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

PAULO DA SILVA BELIZARIO

Aritmética e Criptografia com Aplicações no Ensino Médio

PALMAS - TO
2015

PAULO DA SILVA BELIZARIO

Aritmética e Criptografia com Aplicações no Ensino Médio

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para a obtenção do título de Mestre - Área de Concentração: Matemática.
Orientador: Prof. Dr. Rogério Azevedo Rocha.
Coorientador: Prof. Dr. Warley Gramacho da Silva

PALMAS - TO
2015

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

B431a Belizario, Paulo da Silva.

Aritmética e Criptografia com Aplicações no Ensino Médio. / Paulo da Silva Belizario. – Palmas, TO, 2015.

102 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2015.

Orientador: Rogério Azevedo Rocha

Coorientador: Warley Gramacho da Silva

1. Aritmética. 2. Criptografia Simétrica. 3. Criptografia Assimétrica. 4. Aplicação no Ensino Médio. I. Título

CDD 510

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

PAULO DA SILVA BELIZARIO

ARITMÉTICA E CRIPTOGRAFIA COM APLICAÇÕES NO ENSINO MÉDIO

Trabalho de Conclusão de Curso apresentado ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para obtenção do título de Mestre – Área de Concentração: Matemática. Orientador: Dr. Rogério Azevedo Rocha. Co-orientador: Dr. Warley Gramacho da Silva

Aprovado em 11 / 12 / 2015

BANCA EXAMINADORA

Rogério Azevedo Rocha

Prof. Dr. Rogério Azevedo Rocha (Orientador-UFT)

Hellena Apolinário

Prof. Dra. Hellena Christina Fernandes Apolinário (UFT)

Prof. Dr. Claudio Castro Monteiro (IFTO)

Aos meus amados pais
A Mônica, minha querida esposa.
Ao Pedro, meu amado filho.

AGRADECIMENTOS

A Deus, meu protetor e ajudador, pela vida, pela inteligência e por me guiar sempre.

Ao meu pai Wilson Belizario Santana e minha mãe Irani da Silva Souza Belizario, os principais responsáveis por ter chegado até aqui. Através de seu ensinamentos que me foram passados com amor, aprendi a viver, ver e conviver nesse mundo, buscando sempre seguir em frente, mesmo com as dificuldades que aparecem, sem nunca perder a fé e a esperança.

A minha esposa Mônica de Jesus Reis Belizario, pois tem sempre estado ao meu lado desde que nos casamos, e durante essa caminhada tem ajudado com carinho e compreensão.

Ao professor Dr Rogério Azevedo Rocha meu orientador, que contribuiu bastante para a realização desse trabalho, com suas observações e sugestões que colaborou muito para meu aprendizado. E ao professor Dr Warley Gramacho da Silva meu coorientador, por ter me ajudado na parte computacional, com a implementação da codificação em matriz.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro.

Aos meus colegas de turma do mestrado pela vivência durante os anos de aulas, conviver com vocês me trouxe um grande aprendizado.

A escada da Sabedoria tem os degraus feitos de números.
(Blavatsky)

RESUMO

Esta dissertação apresenta a Criptografia (escrita de mensagens originais em mensagens ocultas), mostrando alguns algoritmos de criptografia simétrica, que usa a mesma chave para codificar e descodificar, e o algoritmo RSA de criptografia assimétrica (de chave pública), que usa uma chave para codificar e outra chave para decodificar. Apresentamos um pouco da história da criptografia e a teoria necessária para um desejável entendimento dos métodos criptográficos, através de um estudo das congruências módulo m. Propomos atividades envolvendo a Criptografia para turmas do ensino médio e mostramos como funcionam determinados algoritmos de criptografia simétrica no computador, através de programas executáveis criados em linguagem C. Os programas executáveis servem para que os estudantes visualizem o funcionamento dos métodos criptográficos, e possam associar ao seu cotidiano, despertando assim, um maior interesse em estudar matemática, visto que muitos deles não percebem os conteúdos como algo útil para sua vida.

Palavras-chave: Congruências. Criptografia simétrica. Criptografia assimétrica. Aplicação ao ensino médio. Programação em linguagem C.

ABSTRACT

This thesis presents the Encryption (writing original messages in hidden messages), showing some symmetric encryption algorithm, which uses the same key for encoding and decoding, and the RSA asymmetric encryption (public key), which uses a key to encode and another key to decode. We present some of the history of cryptography and theory necessary for a desirable understanding of cryptographic methods, through a study of congruence modulo m. We propose activities involving encryption for high school classes and show how they work certain symmetric encryption algorithms in the computer via executable programs written in C language Executable programs are for students to visualize the operation of cryptographic methods, and can join the their daily lives, thus arousing a greater interest in studying mathematics, since many of them do not realize the content as something useful for your life.

Keywords: Congruences. Symmetric encryption. Asymmetric encryption. The high school application. Programming in C language

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

RSA	Sistema de Criptografia com chave pública
DHM	Sistema de cifragem com duas chaves
BCPL	Basic Combined Programming Language (Linguagem de Programação Básica Combinada)
ASCII	American Standard Code for Information Interchange

LISTA DE SÍMBOLOS

$\equiv$	Congruência, ou congruente
A^{-1}	Inversa da matriz quadrada A
$\vec{v}$	Vetor
Δ	Matriz dos cofatores

SUMÁRIO

1 INTRODUÇÃO

Todas as áreas da Matemática nos fazem compreender o funcionamento da natureza, das coisas que estão ao nosso redor e nos ajudam a solucionar os problemas existentes, os que surgem e os que surgirão como desafios ao homem. Congruência módulo m é parte da Teoria dos Números que nos faz entender como trabalhar certos tipos de operações aritméticas quando não trabalhamos com a aritmética usual (clássica) conhecida por nós. É por meio dela que podemos obter o entendimento de certos fenômenos, os quais, apenas com a aritmética clássica, não poderíamos ter a oportunidade de saber explicar. Um exemplo disso são os fenômenos cíclicos. É também com ela que podemos trabalhar melhor as questões de divisibilidade, e ter um fundamental auxílio no estudo da Criptografia.

A Criptografia é a ciência que estuda a escrita em códigos, tendo como um dos seus apoios a aritmética modular. Nela, a questão principal é transmitir uma mensagem, um texto de uma determinada fonte para outra, de modo que fontes não autorizadas não tenham acesso a conteúdos da mensagem, do texto, ou seja, a preocupação é a segurança. Vem sendo desenvolvida desde os tempos antigos, e, ao longo da História, contribuiu muito e ainda contribui para a humanidade, principalmente, quando tratamos de privacidade em comunicação. Conta com vários métodos de cifragem que foram surgindo em seu desenvolvimento. Um deles é o algoritmo de Criptografia desenvolvido por três professores do Instituto de Tecnologia de Massachusetts (MIT), Ronald Rivest, Adi Shamir e Leonard Adleman, denominado como RSA, que é um método considerado o mais seguro. Utilizado hoje em vários meios de comunicação, o RSA é adotado por ser um sistema praticamente inquebrável, transmitindo assim comodidade aos seus usuários.

O Ensino Médio no Brasil, tem sofrido muito com a falta de professores preparados nas áreas específicas das disciplinas que são ensinadas. A Matemática é a que mais sofre, pois, além de não termos profissionais bem preparados, temos ainda que lidar com situações em que o desinteresse do aluno pela matéria é constante. Ora por não ter pré-requisitos suficientes, ora por não ver aplicação de parte do conteúdo estudado no seu mundo concreto, em seu dia a dia.

Este trabalho mostra uma aplicação da Matemática no dia a dia das pessoas e objetiva despertar nos estudantes o interesse pelo estudo dessa disciplina que tem grande importância. Com a aplicação de funções, matrizes e vetores em códigos, e dos restos da divisão euclidiana, queremos mostrar que a Matemática é essencial não só em áreas mais evoluídas, mas desde a base.

Trabalhando com divisão modular, queremos mostrar que conhecer bem divisão é importante, por exemplo, por suas várias aplicações. Trabalhando ainda com alguns

conteúdos do Ensino Médio aplicados à cifragem e decifragem de mensagens, procuramos mostrar que estudar Matemática é importante e, assim, despertar o interesse do aluno ao aprendizado dessa ciência. Desvendando o RSA, queremos deixar claro que a Matemática, é sobretudo, uma ferramenta para a atividade humana geral.

Este trabalho é estruturado em 5 capítulos, os quais descreveremos sucintamente a seguir.

No Capítulo 2, descreveremos um pouco sobre a história da Criptografia, iniciando pela história do sistema de numeração.

No Capítulo 3, realizamos um estudo sobre congruências, que são a base para entender os métodos criptográficos que serão estudados neste trabalho.

No Capítulo 4, apresentamos diversos métodos de Criptografia simétrica e o método de criptografia assimétrica RSA.

No capítulo 5, propomos diversas atividades envolvendo Criptografia, para turmas do Ensino Médio.

No Capítulo 6, apresentamos alguns programas executáveis do algoritmo da divisão e de Criptografia, para que o professor possa utilizar nas aulas. Não o código fonte de cada executável, mais sim o programa executável, para que os alunos possam enxergar o real funcionamento do códigos.

Há, ainda, um anexo que trata do cálculo de determinantes por meio do Teorema de Laplace, pelo fato de que esse teorema possibilita tal cálculo de qualquer matriz de qualquer ordem.

2 UM BREVE HISTÓRICO DA CRIPTOGRAFIA

Nesse capítulo [1], falaremos um pouco da história da criptografia, dividindo em períodos, citando alguns acontecimentos importantes na criptografia e alguns nomes dos que contribuíram para a sua evolução.

2.1 História da Criptografia

A Criptografia está presente nas atividades da humanidade desde a antiguidade, sendo utilizada pelos povos tanto em tempos de guerra, como em tempos de paz. Isso pelo fato de cada povo ter sua própria escrita, cultura e seus próprios valores. Além, disso possuía cada um seu sistema de governo, onde se passa a administração das riquezas e da unidade da nação. Assim esses povos precisavam de métodos para que pudessem transmitir mensagens, arquivos de propriedade de seu povo de forma segura, ou seja, em segredo, dessa forma, criptografadas para que se caísse em mãos erradas, não comprometessem a segurança do povo, ou de seu governo.

A Criptografia vem se desenvolvendo e evoluindo assim como a história da humanidade, e assim, podemos falar um pouco dessa história dividindo-a em períodos, assim como a própria história humana.

Para melhor entender a história da Criptografia, dividi-la-emos em três períodos, a saber: antiguidade (antes da idade média), idade média (antes da idade moderna e contemporânea) e histórias recente e atual (depois do fim da idade média até os tempos atuais).

2.1.1 Antiguidade

Considerado o período antes de Cristo até o ano de 476, a Criptografia, não existia como ciência, porém alguns povos já a usavam na prática. A antiguidade abrange as civilizações dos povos dos assírios, egípcios, hebreus, hititas, persas, Romana, Grega, dentre outras. Cada uma dessas civilizações desenvolveu seu próprio sistema de numeração alguns povos tendo sistemas semelhantes de outros povos, e alguns deram contribuições significativas para a ciência.

[1] Para escrever esse capítulo usamos como referência os livros (AABOE, 2013), (EVES, 2004), porém usamos como fonte principal o site (NUMABOA, 2015)

Os antigos babilônios, por exemplo, foram grandes matemáticos, e o seu sistema de numeração era de base 60 (com a aritmética bastante parecida com a utilizada nos dias atuais), o qual, até os dias atuais, usamos para marcação do tempo e estudo de ângulos. Aos fenícios é dada a honra da invenção do alfabeto. Apesar de não se saber ao certo quem inventou o alfabeto, foram eles que o difundiram pelo mediterrâneo.

Os Romanos desenvolveram um sistema de numeração que é utilizado até os dias de hoje para marcação de períodos de fatos históricos da humanidade, o sistema de numeração Romano possuía como ponto fraco a impossibilidade de realizar operações aritméticas mais sofisticadas.

Os Gregos por exemplo possuíam um sistema de numeração cifrado (um sistema de numeração cifrado é aquele em que se escolhe, primeiro se escolhe a base b, depois adota-se símbolos para $1,\ 2,\ \ldots,\ b-1;\ b,\ 2b,\ \ldots,\ (b-1)b,\ b^2,\ 2b^2,\ \ldots,\ (b-1)b^2$; e assim por diante). Ele é decimal e emprega 27 caracteres, as 24 letras do alfabeto grego e mais três outras obsoletas: *digamma, koppa* e *sampi*. Ilustraremos o sistema de numeração Grego na tabela a seguir.

Tabela 1 – Sistema de numeração Grego

1	α	10	ι	100	ρ
2	β	20	κ	200	σ
3	γ	30	λ	300	τ
4	δ	40	μ	400	υ
5	ϵ	50	ν	500	ϕ
6	digamma	60	ξ	600	χ
7	ζ	70	o	700	ψ
8	η	80	π	800	ω
9	θ	90	koppa	900	sampi

Apesar de ter que memorizar muitos símbolos nesse sistema de numeração (sistema cifrado), a representação dos números é compacta.

Por exemplo, usando esses símbolos temos os números a seguir:

$$13 = \iota\gamma,\ 58 = \nu\eta,\ 874 = \omega\mathrm{o}\delta$$

Listaremos aqui alguns acontecimentos importantes para Criptografia no período de $\pm$ 1900 a.C. a 400 a.C.

A Criptografia da Mesopotâmia ultrapassou a egípcia, chegando a um nível bastante avançado. O primeiro registro do uso da criptografia nesta região está numa fórmula para fazer esmaltes para cerâmica. O tablete de argila que contém a fórmula tem apenas cerca de $8\ cm \times 5\ cm$ e foi achado às margens do rio Tigre. Usava símbolos especiais que podem ter vários significados diferentes.

Escribas hebreus, escrevendo o Livro de Jeremias, usaram a cifra de substituição simples pelo alfabeto reverso, conhecida como ATBASH. As cifras mais conhecidas da época são o ATBASH, o ALBAM e o ATBAH, as chamadas cifras hebraicas.

Textos gregos antigos, de Enéas, o Tático, descrevem vários métodos de ocultar mensagens. Esse cientista militar e criptógrafo inventou um telégrafo hidro-ótico, um sistema de comunicação à distância. Dois grupos, separados por uma distância em que ainda era possível reconhecer a luz de uma tocha e que quisessem enviar mensagens, deviam possuir dois vasos iguais. Os vasos tinham cada qual, uma abertura no fundo, fechada por uma rolha, e eram preenchidos com água. Um bastão, que tinha mensagens inscritas, era colocado em pé dentro do vaso. Ao sinal de uma tocha, as rolhas eram retiradas simultaneamente. Quando o nível da água estivesse na altura da mensagem que se queria transmitir, outro sinal luminoso era enviado para que as rolhas fossem recolocadas.

Artha-sastra, um livro atribuído a Kautilya (ca. 370 a.C. — 283 a.C. - foi um estadista e filósofo indiano dos séculos IV e III a.C. que serviu como primeiro-ministro de Chandragupta Máuria (r. 322/321–298/297 a.C.), o fundador do Império Máuria.), foi escrito na Índia. Cita diversas cifras criptográficas e recomenda uma variedade de métodos de criptoanálise (o processo de quebrar códigos) para obter relatórios de espionagem. Esses métodos são recomendados para diplomatas.

Políbio, (200 a.C. a 118 a.C.), descreveu também uma cifra de substituição que converte os caracteres da mensagem clara em cifras que, apesar de não ser da sua autoria, ficou conhecida como Código de Políbio.

O imperador romano Júlio César usou uma cifra de substituição para aumentar a segurança de mensagens governamentais. César alterou as letras deslocando-as em três posições - A se tornava D, B se tornava E, etc. Às vezes, César reforçava sua cifragem substituindo letras latinas por letras gregas. O Código de César é o único da Antiguidade que continua sendo usado até hoje. Atualmente, denomina-se qualquer cifra baseada na substituição cíclica do alfabeto de Código de César.

A fórmula Sator ou quadrado latino (designa-se uma estrutura com forma de quadrado mágico, composta por cinco palavras latinas: SATOR, AREPO, TENET, OPERA, ROTAS, que, consideradas em conjunto (da esquerda para a direita ou de cima para baixo), dão lugar a um palíndromo) é encontrado em escavações feitas em Pompéia, também em Cirencester. inscrito numa coluna. Ocorre também num amuleto de bronze, originário da Ásia Menor, datado do século V. As palavras *rotas arepo tenet opera sator* parecem ter o efeito mágico de nunca desaparecem... persistem até hoje como um enigma de transposição.

2.1.2 Idade Média;

Períodos que vai de 476 (queda do Império Romano) a 1453 (queda de Constantinopla), foi marcado pelas migrações e invasões bárbaras, a expansão do islamismo, a fundação do império de Carlos Magno, dentre outros acontecimentos. Ficou conhecido como período das trevas (época de grandes proibições e declínio cultural e econômico da Europa).

Nesse período, a Criptografia era uma necessidade, e o movimento renascentista trouxe grandes novidades. Mesmo assim, essa ciência, sofreu danos no conhecimento sobre o assunto, muita coisa se perdeu, por ser considerada, bruxaria ou magia negra.

Esse período teve contribuições significativas da comunidade árabe-islâmica, principalmente com a invenção da Criptoanálise para a substituição monoalfabética.

A Itália foi a primeira a acordar do pesadelo medieval, iniciando o movimento renascentista ao redor da Europa, por volta de 1300. Foi responsável pelos primeiros grandes avanços e, como não podia deixar de ser, também na Criptografia. Em 1452, Veneza criou uma organização especializada em Criptografia, cujo único objetivo era lidar com os segredos, as cifras e as decifrações. Essa organização possuía três secretarias que quebravam e criavam cifras que eram usadas pelo governo.

Período de 718 a 1412

Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, escreveu o livro Kitab al Mu'amma (O livro das mensagens criptográficas), em grego, para o imperador bizantino. Infelizmente, esse livro foi perdido. Além disso, al-Khalil decifrou um criptograma bizantino muito antigo. Sua solução baseou-se no início do texto original, que ele supôs corretamente como sendo "Em nome de Deus" - modo comum de começar qualquer texto naquela época. Esse método criptoanalítico, conhecido como método da palavra provável, tornou-se padrão. Foi usado até na decifração de mensagens cifradas pela máquina Enigma, durante a Segunda Guerra Mundial.

