relógio

módulo 12. Quando divididos por 12 deixam reste igual a 1. 18 horas é congruente a 6 horas no módulo 12, pois quando divididos por 12 deixam o mesmo resto.

Como vemos a seguir:

$$1 \equiv 13 \equiv 25 \equiv mod\ 12$$
$$5 \equiv 17 \equiv 29 \equiv mod\ 12$$

Nosso contexto do dia a dia está repleto de aplicações simples de Aritmética Modular. Indubitavelmente, as mais usuais são os chamados Sistemas de Identificação que estão em todo tipo de documentos, SÁ[20].

Um exemplo clássico é o Cadastro de Pessoas Físicas, chamado comumente de CPF, documento cuja numeração possui 11 dígitos, sendo os dois últimos chamados dígitos de controle ou verificação. Eles têm a função de evitar fraudes e enganos e são encontrados em função dos 9 primeiros.

Exemplo 2.4.8. (CPF)

Uma aplicação prática muito importante de Aritmética Modular é o caso do CPF (Cadastro de Pessoa Física), onde se faz a verificação do dígito de controle. O número do CPF é constituido de 11 digitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos- dígitos de controle ou de verificação.

O décimo dígito(o primeiro dígito verificador) é um caso de congruência módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Sendo a_1, a_2, a_3, a_4, a_6, a_7, a_8, a_9, a sequência formada pelos 9 primeiros dígitos, então devemos multiplicá-los, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e somar os produtos obtidos. O dígito que está faltando, vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $(S - a_{10})$, deve ser múltiplo de 11, ou seja, $(S - a_{10}) \equiv 0 mod$ 11. Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Exemplo 2.4.9. Se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235 343 104, o primeiro dígito de controle será obtido da seguinte maneira:

$$\begin{array}{ccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

Efetuando as multiplicações correspondentes, teremos:

$2.1 + 3.2 + 5.3 + 3.4 + 4.5 + 3.6 + 1.7 + 0.8 + 4.9 = 116.$

Dividindo o número 116 por 11, teremos: $116 = 11.10 + 6$. Dessa forma, o primeiro dígito de controle será o algarismo 6.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9. Vejamos:

$$\begin{array}{cccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

Efetuando as multiplicações, teremos:

2.0+3.1+5.2+3.3+4.4+3.5+1.6+0.7+4.8+6.9=145, onde:

$145 = 11.13 + 2.$

Logo, o segundo dígito de controle é o 2.

Concluímos então que, no nosso exemplo, o CPF completo seria: 235 343 104 62

Se o resto da divisão fosse 10, ou seja, se o número obtido fosse congruente ao 10 módulo 11, usaríamos, nesse caso, o dígito *zero*.

Um tipo também muito comum é utilizado nos sistemas de identificação é o ISBN e o código de barras que se apoiam na Aritmética Modular. Os códigos de barras e o ISBN são sistemas simples e precisos independente da língua, utilizando a linguagem dos números, SÁ[20].

Exemplo 2.4.10 (Calendário)**.**

O professor poderá encontrar vários tipos de aplicações de forma a motivar o ensino de aritmética modular utilizando um calendário onde é dada uma data e descobrir em que dia da semana caiu. Para o aluno parece obra de adivinhação ou de memória de

computador, mas se trata de um processo onde se pode perceber um algoritmo desenvolvido com base em uma congruência módulo 7.

Para procedermos com um algoritmo prático para achar as datas no calendário devemos ter um caledário antigo, podemos ver que o dia 1º de janeiro de 1900 caiu em uma segunda-feira. Fazendo esse dia como início do problema, tendo que não podemos calcular datas antes de 1900 para não ocorrer erros.

Devemos ter a noção que em um ano não bissexto tem 365 e $365 \equiv 1 \ mod \ 7$, mostra que uma data cai um dia da semana depois no ano seguinte, para anos não bissextos. Os anos bissextos são encontrados como os múltiplos de 4 mas não de 100, a exceção de ser múltiplo de 400, então os anos bissextos depois de 1900 são os da forma onde temos que dividir o quanto o ano exceder 1900 por 4, o quociente exato será quantos anos bissextos ocorreram no período e, para esses anos, $366 \equiv 2 \ mod \ 7$, ou seja, no ano seguinte a mesma data cai dois dias da semana à frente.

Assim a lei de correspondência formada pode descobrir quando caiu 1º de janeiro nesse ano. Basta somar $(ano - 1900)$ com a quantidade de anos bissextos, para descobrirmos quantas vezes a data foi deslocada.

Encontrando esse número, basta dividi-lo por 7 e o resto dará o deslocamento de dias da semana. Por exemplo, no ano de 2014:

$$(2014 - 1900) + \frac{114}{4} = 142$$

Que dividido por 7, deixa resto 2. Logo ocorreram apenas dois deslocamentos, ou seja, 1º de janeiro de 2014 caiu em uma quarta-feira.

Figura 2.3: Janeiro de 2014

Em relação ao deslocamento provocado pelo mês, devemos entender a tabela 2.2, formulada para anos não bissextos.

Mês	Deslocamento
Janeiro	0
Fevereiro	3
Março	3
Abril	6
Maio	1
Junho	4
Julho	6
Agosto	2
Setembro	5
Outubro	0
Novembro	3
Dezembro	5

Tabela 2.2: Deslocamento dos Dias nos Meses

De acordo com a tabela 2.2 podemos ter as seguintes disposições: Janeiro desloca 1º de fevereiro em 3 dias da semana para frente, pois são 31 dias divididos por 7, obtemos 4 semanas e 3 dias. O mês de fevereiro não desloca o mês seguinte nos anos bissextos, pelo fato de ser 4 semanas. Abril é deslocado em 3 dias por março. Dessa forma temos 6 dias acumulados de deslocamento. Maio é deslocado em seus dias 2 por abril, pois são 30 dias e, dividindo por 7, são 4 semanas e 2 dias. Dias acumulados são 8 de deslocamento, e 8 dividido por 7 deixa resto 1, ou seja, a semana é deslocado em 1 dia.

Assim, estamos capacitados a descobrir quando foi o dia 1º em um referido mês de um ano. Por exemplo, o dia 1º de fevereiro de 2014 caiu em uma sábado, pois 1º de janeiro de 2014 foi quarta e o mês de janeiro provoca 3 dias de deslocamento em fevereiro quarta mais três dias resulta em sábado.

Figura 2.4: Fevereiro de 2014

Podemos verificar a ocorrência de uma congruência que tomando dia 1º como referência, a cada 7 dias voltamos a cair no mesmo dia da semana. Então os dias 9, 16, 23 e 30 (exceto fevereiro não bissexto) serão o mesmo dia da semana igualmente o dia 1º.

É de simples observação então que sendo número de dia, $(n-1)$ é múltiplo de 7 e cai no mesmo dia da semana que o dia 1º. Assim, o resto deixado na divisão de $(n-1)$ por 7 sinaliza o número de deslocamento nos dias da semana provocado pela data.

Um rápido roteiro para fazer mentalmente esse processo seria:

Para encontrar o dia da semana que caiu a data $A/B/C$, faça:

1. Encontre $x = C$ - 1900;
2. Encontre y, a parte inteira do quociente de x por 4;
3. Encontre z, recordando da tabela dos meses;
4. Encontre w, tal que seja o resto da divisão de $n-1$ por 7, ou seja, $w \equiv (n-1)\ mod\ 7$ e
5. Calcule $x + y + z + w = r$, divida por 7 e obtenha seu resto. Esse número indica o número de deslocamentos em relação à segunda feira.

Ou seja, $x + y + z + w \equiv mod\ 7$

Que dia da semana foi 20 de julho de 1984?

- 1º) $1984 - 1900 = 84$.
- 2º) 84 dividido por 4 resulta na parte inteira 21.
- 3º) pela tabela, julho vale 6.
- 4º) $20 - 1 = 19$, que dividido por 7 gera resto 5;
- 5º) $84 + 21 + 6 + 5 = 116$, que dividido por 7 deixa resto 4.