Outra pessoa notável na área de Criptografia foi Abu Yusuf Yaqub ibn Is-haq ibn as Sabbah ibn 'omran ibn Ismail Al-Kindi, que escreveu Risalah fi Istikhraj al Mu'amma (Escritos sobre a decifração de mensagens Criptográficas). Esse livro está conservado, sendo o mais antigo sobre criptologia. Nele, o autor faz análises de frequência, razão pela qual Al-Kindi pode ser considerado o bisavô da Matemática Estatística.

Outro importante criptógrafo foi Ibrahim ibn Mohammad ibn Dunainir, que é autor do livro redescoberto em 1987, Maqasid al-Fusul al-Mutarjamah an Hall at-Tarjamah (Explicações claras para a solução de mensagens secretas). Esse livro contém uma inovação importante: 19 cifras algébricas, ou seja, a substituição de letras por números que podem ser transformados aritmeticamente.

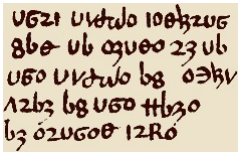
Em 1226, uma criptografia política discreta apareceu nos arquivos de Veneza, onde pontos e cruzes substituíam as vogais em algumas palavras esparsas.

O frade franciscano inglês Roger Bacon (1214-1294), conhecido como Doctor mirabilis, descreveu sete métodos de cifras e escreveu: "Um homem é louco se escrever um segredo de qualquer outra forma que não seja a de dissimulá-lo do vulgar." Um nome importante era Taj ad-Din Ali ibn Muhammad ibn Abdul'aziz ibn ad-Duraihim, que é autor do livro redescoberto em 1987, Miftah al-Kunuz fi Idah al-Marmuz (Chaves para a elucidação de mensagens secretas), que contém uma classificação das cifras, análises de frequência em várias línguas, uma tabela de Trithemius (Vigenère) e grades de transposição.

Em 1378, depois do Cisma de Avignon, o antipapa Clemente VII decidiu unificar o sistema de cifras da Itália Setentrional, designando Gabriele Lavinde para coordenar a tarefa. Lavinde compilou uma coleção de cifras em um manual, do qual o Vaticano conserva uma cópia de 1379. Com seu alfabeto de substituição combinada (código/cifra), Lavinde uniu a cifra de substituição a um código com listas de palavras, sílabas e nomes equivalentes. Esse sistema foi amplamente utilizado por diplomatas e alguns civis europeus e americanos por mais de 450 anos.

Geoffrey Chaucer, considerado o melhor poeta inglês antes de Shakespeare, no seu "The Equatorie of the Planetis", um suplemento do seu "Treatise on the Astrolabe", incluiu seis passagens escritas em cifras. O sistema de cifras consiste num alfabeto de símbolos de substituição.

Figura 1 – Criptograma feito pela cifra de substituição

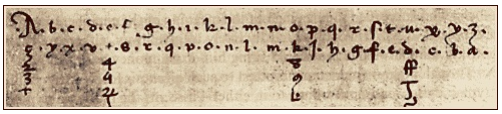


FONTE: www.numaboa.com.br/images/stories/chaucer.gif (julho 2015)

A solução do criptograma mostrado acima é: "This table servith for to entre in to the table of equacion of the mone on either side".

Simeone de Crema usou uma chave na qual cada vogal do texto original possuía vários equivalentes. Isso comprova silenciosamente que, naquela época, o Ocidente conhecia a criptoanálise. Não pode haver outra explicação para o aparecimento desses múltiplos substitutos ou homófonos. O fato dos homófonos serem aplicados a vogais, e não apenas indiscriminadamente, indica, no mínimo, o conhecimento do esboço de uma análise de frequência.

Figura 2 – Análise de frequência de Simeone de Crema



FONTE: www.numaboa.com.br/images/stories/cremakey.gif (julho 2015)

Michele Steno, doge de Veneza, fornece-nos um dos primeiros exemplos de cifras homofônicas: escolhia um dos muitos símbolos para cada caractere, além de utilizar nulos e caracteres especiais para certas palavras de uso frequente.

2.1.3 Histórias recente e atual

Época das grandes invenções, dos descobrimentos marítimos, da Renascença. Teve fatos marcantes como a centralização monárquica e o absolutismo, as guerras religiosas, a nova política econômica, o advento da ciência moderna e da formação das potências modernas e expansão colonial. É a época de grandes invenções relacionadas à comunicação como, o telégrafo e o rádio, que tiveram um papel fundamental na mudança radical da criptografia.

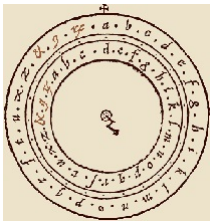
No século XIX o desenvolvimento tecnológico continua, e as duas Grandes Guerras Mundiais aumentaram exponencialmente a importância da Criptografia, da Criptoanálise e da Criptologia. O surgimento do computador tem um impacto ainda maior que os já causados pelo telégrafo e pelo rádio. A Criptografia distancia-se dos conceitos tradicionais para entrar numa nova era.

Durante o período de 1466 até a atualidade, várias pessoas contribuíram para o desenvolvimento da Criptografia. Citaremos alguns deles.

Substituição Polialfabética e Criptoanálise

Leon Battista Alberti (1404-1472) era amigo de Leonardo Dato, um secretário Pontifical, que o aproximou da criptologia. Alberti inventou e publicou a primeira cifra polialfabética, criando um disco de cifragem, conhecido como Disco de Alberti. Ao que tudo indica esta classe de cifra não foi quebrada até os anos de 1800. Alberti também tem muitos escritos sobre o estado da arte de cifras, além da sua própria invenção. Usou seu disco para facilitar a obtenção de criptogramas. Estes sistemas eram muito mais fortes do que a nomenclatura usada pelos diplomatas da época e foram aplicados durante muitos séculos. O Trattati in cifra de Leon Battista Alberti foi publicado em Roma, na Itália, em 1470. Continha especialmente teorias e métodos de cifragem, de decifragem e dados estatísticos.

Figura 3 – Disco de cifragem



FONTE: www.numaboa.com.br/images/stories/cremakey.gif (julho 2015)

Johannes von Heydenberg aus Trittenheim/Mosel, ou Johannes Trithemius (1462-1516), escreveu o primeiro livro impresso de Criptologia. Inventou uma cifra esteganográfica na qual cada letra era representada por uma palavra obtida de uma sucessão de colunas. A série de palavras resultantes parecia-se com uma oração legítima. Também descreveu cifras polialfabéticas na forma de tabelas de substituição retangulares que, na época, já tinham se tornado padrão. Introduziu a noção da troca de alfabetos a cada letra. Trithemius escreveu, porém não publicou sua Steganographia, a qual circulou como manuscrito por mais de cem anos, sendo copiada por muitas pessoas que desejavam extrair os segredos que se pensava que continha. A verdadeira história do feiticeiro que conjurava espíritos e praticava magia negra você encontra em "O Segredo do Terceiro Livro".

Substituição Polialfabética, Nomenclaturas e Criptoanálise

Período de 1550 a 1691

Foi publicado o *De subtilitate libri XXI* de Girolamo Cardano (1501-1576). Uma obra famosa, de um notável matemático, físico e filósofo contém uma quantidade considerável de informações a respeito de processos de cifragem. Sendo reimpressa várias vezes. Cardano inventou o primeiro método com auto-chave, mas seu sistema era imperfeito. Outra invenção, a grelha de Cardano, consiste numa folha de material rígido onde se, encontram, em intervalos irregulares, pequenas aberturas retangulares da altura de uma linha de escrita e de comprimento variável. O remetente escreve o texto nas aberturas, depois retira a folha e completa os espaços vazios com letras quaisquer. O destinatário põe a mesma grelha sobre o texto cifrado para ler a mensagem. Em 1556, Cardano publica De *rerum varietate libri XVII*, o qual contém informações criptográficas e era a continuação do seu popular *De Subtilitate*.

François Viète (1540-1603), matemático francês, também foi um dos melhores especialistas em cifras de todos os tempos. No final do século XVI, o império espanhol dominava grande parte do mundo e, justamente por isso, os agentes espanhóis precisavam se comunicar usando uma cifra muito intrincada. Na realidade, a cifra era composta por mais de 500 caracteres, usados pelo rei Felipe II da Espanha durante sua guerra em defesa do Catolicismo Romano e dos huguenotes franceses. Algumas mensagens de soldados espanhóis foram interceptadas pelos franceses e acabaram nas mãos do rei Henrique IV da

França que as entregou para Viète, o matemático, na esperança de que ele as decifrasse. Viète teve sucesso e guardou segredo quando, após dois anos, os espanhóis descobriram seu feito.

Blaise de Vigenère (1523-1596) escreveu um livro sobre cifras, incluindo os primeiros sistemas autênticos de texto claro e texto cifrado com auto-chave, nos quais letras prévias do texto claro ou cifrado são usadas para a letra chave atual.

Em 1586, Blaise de Vigenère publica seu Traicté des chiffres, de 600 páginas. Nele discute muitas cifras, inclusive o sistema da auto-chave progressiva usada em algumas máquinas de cifragem modernas, e o assim chamado método Vigenère tableau.

Gottfried Wilhelm von Leibniz (1646-1716), filósofo e matemático alemão, inventou o Cálculo Diferencial (independentemente de Sir Isaac Newton, outro inventor do Cálculo Diferencial), a máquina de calcular e descreveu minuciosamente o sistema binário. Sua máquina de calcular usava a escala binária. Essa escala, obviamente mais elaborada, é utilizada até hoje, sendo conhecida como código ASCII (American Standard Code for Information Interchange).

Substituição Polialfabética, Nomenclaturas e Criptoanálise. A eletricidade começa a mudar as comunicações.

Período do Século XVIII ao Século XIX

Crystobal Rodriguez (?1677-1735) escreveu a *Bibliotheca Universal de la Polygraphía Española*, publicada em Madrid em 1738. Essa obra é considerada como o primeiro estudo completo da Criptografia e da paleografia da Espanha.

Thomas Jefferson (1743-1826), possivelmente com a ajuda de Dr. Robert Patterson, um matemático da Universidade da Pensilvânia, inventa um cilindro cifrante (ou cifra de roda).

Louis Braille (1809-1852), educador francês, ficou cego aos 3 anos de idade. Interessou-se por um sistema de escrita, apresentado na escola Charles Barbier, no qual uma mensagem codificada em pontos era cunhada em papel-cartão. Aos 15 anos de idade, trabalhou numa adaptação, escrita com um instrumento simples. O Sistema Braille consiste de 63 caracteres, cada um deles constituído por 1 a 6 pontos dispostos numa matriz ou célula de seis posições. Mais tarde, adaptou este sistema para a notação musical. Publicou tratados sobre esse sistema em 1829 e 1837. O Sistema Braille é universalmente aceito e utilizado até os dias de hoje.

O assistente de Samuel Morse (1791-1872) desenvolve o código que recebeu o nome do chefe. Na verdade, não é um código, mas sim um alfabeto cifrado em sons curtos e longos. Morse foi o inventor de um dispositivo que chamou de telégrafo e, em 1844, enviou sua primeira mensagem com os dizeres “What hath God wrought ’ ’.

Em 1854, figura polêmica, Charles Babbage (1791-1871), matemático inglês e hoje chamado de "o pai do computador", Babbage quebra a cifra de Vigenère e projeta as primeiras máquinas de cálculo sofisticadas, precursoras do computador: a Máquina das Diferenças e a Máquina Analítica.

Substituição polialfabética e máquinas cifrantes. Estatística e Criptoanálise.

Período do Século XX.

Os computadores revolucionaram a informação, causando uma reviravolta na Criptografia. Por um lado ampliaram seus horizontes, por outro tornaram a Criptografia quase que indispensável.

Guglielmo Marconi (1874-1937), Prêmio Nobel de Física em 1909, inicia a era da comunicação sem fio. Apesar da vantagem da comunicação de longa distância sem o uso de fios ou cabos, o sistema é aberto e aumenta o desafio da Criptologia. Inicialmente, a telegrafia sem fio utilizava apenas o código Morse, acessível a todos que captassem os sinais. Impunha-se a necessidade de codificações que garantissem o sigilo das mensagens.

Em 1913, o capitão Parket Hitt reinventou o cilindro cifrante, dessa vez em forma de fita, abrindo caminho para o M-138-A da Segunda Guerra Mundial. O major Joseph Oswald Mauborgne (1881-1971) passou a cifra de fita de Hitt novamente para a forma de cilindro, fortaleceu a construção alfabética e produziu o dispositivo que se transformaria no M-94. Em 1918 aperfeiçoou a cifra de Vernam, o One-Time-Pad (OTO) cuja tradução livre para o Português seria Bloco Descartável, essa cifra será discutida no capítulo 4.

Figura 4 – Cilindro Cifrante

FONTE: http://criptografia101.blogspot.com.br/2011/09/contexto-historico.html

Em 1929, Lester S. Hill (1891-1961), matemático americano e educador que se interessou por aplicações da Matemática, publica seu livro *Cryptography in an Algebraic Alphabet*, no qual um bloco de texto claro é cifrado através de uma operação com matrizes.

Período de 1927 a 1933.

O uso da criptografia não estava restrito apenas a pesquisadores para aplica-la para o bem. Criminosos também usavam a criptografia para seus propósitos, formando

sistemas de contrabando cada vez mais complexos. Assim começam a utilizar máquinas para decifrar códigos. Nos anos 1930 a máquina SIGABA (M-134-C) é inventada nos EUA por William F. Friedman. Depois surgiram outras máquinas, como por exemplo: A máquina Enigma usada por militares alemães, a máquina inglesa TYPEX que era uma imitação da Enigma.

Os computadores mudam radicalmente o cenário

Com o advento dos computadores, os EUA adotam como padrão de encriptação de dados o FIPS PUB-46, conhecido hoje como DES (Data Encryption Standard). Na ocasião, Diffie e Martin lançaram dúvidas quanto à segurança do DES, apontando que não seria impossível obter a chave através da "força bruta", o que acabou acontecendo 20 anos mais tarde a um custo 100 vezes inferior ao inicialmente estimado.

Inspirados no texto publicado por Diffie (matemático e criptógrafo estadunidense) e Martin (criptógrafo estadunidense) e apenas principiantes na Criptografia, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman começaram a discutir como poderiam criar um sistema de chave pública que fosse prático. Ron Rivest acabou tendo uma grande ideia e a submeteu à apreciação dos amigos: era uma cifra de chave pública, tanto para confidencialidade quanto para assinaturas digitais, baseada na dificuldade da fatoração de números grandes. Foi batizada de RSA, de acordo com as primeiras letras dos sobrenomes dos autores. Confiantes no sistema, em 4 de abril de 1970 os três entregaram o texto para Martin Gardner, para que fosse publicado na revista Scientific American. Em 1978 o algoritmo RSA é publicado nas "Communication"da ASM.

Em 1986, o algoritmo de Criptografia da curva elíptica é sugerida. Na década de 1990, os trabalhos com computadores quânticos e criptografia quântica se intensificam, e os trabalhos com biometria aplicada na autenticação (impressões digitais, íris, etc) tomam impulso e são aplicados na autenticação tomam impulso. Surge então A Proposal for a New Block Encryption Standard (Uma Proposta para um Novo Padrão de Encriptação de Bloco), o que viria a ser o IDEA (International Data Encryption Algorithm), para substituir o DES. O IDEA utiliza uma chave de 128 bits e emprega operações adequadas para computadores de uso geral, tornando as implementações do software mais eficientes.

Os computadores e a Internet globalizam os sistemas de comunicação.

O professor Ron Rivest, autor dos algoritmos RC2 e RC4 incluídos na biblioteca de criptografia BSAFE do RSADSI, publica a proposta do algoritmo RC5 na Internet. Este algoritmo usa rotação dependente de dados como sua operação não linear e é parametrizado de modo que o usuário possa variar o tamanho do bloco, o número de estágios e o comprimento da chave. Ainda é cedo para se avaliar corretamente os parâmetros em relação à força desejada, apesar de que uma análise feita pelo RSA Labs, mostrada na CRYPTO 95, tenha sugerido que $w = 32$ e $r = 12$ proporcionam uma segurança maior

que a do DES. O algoritmo blowfish, uma cifra de bloco de 64 bits com uma chave de até 448 bits de comprimento, é projetado por Bruce Schneier.

Em novembro de 1994, David Wheeler (pioneiro da computação britânico) e Roger Needham (Professor de Sistemas de Computação, da Universidade de Cambridge), na Universidade de Cambridge, Inglaterra, lançam o TEA - Tiny Encryption Algorithm, uma cifra de bloco do tipo Feistel que rivaliza com o IDEA pela velocidade de processamento, pela simplicidade da implementação e por ser de domínio público (sem patentes como a IDEA). O algoritmo TEA é uma cifra de bloco com chaves de 128 bits.

Em 1998, o padrão de encriptação DES de 56 bits é quebrado em 56 horas por pesquisadores da Electronic Frontier Foundation – EFF do Vale do Silício. Wheeler e Needham divulgam mais um aperfeiçoamento do TEA (e do XTEA e BlockTEA) – o XXTEA usa uma função de arredondamento mais elaborada, sendo substituído alguns anos mais tarde pelo algoritmo Rijndael e é denominado AES - Advanced Encryption Standard.

3 CONGRUÊNCIA MÓDULO M E APLICAÇÕES

Nesse capítulo[1], faremos uma breve abordagem sobre Congruência módulo m, em que aplicaremos os resultados obtidos nos capítulos seguintes.

Congruência é uma parte da Teoria dos Números que estuda a aritmética dos restos da divisão euclidiana módulo m e possui várias aplicações em diversas áreas da Matemática Pura e Aplicada, como por exemplo, nos números de Fermat, em problemas de divisão, na Criptografia, dentre outros. Nosso trabalho abordará algumas das aplicações da Criptografia.

O estudo das congruências mostra que nem sempre os resultados das contas ocorrem como dita a aritmética clássica ou usual. Um exemplo ocorre quando falamos em horas, onde temos $17+21=14$, pois se são 5 horas da tarde (dezessete horas do dia), então, daqui a 21(vinte e uma horas), serão 14 horas do dia seguinte (duas horas da tarde). Isso não ocorre somente com horas, mas também com qualquer fenômeno cíclico que produza uma aritmética peculiar, semelhante a essa, conhecida como *aritmética modular*. Nesse tipo de aritmética, há como adicionar, multiplicar e até resolver equações a uma ou mais variáveis.