Aplicando 4 deslocamentos à segunda feira, observamos que 20 de julho de 1984 foi uma sexta feira(Ver figura 2.5).

Portanto temos que construindo passos elaborados com determinados algoritmos simples pode levar-nos a criar situações relativas a outras técnicas matemáticas como o caso dos sistemas de identificação, criptografia e dias da semana, onde se mostram contextualizadas e condizentes com a faixa etária dos alunos das séries finais do ensino fundamental e no ensino médio. São de fácil compreensão e não exigem conhecimentos

Figura 2.5: Julho de 1984

matemáticos fora das operações fundamentais, ou seja, é uma ótima oportunidade para introduzir e mostrar a relevância das congruências.

Essas técnicas são de grande importância pelo fato de introduzir formas de raciocínio lógicos descritos em forma de algoritmos e se torna uma ferramenta para futuras conjecturas por parte dos alunos. Levando o aluno a uma reflexão e análises de instrumentos que nortearam no conteúdo de matérias corelatas a aritmética, álgebra e áreas afins.

Capítulo 3

Criptografia

É o estudo sobre o envio de mensagens criptografadas com chaves onde será útil o conhecimento de congruência modular e exponenciação, e um pouco de lógica. Portanto, o professor poderá nortear, de inicio, situações problemas que acontecem durante todos os instantes nas comunicações comerciais como uma compra pela internet, utilização de terminais de autoadentimentos dos bancos com situações simples e as suas motivações para a sua utilização hoje em larga escala, desenvolvimento e implementação de novas técnicas, fazendo o aluno mostrar-se interesse em pesquisar e se aprofundar no assunto.

3.1 Criptografia de Chave Pública- Criptografia Assimétrica

A criptografia de chave pública ou criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. Dessa forma obtemos uma comunicação mais segura através de canais de comunicação inseguros.

Cada participante possui uma chave pública e uma privada. A chave privada é secreta, e só o proprietário a conhece, ao passo que a chave pública é compartilhada com todos que se comunicarão conosco.

Exemplo 3.1.1.

Fábio quer se comunicar com Ana de forma segura. Então, Fábio encripta a mensagem com a chave pública de Ana, de modo que a mensagem só pode ser aberta usando-se a chave privada de Ana que só ela possui.

É necessária que o emissor de mensagens, antes de enviar sua mensagem, utilize

a chave-pública do destinatário para encriptar a mensagem. A chave-pública é, a princípio, disponível a qualquer um. Ao receber a mensagem encriptada, o destinatário utiliza a chave-privada para decriptar a mensagem. Ou seja, qualquer pessoa pode enviar uma mensagem confidencial apenas utilizando chave- pública, mas esta mensagem só poderá ser decriptada com a chave- privada do destinatário.

Os sistemas de criptografia assimétrica, geralmente, são mais custosos computacionalmente, em relação aos simétricos; eles normalmente são utilizados para a distribuição da chave simétrica ao destinatário. Após esta passagem, utiliza-se a criptografia simétrica em cima dos dados.

Exemplos de algoritmos assimétricos muito utilizados: DAS, RSA, GPG.

3.2 Propostas de Atividades: Utilizando Chave Pública e Privada.

3.2.1 Chave Secreta Compartilhada- Criptografia simétrica

Este tipo de criptografia utiliza uma única chave. O emissor utiliza essa chave para encriptar a mensagem, e o receptor utiliza a mesma chave para descriptá-la (chave compartilhada). Por utilizar a mesma chave de encriptação e descriptação, essa técnica é chamada de criptografia simétrica.

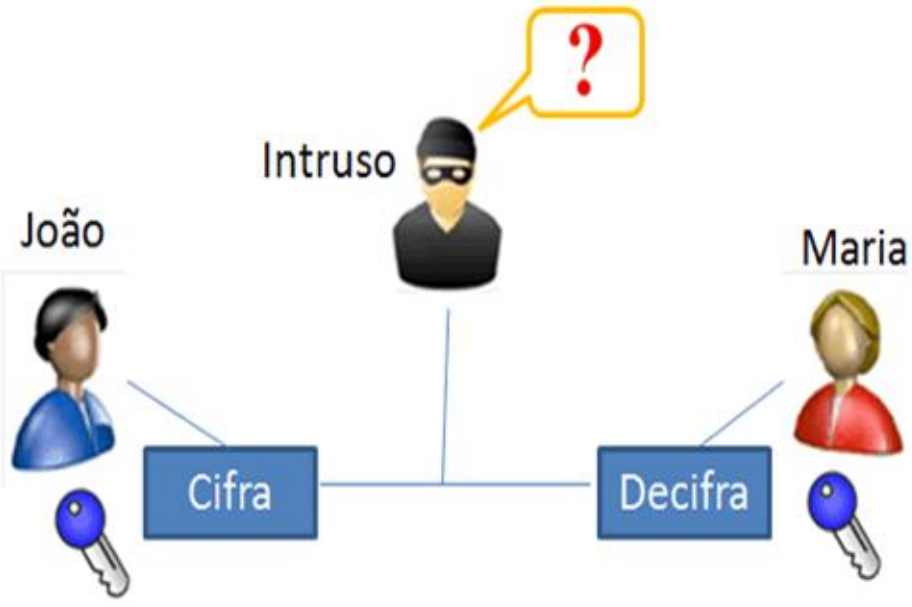

Figura 3.1: Instruso não deve Conhecer a Chave Secreta

Quando é enviada uma mensagem é aplicado um algoritmo de criptografia de chave privada sobre essa mensagem que é enviado pelo canal de comunicação que é inseguro. Chegando ao destinatário será aplicado um algoritmo de descriptografia e será utilizado a mesma chave de criptografia e a mensagem será novamente legível. Caso a mensagem seja interceptada no meio do caminho por uma terceira pessoa a mensagem não será legível, pois ela estará tendo acesso apena ao texto encriptado que não faz sentido algum.

Exemplo 3.2.1.

Um aluna Alice pretende enviar uma mensagem secreta ao aluno Bob e existe uma terceira pessoa que pode interceptar a mensagem enviada ao destinatário. A chave privada é comum tanto ao remetente como o destinatário. Vamos supor que a chave privada ou secreta é 322. Então Alice pretende enviar o número 07 ao Bob, então ela soma (322 + 7) e envia 329. Bob recebendo o número subtrai (329 − 322) e encontra a mensagem original. Mesmo a terceira pessoa interceptando a mensagem não conseguirá saber o conteúdo, pois não possui a chave secreta. **Algoritmo:** Alice e Bob devem combinar uma chave secreta.

A chave deve ser grande, caso contrario, a terceira pessoa poderá descobrir a chave por força bruta.

O algoritmo deve fazer não só apenas uma operação matemática. Para dificultar, devem-se utilizar outras operações, soma, subtração, multiplicação e divisão.

3.2.2 Chave Assimétrica

Exemplo de criptografia com Lata de Tinta.

Aluno A e B escolhem uma cor privada. Um dos dois anuncia publicamente uma cor pública.

Aluno A e B criam uma mistura de cores combinando com uma lata com a cor pública e outra lata com a sua cor privada, produzindo uma coloração público-privada. Conforme a ilustração abaixo 3.2:

Depois é misturando a cor pública com a suas respectivas cores privadas como se ver na figura 3.3.

Na mistura surge uma nova cor. Essa nova cor será secreta e comum aos dois.

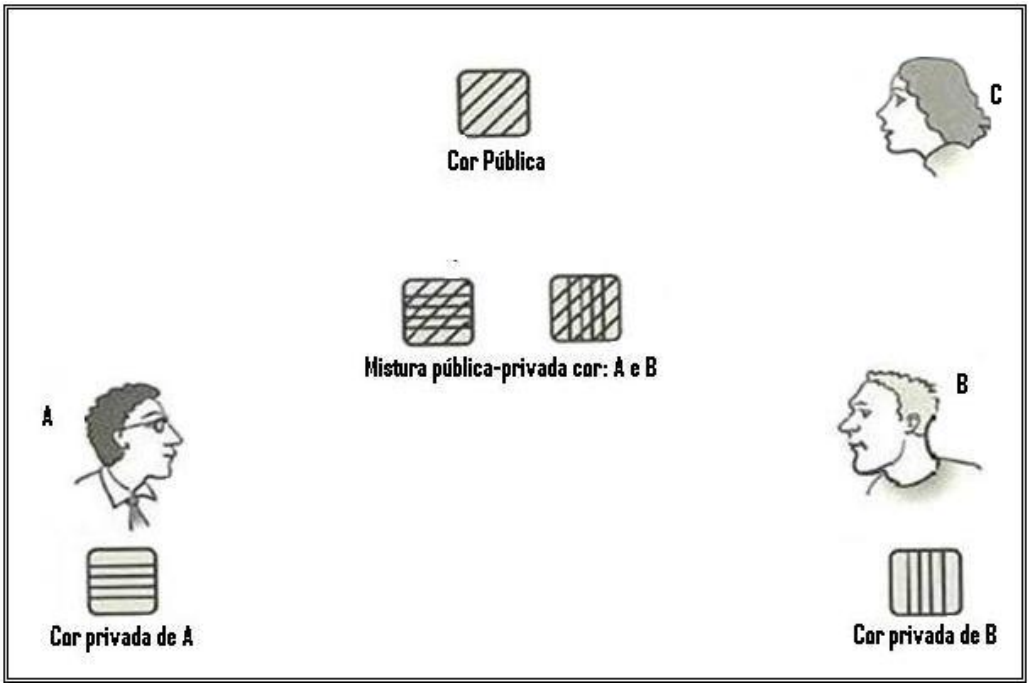

Figura 3.2: Misturas de Cores do aluno A e B

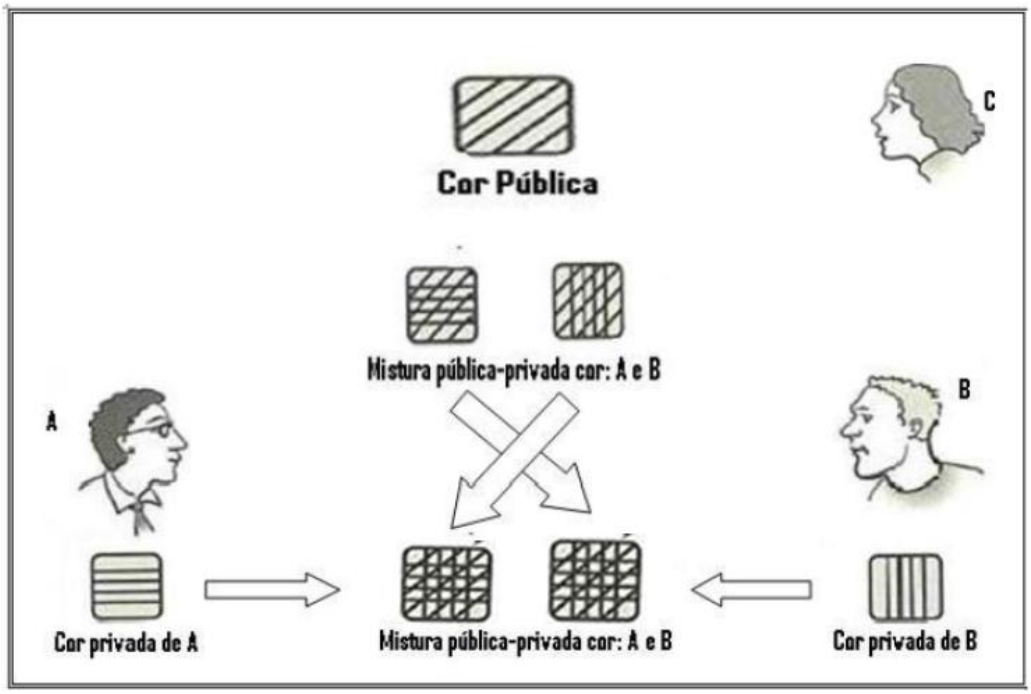

Figura 3.3: Cor Privada Comum aos Dois Alunos

Mistura das duas cores privadas com a pública. Essa maneira descreve um algoritmo que permite compartilhar uma chave sem que a aluna C pudesse ter conhecimento.

3.3 Algoritmo de Criptografia Simétrica

Vamos supor uma situação hipotética onde só temos a operação de multiplicação e não existe a divisão.

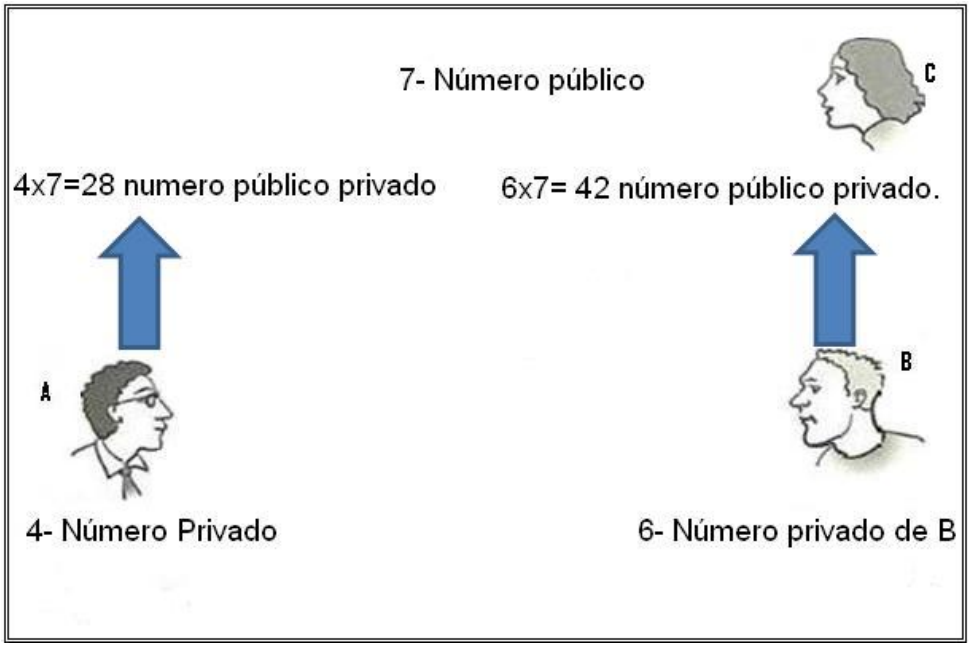

Figura 3.4: Aluno A e B com troca de chaves

Então a aluna C que está observando todas as operações só sabe multiplicar. O aluno A tem como número privado o 4 e o aluno B tem como número privado o 6. Existe uma chave pública, o número primo 7, em que é de conhecimento geral. O aluno A irá pegar a chave pública e multiplicar pela privada, onde teremos o resultado o número 28. O aluno B multiplica a chave dele por 7 e encontra 42.

O aluno A irá pegar o resultado 42 do Aluno B e irar multiplicar pela sua chave privada e o aluno B irá pegar o seu resultado que será uma chave pública e multiplicará pela sua chave privada.

Portanto se terá uma chave secreta: 168.

Essa operação não admite um inverso, ou seja, do final não conseguimos chegar ao começo.

Problemas deste tipo só podem acontecer hipoteticamente, pois, sabe-se que em um contexto real, não é possível fazer com que esse algoritmo não apresente falhas. Qualquer um conseguiria encontrar as chaves privadas. Para resolver esse dilema, e esconder de forma segura a chave privada utiliza-se operação modular.

Se trabalharmos em módulo 11. Temos a seguinte tabela 3.7.