3.1 Relação de equivalência

Definição 3.1.1 (Produto Cartesiano)**.** *Dados dois conjuntos X e Y não vazios, chama-se* ***produto cartesiano*** *X por Y (representa-se $X\times Y$) desses conjuntos o conjunto de todos os pares ordenados (a,b), com $a\in X$ e $b\in Y$, isto é,*

$$X\times Y=\{(a,b)|\ a\in X\ e\ b\in Y\}.$$

Quando $X=Y$, temos $X\times X=\{(a,b)|\ a,b\in X\}$.

Considere um conjunto $X\subset\mathbb{Z}$ e uma relação R em X, ou seja, R é um subconjunto qualquer de $X\times X$ ($R\subset X\times X$). Denotamos por aRb se o par ordenado (a,b) pertence a R ($(a,b)\in R$).

Considere dois conjuntos: X, o conjunto de músicos, e Y o conjunto de peças musicais. Quando dizemos que "x tocou y", estamos querendo dizer que x está em relação

[1] Os resultados apresentados neste capítulo podem ser encontrados em diversos livros de ***Teoria dos Números***, tais como: (COUTINHO, 2003), (HEFEZ, 2014), (LANDAU, 2013), (SHOKRANIAN, 2005), (HEFEZ, 2003), (FERREIRA, 2010), (HALMOS, 2001) dentre outros.

com y. Se dizemos que "Beethoven tocou a Nona Sinfonia", estamos querendo dizer que "Beethoven" está relacionado com a "Nona Sinfonia".

Definição 3.1.2 (Relação de equivalência)**.** *Uma relação R em X é denominada relação de equivalência em X se, quaisquer que sejam $a,b,c,\in X$, R tem as seguintes propriedades:*

(i) aRa (reflexiva);

(ii) Se aRb, então bRa (simétrica);

(iii) Se aRb e bRc, então aRc (transitiva).

Exemplo 3.1.1. *Seja $A = \{x|x$ é um triângulo no plano euclidiano$\}$. Para x,y em A, considere a seguinte relação R em A:*

$$(x,y) \in R \text{ se, e somente se "}x \text{ é semelhante a } y\text{".}$$

Então R é uma relação de equivalência em A.

Exemplo 3.1.2. *Dado $n \in \mathbb{N},\ n > 2$, considere a seguinte relação R no conjunto dos números inteiros:*

$$(a,b) \in R \text{ se, e somente se, } a-b \text{ é divisível por } n.$$

. R possui as seguintes propriedades:

(i) reflexiva, pois para todo $a \in \mathbb{Z}$, temos $a-a=0$ e 0 é um número divisível por n. De fato, temos $0 = 0.n$.

(ii) simétrica, pois para todos $a,b \in \mathbb{Z}$, se $a-b$ é divisível por n, então $a-b=k.n$ com $k \in \mathbb{Z}$. Multiplicando essa igualdade por -1, obtemos $b-a=-kn$. Como $-k \in \mathbb{Z}$, $b-a$ é divisível por n. Logo, se a está relacionado com b, então, b está relacionado com a.

(iii) transitiva, pois, para todos, $a,b,c \in \mathbb{Z}$ tais que aRb e bRc, temos $a-b=k.n$ e $b-c=m.n$, onde $k,m \in \mathbb{Z}$. Logo,

$$a-c=(a-b)+(b-c)=k.n+m.n=(k+m).n$$

Como $(k+m) \in \mathbb{Z}$, $a-c$ é divisível por n. Logo, aRc.
Portanto, R é uma relação de equivalência.

Seja R uma relação de equivalência em um conjunto X.

Definição 3.1.3. ***a)*** *O conjunto de todos os elementos que são relacionados a um elemento a de X é chamado de* ***classe de equivalência*** *de a. Notação: $\overline{a} = \{b \in X \mid bRa\}$.*

b) *O conjunto de todas as classes de equivalência módulo R chamado conjunto quociente de X por R. Notação: $X/R = \{\bar{a} \mid a \in X\}$*

Exemplo 3.1.3. *A relação de equivalência em um conjunto X obtida pelo produto cartesiano $X \times X$ determina apenas uma classe de equivalência. De fato, para todo $a \in X$, temos:*

$$\overline{a} = \{x \in X \mid xRa\} = \{x \in X \mid (x,a) \in X \times X\} = X.$$

Observe que, independentemente de a classe de equivalência ser o mesmo conjunto, o conjunto quociente de X por $X \times X$ é um conjunto unitário cujo único elemento é o conjunto X. Denotamo-lo por

$$X/(X \times X) = \{X\}.$$

Exemplo 3.1.4. *Seja $R = \{(x,x),(x,y),(y,x),(y,y),(z,z)\}$ uma relação em $X = \{x,y,z\}$ dada. Vamos obter as classes de equivalência. Temos:*

$$\begin{aligned} \overline{x} &= \{a \in X \mid aRx\} = \{x,y\}, \\ \overline{y} &= \{a \in X \mid aRy\} = \{x,y\}, \\ \overline{z} &= \{a \in X \mid aRz\} = \{z\}. \end{aligned}$$

Como $\overline{x} = \overline{y}$, temos apenas duas classes de equivalência distintas. Logo, o conjunto quociente possui dois elementos. $X/R = \{\overline{x},\overline{z}\} = \{\{x,y\},\{z\}\}$.

Na próxima seção, definiremos as operações de adição e multiplicação em uma classe de equivalência módulo m.

3.2 Congruência módulo m

Para estudar a aritmética módulo m, precisamos ter conhecimento de *divisão euclidiana*, a qual se baseia no seguinte fato: quando não existe uma relação de divisibilidade entre dois números, é possível efetuar uma divisão com resto pequeno.

Definição 3.2.1 (Algoritmo da divisão de Euclides)**.** *Se $a,b \in \mathbb{Z}$, são tais que $0 < |a| < |b|$, então existem $q,r \in \mathbb{Z}$ tais que $b = a.q + r$, com $0 \leq r < |a|$.*

O algoritmo da divisão aparece desde o início dos estudos escolares. A aplicação desse algoritmo, no entanto, não se passa apenas em divisões simples que aprendemos na educação básica: aplicações em Teoria dos Números nos mostra que o algoritmo de

Euclides tem fundamental utilidade em demonstrações de Lemas, Teoremas, Proposições e Corolários. Além disso, esse algoritmo é aplicado em Criptografia, no uso da cifragem e decifragem de textos.

Notações: Sejam a e b dois números naturais.

(a) O máximo divisor comum (mdc) de $|a|$ e $|b|$ será representado por (a,b);

(b) $a \mid b$ significa que existe $n \in \mathbb{Z}$ tal que $b = a.n$ (Lê-se "a" divide "b").
Denotamos por $a \nmid b$ quando a não divide b.

Enunciaremos um importante Lema, cuja demonstração pode ser encontrada em (HEFEZ, 2003)

Lema 3.2.1 (Lema de Euclides)**.** *Sejam $a,b,n \in \mathbb{N}$ tais que $a < n.a < b$. Se $(a,b-n.a)$ existe, então (a,b) existe e $(a,b) = (a,b-n.a)$.*

Definição 3.2.2. *Dados a e b naturais dizemos que a é congruente a b módulo m $(m > 1)$ se $m \mid b-a$. Denotemos isso por $a \equiv b \ mod \ m$. Se $m \nmid b-a$, dizemos que a é incongruente a b módulo m e denotamos por $a \not\equiv b \ mod \ m$.*

Considere um número natural m diferente de zero. Se a e b são dois números inteiros tais que os restos (r_a e r_b) de suas respectivas divisões por m são iguais, então existe uma relação de congruência módulo m entre a e b e reciprocamente. Segue o resultado pertinente:

Proposição 3.2.1. *A seguinte equivalência é verdadeira:*

$$a \equiv b \ mod \ m \Longleftrightarrow r_a = r_b$$

Prova:

$a \equiv b \ mod \ m$ significa, de acordo com a Definição 3.2.2 que, $m \mid b-a$. Assim, existe $q \in \mathbb{Z}$ tal que $b-a = m.q$. Ora, $b-a = m.q$ só é possível se $a = m.q_a$ e $b = m.q_b$ $(r_a = r_b = 0)$, ou então $a = m.q_a + r_a$ e $b = m.q_b + r_b$, em que $r_a = r_b$.

Por outro lado, $r_a = r_b$ implica $b-a = (m.q_b + r_b) - (m.q_a + r_a) = m.(q_b - q_a) + (r_b - r_a)$ de maneira que $b-a = m.(q_b - q_a)$. Logo, $m \mid b-a$. Portanto, $a \equiv b \ mod \ m$.

□

Exemplo 3.2.1. *(a)* $18 \equiv 33 \ mod \ 5$. *De fato,* $18 = 5.3+3$ *e* $33 = 5.6+3$, *e portanto* $r_{18} = r_{33}$.

(b) $19 \not\equiv 33 \ mod\ 5$. *De fato,* $19 = 5.3+4$ *e* $33 = 5.6+3$, *e portanto* $r_{18} \neq r_{33}$.

A congruência módulo m é uma relação de equivalência. Segue o resultado.

Proposição 3.2.2. *Seja* $m \in \mathbb{N}$, $m > 1$. *Para todos* $a, b, c \in \mathbb{Z}$, *temos:*

(a) Se $a \equiv a \ mod\ m$ *(reflexiva);*

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

(c) Se $a \equiv b \ mod\ m$ *e* $b \equiv c \ mod\ m$, *então* $a \equiv c \ mod\ m$ *(transitiva).*

Prova:

(a) Sabemos que $m \mid 0$, e, portanto, $m \mid a-a$;

(b) Se $a \equiv b \ mod\ m$ temos $m \mid b-a$, ou seja, existe $n \in \mathbb{Z}$ tal que $b-a = m.n$. Logo $a-b = m.(-n)$, $-n \in \mathbb{Z}$ e, assim, $m \mid a-b$. Portanto, $b \equiv a \ mod\ m$.

(c) Se $a \equiv b \ mod\ m$ e $b \equiv c \ mod\ m$, temos $m \mid b-a$ e $m \mid c-b$, ou seja, existem n_1 e $n_2 \in \mathbb{Z}$ tais que $b-a = m.n_1$ e $c-b = m.n_2$. Logo, $c-a = m.(n_1+n_2)$ e, assim, $m \mid c-a$. Portanto, $a \equiv c \ mod\ m$.

□

Entre os números inteiros estão definidas duas operações fundamentais: a adição, que aos números $m, n \in \mathbb{Z}$, faz corresponder a soma $m+n$, e a multiplicação, que lhes associa o produto $m.n$.

Definição 3.2.3 (Relação de congruência módulo m)**.** *Dado um número inteiro* m, *considere a seguinte relação em* $\mathbb{Z}$, *chamada* ***relação de congruência módulo m****, e definida por*

$$R_m = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \ mod\ m\}.$$

Pela Proposição 3.2.2, R_m é uma relação de equivalência. Em seguida, considere o conjunto das classes de equivalência, denotada por $\mathbb{Z}_m$. Com auxilio do algoritmo da divisão de Euclides, concluí-se que

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Define-se uma adição e uma multiplicação em $\mathbb{Z}_m$ da seguinte forma: para $\overline{a}$ e $\overline{b}$ em $\mathbb{Z}_m$, temos:

(i) $\overline{a}+\overline{b}=\overline{a+b}$

(ii) $\overline{a}.\overline{b}=\overline{a.b}$

Mostraremos que essas operações de adição e multiplicação em $\mathbb{Z}_m$ estão bem definidas, isto é, quaisquer que sejam os representantes escolhidos de uma classe para calcular a soma ou o produto de duas classes o resultado sempre será o mesmo. Veja:

(i) Se $\bar{a}=\bar{a'}$ e $\bar{b}=\bar{b'}$, então $\overline{a+b}=\overline{a'+b'}$. De fato, $\overline{a}=\overline{a'}$ e $\overline{b}=\overline{b'}$ equivale a dizer que $a-a'$ e $b-b'$ são múltiplos de m e então, somando os dois obtemos como resultado um múltiplo de m, isto é, $(a-a')+(b-b')=(a+b)-(a'+b')$ é múltiplo de m. Portanto, $\overline{a+b}=\overline{a'+b'}$.

(ii) Se $\bar{a}=\bar{a'}$ e $\bar{b}=\bar{b'}$, então $\overline{a.b}=\overline{a'.b'}$. De fato, $\overline{a}=\overline{a'}$ e $\overline{b}=\overline{b'}$ equivale dizer que $a-a'$ e $b-b'$ são múltiplos de m. Daí, existem $\alpha,\beta\in\mathbb{Z}$ tais que $a=a'+m.\alpha$ e $b=b'+m.\beta$. Logo $a.b=(a'+m.\alpha)(b'+m.\beta)=a'.b'+a'.m.\beta+b'.m.\alpha+m^2.\alpha.\beta$, que nos fornece $ab=a'b'+m.(a'\beta+b'\alpha)+m^2\alpha\beta$. Assim $a.b-a'.b'$ é múltiplo de m. Portanto, $\overline{a.b}=\overline{a'.b'}$.

Dizemos que $\overline{a}\in\mathbb{Z}_m$ possui inverso $\overline{x}\in\mathbb{Z}_m$ quando $\overline{a}.\overline{x}=\overline{1}$ é verificada em $\mathbb{Z}_m$. Observe que, quaisquer que sejam $a,b\in\mathbb{Z}$, $a\equiv b\ mod\ 1$. Portanto, podemos supor, sem perda de generalidade, que $m>1$.

Essas operações possuem as mesmas propriedades da aritmética usual, que são:

Propriedade 3.2.1 (**Propriedades da Adição e Multiplicação**). *Dados $a,b,c\in\mathbb{Z}_m$ temos,*

(P1) Associativa: $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$ e $(\overline{a}.\overline{b}).\overline{c}=\overline{a}.(\overline{b}.\overline{c})$;

(P2) Comutativa: $\overline{a}+\overline{b}=\overline{b}+\overline{a}$ e $\overline{a}.\overline{b}=\overline{b}.\overline{a}$;

(P3) Elemento neutro: $\overline{a}+\overline{0}=\overline{a}$ e $\overline{a}.\overline{1}=\overline{a}$;

(P4) Simétrico da adição: Existe $\overline{a'}\in\mathbb{Z}_m$, tal que $\overline{a}+\overline{a'}=\overline{0}$ em que $\overline{a'}=\overline{-a}$ é simétrico ou oposto de $\overline{a}$;

(P5) Inverso multiplicativo: Seja $\overline{x}\in\mathbb{Z}_m$ tal que $\overline{a}.\overline{x}=\overline{1}$. $\overline{x}=\overline{a}^{-1}$ é chamado de inverso multiplicativo de $\overline{a}$;

(P6) Distributiva: $\overline{a}.(\overline{b}+\overline{c})=\overline{a}.\overline{b}+\overline{a}.\overline{c}$.

Em congruências há uma aritmética que se baseia no trabalho com restos da divisão euclidiana, conforme Proposição a seguir.

Proposição 3.2.3. *Seja $a,b,c,d \in \mathbb{Z}$. Se $a \equiv b \ mod \ m$, e $c \equiv d \ mod \ m$ então:*

(a) $a+c \equiv b+d \ mod \ m$;

(b) $a.c \equiv b.d \ mod \ m$.

Prova:

(a) $a+c = m(q_a+q_c)+(r_a+r_c)$ e $b+d = m(q_b+q_d)+(r_b+r_d)$, $r_a = r_b$ e $r_c = r_d$. Assim, $r_a+r_c = r_b+r_d$ e, portanto, pela Proposição 3.2.1, $a+c \equiv b+d \ mod \ m$.

(b) $a.c = m^2.q_a.q_c + m.(q_a.rc + q_c.r_a) + r_a.r_c$ e $b.d = m^2.q_b.q_d + m.(q_b.r_d + q_d.r_b) + r_b.r_d$. Como $r_a = r_b$ e $r_c = r_d$, temos $r_a.r_c = r_b.r_d$. Assim, $m \mid (b.d - a.c)$, e, portanto, $a.c \equiv b.d \ mod \ m$.

□

Exemplo 3.2.2. *Observe que*

$$32 \equiv 47 \ mod \ 15 \ e \ 19 \equiv 64 \ mod \ 15.$$

Assim, pela Proposição 3.2.3, $32+19 \equiv 47+64 \ mod \ 15$ *e* $32.19 \equiv 47.64 \ mod \ 15$. *Isto é,* $51 \equiv 111 \ mod \ 15$ *e* $608 \equiv 3008 \ mod \ 15$. *De fato,* $111-51 = 60 = 15.14$ *e* $3008-608 = 2400 = 15.160$.

O próximo Corolário é uma consequência direta da Proposição 3.2.3.

Corolário 3.2.1. *Para todo $n \in \mathbb{N}^*$, $a,b \in \mathbb{Z}$, se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$.*

A demonstração do Corolário 3.2.1 também pode ser feita por indução sobre n.