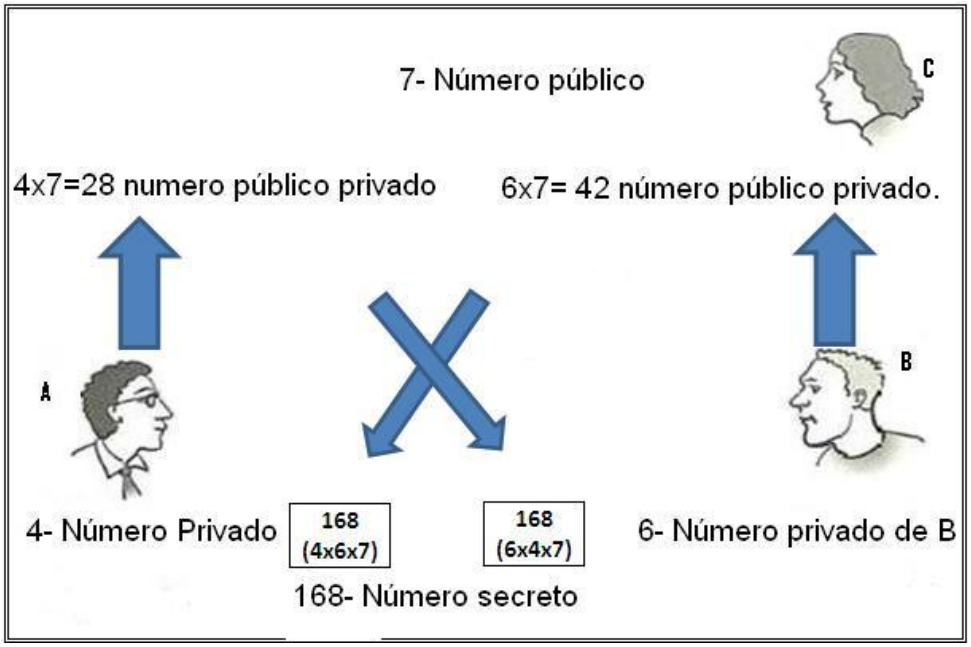

Figura 3.5: Encontrando a chave secreta e comum a A e B

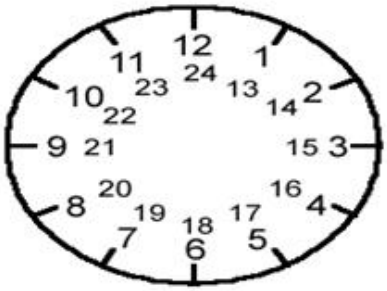

Figura 3.6: Relógio Modular

Então se trabalharmos com a base 2 e $n = 2$ temos, que o resto é 4. Se tivermos $n = 5$ temos que 2^5 *mod* $11 \equiv 10$.

Algoritmo

Como a chave privada do aluno A é 8. Pegamos a chave pública 2 como base e elevamos a 8. Pela tabela percebemos que $2^8 \equiv 3 \mathrm{mod} 11$($2^8$ modulo 11 é 3, o 3 é o resto). Portanto, será transmitido o número 3. O resto de 2^9 módulo 11 é 6 ou $6 \equiv 2^9$ *mod* 11 que será transmitido.

Fazendo agora a operação e pegando o número 6 do aluno B e transformando na base do aluno A e elevando a chave pública de A encontramos como resultado no módulo 11 o número 4. Da mesma forma o aluno B utiliza o número gerado por A, (número 3) e o transforma em base, $4 \equiv 3^9$ *mod* 11; (3^9 *mod* $11 \equiv 4$.). A aluna C não tem como saber o resultado final da operação, ela não vê o número 4. A operação de

N	2^n	3^n	6^n
1	2	3	6
2	4	9	3
3	8	5	7
4	5	4	9
5	10	1	10
6	9	3	5
7	7	9	8
8	3	5	4
9	6	4	2
10	1	1	1

Figura 3.7: Tabela de Correspondência Modular

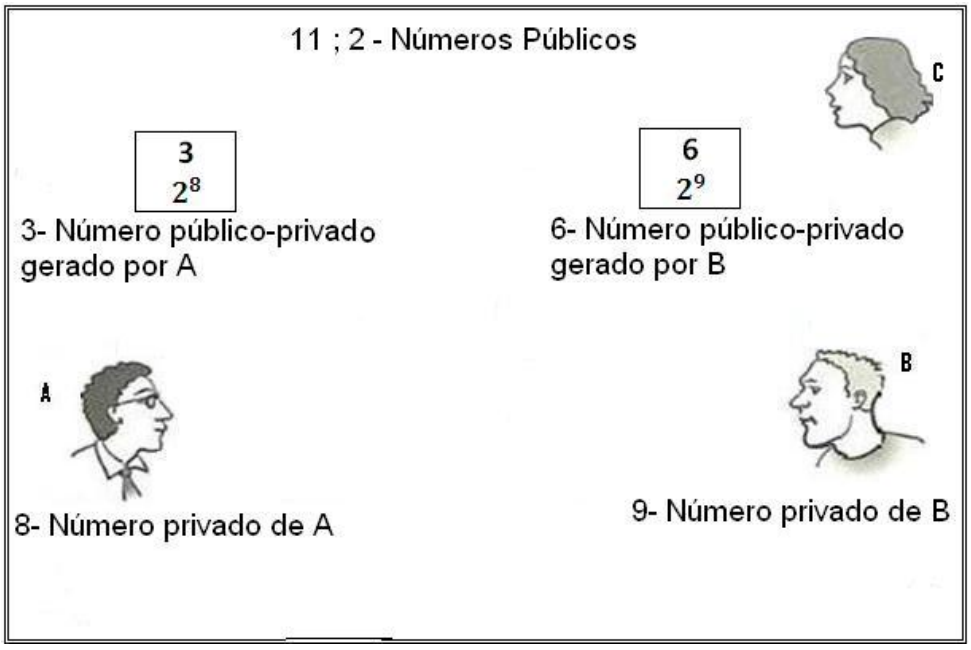

Figura 3.8: Chave Públicas são Números Primos

exponenciação aritmética em módulos me garante que o resultado será feita em um único sentido.

Esse algoritmo de troca de chave foi desenvolvido em 1976 por Whitfiel e

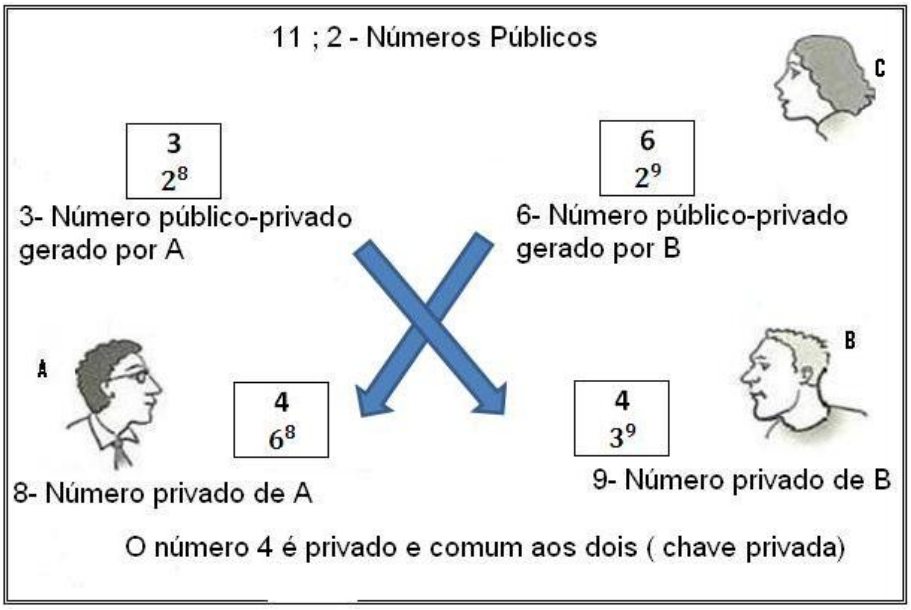

Figura 3.9: Criando Chaves Secreta para Troca de Messagens Utilizando Aritmética Modular.