Corolário 3.2.2. *Sejam $a,b \in \mathbb{Z}^*$ e $m \in \mathbb{N}$, $m > 1$. Se $a+b \equiv 0 \ mod \ m$, então, $\forall n \in \mathbb{N}^*$, $a^{2n} \equiv b^{2n} \ mod \ m$ e $a^{2n+1}+b^{2n+1} \equiv 0 \ mod \ m$.*

Prova:

Como $a+b \equiv 0 \ mod \ m$, então $m \mid a+b$ e, portanto, $m \mid (a+b)(a-b)$. Desde que $(a+b)(a-b) = a^2-b^2$; $m \mid a^2-b^2$, então $a^2 \equiv b^2 \ mod \ m$. Assim, pelo Corolário 3.2.1, temos $a^{2n} \equiv b^{2n} \ mod \ m$, $\forall \ n \in \mathbb{N}^*$. Por outro lado, como $a^{2n+1}+b^{2n+1} = (a+b)(a^{2n} - b.a^{2n-1} + \ldots - b^{2n-1}a + b^{2n})$ e
$a+b \equiv 0 \ mod \ m$, temos $m \mid a^{2n+1}+b^{2n+1}$ e, portanto,

$$a^{2n+1} + b^{2n+1} \equiv 0 \ mod \ m.$$

□

A demonstração do próximo e importante teorema pode ser encontrado em (HEFEZ; FERNANDEZ, 2013) ou (SHOKRANIAN MARCUS SOARES, 1999)

Teorema 3.2.1 (Pequeno Teorema de Fermat)**.** *Se p é um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \ mod \ p$. Além disso, se $p \nmid a$, então $a^{p-1} \equiv 1 \ mod \ p$.*

Como consequência desse Teorema temos:

Proposição 3.2.4. *p é um número primo e $a, b \in \mathbb{Z}$, então*

$$(a+b)^p \equiv (a^p + b^p) \ mod \ p.$$

Prova:
Pelo Teorema 3.2.1 e pela Proposição 3.2.3(a) temos

$$(a+b)^p \equiv a+b \ mod \ p \text{ e } a^p + b^p \equiv a+b \ mod \ p.$$

Então, $r_{(a+b)^p} = r_{a+b}$ e $r_{(a^p+b^p)}$, e, assim, $r_{(a+b)^p} = r_{(a^p+b^p)}$. Portanto $(a+b)^p \equiv (a^p + b^p) \ mod \ p$.

□

Proposição 3.2.5. *Sejam $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{N}$. Temos*

$$a + c \equiv b + c \ mod \ m, \ se \ e \ somente \ se \ a \equiv b \ mod \ m.$$

Prova:

Suponhamos que $a \equiv b \ mod \ m$. Desde que $c \equiv c \ mod \ m$, pela Proposição 3.2.3(a), temos

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

Suponhamos, agora que $a + c \equiv b + c \ mod \ m$. Logo, $m \mid (a+c) - (b+c)$, ou seja, $m \mid a - b$. Portanto, $a \equiv b \ mod \ m$.

□

Exemplo 3.2.3. *Observe que $30 \equiv 78 \ mod \ 8$, pois $8 \mid (78 - 30)$. Considerando o número inteiro 7, temos: $30 + 7 \equiv 78 + 7 \ mod \ 8$, pois $8 \mid (85 - 37)$.*

Proposição 3.2.6. *Sejam $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{N}$, $c \neq 0$ e $m > 1$. Temos*

$$a.c \equiv b.c \ mod \ m \ se \ e \ somente \ se \ a \equiv b \ mod \ \frac{m}{(c,m)}.$$

Prova:

Observe que $\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1$. De fato:

Suponhamos que $\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = k, k \in \mathbb{N} - \{0,1\}$. Então $k \mid \frac{c}{(c,m)}$ e $k \mid \frac{m}{(c,m)}$. Logo, existem $q_1, q_2 \in \mathbb{Z}$ tais que $m = kq_1(c,m)$ e $c = kq_2(c,m)$. Assim $c(c,m) \mid m$ e $k(c,m) \mid c$, $k(c,m) > (c,m)$. Contradição, pois (c,m) é o mdc de c e m. Portanto,

$$\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1.$$

Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são primos entre si, decorre que $a.c \equiv b.c \ mod \ m$ se e somente se $m \mid (b-a).c$. Isto que equivale dizer que $\frac{m}{(c,m)} \mid (a-b)\frac{c}{(c,m)}$ e então $\frac{m}{(c,m)} \mid b-a$. Portanto,

$$a \equiv b \ mod \ \frac{m}{(c,m)}.$$

□

Exemplo 3.2.4. *Observe que* $9.6 \equiv 5.6 \ mod \ 8$, *pois* $8 \mid 24$ *e* $9 \equiv 5 \ mod \ \frac{8}{(6,8)}$, *isto é,* $9 \equiv 5 \ mod \ \frac{8}{2}$, $[4 \mid (9-5)]$. *Observe, também que* $9 \not\equiv 5 \ mod \ 8$.

O próximo corolário é uma consequência direta da Proposição 3.2.6.

Corolário 3.2.3. *Sejam* $a, b, c, m \in \mathbb{Z}$ *e* $(c,m) = 1$. *Então*

$$a.c \equiv b.c \ mod \ m \ se, \ e \ somente \ se \ a \equiv b \ mod \ m.$$

Definição 3.2.4 (Sistema Completo de resíduos módulo m)**.** *Um sistema completo de resíduos módulo* m *é todo conjunto de números naturais cujos restos pela divisão por* m *são os números* $0, 1, \ldots, m-1$, *sem repetições numa ordem qualquer.*

Exemplo 3.2.5. *O conjunto* $\{44, 15, 38, 21, 27\}$ *é um sistema completo de resíduos módulo 5.*

Proposição 3.2.7. *Sejam* $a, k, m \in \mathbb{Z}$, $m > 1$ *e* $(k,m) = 1$. *Se* $a_1, \ldots, a_m$ *é um sistema completo de resíduos módulo* m, *então*

$$a + ka_1, a + ka_2, \ldots, a + ka_m$$

também é um sistema de resíduos módulo m.

Prova:

Pela Proposição 3.2.5 e pelo Corolário 3.2.3, para $i, j = 0, 1, \ldots, m-1$, temos

$$a + ka_i \equiv a + ka_j \ mod\ m \text{ se e somente se } ka_i \equiv ka_j \ mod\ m$$
$$\text{se e somente se } a_i \equiv a_j \ mod\ m, \text{ somente quando } i = j.$$

Isso mostra que $a+ka_1, a+ka_2, \ldots, a+ka_m$, são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m.

□

Proposição 3.2.8. *Sejam $a, b \in \mathbb{Z}$, $m, n, m_1, \ldots, m_r$ inteiros maiores que 1, e $[m_1, \ldots, m_r]$ o mínimo múltiplo comum (mmc) de $m, n, m_1, \ldots, m_r$. Temos:*

(i) Se $a \equiv b \ mod\ m$ e $n \mid m$, então $a \equiv b \ mod\ n$;

(ii) $a \equiv b \ mod\ m_i$, $i = 1, \ldots, r$ se e somente se $a \equiv b \ mod\ [m_1, \ldots, m_r]$;

(iii) Se $a \equiv b \ mod\ m$, então $(a, m) = (b, m)$.

Prova:

(i) Se $a \equiv b \ mod\ m$ e $n \mid m$, então $m \mid b-a$ e $n \mid m$. Logo, existem $q_1, q_2 \in \mathbb{Z}$ tais que $b - a = m.q_1$ e $m = n.q_2$. Assim, $b - a = n.q_1.q_2$ e, portanto, $a \equiv b \ mod\ n_0$;

(ii) Se $a \equiv b \bmod m_i$, então $m_i \mid b-a$. Sendo $b-a$ um múltiplo de cada m_i, temos que $[m_1, \ldots, m_r] \mid b-a$, o que prova que $a \equiv b \bmod [m_1, \ldots, m_r]$.
A recíproca decorre do item (i);

(iii) Se $a \equiv b$, então $m \mid b-a$, e, portanto, $b = a + tm$, $t \in \mathbb{Z}$. Logo, pelo Lema de Euclides (Lema 3.2.1), temos $(a, m) = (a + tm, m) = (b, m)$ ou, $(m, b) = (m, b - tm) = (m, a)$.

□

Exemplo 3.2.6. $19 \equiv 11 \ mod\ 8$, *pois* $8 \mid (19-11)$ *e, como* $4 \mid 8$ *decorre que* $19 \equiv 11 \ mod\ 4$. *Também* $15 \equiv 33 \ mod\ 9$ *e* $(15, 9) = (33, 9) = 3$.

3.3 Congruências Lineares

Para resolvermos uma congruência (equações) linear precisamos ter um conhecimento básico de *equações diofantinas lineares*, que são equações do tipo $aX + bY = c$, $a, b, c \in \mathbb{Z}$, cujo interesse é obter soluções inteiras dessas equações.

Enunciaremos uma Proposição, cuja demonstração o leitor pode encontrar em (HEFEZ, 2003).

Proposição 3.3.1. *Dados $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{N}$, a equação $aX + bY = c$ admite solução em números inteiros se, e somente se $(a, b) \mid c$.*

A equação $27X + 39Y = 16$ não tem solução inteira, pois $(27, 39) \nmid 16$. A equação $30X - 48Y = 216$ tem solução, pois $(30, 48) \mid 216$, e uma das soluções é $(x = 4, y = -2)$. Em geral sempre que os valores de a e b forem primos entre si a equação $aX + bY = c$ terá soluções inteiras.

A demonstração do próximo e importante Teorema pode ser encontrada em (HEFEZ, 2013).

Teorema 3.3.1. *Seja o par ordenado (x_0, y_0) uma solução particular da equação diofantina $aX + bY = c$. Então as soluções dessa equação são da forma:*

$$x = x_0 + t\frac{b}{(a,b)} \text{ e } y = y_0 - t\frac{a}{(a,b)};\ t \in \mathbb{Z}$$

Exemplo 3.3.1. *Determinaremos o menor múltiplo positivo de 17 que deixa resto 1, quando for dividido por $3, 4, 5, 6$ e 7.*

Solução:

Queremos obter a menor solução positiva do sistema de congruências:

$$\begin{cases} 17X \equiv 1 \ mod\ 3 \\ 17X \equiv 1 \ mod\ 4 \\ 17X \equiv 1 \ mod\ 5 \\ 17X \equiv 1 \ mod\ 6 \\ 17X \equiv 1 \ mod\ 7 \end{cases}$$

Pela Proposição 3.2.8 (ii), temos que toda solução simultânea das congruências acima é solução da congruência:

$$17X \equiv 1 \ mod\ [3, 4, 5, 6, 7], \text{ ou seja, } 17X \equiv 1 \ mod\ 420.$$

Por outro lado, resolver a congruência $17X \equiv 1 \ mod\ 420$ é equivalente a resolver a equação diofantina $17X - 420Y = 1$. Desde que $(17, 420) = 1$, pela Proposição 3.3.1 a equação $17X - 420Y = 1$ admite solução. Uma solução particular dessa equação é $x_0 = -247$ e $y_0 = -10$, pois

$$17.(-247) - 420.(-10) = 1.$$

Portanto, pelo Teorema 3.3.1, as soluções dessa equação são da forma:

$$S = (-247 - 420t, -10 - 17t),\ t \in \mathbb{Z}.$$

Como $-247-420t>0$ é equivalente a $t<\dfrac{-247}{420}=0,588\ldots$, o menor valor inteiro positivo de x ocorre quando $t=-1$, ou seja, $x=-247-420.(-1)=173$. Portanto, o menor número que satisfaz o sistema de congruências é $17\cdot 173=2941$.

Definição 3.3.1 (Congruência linear)**.** *Uma* ***congruência linear*** *é toda congruência da forma $ax\equiv c\ mod\ m$, em que a,c são inteiros e x é a incógnita. Desde que $ax\equiv c\ mod\ m$ é equivalente a $ax-c\equiv 0\ mod\ m$ queremos determinar números inteiros x tais que*

$$ax\equiv c\ mod\ m\ \text{ou, equivalentemente, } ax-c\equiv 0\ mod\ m.$$

Proposição 3.3.2. *Dados $a,c,m\in\mathbb{Z}^*$, $m>1$, as congruências $ax\equiv c\ mod\ m$ e $ax-c\equiv 0\ mod\ m$ possuem soluções se e somente se $(a,m)\mid c$.*

Prova:

Suponhamos que $ax\equiv c\ mod\ m$ tenha uma solução x. Então, $m\mid c-ax$ ou $m\mid ax-c$, o que equivale à existência de $y\in\mathbb{Z}$ tal que $c-ax=my$ ou $ax+my=c$. Logo, a equação $my+ax=c$ admite solução. Portanto, pela Proposição 3.3.1, $(a,m)\mid c$.

Suponhamos, agora, que $(a,m)\mid c$. Logo a equação $ax-my=c$ admite uma solução x,y. Portanto, $ax=c+my$ e consequentemente, x é solução de $ax\equiv c$ mod m.

□

Exemplo 3.3.2. *Resolva a congruência linear $40x\equiv 8\ mod\ 18$.*

Solução

Como $(40,18)=2$, $(40,18)\mid 8$ e, portanto, pela Proposição 3.3.2, a congruência linear $40x\equiv 8\ mod\ 18$ possui solução, e a equação diofantina $40x-18y=8$ também. Vamos obter uma solução particular x_0,y_0. Simplificando a última equação, obtemos $20x-9y=4$. Desde que $20=9.2+2$, temos $20.2-9.4=4$ e, então, $x_0=2$ e $y_0=4$ é uma solução particular da equação $20x-9y=4$. Portanto, pelo Teorema 3.3.1, a solução geral da congruência linear dada é $x=2-9t$, $t\in\mathbb{Z}$

Observe que, se x_0 é uma solução particular da congruência $ax\equiv c\ mod\ m$, então todo x_1 tal que $x_1\equiv x_0\ mod\ m$ é também solução da congruência. No exemplo anterior, $40x\equiv 8\ mod\ 18$ tem solução particular $x_0=2$, assim, qualquer número congruente a 2 módulo 18 também é solução de $40x\equiv 8\ mod\ 18$, como, por exemplo o número 20 pois $20\equiv 2\ mod\ 18$. Deste modo, a solução particular determina, automaticamente uma infinidade de soluções da congruência. Essas soluções serão identificadas (módulo m), já que são congruentes entre si, e portanto, se determinam mutuamente.

A próxima Proposição mostra como determinar uma coleção completa de soluções duas a duas incongruentes módulo m, as quais serão chamadas de *sistema completo de soluções incongruentes da congruência.*

Proposição 3.3.3. *Sejam $a, c, m \in \mathbb{Z}^*$, $m > 1$ e $(a,m) \mid c$. Se x_0 é uma solução particular da congruência linear $ax \equiv c \ mod \ m$ (respectivamente, $ax - c \equiv 0 \ mod \ m$), então*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d},$$

em que $d = (a,m)$ formam um sistema completo de soluções incongruentes da congruência.

Exemplo 3.3.3. *Resolva a congruência linear $8x \equiv 4 \ mod \ 12$.*

Solução

Como $(8,12) = 4$, $(8,12) \mid 4$ e, portanto, pela Proposição 3.3.2, a congruência linear $8x \equiv 4 \ mod \ 12$ admite solução (em particular, $x_0 = 2$). Então, pela Proposição 3.3.3, a congruência linear possui $d = 4$ soluções módulo 12, que são:

$$\left\{2, 2 + \frac{12}{4}, 2 + 2\frac{12}{4}, 2 + 3\frac{12}{4}\right\} = \{2, 5, 8, 11\}.$$

A demonstração do próximo e importante Teorema pode ser encontrado em (HEFEZ, 2013), (COUTINHO, 2003), (SHOKRANIAN MARCUS SOARES, 1999)

Teorema 3.3.2 (Teorema chinês dos restos)**.** *O sistema*

$$\begin{cases} x \equiv c_1 \ mod \ n_1 \\ x \equiv c_2 \ mod \ n_2 \\ \qquad \vdots \\ x \equiv c_r \ mod \ n_r \end{cases},$$

onde $(n_i, n_j) = 1$ para todo par n_i, n_j com $i \neq j$, possui uma única solução módulo $N = n_1 n_2 \ldots n_r$. Tal solução pode ser obtida como segue:

$$x = N_1 y_1 c_1 \ldots N_r y_r c_r,$$

em que $N_i = \dfrac{N}{n_i}$ e y_i é solução de $N_i y_i \equiv 1 \ mod \ n_i$, $i = 1, \ldots, r$.

"O Exemplo abaixo apresentado por Coutinho (COUTINHO, 2003)".

Exemplo 3.3.4 (Uma plicação do Teorema chinês do "resto"). *Três satélites passarão sobre uma cidade esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra; o segundo, 15 horas, e o terceiro, 19 horas. Determinar quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre essa cidade.*

Solução

Seja x o número de horas, contadas a partir da meia-noite de hoje, quando os três satélites passarão juntos sobre a cidade. O primeiro satélite passa sobre a cidade a cada 13 horas, a contar da 1 da madrugada. Logo, precisamos ter $x = 1 + 13t$, para $t \in \mathbb{Z}$. Equivalentemente $x \equiv 1 \ mod\ 13$ e para os outros dois satélites, temos as equações $x = 4 + 15t$ e $x = 8 + 19t$, equivalentemente $x \equiv 4 \ mod\ 15$ e $x \equiv 8 \ mod\ 19$. Os três satélites passarão juntos sobre a cidade para os valores de x que satisfazem simultaneamente as seguintes congruências lineares.

$$\begin{cases} x \equiv 1 \ mod\ 13 \\ x \equiv 4 \ mod\ 15 \\ x \equiv 8 \ mod\ 19 \end{cases}$$

Precisamos resolver esse sistema.

Não podemos adicionar as equações entre si, já que os módulos são diferentes. Para resolvê-lo, iremos converter as congruências lineares em equações, sempre que necessário.

Assim, $x \equiv 1 \mod 13$ corresponde a $x = 1 + 13t$, que é um número inteiro e, como tal, pode ser substituído na segunda equação, o fornece:

$$1 + 13t \equiv 4 \ mod\ 15, \text{ ou seja, } 13t \equiv 3 \ mod\ 15.$$

Mas 13 é invertível módulo 15, e seu inverso é 7. Multiplicando $13t \equiv 3 \ mod\ 15$ por 7, e reduzindo os números módulo 15, obtemos $t \equiv 6 \ mod\ 15$.
Assim, t é da forma $t = 6 + 15u,\ u \in \mathbb{Z}$. Portanto,

$$x = 1 + 13t = 1 + 13(6 + 15u) = 79 + 195u.$$

Observe que qualquer número da forma $79 + 195u$ satisfaz as duas primeiras congruências lineares do sistema acima. Finalmente, vamos substituir $x = 79 + 195u$ na última equação do sistema. Com isso obtemos:

$$79 + 1895u \equiv 8 \ mod\ 19, \text{ ou seja, } 5u \equiv 5 \ mod\ 19.$$

Como 5 é invertível módulo 19, podemos eliminá-lo da equação acima, obtendo $u \equiv 1 \ mod \ 19$.

Reescrevendo essa congruência linear em termos de números inteiros, temos $u = 1 + 19v$, para qualquer inteiro v. Substituindo esse valor de u em $x = 79 + 195u$, obtemos

$$x = 79 + 195u = 79 + 195(1 + 19v) = 274 + 3705v.$$

Queremos descobrir qual o menor valor de x que satisfaz as equações, sabendo que x corresponde ao tempo contado a partir de meia-noite. Para saber qual o menor valor de x basta considerarmos $v = 0$ na equação $x = 274 + 3705v$, ou seja. Logo $x = 274$. Portanto, os satélites passarão juntos pela primeira vez 274 horas depois da meia noite de hoje. Isso corresponde a 11 dias e 10 horas. Porém, a solução que obtivemos nos diz mais. Somando um múltiplo qualquer de 3705 a 274 obtemos uma nova solução do sistema. Em outras palavras, os satélites voltarão a passar juntos a cada 3705 horas, o que corresponde a 154 dias e 9 horas.

4 CRIPTOGRAFIA

Desde os primórdios, quando não sabia escrever, o homem desenvolveu formas de registrar acontecimentos por meio de sinais, nascendo, assim, os primeiros códigos humanos, ainda bem rudimentares. Com o passar do tempo, o homem começou a se organizar em sociedades, alcançando um nível evoluído de convívio, sob as ordens de um poder central. Com essa evolução aconteceram o desenvolvimento da escrita e outros meios de comunicações, dentre eles a Criptografia, que surgiu com o interesse de enviar mensagens escondidas por trás de sinais, com o propósito de garantir privacidade. Estudos mostram que a Criptografia é tão antiga quanto a própria escrita, e desenvolveu-se em vários povos com várias finalidades. Uma delas é a de comunicar estratégias e ações de batalhas, como por exemplo, o imperador romano Júlio César que fazia uso de um sistema de cifragem inventado por ele para se comunicar com seu exército. O método de César é usado até hoje.

Durante a Idade Média, conhecida como época cheia de trevas para a ciência, a história de codificações foi cheia de surpresas, contando com a invenção de sistemas cada vez mais sofisticados de cifras e, consequentemente, o desenvolvimento de estudos cada vez mais aprofundados. Porém, muito conhecimento sobre esse tema se perdeu, por ser considerado pelos inquisidores magia negra ou bruxaria. A Criptografia vem se desenvolvendo até os dias atuais, surgindo vários métodos de cifragem para uso dos povos em benefício próprio. Com isso ela foi bastante usada durante as guerras, em especial na Segunda Guerra Mundial. Hoje em dia, esses métodos são utilizados pelo homem para garantir segurança nas suas ações, como por exemplo, fazer operações bancárias, ter acesso à internet e a vários outros meios de comunicações nos quais é exigida privacidade na comunicação.

A Criptografia (do grego *cryptos* = secreto, oculto; *grafia* = escrita) estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Consiste em converter dados legíveis em algo ilegível, com a capacidade de recuperar os dados originais com base nesses dados ilegíveis. Intuitivamente, é a arte de escrever em códigos secretos.

Para interpretar uma mensagem, é preciso decodificar. Isso é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la, ou seja, para decifrar, ele precisa "quebrar"o código.

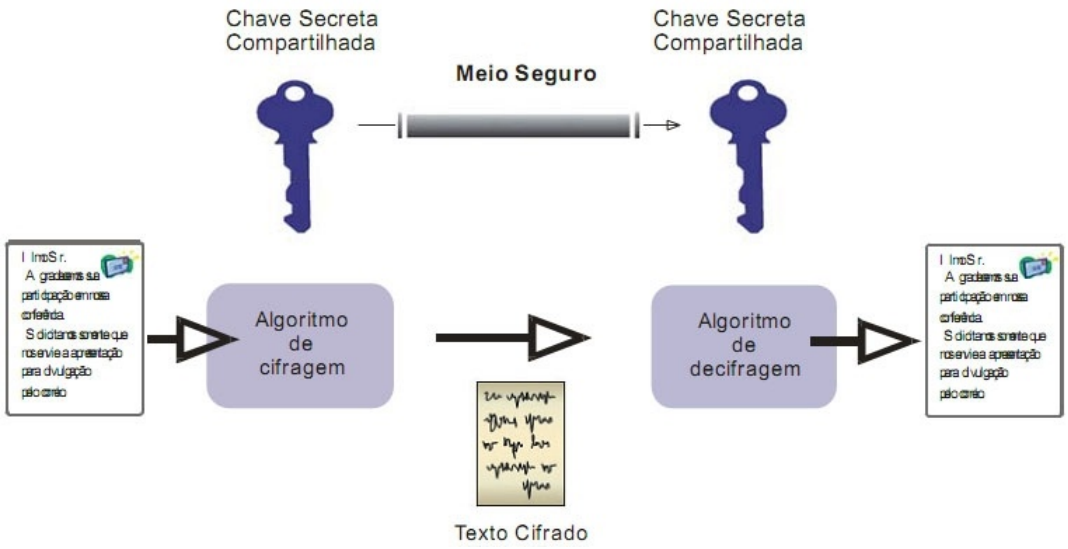
Vejamos o que é um Sistema Criptográfico, para que possamos entender e caminhar para os processos da criptografia.

Suponhamos que uma fonte A queira enviar um texto (mensagem) T para uma

pessoa B. A fonte A encifra (encripta) o texto por algum método de encifração K (algoritmo de cifragem), aplica esse método a T e define as cifras $T_k = T.K$, onde T_k é o texto codificado. De alguma maneira, a fonte A envia T_k para a fonte B. Na chegada, a fonte B aplica a chave (fórmula que é conhecida por A e B) e decifra T_k usando um método de decifração K_t (algoritmo de decifragem) que transforma (converte) T_k no texto (mensagem) T. Esse processo de decifragem, pode ser visto como $T_k.K_t$. Assim, podemos escrever esses processos (cifragem e decifragem) por meio da seguinte sentença matemática:

$$T_k = T.K \text{ e } T_k.K_t = (T.K).K_t = T$$

Figura 5 – Sistema Criptográfico



FONTE: www.gta.ufrj.br (julho 2015)

A Criptografia consiste em basicamente três processos que são: *pré-codificação, codificação* e *decodificação*. A **pré-codificação** é o processo que consiste em converter as letras em números usando uma tabela de conversão. A **codificação** é o método utilizado para codificar o texto, ou seja, deixa-lo em códigos. A **decodificação** é o método que se usa para decifrar o texto, ou seja, escreve-lo em sua forma original.

Para cifrar e decifrar uma mensagem, inicialmente associamos a cada letra do alfabeto um número. Consideremos a tabela a seguir como um exemplo:

Tabela 2 – Pré-codificação do alfabeto

Sexo	A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	♯
14	15	16	17	18	19	20	21	22	23	24	25	26	00

Converteremos o texto em uma sequência numérica, e, logo após, aplicamos algum método criptográfico. O espaço entre as palavras será substituído pelo símbolo ♯ e, consequentemente, pelo número 00.

Para decifrar um código, o usuário precisa de um elemento que o autorize a decodificar a mensagem. Esse elemento é denominado *chave*, que é utilizada para codificar e decodificar uma mensagem, fazendo o processo inverso da codificação. O termo chave origina-se do fato de que o número secreto escolhido funciona da mesma maneira que uma chave convencional, ou seja, para proteger de invasores. O uso da chave permite alterar o texto simples e convertê-lo em texto cifrado, de maneira que apenas com ela se pode decriptar o texto.

A Criptografia tem dois tipos de codificação: um é conhecido como ***Criptografia de Chave Simétrica*** e o outro como ***Criptografia de Chave Assimétrica***. Nas seções a seguir, estudaremos esses dois tipos de Codificação e alguns métodos de cada um deles.

Alguns métodos e informações presentes aqui podem ser encontradas em: (BURNETTS S., 2002), (SA, 2012), (LEMOS, 2001)

4.1 Métodos Simétricos

Na criptografia de chave simétrica, a chave que é utilizada para criptografar o texto é a mesma que usamos para decriptá-lo. **Simétrica** significa "a mesma nos dois lados" ou seja, é isto o que temos: a mesma chave nos dois lados no processo de criptografia. Esse tipo de cifragem pode manter seu texto seguro, mas, pelo fato de precisar da chave para recuperar o texto cifrado, é preciso também mantê-la segura.

Um método simétrico tem um algoritmo com a função cifragem c, ou seja, c tem como parâmetros uma chave a e um texto t, em que se obtém como resultado um novo texto (texto cifrado) t_i, definido pela fórmula:

$$t_i = c(a,t).$$

Essa função cifragem c tem uma função inversa d (desencriptação), que restabelece t_i à forma original t. Sendo a_i a chave de desencriptação, obteremos o texto original por meio da seguinte fórmula:

$$t = d(a_i, c(a,t)), \text{ ou seja, } t = d(a_i, t_i).$$

Na cifragem simétrica, temos que $a = a_i$, sendo escrito apenas como chave a.

Apresentaremos alguns métodos de cifragem simétrica que são utilizados em cifras simples. Utilizaremos aritmética modular nas operações (adição e multiplicação), como sendo a classe de equivalência módulo 60.

Dessa forma, para nosso texto, temos a seguinte tabela de Pré-Codificação.

Tabela 3 – Conversão de textos para Cifras Simétricas

♯	Â	Á	Ê	É	Î	Í	Ô	Ó	Û	Ú	Ã
00	01	02	03	04	05	06	07	08	09	10	11
Ẽ	Õ	À	Ç	/	=	+	-	×	÷	∼	%
12	13	14	15	16	17	18	19	20	21	22	23
0	1	2	3	4	5	6	7	8	9	A	B
24	25	26	27	28	29	30	31	32	33	34	35
C	D	E	F	G	H	I	J	K	L	M	N
36	37	38	39	40	41	42	43	44	45	46	47
O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59

Para trabalhar os métodos de Criptografia a seguir, usaremos uma tabela de Pré-Codificação com 60 caracteres. Isso pelo fato de termos uma maior quantidade de símbolos que usamos na nossa escrita, como por exemplo, letras acentuadas, os dez algarismos, o alfabeto, dentre outros símbolos. Dessa forma, facilita a conversão de qualquer caractere do texto da mensagem em um texto numérico. Sendo assim, toda vez em que fazemos uma cifra de uma mensagem, estaremos com aritmética modular de módulo 60.

Método 4.1.1 (**Cifra de César**). *A cifra de César consiste em adicionar (módulo m) os elementos de um texto (mensagem) a um elemento a (chave de codificação) de $\mathbb{Z}_m$. Podemos, então, escrever a relação entre os textos e as cifras na seguinte fórmula de congruência:*

$$c \equiv (t+a) \ mod \ m.$$

Para determinar a chave de decodificação (d) é necessário encontrar d de maneira que seja simétrico aditivo de a módulo m, ou seja, $d = m - a$, pois $a + d = a + (m - a) = m$. Obtemos então a congruência de deficragem

$$t \equiv (c+d) \ mod \ m.$$

Exemplo 4.1.1. *Vamos codificar a mensagem a seguir,*

O PROFMAT É O MESTRADO PROFISSIONAL EM MATEMÁTICA

utilizando a chave $a = 08$.

Solução:

Vamos organizar o texto dado em uma forma tabular e pré-codificá-lo.

0	♯	P	R	O	F	M	A	T	♯	É	♯	O	♯	M	E	S	T	R	A
48	00	49	51	48	39	46	34	53	00	04	00	48	00	46	38	52	53	51	34
D	O	♯	P	R	O	F	I	S	S	I	O	N	A	L	♯	E	M	♯	M
37	48	00	49	51	48	39	42	52	52	42	48	47	34	45	00	38	46	00	46
A	T	E	M	Á	T	I	C	A											
34	53	38	46	02	53	42	36	34											

A mensagem pré-codificada é:

$$480049514839463453000400480046385253513437484951$$
$$483942525242484734450038460046345384602534236 34$$

Agora, vamos adicionar a chave a cada elemento do texto, assim como César fazia.

	48	00	49	51	48	39	46	34	53	00	04	00	48	00	46	38	52
+08																	
	56	08	57	59	56	47	54	42	01	08	12	08	56	08	54	46	00
	W	Ó	X	Z	W	N	U	I	Â	Ó	Ẽ	Ó	W	Ó	U	M	♯
	45	00	38	46	00	46	34	53	38	46	02	53	42	36	34		
+08																	
	53	08	46	54	08	54	52	01	46	54	10	01	50	44	42		
	T	Ó	M	U	Ó	U	S	Â	M	U	Ú	Â	Q	K	I		

Temos então a seguinte mensagem codificada:

WÓXZWNUIÂÓẼÓWÓUM♯TÓMUÓUSÂMUÚÂQKI

Vamos, agora determinar a chave de decodificação d que deve ser o simétrico aditivo de $a = 8$ módulo 60. Assim,

$$d = m - a$$
$$d = 60 - 8$$
$$d = 52$$

A congruência de decifragem é $t \equiv (c + 52)\ mod\ 60$

$$t_1 \equiv (56+52)\ mod\ 60 \Rightarrow t_1 \equiv 108\ mod\ 60 \Rightarrow t_1 = 48,$$
$$\vdots$$
$$t_{32} \equiv (42+52)\ mod\ 60 \Rightarrow t_1 \equiv 94\ mod\ 60 \Rightarrow t_1 = 34.$$

Obtemos, assim, a mensagem original:

O PROFMAT É O MESTRADO PROFISSIONAL EM MATEMÁTICA

Método 4.1.2 (**Cifra de Sistema de Vetor**). *A cifra de sistema de vetor é um método semelhante ao de César. É obtido escolhendo-se como chave um vetor* $\vec{a} = (a_1, a_2, \ldots, a_k)$ *de coordenadas em* $\mathbb{Z}_m$. *Para cifrar um texto, é necessário dividi-lo em vetores* $\vec{t_1} = (t_{1_1}, t_{1_2}, \ldots, t_{1_k}), \vec{t_2} = (t_{2_1}, t_{2_2}, \ldots, t_{2_k}), \ldots, \vec{t_n} = (t_{n_1}, t_{n_2}, \ldots, t_{n_k})$, *com mesmo número de coordenadas da chave. Assim temos:*

$$\vec{c_1} \equiv \vec{t_1} + \vec{a}\ mod\ m,$$
$$\vec{c_2} \equiv \vec{t_2} + \vec{a}\ mod\ m,$$
$$\vdots$$
$$\vec{c_n} \equiv \vec{t_n} + \vec{a}\ mod\ m.$$

Para decodificar a mensagem, é preciso que cada vetor-cifra seja transformado no vetor texto novamente. Para isso a chave $\vec{a} = (a_1, a_2, \ldots, a_k)$ *deve ter um vetor simétrico* $\vec{d} = \vec{m} - \vec{a}$ *em que* $\vec{d} = (m - a_1, m - a_2, \ldots, m - a_k)$ *que nos fornece a chave de decodificação* $\vec{d} = (d_1, d_2, \ldots, d_k)$ *e assim*

$$\vec{t_i} \equiv (\vec{c_i} + \vec{d})\ mod\ m; \quad i = 1, \ldots, k$$

Esse tipo de cifragem é mais seguro que o de César, pois, para poder quebrar o código é preciso conhecer o número de coordenadas que tem a chave de cifragem e descobrir seus elementos, uma vez que a chave pode ser um vetor de $\vec{n}$ elementos.

Exemplo 4.1.2. *Tendo como chave o vetor* $\vec{a} = (09, 15, 21)$, *cifraremos a mensagem:*

QUE BOM SERIA QUE TODOS VIVESSEM EM PAZ.

Solução:

Para codificar essa mensagem, primeiro dividimos a sequência numérica encontrada em vetores com o mesmo número de coordenadas da chave. Caso faltem coordenadas no último vetor, este será completado com coordenadas 00.