Martin Hellman, é utilizado na internet nos endereços HTTPS, onde é estabelecido uma chave comum com o servidor, e ao invés de módulo 11 que foi utilizado no exemplo, se utiliza um número primo muito grande.

Tomando como base esse exemplo demostrado anteriormente, pode-se realizar uma tabela para exemplificar de forma mais simples o contexto da aplicação, mostrando como o esquema pode ser generalizado para qualquer valor numérico de números naturais primos.

Podemos utilizar um exemplo para implementação do protocolo onde é utilizada números inteiros módulo p, onde p é um número primo e g é uma raiz primitiva módulo p. Então fica estabelecido que os valores públicos estão em azul e os valores secretos estão em vermelho.

Podemos implementá-lo como um experimento na sala de aula. Supondo que dois alunos em uma sala de aula com o nome Alice e Bob queiram fazer uma troca de mensagem sem que uma terceira pessoa saiba qual é a chave secreta comum. Utilizando o algoritmo de criptografia de Diefi- Hellman, fica da seguinte forma:

Exemplo 3.3.1.

1. Ana e Bob entram em acordo para usar um número primo $p = 23$ e como base é $g = 5$.

2. Ana escolhe um inteiro secreto $a = 6$, e então envia a Bob $A \equiv g^a \bmod p$.

3. $A \equiv 5^6 \text{mod} 23 \longrightarrow A \equiv 15625 \ mod \ 23 \longrightarrow \boxed{A = 8.}$

4. Bob escolhe um inteiro secreto $b = 15$, e então envia a Ana $B \equiv g^b \ mod \ p$. $B \equiv 5^{15} \ mod \ 23$.

$$B \equiv 30.517.578.125 \ mod \ 23.$$

$$\boxed{\text{B=19}}.$$

5. Ana calcula $s \equiv \text{B}^a \text{mod} p \longrightarrow \text{s} \equiv 19^6 \text{mod} 23 \longrightarrow \text{s} \equiv$ 47.045.881mod23

$$\boxed{\textbf{s=2}}.$$

6. Bob calcula $s \equiv \text{A}^b \ mod \ p$. $s \equiv 8^{15} \ mod \ 23$. $s \equiv$ 35.184.372.088.832mod23.

Portanto, temos que a chave compartilhada e secreta entre os dois será:

$$\boxed{\textbf{s = 2.}}$$

Uma vez que Ana e Bob calculam a chave secreta, eles podem então usá-la como chave de encriptação, conhecida apenas por eles, para enviar e receber mensagens ao longo do mesmo canal de comunicação.

Alguém que tenha descoberto estes dois inteiros privados também será capaz de calcular s da seguinte maneira:

$$s \equiv 5^{6*15} \ mod \ 23.$$

$$s \equiv 5^{90} \ mod \ 23.$$

$$s \equiv 807.793.566.946.316.088.741.610.050.849.573.099.185.363.389.551.639.556.884.765.625 mod 23.$$

Ou seja, o valor de $\boxed{s = 2.}$

É claro que valores bem maiores de a, b, e p seriam necessários para tornar este exemplo seguro, uma vez que é fácil tentar todos os possíveis valores de $g^{ab} \ mod \ 23$. Existem apenas 23 possíveis inteiros que possuem os resultados observados para $mod \ 23$. Por outro lado, se p for um primo de ao menos 300 dígitos e a e b tenham ao menos 100 dígitos, então até os melhores algoritmos conhecidos atualmente não poderiam encontrar a dado apenas g, p e $g^p \ mod \ 23$ e $g^a \ mod \ p$, mesmo usando todo o poder computacional existente na humanidade. Tal problema é conhecido como problema do *logaritmo discreto*. Note que g não precisa ser necessariamente grande, e seus valores podem ser 2 ou 5.

3.4 Aplicação com Criptografia RSA

RSA - Desenvolvido por Ronald Rivest, Adi Shamir e Len Adleman, o algoritmo tomou por referência o estudo feito por Diffie e Hellman, porém usando outro embasamento matemático para a criação das chaves públicas. Eles utilizaram o fato de que é fácil obter o resultado da multiplicação de dois números primos extensos e a grande dificuldade de se fatorar esse número, a fim de obter os fatores primos.

O código ASCII é utilizado em várias aplicações da criptografia RSA, isso é devido ao uso constante de grande parte das codificações de caracteres diferentes que encontramos de diversas formas no dia a dia, como exemplo mais comum, os computadores. As inicias da frase American Standard Code for Information Interchange (Código Padrão norte-americano para Intercâmbio de Informações) corresponde à sigla do código. A representação do código ASCII é feita por caracteres, utilizando uma escala decimal de 0 a 127. Então o computador converte para linguagem binária e ele processa o comando. Sendo assim, ao digitar uma letra automaticamente ela corresponderá a um número desse código. O código foi proposto por Robert W. Bemer tenta arranjar um modelo padrão para códigos caracteres alfanuméricos (letras, sinais, números...).

> O que fazemos para codificar uma mensagem no RSA é calcular sua potência módulo n relativamente a um expoente especialmente escolhido. Entretanto, para que isto seja viável, a mensagem deve ser um número inteiro. Mas não é isto o que ocorre em geral: a maior parte das mensagens é um texto. Por isso, a primeira coisa a fazer, se desejamos usar o método RSA, é inventar uma maneira de converter a mensagem em uma sequência de números, COUTINHO[4]

Vamos ilustrar aqui um exemplo utilizando a criptografia RSA para endê-la melhor.

Exemplo 3.4.1. (Algoritmo de Criptografia RSA)

Só ressaltando que M é a mensagem que queremos cifrar, C é a mensagem cifrada, temos também a chave pública e, a chave privada d e n um número que é calculado através dos números primos p e q.

$$\begin{array}{ll} \text{Criptografar:} & C \equiv M^e \ (mod\text{n}). \\ \text{Descriptografar:} & M \equiv C^d \ (mod\text{n}). \end{array}$$

Para cada bloco a ser cifrado deve-se fazer o cálculo acima. Ambos devem

saber o valor de n (publico). Portanto, a chave pública definida pela dupla e e n, sendo CH_{pb} = (e,n). A chave privada é definida pela dupla d e n, sendo CH_{pv}=(d,n).

Para gerar a chave precisamos de algumas coisas:

1. Selecionar dois números primos p e q grandes.
2. Calcule o valor de $n = p.q$.
3. Calcule $\Phi(n) = (p-1)(q-1)$.
4. Selecione um inteiro e relativamente primo à $\Phi(n)$.
5. Calculamos d de forma que $(e.d) \equiv 1\ mod\ \Phi(n)$.

Vejamos um exemplo:

- (1^o) se $p = 3$ e $q = 11$.
- (2^o) $n = 3.11 = 33$, logo $n = 33$.
- (3^o) $\Phi(n)$=$(3-1).(11-1)$=2.10 =20, portanto $\Phi(n)$=20.
- (4^o) e é um inteiro relativamente primo à $\Phi(n)$, e atende $1 \leq e \leq \Phi(n)$, daí $e = 7$. Observe: sendo que (5, 11, 13, 15, 17 e 19 seriam outras opções).
- (5^o) Calculando e de forma $(7.d)\ mod$ 20=1.
  $d = 1 \longrightarrow (7.1) = 7\ mod\ 20 \neq 1$
  $d = 2 \longrightarrow (7.2) = 14\ mod\ 20 \neq 1$
  $d = 3 \longrightarrow (7.3) = 21\ mod\ 20 \equiv 1$ Múltiplos de três seriam possíveis (6,9,12,...).

Portanto teríamos CH_{pb}=(7, 33) e CH_{pv}=(3 ,33).

Se tivéssemos um texto com o número 20, a mensagem cifrada seria:

- $C \equiv M^e\ (mod\text{n})$
- $C \equiv 20^7\ (mod 33)$
- $C \equiv (20^3)^2.20\ (mod 33)$
- $C \equiv 14^2.20 \equiv 26\ (mod 33)$

E para decifrar:

- $M \equiv C^d \ (mod \text{n})$
- $M \equiv 26^3 \ (mod 33)$
- $M \equiv 20 \ (mod 33)$
- $M \equiv 20 \ (mod 33)$

Portanto, o número 20 é a mensagem original.

Capítulo 4

Criptografia em Funções e Matrizes

Podemos utilizar conceitos de adição, multiplicação entre duas matrizes, inversa e determinante utilizando os métodos de criptografia.

Primeiramente deve-se converter da forma alfabética para a numérica. A codificação pode ser da seguinte forma:

a =1	b=2	c=3	d= 4
e=5	f=6	g=7	h=8
m=13	n=14	o=15	p=16
q=17	r=18	s=19	t=20
u=21	v=22	w=23	x=24
y=25	z=26	27= .	28= !
# = 29	espaço = 30		

Tabela 4.1: Números e Letras do Alfabeto

A tabela alfa-numérica deve ser conhecida tanto pelo destinatário como pelo remetente. Vamos codificar a seguinte mensagem: mestrado profissional.

O remetente e o destinatário devem conhecer essa tabela alfa-numérica e também pode fazê-la usando outras correspondências entre números e letras. Vamos codificar a seguinte mensagem: mestrado profissional. Vamos fazer a correspondência entre as letras e os números usando a tabela dada.

Sabemos que a chave é uma matriz (2x2), vamos colocar a sequência de números dispostos em uma matriz de duas linhas. Então se o número de elementos da mensagem for um impar, temos que acrescentar um caractere vazio que irá alterar a mensagem. No caso o número 30.

Chave A é :

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

A matriz L (2x11) é dada na tabela seguinte.

13	05	19	20	18	01	04	15	30	16	18
15	06	09	19	19	09	15	14	01	12	30

Tabela 4.2: Matriz 2x11

Devemos saber que a ordem das matrizes é um fator muito importante. Quando uma matriz tem inversa, o seu determinante é igual a 0. Em termos de função, podemos dizer que se trata de uma função injetora.

A matriz inversa de A é:

$$A^{-1} = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}$$

A chave de criptografia será dada por A (2x2):

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

Dessa forma, para encriptar o conteúdo , multiplicamos a matriz A por L, tal que O=$A.L$.

$$O = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 13 & 05 & 19 & 20 & 18 & 01 & 04 & 15 & 30 & 16 & 18 \\ 15 & 06 & 09 & 19 & 09 & 15 & 15 & 14 & 01 & 12 & 30 \end{pmatrix}$$

$$O = \begin{pmatrix} 54 & 21 & 66 & 79 & 63 & 18 & 27 & 59 & 91 & 60 & 84 \\ 41 & 16 & 47 & 59 & 45 & 17 & 23 & 44 & 61 & 44 & 66 \end{pmatrix}$$

Os elementos da matriz O constituem a mensagem codificada. Quando a mensagem codificada chegar ao destinatário, ele usará a matriz A^{-1} decodificadora para ler a mensagem. Sabendo que $A^{-1}.O$=$A^{-1}.A.L = I.L = L$, temos.

Multiplicamos a matriz A^{-1} por O.

$$\mathrm{A}^{-1}.O = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 54 & 21 & 66 & 79 & 63 & 18 & 27 & 59 & 91 & 60 & 84 \\ 41 & 16 & 47 & 59 & 45 & 17 & 23 & 44 & 61 & 44 & 66 \end{pmatrix}$$

A multiplicação entre essas duas matrizes revela a mensagem secreta da criptografia.

$$L = \begin{pmatrix} 13 & 05 & 19 & 20 & 18 & 01 & 04 & 15 & 30 & 16 & 18 \\ 15 & 06 & 09 & 19 & 09 & 15 & 15 & 14 & 01 & 12 & 30 \end{pmatrix}$$

Agora é só reverter os números utilizando novamente a tabela alfa-numérico para encontrar o significado da mensagem original.

4.1 Propostas de Atividades para a Sala de Aula.

O professor em sala de aula poderá apresentar aos alunos diversas maneiras de atividades em criptografia de mensagens usando matrizes, TOREZZAN [6]. Dividindo a sala em grupos, o professor explica como pode ser feito e fornecer uma mensagem codificada, solicitando para eles tentem decifrá-la. Depois, cada grupo deve criar sua própria mensagem criptografada e traça-la com os outros grupos. Assim, cada grupo tenta descobrir o que o outro está escondendo com a matriz e a chave que usaram.

O processo de codificação é uma função que associa cada mensagem unitária de um conjunto do texto original a uma mensagem unitária de outro conjunto. Em muitas aplicações é util substituir os símbolos de um alfabeto por números inteiros, para tornar mais fácil a construção do sistema, ANDRADE[1].

Podemos dizer que uma função f que transforma um conjunto P em C com a estrutura.

$P \xrightarrow{f}$C$\xrightarrow{f^{-1}}$P.

Onde P é conjunto das mensagens u originais do remetente a ser codificado e C é conjunto das mensagens c a ser decoficadas.

Dessa forma, o processo de codificação é definido pela função:

$f : P \to C \; talque \; f(u) = c$;

O processo de decoficação é definido por:

f^{-1}:$C \to P \; talque \; f^{-1}(c) = u$;

Um aplicação bastante utilizada para ilustrar essa situação é o caso dos símbolos do alfabeto por elementos de $\mathbb{Z}_{27}$.

Vemos que o conjunto F é o conjunto das letras do alfabeto.

Teorema 4.1.1. Seja $n \in \mathbb{N}$ e a, $b \in \mathbb{Z}$ fixados. Se $mdc(a, n) = 1$, então a função:

$f : \mathbb{Z}_n \to \mathbb{Z}_n$.

dada por,

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

Tabela 4.3: Correpondência entre Letras e Números

$f(x) = ax + b$. é um criptossistema.

No criptossistema $f(x) = ax + b$ o par (a, b) é denominado chave de codificação.

Exemplo 4.1.1. Seja o símbolo $x \in \mathbb{Z}_{27}$ correspondendo a uma mensagem de blocos, onde $a = 2$, $b = 1$, e a função:

$f : \mathbb{Z}_{27} \to \mathbb{Z}_{27}$,

onde $f(x) = 2x + 1$ é um criptossitema.

Codificando a mensagem:

MATEMATICA, temos a seguinte situação de acordo com a função dada acima:

$M \to 13$, $A \to 1$, $T \to 20$, $E \to 5$, $I \to 9$, $C \to 3$.

Calculando:$f(13) = 27$; $f(1) = 3$; $f(20) = 41$, sendo $41 \equiv 14\ mod\ 27$; $f(5) = 11$; $f(9) = 19$; $f(3)$=7.

A mensagem cifrada é: **!CNK!CNSGC**

Para decodificar a mensagem utiliza-se a função inversa. Portanto, $f^{-1}(x) = 14x - 14$, para se obter a mensagem original.

Quando n=27, $a = 1$ e $b \in \mathbb{Z}_{27}$ o criptossistema $f(x) = x + b$ é chamado de Cifra de César, pois Júlio César a utilizava. Quando b=0 a função $f(x)$=ax é uma transformação linear.

Portanto, as transformações que ocorrem nas codificações em criptografia são baseadas nas funções bijetivas f entre um conjunto de mensagens originais, sem codificações e um conjunto de mensagens codificadas. A função f deve ser inversível para garantir que o processo seja reversível e que as mensagens possam ser reveladas pelos receptores.

O experimento abordado traz um tipo específico de sistema criptográfico, onde

temos uma função f e sua inversa f^{-1} são determinadas por alguma matriz A e sua inversa A^{-1}.

Para codificar uma mensagem usando este método é necessário que, primeiramente, cada letra do nosso alfabeto e símbolos desejados sejam associados a vetores 2x1. Na tabela onde se tem a correspondência letra e número pode ser feita associando cada símbolo a vetores.