Q	U	E	♯	B	O	M	♯	S	E	R	I	A	♯	Q	U	E	♯	T	O
50	54	38	00	35	48	46	00	52	38	51	42	34	00	50	54	38	00	53	48
D	O	S	♯	V	I	V	E	S	S	E	M	♯	E	M	♯	P	A	Z	
37	48	52	00	55	42	55	38	52	52	38	46	00	38	46	00	49	34	59	

Temos, então, os seguintes vetores:

$$\vec{t_1} = (50,54,38);\ \vec{t_2} = (00,35,48);\ \vec{t_3} = (46,00,52);\ \vec{t_4} = (38,51,42);$$
$$\vec{t_5} = (34,00,50);\ \vec{t_6} = (54,38,00);\ \vec{t_7} = (53,48,37);\ \vec{t_8} = (48,52,00);$$
$$\vec{t_9} = (55,42,55);\ \vec{t_{10}} = (38,52,52);\ \vec{t_{11}} = (38,46,00);\ \vec{t_{12}} = (38,46,00);$$
$$\vec{t_{13}} = (49,34,59)$$

A cifra da mensagem é

$$\vec{c_i} \equiv (\vec{t_i} + \vec{a})\ mod\ 60 \Rightarrow (c_{i_1}, c_{i_2}, c_{i_3}) \equiv ((t_{i_1}, t_{i_2}, t_{i_3}) + (09,15,21))\ mod\ 60$$

$$\vec{c_1} \equiv (\vec{t_1} + \vec{a})\ 60 mod\ 60 \Rightarrow (c_{1_1}, c_{1_2}, c_{1_3}) \equiv ((50,54,38) + (09,15,21))\ mod\ 60$$
$$(c_{1_1}, c_{1_2}, c_{1_3}) \equiv (59,69,59)\ mod\ 60 \Rightarrow \vec{c_1} = (59,09,59)$$
$$(c_{2_1}, c_{2_2}, c_{2_3}) \equiv ((00,35,48) + (09,15,21))\ mod\ 60 \Rightarrow \vec{c_2} = (09,50,09)$$
$$\vdots$$
$$(c_{13_1}, c_{13_2}, c_{13_3}) \equiv ((49,34,59) + (09,15,21))\ mod\ 60 \Rightarrow \vec{c_{13}} = (58,49,20)$$

Obtemos os seguintes vetores texto:
$\vec{c_1} = (Z,\hat{U},Z)$; $\vec{c_2} = (\hat{U},Q,\hat{U})$; $\vec{c_3} = (V,Ç,\tilde{O},)$; $\vec{c_4} = (N,\acute{I},\hat{E})$; $\vec{c_5} = (I,Ç,\tilde{A})$;
$\vec{c_6} = (\hat{E},T,\div)$; $\vec{c_7} = (\acute{A},\hat{E},Y)$; $\vec{c_8} = (X,\hat{O},\div)$; $\vec{c_9} = (\acute{E},X,/)$; $\vec{c_{10}} = (N,\hat{O},\tilde{O})$;
$\vec{c_{11}} = (N,\hat{A},\div)$; $\vec{c_{12}} = (N,\hat{A},\div)$; $\vec{C_{13}} = (Y,P,\times)$

A mensagem codificada é:

$$ZÛZÛQÛVÇÕNÍÊIÇÃÊT\div ÁÊYXÔ\div ÉX/NÔÕNÂ\div NÂ\div YP\times.$$

Vamos determinar o vetor decodificação d:

$$\vec{d} = (60,60,60) - (09,15,21) = (51,45,39).$$

A congruência de decodificação é

$$\vec{t_i} \equiv (\vec{c_i} + \vec{d})\ mod\ 60 \Rightarrow (t_{i_1}, t_{i_2}, t_{i_3}) \equiv ((c_{i_1}, c_{i_2}, c_{i_3}) + (51,45,39)).$$

$$\vec{t_1} \equiv (\vec{c_1} + \vec{d})\ mod\ 60 \Rightarrow (t_{1_1}, t_{1_2}, t_{1_3}) \equiv ((59,09,59) + (51,45,39))$$
$$(t_{1_1}, t_{1_2}, t_{1_3}) \equiv (110,54,98)\ mod\ 60 \Rightarrow \vec{t_1} = (50,54,38)$$

$$\vdots$$

$$\vec{t_{13}} \equiv (\vec{c_{13}} + \vec{d}) \ mod\ 60 \Rightarrow (c_{13_1}, c_{13_2}, c_{13_3}) \equiv ((58,49,20) + (51,45,39)) \ mod\ 60$$
$$(t_{13_1}, t_{13_2}, t_{13_3}) \equiv (109,94,59) \ mod\ 60 \Rightarrow \vec{t_{13}} = (49,34,59)$$

Obtemos, assim, voltamos a mensagem original:

QUE BOM SERIA QUE TODOS VIVESSEM EM PAZ

Método 4.1.3 (**Cifra Afim**). *Essa é a cifra que generaliza a Cifra de César, pois, ao invés de usar uma chave, são utilizadas duas chaves.*

Considere a chave um número inteiro positivo k, $0 \leq k \leq m-1$. Em vez de usarmos o número a, da cifra de César, podemos usar k e definir a cifra sendo:

$$c \equiv (t+k) \ mod\ m.$$

É claro que quando $k = a$, a cifra é de César, e quando $k = 0$, a cifra é exatamente o texto sem nenhuma alteração.

Definição 4.1.1. *Consideremos dois números $a, b \in \mathbb{Z}_m$, tais que $0 \leq a, b \leq m-1$, $mdc(a,m) = 1$. Denominamos de **cifra afim** a cifra*

$$c \equiv (at+b) \ mod\ m.$$

*Os números $a, b \in \mathbb{Z}_m$ são chamados **chaves de cifra afim**.*

Para decifrar uma mensagem escrita na cifra afim, devemos calcular o texto T, pela congruência $at \equiv (c-b) \ mod\ m$ (onde a e b são chaves, t é o texto e c é cifra). Após multiplicar os dois lados dessa congruência por a^{-1}, obtemos $t \equiv a^{-1}(c-b) \ mod\ m$. A congruência fica, então, da seguinte forma $t \equiv d(c+h) \ mod\ m$, sendo d o inverso multiplicativo de a módulo m e, portanto, $d = a^{-1}$ e h é o simétrico aditivo de b módulo m, e portanto, $h = m-b$. Essa congruência determina o texto (o conteúdo da mensagem).

Uma observação importante é que para usar a Cifra Afim, a e m devem ser primos entre si. Uma vez que a só terá inverso multiplicativo módulo m se $(a,m) = 1$, pois terá a congruência $ax \equiv 1 \ mod\ m$ satisfeita.

Exemplo 4.1.3. *Vamos cifrar a mensagem*

EDUCAÇÃO TRAZ MELHORIA

com as chaves $a = 7$ e $b = 9$.

Solução:

Temos:

E	D	U	C	A	Ç	Ã	O	♯	T	R
38	37	54	36	34	15	11	48	00	53	51
A	Z	♯	M	E	L	H	O	R	I	A
34	59	00	46	38	45	41	48	51	42	34

$$c_1 \equiv (7.38+9)\ mod\ 60$$
$$c_1 \equiv 275\ mod\ 60 \Longrightarrow c_1 = 35$$

Assim, temos:

$$c_2 \equiv (7.37+9)\ mod\ 60 \Rightarrow c_2 = 28$$
$$c_3 \equiv (7.54+9\ mod\ 60 \Rightarrow c_3 = 27$$
$$c_4 \equiv (7.36+9)\ mod\ 60 \Rightarrow c_4 = 21$$
$$\vdots$$
$$c_{22} \equiv (7.34+9)\ mod\ 60 \Rightarrow c_{18} = 07$$

Obtemos, então, a seguinte tabela de conversão:

35	28	27	21	07	54	26	45	09	20	06
B	4	3	÷	Ô	U	2	L	Û	Ú	Í
07	02	09	31	35	24	56	45	06	03	07
Ô	Á	Û	7	B	0	W	L	Í	Ê	Ô

A mensagem codificada fica, então:

B43÷ÔU2LÛÚÍÔÁÛ7B0WLÍÊÔ

Vamos, então, decodificar a mensagem que foi codificada.
Sabemos que $t_i \equiv d(c_i+h)\ mod\ 60$, onde d é o inverso multiplicativo de $a=7$ módulo 60 e h é o simétrico aditivo de $b=9$ módulo 60. Assim, $7.d \equiv 1\ mod\ 60$ e $9+h \equiv 0\ mod\ 60$. Sabemos que o resto da divisão do produto $7.d$ por 60 deve ser 1, para que a congruência $7.d \equiv 1\ mod\ 60$ seja satisfeita. Assim, o produto $7.d$ deve ter como último algarismo o 1, então, $d \in \{3,13,23,33,43,53\}$, pois são os únicos que multiplicado por sete terminam em um. Logo, $d=43$ e $h=51$. Portanto, as mensagens serão decodificadas pela congruência:

$$t_i \equiv 43(c_i+51)\ mod\ 60$$

Então:

$$t_1 \equiv 43(35+51)\ mod\ 60 \Rightarrow t_1 \equiv 3698\ mod\ 60.$$

Desde que $3698 = 60.61 + 38$ e $t_1 = 60.p + r_{t_1}$; $r_{t_1} = 38 \Rightarrow p = 0$ e $t_1 = 38$.
De forma análoga obtemos

$$t_2 = 37;\ t_3 = 54;\ \ldots t_{22} = 34$$

Obtemos, assim, para a mensagem original:

EDUCAÇÃO TRAZ MELHORIA.

Método 4.1.4 (**Cifra linear**). *Essa cifra é a cifra afim sem a constante b.*
Obtemos a cifra linear pela fórmula de congruência

$$c \equiv at\ mod\ m,$$

onde a é a chave de codificação.
A chave de decodificação (d) do texto é o inverso multiplicativo de a módulo m, e portanto $a.d \equiv 1\ mod\ m \Rightarrow d = a^{-1}$, *obtendo a congruência de decodificação*

$$t \equiv d.c\ mod\ m.$$

Exemplo 4.1.4. *Vamos codificar a frase:*

HOJE É DIA BOM,

usando como chave $a = 13$.

Solução:

Iniciamos com a pré-codificação:

H	O	J	E	♯	É	♯	D	I	A	♯	B	O	M
41	48	43	38	00	04	00	37	42	34	00	35	48	46

Para codificar a frase, temos que aplicar a congruência $c_i \equiv 13t_i\ mod\ 60$. Temos, então:

$$c_1 \equiv 13.41\ mod\ 60 \Rightarrow c_1 \equiv 533\ mod\ 60$$
$$\text{Como } 533 = 60.8 + 53 \text{ temos } c_1 = 53$$

Aplicando a congruência da cifra linear nas demais letras temos:

$$c_2 = 24,\ c_3 = 19,\ \ldots,\ c_{14} = 58.$$

Assim,

53	24	19	14	00	52	00	01	06	22	00	35	24	58
T	0	-	À	♯	S	♯	Â	Í	∼	♯	B	0	Y

que nos dá a frase codificada:

$$\text{T0-À♯S♯ÂÍ}\sim\text{♯B0Y}$$

Para decodificar a frase que foi criptografada, precisamos encontrar o inverso multiplicativo (d) de $a = 13$ módulo 60. Assim, temos $13.d \equiv 1 \ mod\ 60$, e portanto $d = 37$. Obtemos, assim, a congruência

$$t_i \equiv 37c_i \ mod\ 60,$$

de decifragem.
Agora vamos descriptografar a frase que foi codificada.

$$t_1 \equiv 37.53 \ mod\ 60 \Rightarrow t_1 \equiv 1961 mod\ 60 \Rightarrow t_1 = 41$$

Aplicando a descriptografia de maneira análoga às outras cifras, obtemos

$$t_2 = 48,\ t_3 = 43,\ \ldots,\ t_{14} = 46$$

Voltando assim, a frase original:

HOJE É DIA BOM

Método 4.1.5 (**Cifra Permutacional**). *Essa cifra está baseada no conceito de permutação, ou seja, para gerar um cifra permutacional, basta aplicar uma das* $(m-1)!$ *permutações dos símbolos utilizados (no caso, é* 59!*), e trocar a posição das letras e obter uma cifra. Quando, para cada simbolo de texto se usa somente um símbolo na cifra, essa cifra é chamada* ***cifra monoalfabética****.*

Exemplo 4.1.5. *Vamos codificar o texto*

CASA EM CONSTRUÇÃO,

permutando apenas cinco posições nas letras.

Solução:

Precisamos apenas trocar as letras de posições[1].

[1] Aqui consideramos o Ç como sendo apenas C. Assim, se obtemos a letra original ao formar a frase decodificada.

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

O texto codificado fica, então, da seguinte forma:

HFXF JR HTSXYWZHFT.

Observe que as letras em negrito da primeira linha da tabela foram alteradas pelas letras em negrito da segunda linha da tabela, e igualmente referente às linhas terceira e quarta.

Para decodificar, basta voltarmos cinco posições e teremos o texto original.

Observe que para a frase que foi codificada, temos, 26! maneiras de criptografar usando a tabela do exemplo,

Em caso geral, se tivermos n letras em um texto, para que possamos criptografar o texto, teremos $n!$ permutações diferentes, e somente n delas respeitam a ordem usual (ordem em que as letras permanecem como se não houvesse sido criptografadas). Há também como determinar os desordenamentos (em que nenhuma letra fica em seu lugar natural) através de

$$n!\left(\frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\ldots+\frac{(-1)^n}{n!}\right).$$

Esse resultado pode ser encontrado em (MORGADO *et al.*, 2006)

Método 4.1.6 (**Cifra one-timepad**). *Este método consiste em escolher, ao acaso, uma chave* $\boldsymbol{a}$ *para cada símbolo da mensagem, de maneira que cada letra seja cifrada com uma chave diferente. Desse modo, não é difícil compreender por que o* ***one-timepad*** *é inquebrável. O único inconveniente é o fato de ser necessária a comunicação prévia de longas sequências de chaves entre o emissor e o receptor.*

Seja t *o texto a ser criptografado. Temos que* a_j *é a chave de cifragem do texto. Temos, então, que* t *é dividido em cada letra* t_i *e, assim:*

$$ti \equiv a_j \ mod \ m$$

Exemplo 4.1.6. *Para cifrar a palavra*

PROVIDÊNCIA,

precisamos de 11 chaves, pois essa palavra tem 11 letras.

Observe que o número de chaves possíveis para codificar essa palavra é 59^{11}. Assim, para um texto de n símbolos (letras, algarismos, caracteres e espaços), o número de chaves possíveis é 59^n. Mais genericamente, o número de chaves possíveis para um texto de n símbolos a ser pré-codificado por uma tabela de m símbolos, é obtido por $(m-1)^n$. Por esse motivo esse método é praticamente inquebrável, como também difícil de usar.

Método 4.1.7 (**Cifra por meio de Matriz**). *Este sistema criptográfico é um método que utiliza matrizes invertíveis para codificar textos, sendo uma maneira de cifrar bem segura. Esse tipo de cifra consiste em montar uma matriz texto T, multiplicar pela matriz-chave A e transmitir a mensagem codificada para o receptor que para decriptá-la irá multiplicar a mensagem $A.T$ por A^{-1}, obtendo o texto original T.*

$$C \equiv (A.T) \ mod \ m \ e \ T \equiv A^{-1}.C \ mod \ m$$

Exemplo 4.1.7. *Utilizando a matriz-chave*

$$A = \begin{bmatrix} 2 & 0 & 3 \\ 1 & 1 & 2 \\ 0 & 3 & 2 \end{bmatrix}$$

iremos cifrar o texto

MESTRADO EM MATEMÁTICA

Solução:
Inicialmente observamos que $detA = 1$ e portanto A é uma matriz inversível. Em seguida pré-codificaremos o texto:

M	E	S	T	R	A	D	O	♯	E	M
46	38	52	53	51	34	37	48	00	38	46
♯	M	A	T	E	M	Á	T	I	C	A
00	46	34	53	38	46	02	53	42	36	34

E associamos as matrizes texto e código correspondentes:

$$T = \begin{bmatrix} M & T & D & E & M & E & T & A \\ E & R & O & M & A & M & I & \sharp \\ S & A & \sharp & \sharp & T & Á & C & \sharp \end{bmatrix}$$

$$T = \begin{bmatrix} 46 & 53 & 37 & 38 & 46 & 38 & 53 & 34 \\ 38 & 51 & 48 & 46 & 34 & 46 & 42 & 00 \\ 52 & 34 & 00 & 00 & 53 & 02 & 36 & 00 \end{bmatrix}$$

Obteremos agora a matriz criptografada que corresponde ao produto da matriz-chave A pela matriz de código T, isto é, $C = A.T$.

$$C = \begin{bmatrix} 2 & 0 & 3 \\ 1 & 1 & 2 \\ 0 & 3 & 2 \end{bmatrix} . \begin{bmatrix} 46 & 53 & 37 & 38 & 46 & 38 & 53 & 34 \\ 38 & 51 & 48 & 46 & 34 & 46 & 42 & 00 \\ 52 & 34 & 00 & 00 & 53 & 02 & 36 & 00 \end{bmatrix}$$

$$C = \begin{bmatrix} 248 & 208 & 74 & 76 & 251 & 82 & 214 & 68 \\ 188 & 172 & 85 & 84 & 186 & 88 & 167 & 34 \\ 218 & 221 & 144 & 138 & 208 & 142 & 198 & 00 \end{bmatrix}$$

Desde que, a matriz P tem que ter seus elementos módulo 60, temos:

$$C = \begin{bmatrix} 08 & 28 & 14 & 16 & 11 & 22 & 34 & 08 \\ 08 & 12 & 25 & 24 & 06 & 28 & 07 & 34 \\ 38 & 41 & 24 & 18 & 28 & 22 & 18 & 00 \end{bmatrix}$$

Obtemos a seguinte, a matriz código em símbolos

$$C = \begin{bmatrix} \text{Ó} & 4 & \text{À} & / & \tilde{\text{A}} & \sim & A & \text{Ó} \\ \text{Ó} & \tilde{\text{E}} & 1 & 0 & \text{Í} & 4 & \hat{\text{O}} & A \\ E & H & 0 & + & 4 & \sim & + & \sharp \end{bmatrix}$$

A mensagem codificada é

$$\text{ÓÓE4}\sim E\text{HÀ10/0+ÃÍ4}\sim 4\sim \text{AÔ+ÓA}\sharp$$

Para decodificar o texto precisamos usar um processo semelhante, porém com a matriz C e a matriz $D = A^{-1}$ que é a matriz inversa de A.

Para que D seja inversa da matriz A é preciso que o produto de A e D resulte na matriz identidade I, isto é,

$$A.D = I \Rightarrow \begin{bmatrix} 2 & 0 & 3 \\ 1 & 1 & 2 \\ 0 & 3 & 2 \end{bmatrix} . \begin{bmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Assim, resolvendo o sistema correspondente, obtemos que, a matriz inversa de A é

$$D = \begin{bmatrix} -4 & 9 & -3 \\ -2 & 4 & -1 \\ 3 & -6 & 2 \end{bmatrix}$$

Logo:

$$T = \begin{bmatrix} -4 & 9 & -3 \\ -2 & 4 & -1 \\ 3 & -6 & 2 \end{bmatrix} . \begin{bmatrix} 08 & 28 & 14 & 16 & 11 & 22 & 34 & 08 \\ 08 & 12 & 25 & 24 & 06 & 28 & 07 & 34 \\ 38 & 41 & 24 & 18 & 28 & 22 & 18 & 00 \end{bmatrix}$$

$$T = \begin{bmatrix} -74 & -127 & 97 & 98 & -74 & 98 & -127 & 274 \\ -22 & -49 & 48 & 46 & -26 & 46 & -58 & 120 \\ 52 & 94 & -60 & -60 & 53 & -58 & 96 & -180 \end{bmatrix}$$

Como estamos trabalhando com o conjunto dos números naturais módulo 60 e a matriz T tem elementos que não são naturais e nem estão em módulo 60, precisamos transformar esses elementos para naturais módulo 60:

$$t_{11} = -74 + 60 = -14 \Rightarrow t_{11} = -14 + 60 = 46,$$

$$\begin{aligned} t_{12} &= -127 + 3.60 = 53, \\ t_{15} &= -74 + 2.60 = 46, \\ t_{16} = 98 &= 60 \cdot 1 + 38 \Rightarrow t_{16} = 38, \\ &\vdots \\ t_{37} = 96 &= 60.1 + 36 \Rightarrow t_{37} = 36, \\ t_{38} &= -180 + 3.60 = 00. \end{aligned}$$

$$T = \begin{bmatrix} 46 & 53 & 37 & 38 & 46 & 38 & 53 & 34 \\ 38 & 51 & 48 & 46 & 34 & 46 & 42 & 00 \\ 52 & 34 & 00 & 00 & 53 & 02 & 36 & 00 \end{bmatrix}$$

Obtemos, assim, a mensagem original:

MESTRADO EM MATEMÁTICA

Método 4.1.8 (**Cifra em Blocos**). *Este método consiste em criptografar a mensagem por meio de duas matrizes, uma matriz quadrada $A_{n\times n}$ e uma matriz coluna $B_{n\times 1}$. Devemos dividir o texto da mensagem em blocos de matrizes $T_{n\times n}$. Cada cifra obtém-se por meio do produto da matriz quadrada por cada matriz texto, somando o produto obtido com a matriz coluna dada. Representamos esse método pela seguinte congruência:*

$$C \equiv AT + B \ mod \ m.$$

Para descriptografar precisamos determinar a matriz inversa $D = A^{-1}$ de A e a matriz simétrica $H = M - B$ de B módulo m, em que M é a matriz coluna cujos elementos

são iguais a m. Assim, primeiro soma-se a matriz H com a matriz C, depois multiplica-se a matriz D pelo resultado. A decodificação é obtida ela congruência.

$$T \equiv D.(C+H) \ mod \ m$$

Exemplo 4.1.8. *Vamos codificar a mensagem*

O BRASIL PODE MELHORAR

com as matrizes chaves $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ *e* $B = \begin{bmatrix} 16 \\ 21 \end{bmatrix}$.