A seguir, apresentamos a figura 4.1 de uma tabela com um exemplo para essa associação.

A	B	C	D	E	F	G	H	I	J
$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}2\\0\end{pmatrix}$	$\begin{pmatrix}3\\0\end{pmatrix}$	$\begin{pmatrix}4\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}2\\1\end{pmatrix}$	$\begin{pmatrix}3\\1\end{pmatrix}$	$\begin{pmatrix}4\\1\end{pmatrix}$
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
$\begin{pmatrix}0\\2\end{pmatrix}$	$\begin{pmatrix}1\\2\end{pmatrix}$	$\begin{pmatrix}2\\2\end{pmatrix}$	$\begin{pmatrix}3\\2\end{pmatrix}$	$\begin{pmatrix}4\\2\end{pmatrix}$	$\begin{pmatrix}0\\3\end{pmatrix}$	$\begin{pmatrix}1\\3\end{pmatrix}$	$\begin{pmatrix}2\\3\end{pmatrix}$	$\begin{pmatrix}3\\3\end{pmatrix}$	$\begin{pmatrix}4\\3\end{pmatrix}$
U	**V**	**W**	**X**	**Y**	**Z**	**espaço**	**.**	**,**	**?**
$\begin{pmatrix}0\\4\end{pmatrix}$	$\begin{pmatrix}1\\4\end{pmatrix}$	$\begin{pmatrix}2\\4\end{pmatrix}$	$\begin{pmatrix}3\\4\end{pmatrix}$	$\begin{pmatrix}4\\4\end{pmatrix}$	$\begin{pmatrix}0\\5\end{pmatrix}$	$\begin{pmatrix}1\\5\end{pmatrix}$	$\begin{pmatrix}2\\5\end{pmatrix}$	$\begin{pmatrix}3\\5\end{pmatrix}$	$\begin{pmatrix}4\\5\end{pmatrix}$

Figura 4.1: Letras e Pontos

Observação: Podemos representar esses vetores como pontos de um plano conforme a figura 4.2.

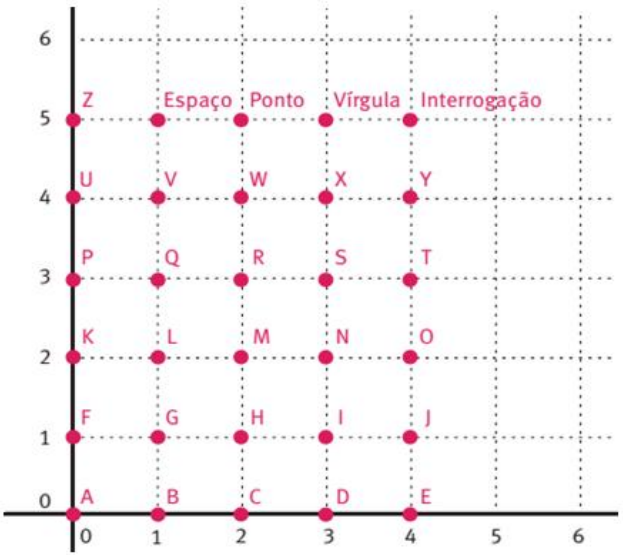

Figura 4.2: Pontos no Plano Cartesiano

Codificando uma mensagem utilizando uma matriz M de apenas 2 linhas iremos codificá-la. Decidido qual associação usar, construa uma matriz M de apenas 2 linhas

e codifique uma mensagem. Para isso, basta colocar os vetores que representam as letras da mensagem um na frente do outro. Vamos, por exemplo, colocar a mensagem Boa aula. em uma matriz, usando a associação da mensagem um na frente do outro.

$$M = \begin{bmatrix} 01 & 04 & 0 & 1 & 0 & 0 & 01 & 0 & 2 \\ 0 & 02 & 0 & 05 & 0 & 04 & 02 & 0 & 05 \end{bmatrix}$$

Criando uma matriz chave 2x2 para prosseguir na codificação. A matriz 2x2 deve ser inversível para garantir que a mensagem poderá ser codificada. Utilizando a matriz C como segui abaixo:

$$C = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

Fazendo a multiplicação entre as matrizes obtemos a mensagem criptografada, transformando em uma matriz chamada de M.

$$M' = C.M = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 01 & 04 & 0 & 1 & 0 & 0 & 01 & 0 & 2 \\ 0 & 02 & 0 & 05 & 0 & 04 & 02 & 0 & 05 \end{bmatrix}$$

Agora, transmita aos alunos a tabela com a associação entre as letras e os vetores, a matriz chave C e a matriz com a mensagem codificada M.

Com o roteiro descrito anteriormente, peça aos alunos para criptografar sua mensagem original M e peça que eles tentem decifrar sua frase.

Para os alunos encontrar a mensagem secreta deveram achar através do conhecimento já adquirido para decodificá-la encontrando a matriz inversa de C e multiplicar por M pois:

$$M = (C^{-1}.C).M = C^{-1}.(C.M) = C^{-1}.M'$$

Portanto, o professor deve exigir que os seus alunos façam prática das aplicações já feitas e criar novas mensagens com um numero de caracteres limitado e codificá-las. Em seguida, eles traçarão mensagens com outros grupos, sempre divulgando a matriz (M) e a chave (C). Assim cria-se uma disputa saudável entre as equipes fazendo com que

eles aprendam fixando o conteúdo como multiplicação e inversão de matrizes de um modo mais prazeroso. O professor pode aproveitar a oportunidade para está introduzindo ou revisando conteúdos de matérias dentro da matemática ou afins como, por exemplo, da mensagem Boa aula, podem ser representadas na figura 4.3:

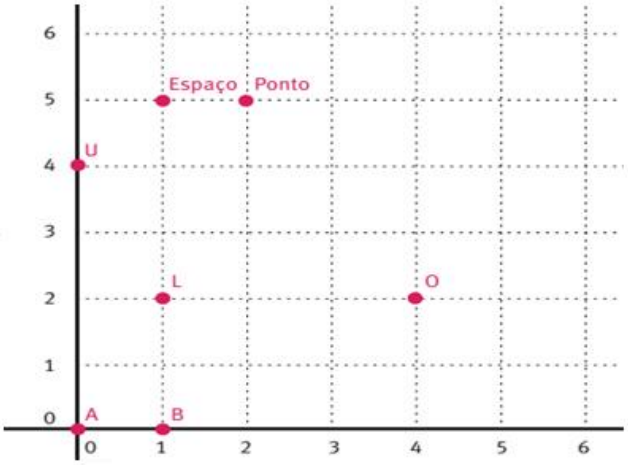

Figura 4.3: Representação gráfica

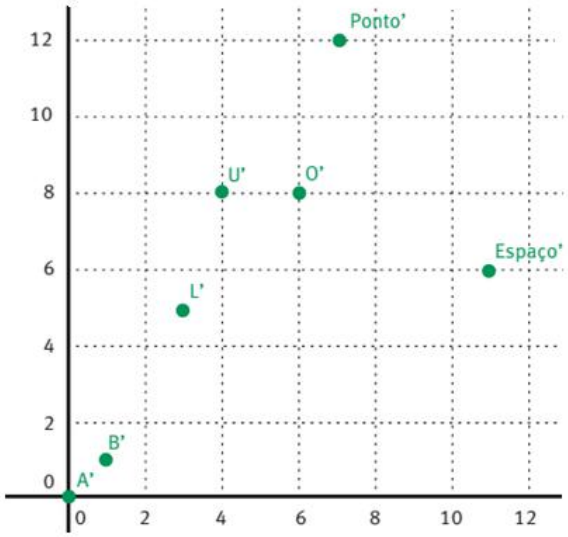

Figura 4.4: Figura dos Pontos no Plano

E, desenhando cada letra dessa frase depois de multiplicadas pela matriz C do nosso, temos como mostrado na figura 4.4:

Observe o que acontece com cada vetor letra na transformação:

$$B = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow C. \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$O = \begin{pmatrix} 4 \\ 2 \end{pmatrix} \longrightarrow C. \begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 6 \\ 8 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \longrightarrow C. \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

A multiplicação dos pontos que representam letras pela matriz chave C é um dos fatores a ser observado e instigado pelo professor aos alunos para inferirem outras visualizações gráficas. De acordo com a figura abaixo onde é mostrado um conjunto de quatro letras do alfabeto representado por pontos abertos e o efeito que a multiplicação por C ocasionou conforme a figura 4.5.