Solução:

Como $detA = 1 \ (\neq 0)$ a matriz A tem inversa.
Com as chaves de criptografia que são dadas no par de matrizes

$$\left(\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}; \begin{bmatrix} 16 \\ 21 \end{bmatrix} \right).$$

Com o auxílio da tabela de pré-codificação, associamos as matrizes

$$\begin{bmatrix} O \\ \sharp \end{bmatrix}; \begin{bmatrix} B \\ R \end{bmatrix}; \begin{bmatrix} A \\ S \end{bmatrix}; \begin{bmatrix} I \\ L \end{bmatrix}; \begin{bmatrix} \sharp \\ P \end{bmatrix}; \begin{bmatrix} O \\ D \end{bmatrix}; \begin{bmatrix} E \\ \sharp \end{bmatrix}; \begin{bmatrix} M \\ E \end{bmatrix}; \begin{bmatrix} L \\ H \end{bmatrix}; \begin{bmatrix} O \\ R \end{bmatrix}; \begin{bmatrix} A \\ R \end{bmatrix}$$

as seguintes matrizes numéricas

$$\begin{bmatrix} 48 \\ 00 \end{bmatrix}; \begin{bmatrix} 35 \\ 51 \end{bmatrix}; \begin{bmatrix} 34 \\ 52 \end{bmatrix}; \begin{bmatrix} 42 \\ 45 \end{bmatrix}; \begin{bmatrix} 00 \\ 49 \end{bmatrix}; \begin{bmatrix} 48 \\ 37 \end{bmatrix}; \begin{bmatrix} 38 \\ 00 \end{bmatrix}; \begin{bmatrix} 46 \\ 38 \end{bmatrix}; \begin{bmatrix} 45 \\ 41 \end{bmatrix}; \begin{bmatrix} 48 \\ 51 \end{bmatrix}; \begin{bmatrix} 34 \\ 51 \end{bmatrix}$$

A fórmula para codificar é dada pela congruência

$$\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \left(\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} t_{11} \\ t_{21} \end{bmatrix} + \begin{bmatrix} 16 \\ 21 \end{bmatrix} \right) \ mod \ 60$$

Vamos aplicar essa fórmula a cada uma das matrizes que compõem o texto:

$$\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \left(\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 48 \\ 00 \end{bmatrix} + \begin{bmatrix} 16 \\ 21 \end{bmatrix} \right) \ mod \ 60 \Rightarrow \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \left(\begin{bmatrix} 48 \\ 48 \end{bmatrix} + \begin{bmatrix} 16 \\ 21 \end{bmatrix} \right) \ mod \ 60$$

$$\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \begin{bmatrix} 64 \\ 69 \end{bmatrix} \ mod \ 60 \Rightarrow \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} = \begin{bmatrix} 04 \\ 09 \end{bmatrix}$$

$$\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \left(\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 35 \\ 51 \end{bmatrix} + \begin{bmatrix} 16 \\ 21 \end{bmatrix} \right) \ mod\ 60 \Rightarrow \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} = \begin{bmatrix} 33 \\ 29 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \left(\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 34 \\ 51 \end{bmatrix} + \begin{bmatrix} 16 \\ 21 \end{bmatrix} \right) \ mod\ 60 \Rightarrow \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} = \begin{bmatrix} 32 \\ 28 \end{bmatrix}$$

Substituindo os números obtidos pelos correspondentes símbolos, obtemos a mensagem codificada a seguir:

ÉÛ95A7OOUO+♯UZÂ%ÛMI84.

Para decodificar precisamos determinar a matriz $D = A^{-1}$, que é a inversa de A, e a matriz $H = 60 - B$, que é simétrica de B módulo 60.

Assim, temos:

$$A.D = D.A = I \Rightarrow \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Logo, a matriz inversa de A é $D = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$.
Vamos determinar a matriz H simétrica de B módulo 60.

$$H = 60 - B \Rightarrow \begin{bmatrix} h_{11} \\ h_{21} \end{bmatrix} = \begin{bmatrix} 60 \\ 60 \end{bmatrix} - \begin{bmatrix} 16 \\ 21 \end{bmatrix}. \text{ Portanto } H = \begin{bmatrix} 44 \\ 39 \end{bmatrix}.$$

Assim, as chaves de decodificação são dadas pelos pares de matrizes

$$\left(\begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} ; \begin{bmatrix} 44 \\ 39 \end{bmatrix} \right).$$

Logo, a fórmula da congruência de decodificação é:

$$\begin{bmatrix} t_{11} \\ t_{21} \end{bmatrix} \equiv \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \left(\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} + \begin{bmatrix} 44 \\ 39 \end{bmatrix} \right) \ mod\ 60$$

Então, para decodificar o texto basta aplicar a fórmula acima:

$$\begin{bmatrix} t_{11} \\ t_{21} \end{bmatrix} \equiv \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \left(\begin{bmatrix} 04 \\ 09 \end{bmatrix} + \begin{bmatrix} 44 \\ 39 \end{bmatrix} \right) \ mod\ 60 \Rightarrow \begin{bmatrix} t_{11} \\ t_{21} \end{bmatrix} = \begin{bmatrix} 48 \\ 00 \end{bmatrix}$$

Continuando assim, com o mesmo procedimento voltamos a mensagem original:

O BRASIL PODE MELHORAR

Método 4.1.9 (Criptografia baseada em Senhas). *Consiste em criptografar a chave de codificação. Uma vez que a chave é simétrica, se cair em mãos erradas, toda a mensagem estará em risco. Na realidade, esse sistema baseia-se em oferecer segurança a quem utiliza chaves simétricas para o uso pessoal. É um sistema utilizado em meios eletrônicos, no qual somente quem possui a senha pode ter acesso à mensagem. É a partir da senha que o usuário terá acesso a chave de decodificação.*

O exemplo a seguir pode ser encontrado em (COUTINHO, 2003)

Exemplo 4.1.9. *Partilha de senhas*

Benjamim Franklin, o inventor do pára raios, disse uma vez que *'três pessoas só conseguem guardar um segredo, se duas já estiverem mortas'.*

Vamos apresentar um método que permite compartilhar um segredo entre várias pessoas que ainda estão vivas. Mais precisamente, imagine que o cofre de um banco seja aberto por meio de uma senha. Certo número de funcionários do banco tem acesso ao cofre. Mas o banco deseja, por segurança, que não seja possível abrir o cofre quando houver menos de três funcionários presentes na agência. Digamos que na agência haja vinte e dois funcionários com acesso ao cofre. Como garantir que não será possível abrir o cofre, a menos que haja pelo menos três desses funcionários presentes na agência?

Solução:

Para abrir o cofre, é necessário conhecer a senha, que é um número s. Queremos partilhar s entre n pessoas. A cada pessoa vai ser dado um elemento (sua "parte" da senha) de um conjunto S de n *pares* de números inteiros positivos, de modo que, para um $k \leq n \in \mathbb{Z}$, previamente escolhido, tenhamos:

1. qualquer subconjunto de S com k elementos permite determinar s facilmente;
2. é muito difícil determinar s conhecendo menos de k elementos de S.

A inspiração para a construção do conjunto S vem do teorema chinês dos restos. Comecemos escolhendo um conjunto L de n números inteiros positivos, dois a dois primos entre si. Consideremos N o produto dos k *menores* números de L e M o produto dos $k-1$ *maiores* números de L.

Diremos que esse conjunto tem *limiar* k se $N > s > M$.

Observe que essa condição implica que o produto de k ou mais elementos de L é sempre *maior* que N e o produto de menos de k elementos é sempre *menor* que M. O conjunto S será formado pelos pares da forma (m, s_m), onde $m \in L$ é a forma reduzida de s módulo m.

Note que o fato de termos um conjunto limiar $k \geq 1$ implica $s > m$, para qualquer $m \in L$. Portanto sempre temos $s_m < s$, qualquer que seja $m \in L$.

Suponhamos que mais de k funcionários estejam no banco. Isso equivale a dizer que são conhecidos t dentre os pares de S, com $t \geq k$. Denotaremos esses pares por $(m_1, s_1); \ldots; (m_t, s_t)$.

Vamos resolver o seguinte sistema de congruências

$$\begin{cases} x \equiv s_1 mod m_1 \\ \quad \vdots \\ x \equiv s_t \ mod \ m_t \end{cases}$$

obtendo x_0 como solução. De acordo com o teorema chinês dos restos, $x_0 \equiv s mod[m_1 \ldots m_t]$.

Mas será que são iguais? É aqui que usamos o fato de a sequência de módulos ter limiar k. Sabemos que, como $t \geq k, m_1 \ldots m_t \geq N > s$. Pelo teorema chinês dos restos, o sistema acima tem uma única solução menor que $m_1 \ldots m_t$. Mas s também é solução e $s < m_1 \ldots m_t$. Logo, $s = s_0$.

Nada nos impede de resolver o sistema semelhante para o caso em que $t < k$. O problema é que o produto de menos de k módulos de L é sempre menor que s. Assim, a solução do sistema é um número congruente a s, mas não pode ser igual a s. É claro que sempre é possível obter s fazendo uma busca. De fato, sabemos que $M < s < N$ e que s satisfaz o sistema acima, só que agora $t < k$. Digamos que tenhamos obtido uma solução x_0 do sistema. Como $x_0 < M < s$, não obtemos s. Mas o sistema acima também é satisfeito por s. Logo,

$$s = s_0 + y(m_1 \ldots m_t),$$

em que y é um natural. Como $N > s > M > x_0$, temos

$$\frac{M - x_0}{m_1 \ldots m_t} \leq y = \frac{s - s_0}{m_1 \ldots m_t} \leq \frac{N - x_0}{m_1 \ldots m_t}.$$

Isso significa que precisamos fazer uma busca para conseguir o valor correto de y entre, pelo menos,

$$d = \left[\frac{N - M}{m_1 \ldots m_t}\right].$$

números inteiros positivos. Escolhendo os módulos de modo que d seja muito grande, fica praticamente impossível vir a ter s por meio de uma busca.

Resta um problema: é sempre possível escolher um conjunto L satisfazendo todas essas condições? A resposta é sim. Na prática, os dados iniciais do problema são o número

total de funcionários da agência e o número mínimo de funcionários que têm que estar presentes para que o cofre possa ser aberto. O primeiro determina quantos elementos o conjunto L tem que ter. O segundo determina qual é o limiar de k de L. Com esses dados, escolhemos um conjunto L de limiar k. Só agora escolhemos s (de maneira aleatória) no intervalo entre M e N.

Agora, devemos calcular S, que nos diz quem são as senhas a serem distribuídas. É claro que a segurança do sistema se baseia no fato que, quanto maior o valor de k, mais improvável será que haja k funcionários desonestos no banco. Se todos os funcionários forem desonestos, estaremos perdidos: nenhum sistema é totalmente à prova de desonestidade.

Consideramos um exemplo numérico bem simples. Digamos que haja 5 funcionários, e que pelo menos 2 estejam presentes para que o cofre seja aberto. Logo, o conjunto L deve ter 5 elementos e seu limiar deve ser 2. Uma escolha possível, usando apenas números primos, é

$$L = \{11, 13, 17, 19, 23\}.$$

De fato, o produto dos 2 menores naturais no conjunto é $N = 11 \cdot 13 = 143$. Por outro lado, M é o produto dos $k-1$ maiores elementos de L. Como $k = 2$, temos que M é igual ao maior elemento de L. Logo, $M = 23$. Portanto, L tem limiar 2. Escolhemos s como sendo qualquer números inteiro no intervalo que vai de 23 a 143. Digamos que $s = 30$. Então

$$S = \{(11, 19); (13, 17); (17, 13); (19, 11); (23, 7)\}.$$

Finalmente, o que acontece se os funcionários que têm senhas $(17, 13)$ e $(23, 7)$ estão no banco?

Para obter a senha s do cofre é preciso resolver o sistema

$$\begin{cases} x \equiv 13 \ mod \ 17 \\ x \equiv 7 \ mod \ 23 \end{cases}$$

A solução desse sistema é $x = 30 + 391k$, em que k é um número inteiros positivo. Isto é, $x \equiv 30 \ mod \ 391$. Assim, determinamos $s = 30$. Para garantir a segurança, é preciso que, mesmo se houver 5 dos 20 funcionários, o limiar tem que ser maior que ou igual a 3.

4.1.1 Segurança no Sistema Simétrico

Como havíamos dito, um dos problemas da criptografia de chave simétrica é que ela não é totalmente segura, de modo que para garantir a chegada da mensagem com segurança é preciso manter também a chave segura.

Mostraremos um exemplo do porquê esse tipo de cifra não tem segurança garantida totalmente.

Vamos supor que a mensagem

DIGA NÃO À INTOLERÂNCIA E SIM AO AMOR

seja transmitida a alguém que possua a chave. A mensagem é codificada por meio de cifra afim com chaves $a = 13$ e $b = 11$, que fica da seguinte forma:

Ẽ=R9Ã∼ABÃÕÃ=∼GBW1À0∼Z=9Ã1Ã3=ÛÃ9BÃ9ÛBÀ,

porém, na sua transmissão, ela é interceptada por uma outra pessoa, que ao ver a mensagem, deseja lê-la.

Para que essa pessoa possa ler a mensagem, ela precisa determinar a forma geral da congruência que representa a mensagem. Observando que a letra Ã aparece mais vezes, 7 (sete), pode-se, então, especular que ela representa o **espaço entre as letras** do texto. Com isso, ela pode conseguir à seguinte equação: $c \equiv at + b\ mod 60 \Rightarrow c \equiv 13t + 11\ mod\ 60$, com base na qual ela obtém uma nova equação $t \equiv d(c + h)\ \ mod\ \ 60 \Rightarrow 37(c + 49) \equiv 51\ mod\ 60$. Ela, então, consegue a mensagem original

DIGA NÃO À INTOLERÂNCIA E SIM AO AMOR.

Por esse motivo, a criptografia de chave simétrica é considerada falha, sendo que ela pode ser adaptada como a cifragem baseada em senhas. Há também métodos simétricos menos vulneráveis como a cifra por meio de matriz, a cifra de sistema de vetores, mas todos eles têm fraquezas. Como por exemplo, o sistema de vetores: se um estranho descobrir o número de coordenadas, ele consegue obter a mensagem original. Porém, ele terá mais dificuldades, pois não terá que descobrir uma só coisa (número da chave e coordenada do vetor). E, ainda mais, se não souber que foi cifrada por meio de vetores, ele ficará tentando decifrar por cifra afim até perceber que é outro método de cifras, para que possa tentar pelo método de vetores. Assim também ocorrerá com os outros métodos como matriz, senha, dentre outros.

O problema maior é com a cifra de César, e a Linear que depende somente de uma chave para sua segurança, pois não é necessário nenhum outro processo para a cifragem. A cifra Afim é também bastante vulnerável, pois basta descobrir as duas chaves para decifrar as mensagem. Outros métodos como o Sistema de de vetores, o de Matriz, o em Blocos, apresentam uma dificuldade a mais, pelo fato de antes mesmo de começar a pré-codificação, é necessário mexer no texto da mensagem alterando seu formato original, para poder ir às etapas da criptografia. Porém possuem as mesmas falhas, uma vez descoberto o método e chave, a mensagem será decodificada.

Qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer apresenta o mesmo problema. Isso ocorre porque a frequência média com que cada letra aparece em um texto de uma dada língua é mais ou menos constante. Por exemplo, a frequência média de cada letra na língua portuguesa é dada na tabela a seguir.

Tabela 4 – Frequência média de cada letra na Língua Portuguesa

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

Mesmo estando a chave totalmente segura, o sistema simétrico ainda sim está em risco, pois se a mensagem cair em mãos erradas, ela poderá ser decodificada por um cripto-analista, que faz uso da criptoanálise para quebrar códigos cifrados.

A criptoanálise é o estudo de procedimentos para comprometer métodos (sistemas) criptográficos. Consiste em determinar métodos que possam ”quebrar“ sistemas de criptografia, tornar o sistema falho.

4.2 Métodos Assimétricos

Na criptografia de chave assimétrica são utilizadas chaves diferentes, mesmo estando relacionadas entre si. O fato é que esse relacionamento de uso de chaves é matemático, ou seja, o que uma cifra, a outra decifra. Com a criptografia assimétrica o método criptográfico fica mais seguro, pois a chave que é utilizada para cifrar o texto não é usada para decifrar. Apenas a parte correspondente pode fazê-lo (daí a palavra "assimétrica": partes não correspondentes). Assim, nesse método precisamos criar duas chaves, uma para cifrar outra para decifrar. A que cifra é também conhecida como chave pública e a que decifra como chave privada.

O problema é ter as duas chaves para poder fazer uma troca entre os correspondentes. E esse problema era uma paradigma para a comunidade dos criptologistas: a impossibilidade da troca de senha sem intermédio de um portador.