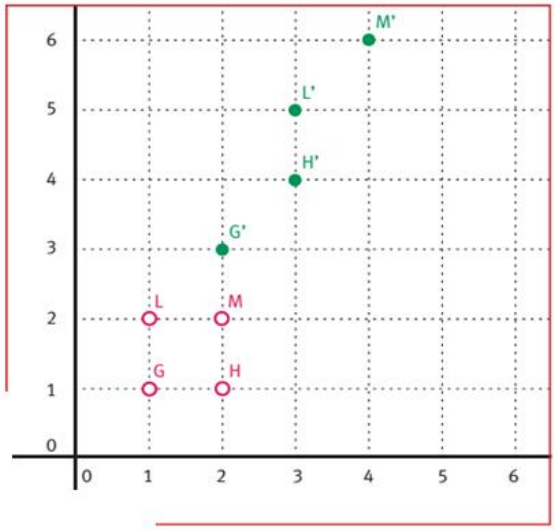

Figura 4.5: Plano Cartesiano

Dessa forma, o aluno pode fazer conjecturas da forma em que o conhecimento das transformações de apenas duas letras no nosso método criptográfico, já é factível que um espião descubra a sequência da matriz chave. Assim, se, por exemplo, ele souber que:

$$B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

e

$$O = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$$

são levados em:

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 6 \\ 8 \end{pmatrix}$$

respectivamente, ele saberia que, se a matriz chave C for igual a:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Então:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

e

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 6 \\ 8 \end{pmatrix}$$

Então:

$$1.a+0.b=1$$
$$1.c+0.d=1$$
$$4.a+2.b=6$$
$$4.c+2.d=8$$

Resolvendo o sistema, ele encontraria que $a = 1$, $b = 1$, $c = 1$, $d = 2$ e portanto:

$$\mathrm{C} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Daí vem a importância de se guardar todas as transformações em segredo.

Capítulo 5

Considerações Finais

Neste trabalho vimos uma aplicação importante da Aritmética Modular, a Criptografia. Como o desenvolvimento da Aritmética está relacionada historicamente com a Criptografia deste as Cifras de César com motivos militares passando pela Análise de Frequência e as descobertas tecnológicas, como criptografia na internet, que decorrem do aperfeçoamento dessa área da Matemática sendo um dos grandes triunfos a possibilidade de manter em segurança transmissão de dados através de canais de comunicação.

Dessa forma, um dos objetivos desse trabalho foi destacar os pricipais tópicos relevantes ao ensino de conteúdos de matemática do ensino básico correlatos a aritmética modular e aplicações, Demonstrando métodos e recursos utilizados em sala de aula no ensino de temas relacionado com a criptografia. Levando ao conhecimento do aluno situações em que possa ser utilizado algoritmos como forma lógica para resoluções de problemas, capacitando o aluno a desenvolver a capacidade de concentração nas atividades e criar estratégias.

Assim, a maneira como se fez a abordagem da criptografia, buscando introduzi-lá na realidade do estudante do ensino básico, demostrando de aplicações da Aritmética em situações como do caledário, CPF e Criptografia de Chave Pública e Privada, e a descrição de um modelo de criptografia RSA com atividades propostas com um roteiros de fácil compreensão.

Funções e Matrizes fazem parte da discursão deste trabalho pelo motivo de serem tópicos da matemática de grande notação dentro do ensino básico, onde a aplicação da aritmética será um facilitador para aprendizagem de funções afim, polinomial, inversa e bijeção. Em Matriz pode se conferir os conceitos de multiplicação de um escalar, entre matrizes, soma, inversas e determinantes.

Para não fugir aos objetivos deste trabalho, não foi apresentados conceitos muito avançados em matemática baseados na Teoria dos Números e alguns conceitos foram omitidos por não se adequarem com o objetivo aqui pretendidos.

Por fim, acreditamos que esse trabalho possa servir como fonte de inspiração e leve a compreensão tanto do professor como do aluno de que o estudo da aplicação de determinadas áreas Matemática estão completamente relacionadas com o desenvolvimento da tecnologia na sociedade.

Referências Bibliográficas

[1] ANDRADE, A. *Números, Relações e Criptografia*. UFPB. Paraíba. 2010.

[2] BARBOSA, BRAGHETTO, l. *RSA- Criptografia Assimétrica e Assinatura Digital*. Campinas, SP. 2003.

[3] COUTINHO, S. C. *Números inteiros e criptografia RSA*.Série de Computação e Matemática nº 2, IMPA e SBM, segunda edição (revisada e ampliada). 2000.

[4] COUTINHO, S. C. *Programa de iniciação Científica da OBMEP 2007*. Rio de Janeiro, Brasil: Instituto Nacional de Matemática Pura e Aplicada- IMPA.

[5] CRISTINA, K.E. *Números Primos e Criptografia: Da Relação Com a Educação Ao Sistema RSA*. TCC- Profmat, UFRRJ. 2013.

[6] CRISTIANO, BARICHELLO, FIRER. *Mensagens Secretas com Matrizes- Matemática Multimídia*. UNICAMP, São Paulo, 2010. http://m3.ime.unicamp.br/recursos/1020.

[7] CHIARADIA, A.P.M. *Atividades: Criptografia usando matrizes*.- Projeto Teia Do Saber 2006. SP.

[8] Canal Preparação Digital. *Cripotografia na Educação*- http://www.youtube.com/userPreparacaoDigitalsearch?query=criptografia. Acesso em 25/11/13.

[9] DIFFIE, H. *Criptografia de Chave Privada*.-http://pt.wikipedia.org/wiki/Diffie-Hellman. pesquisa em 01/02/2014.

[10] SEBASTIANI, E. *Como usar a história da matemática na construção de uma educação matemática com significado*. In: SEMINÁRIO NACIONAL DE HISTÓRIA DA MATEMÁTICA, 3., 1999, Vitória.

[11] HEFEZ, A. *Elementos de Aritmética*. Sociedade Brasileira de Matemática, 2005.

[12] HEFEZ, A. *Iniciação a Aritmética*. Sociedade Brasileira de Matemática, 2009.

[13] MARIA, V.D.AZ. *Noções de Lógica e Algoritmo.* UNIMEP, SP. 2003. http://www.unimep.br/ vmdzilio/mod1_2.html

[14] MALAGUTTI, P.L. *Atividades de Contagem apartir da Criptografia.* Rio de Janeiro, Brasil: Instituto Nacional de Matemática Pura e Aplicada- IMPA, 2009.

[15] OLIVEIRA, D. Kripka, R. *O uso da criptografia no ensino de Matemática.* Conferencia interamericana de educação matemática. 2011.

[16] OLGIN, GROENWALD, FRANKE. *Criptografia no Ensino Médio.* Grupo de Estudos Curriculares de Educação Matemática da Universidade Luterana do Brasil. ULBRA. 2010.

[17] PCN. *Parâmetros Curriculares Nacionais da Matemática.* Brasília: MEC-SEF,1998.

[18] Portal da Educação. *Criptografia* http://www.portaleducacao.com.br/educacao/artigos/38642 /criptografia. Acesso em 25/11/13.

[19] SINGH, S. *O Livro dos Códigos.* São Paulo: Record, 2001.

[20] SÁ, I.P. *Aritmética modular e algumas de suas aplicações.* UERJ. Rio de Janeiro, Brasil, 2010.

[21] TOMAROZZI, A.C. *Codificando e Decifrando Mensagens.* Revista do professor de Matemática. Volumes 45. Sociedade Brasileira de Matemática.