Esse problema foi resolvido por três norte-americanos, que acabaram desenvolvendo um método que acabou quebrando esse paradigma. O sistema foi criado por *Whitfield Driffie, Martin Hellman* e *Ralph Merkle* que ficou conhecido como DHM, e se baseia na seguinte idéia: Duas pessoas A e B, escolhem em comum acordo um par de números inteiros positivos a e m e os tornam públicos, depois usam os seguintes passos:

1. A escolhe outro número inteiro positivo α_A e o mantém secreto;
2. B escolhe outro número inteiro positivo α_B e o mantém secreto;
3. A calcula por meio de α_A, um único número $\beta_A < m$, tal que $a^{\alpha_A} \equiv \beta_A \ mod \ m$;
4. B calcula por meio de α_B, um único número $\beta_B < m$, tal que $a^{\alpha_B} \equiv \beta_B \ mod \ m$;
5. A envia β_A para B e B envia β_B para A, e, então:

   (i) A calcula $\beta_B^{\alpha_A}$, obtendo: $\beta_B^{\alpha_A} \equiv (a^{\alpha_B})^{\alpha_A} \equiv a^{\alpha_A \cdot \alpha_B} \equiv \alpha \ mod \ m$, com $\alpha < m$,

   (ii) B calcula $\beta_A^{\alpha_B}$, obtendo: $\beta_A^{\alpha_B} \equiv (a^{\alpha_A})^{\alpha_B} \equiv a^{\alpha_B \cdot \alpha_A} \equiv \alpha \ mod \ m$, com $\alpha < m$.

Dessa forma, as informações a, m, β_A e β_B são públicas. E as informações α, α_A e α_B são secretas, em que α_A é conhecida apenas por A e α_B é conhecida apenas por B, e α apenas A e B conhecem.

Por exemplo, vamos supor que duas pessoas Pedro e Mônica, tenham escolhido em comum acordo $a = 72$ e $m = 317$. Pedro escolhe sua chave secreta $\alpha_P = 11$, enquanto Mônica escolhe como chave secreta $\alpha_M = 9$. Vamos determinar a chave secreta α que ambos compartilharão.

Primeiro Pedro calcula β_P através da congruência $72^{11} \equiv \beta_P \ mod \ 317$, obtendo $\beta_P = 74$. Após encontrar $\beta_P = 74$, Pedro envia para Mônica o valor encontrado. Mônica calcula β_M através da congruência $72^9 \equiv \beta_M \ mod \ 317$, obtendo $\beta_M = 312$, e envia o valor encontrado para Pedro.

Ao receber de Pedro o valor $\beta_P = 74$, Mônica calcula α através da congruência $74^9 \equiv (74^{\alpha_P})^9 \equiv 74^{\alpha_P \cdot 9} \equiv \alpha \ mod \ 317$, obtendo $\alpha = 19$. Pedro também calcula α ao receber $\beta_M = 312$ de Mônica, obtendo também $\alpha = 19$.

Assim, as informações $a = 72$, $m = 317$, $\beta_P = 74$ e $\beta_M = 312$ são públicas, e as informações $\alpha_P = 11$, $\alpha_M = 9$ e $\alpha = 19$ são secretas.

A eficiência do DHM está no fato de ser difícil descobrir qualquer dos três α_A, α_B ou α, conhecendo a, m, β_A e β_B. De fato, dado x um número inteiro positivo, é fácil calcular o resto da divisão de a^x por m, porém é difícil fazer o caminho oposto, ou seja, dado y um número inteiro positivo, é difícil encontrar $x \in \mathbb{Z}_+$, tal que y é o resto da divisão de a^x por m. Assim, dado y, para resolver em x a equação $a^x \equiv y \ mod \ m$ é necessário construir a tabela dps valores da função

$$\begin{aligned} \mathbb{Z}_+ &\longrightarrow \mathbb{Z}_m \\ x &\longrightarrow [a^x] \end{aligned}$$

o que pode ser computacionalmente inviável, dependendo de uma boa escolha de a e de m.

O sistema DHM foi o primeiro passo para solução do problema de distribuição de chaves, porém serve apenas para troca de chaves secretas entre dois usuários de cada vez, e isso em um mundo globalizado é insatisfatório.

Então Driffie teve a idéia de considerar sistemas com chaves assimétricas, em que a cifragem deveria ser um processo fácil de fazer, com uso de chave pública, porém a decifragem deveria ser um processo praticamente impossível de fazer sem a chave secreta.

O sistema de criptografia, com chave pública pode ser usado nas eletrônicas, como compras pela internet, uso de cartões de crédito e em comunicações, onde é necessário usar assinatura eletrônica, como por exemplo, em cheques eletrônicos. Nesse sistema, é necessário entender como inteiros positivos (números naturais) que não podem ser fatorados facilmente em (dois) fatores primos se comportam, pois esses números podem ser as chaves privadas para usuários de comunicações pelo sistema assimétrico.

O método assimétrico tem um algoritmo com a função cifragem c, ou seja, c tem como parâmetros uma chave a e um texto t, em que obtém-se como resultado um novo texto (texto cifrado) t_i definido pela fórmula:

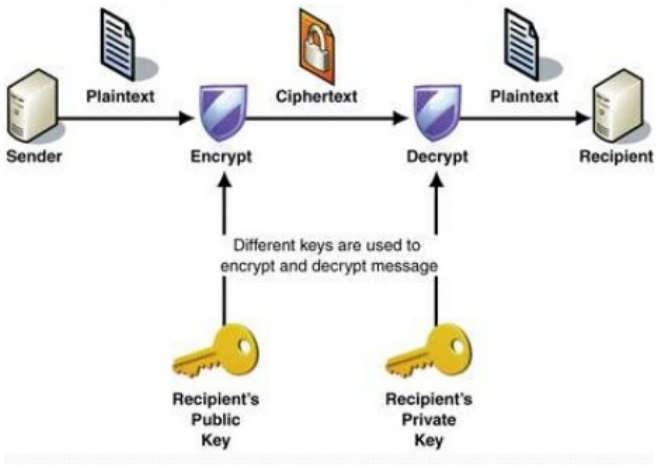
$$t_i = c(a,t).$$

Para que o texto seja decifrado, é preciso uma nova função s, que restabelece t_i à forma original t. Sendo a_i a chave de desencriptação, obtemos o texto original por meio da seguinte fórmula:

$$t = s(a_i, c(a,t)), \text{ ou seja, } t = s(a_i, t_i)$$

Na cifragem simétrica temos que $a = a_i$, sendo escrito apenas como chave a.

Figura 6 – Sistema criptográfico Assimétrico



FONTE: www.gta.ufrj.br (julho 2015)

4.2.1 O método RSA

O sistema de criptografia com chave pública RSA foi inventado por *Ronald L. Rivest, Adi Shamir* e *Leonard M. Adelman,* no ano de 1978 que, na época trabalhavam no *Massachussest Institute of Technology* (MIT). Mesmo existindo outros sistemas de codificação de chave pública, o RSA é atualmente o mais utilizado.

Nesse processo de codificação, a segurança é garantida, pois a chave de cifragem é pública e a chave de decifragem é privada. Assim, no sistema de chave pública, cada fonte receberá um par de dados (a, v), em que a é a chave de encifração, uma operação pública, e v é a operação de decifração privada (chave privada). A teoria do sistema de criptografia de chave pública (RSA) está baseada na idéia de que v deve ser uma operação muito difícil para ser usada por fonte não autorizada, ou seja, mesmo que essa fonte conheça a, ela não deve ter condições de determinar v, por meio de a.

Para podermos usar o RSA precisamos de dois parâmetros básicos: dois números primos p e q. Assim, para codificar um texto com o RSA, temos que conhecer o produto $p.q$ que vamos chamar de n, sendo portanto, a chave de codificação do RSA constituída pelo número $n = p.q$.

Cada usuário tem sua própria chave de códigos, sendo tornada chave pública. Desse modo, um sistema de cifragem é um método de comunicação secreta num canal de comunicação pública entre um grupo de fontes (pessoas, usuários). Para decodificar a mensagem, precisamos conhecer os números primos p e q. Para isso, basta fatorarmos $n = p.q$, e o código será decifrado. Dessa forma, para garantir a segurança do método RSA, precisamos escolher p e q muito grandes para que seja difícil fatorar n.

Para fazer a pré-codificação dos textos no RSA, usaremos uma tabela em que cada letra tem um número consecutivo do outro.

4.2.2 Implementação do RSA

A implementação do RSA consiste em utilizar algumas ferramentas da Teoria dos Números sendo a função ϕ de Euler uma dessas ferramentas. Assim, apresentaremos a definição dessa função e mais alguns teoremas para que possamos chegar ao processo de implementação, do RSA.

Definição 4.2.1 (Função ϕ de Euler)**.** *A função $\phi(n)$ de Euler é designada pelo número de elementos de um sistema reduzido de resíduos módulo n, que corresponde à quantidade de números naturais entre 0 e $n-1$ que são primos com n*

$$\phi : \mathbb{Z}^* \longrightarrow .\mathbb{Z}$$

Se n é um número inteiro positivo, a *função ϕ de Euler*, denotada po $\phi(n)$, é definida como sendo o número de inteiros positivos menores que ou iguais a n que são relativamente primos com n, ou seja, $\phi(n) \leq n-1$.

Enunciaremos um teorema e uma proposição, cujas demonstrações de ambos estão em (HEFEZ, 2013), (HEFEZ, 2003), (HEFEZ, 2014) e (SHOKRANIAN MARCUS SOARES, 1999).

Teorema 4.2.1 (Euler)**.** *Se $n, a \in \mathbb{Z}$ e $(a,n) = 1$, então $a^{\phi(n)} \equiv 1 \ mod \ n$.*

Proposição 4.2.1. *Se $a, b \in \mathbb{Z}$ e $(a,b) = 1$, então $\phi(ab) = \phi(a)\phi(b)$.*

Definição 4.2.2. *Chamamos o número $n = p.q$ de módulo, o número e de potência de encifração, d de potência de decifração e a tripla (n,e,d) de chave do sistema RSA.*

O seguinte teorema mostrará o que é o sistema RSA, como estão definidas as cifras e como podemos decifrá - las.

Teorema 4.2.2. *Sejam T o texto da mensagem e C a cifra. Suponhamos que:*

1. *p e q sejam primos distintos, $n = p \cdot q$;*
2. *$\phi(n) = (p-1)(q-1)$, $e \in \mathbb{Z}$, tal que $(e, \phi(n)) = 1$;*
3. *$T \in \mathbb{Z}$ $T \neq 0 \ mod \ p$ e $T \neq 0 \ mod \ q$;*
4. *$C \in \mathbb{Z}$ seja definido por $C \equiv T^e \ mod \ n$;*
5. *$d \in \mathbb{Z}$ seja definido pelas duas condições $ed \equiv 1 \ mod \ \phi(n)$, $1 \leq d \leq \phi(n)$.*

Então

$$T \equiv C^d \ mod \ n.$$

Prova:

Pela condição (4) temos que $C^d \equiv (T^e)^d \ mod \ n \Rightarrow C^d \equiv T^{ed} \ mod \ n$ Mas $ed \equiv 1 \ mod \ \phi(n)$.
Portanto, $ed = l\phi(n) + 1$, para algum $l \in \mathbb{Z}$. Então

$C^d \equiv T^{ed} \equiv T^{l\phi(n)+1} \ mod \ n$. Logo pelo Teorema 4.2.1 $T^{\phi(n)} \equiv 1 \ mod \ n$.

Logo,

$$C^d \equiv T^{l\phi(n)+1} \equiv (T^{p-1})^l xT \equiv T \ mod \ n,$$

que pode ser representado na seguinte forma:

$$T \equiv C^d \ mod \ n.$$

□

Os números $n, e, d \in \mathbb{Z}$ são todos escolhidos por usuários do sistema RSA de forma que satisfazem as condições do teorema acima.

Definição 4.2.3. *O par (n, e) é a **chave pública do sistema RSA** e o par (n, d) é a **chave privada** do sistema RSA.*

Para que A e B consigam trocar mensagens secretas no sistema RSA, eles precisam seguir as seguintes etapas:

1. B deve conhecer a chave pública (n, e) de A;
2. B traduz a mensagem t no alfabeto digital T_N;
3. B escreve T_N em blocos numéricos $T_1, T_2, \ldots, T_r$. Os blocos devem ser números inteiros positivos menores que n;
4. B encripta os blocos e estabelece as cifras $C_1, C_2, \ldots, C_r$. Logo,

$$C_1 \equiv T_1^e \ mod \ n, C_2 \equiv T_2^e \ mod \ n, \ldots, C_r \equiv T_r^r \ mod \ n;$$

5. B transmite as cifras $C_1, C_2, \ldots, C_r$ para A;
6. Ao receber a cifra, A decifra $C_1, C_2, \ldots, C_r$ usando o Teorema 3.2.2, segundo o qual

$$T_i \equiv C_i^d \ mod \ n; i = 1, 2, \ldots, r,$$

   com chave privada (n, d), onde somente d é privada para A, e somente A sabe esse número;

7. Uma vez que $T_1, T_2, \ldots, T_r$ são conhecidos por A, ele usa o alfabeto digital para transformar os blocos numéricos na mensagem original t,

e o processo está completo.

O exemplo a seguir mostra o processo de implementação mencionado anteriormente.

Exemplo 4.2.1. *Vamos implementar o algarismo 2 usando $p = 5$ e $q = 11$.*

Solução:
Primeiro vamos determinar n, pois a partir de n é que poderemos obter os demais elementos da criptografia RSA. Lembrando que o número e é escolhido e d depende do par $(\phi(n), e)$.
Logo

$$n = p.q \Rightarrow n = 5.11 \Rightarrow n = 55.$$

Assim,

$$\phi(n) = (p-1)(q-1) \Rightarrow \phi(n) = (5-1)(11-1) \Rightarrow \phi(n) = 40.$$

Agora, devemos escolher e para determinar d. Assim, temos que considerar

$$ed \equiv 1 \ mod \ \phi(n) \tag{4.1}$$

$$1 \leq d \leq \phi(n) \tag{4.2}$$

Considerando $e = 7$ (observe que $(e, \phi(n)) = 1$), a congruência (3.2.1) pode ser escrita como

$$ed = 1 + \phi(n)l \Rightarrow 7d = 1 + 40l$$

Temos, então:

$$d = \frac{1+40l}{7} = \frac{1+35l+5l}{7} = \frac{1+5l}{7} + 5l. \tag{4.3}$$

É preciso que d seja um número natural e, portanto, $\frac{1+5l}{7}$ deve ser natural. Para que isso ocorra, $1+5l$ deve ser múltiplo de 7. Desse modo, para algum $x \in \mathbb{N}$, temos que

$$1 + 5l = 7x \Rightarrow 7x - 5l = 1.$$

Resolvendo essa equação diofantina obtemos um valor $l = 4$ e $x = 3$, consequentemente, por (3.2.3) $d = 23$. Esse número é aceitável pela condição (4) do Teorema 3.2.2. Temos, então

$$C \equiv 2^7 \ mod \ 55 \ ou \ C \equiv 128 \ mod \ 55$$

donde, pelo Teorema 3.2.2, temos,

$$2 \equiv 128^{23} \ mod \ 55, \text{ consequência do Teorema,}$$

que é verdade, pois $55 \mid (128^{23} - 2)$.

4.2.3 Aplicação do RSA

Vamos considerar uma aplicação do método RSA. Uma vez implementado, aplicando-o, veremos que todas as etapas da implementação ajudam-nos a constituí-lo. A criptografia RSA é baseada em três etapas que são as mesmas de um sistema de cifragem comum, ou seja, *pré-codificação, codificação* e *decodificação.*

Explicaremos como funciona cada uma dessas etapas e depois cifraremos e decifraremos uma mensagem para melhor entendimento.

Pré-codificação

Para usarmos o método RSA, precisamos converter a mensagem em uma sequência numérica. Essa conversão é feita por meio de uma tabela, na qual cada letra corresponde a um número, supondo que na mensagem dada não haja nenhum número e que também as letras acentuadas sejam consideradas sem acento na hora da conversão.

Tabela 5 – Conversão dos Textos no RSA

∇	A	B	C	D	E	F	G	H	I	J	K	L	M
89	11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	∇
24	25	26	27	28	29	30	31	32	33	34	35	36	89

Escolhemos construir a tabela com esses números, mas também poderíamos ter escolhido outros números. Substituímos o espaço entre duas palavras pelo número 89 para fazermos a conversão, as letras correspondem a dois algarismos para evitar ambiguidade na mensagem com o alfabeto digital T_N, pois, se começássemos com um algarismo poderíamos confundir letras. Por exemplo, o número 25 poderia ser a letra Y ou as letras B e E com dois algarismos, mais isso não ocorre.

Em seguida, escolhemos números primos da tabela que serão os parâmetros do sistema RSA, pois são com eles que determinamos $n = p.q$. Na sequência quebramos em blocos o longo número T_N, de maneira que $T_1, T_2, \ldots, T_r < n$. Assim, a mensagem T_N ficará quebrada em blocos:

$$T_1 T_2 \ldots T_r$$

Codificação

Depois de encerrada a pré-codificação, usamos a chave de codificação (n, e), onde n foi encontrado no processo anterior e e é invertível módulo $\phi(n)$, e codificamos cada bloco, e a cada mensagem seguirá cada bloco codificado em sequência, uma vez que esses blocos não poderão formar um longo número, porque, se isso acontecer, será impossível decodificar a mensagem. Isso porque, quem receber a mensagem não saberá como os blocos foram formados. Mostraremos como se faz a codificação dos blocos.

Consideremos a cifra ou bloco codificado $C_i, i = 1,2,\ldots,r$. A idéia para calcular C_i é a seguinte:

$$C_i = \text{resto da divisão de } T_i^e \text{ por } n, \text{ ou seja, } T_i^e = nb + C_i.$$

Em termos de aritmética modular, C_i é a forma reduzida de T_i^e módulo n. Temos, então, n e $\phi(n)$. Escolhemos e como o menor número primo que não divide $\phi(n)$ para satisfazer a condição (2) do teorema 3.2.2. O bloco T_i^e é codificado como resto da divisão de T_i^e por n. Efetuando a conta por meio do cálculo da forma reduzida de T_i^e módulo n, obtemos

$$T_i^e \equiv C_i \ mod \ n.$$

Logo, a mensagem codificada torna-se

$$C_N = C_1 C_2 \ldots C_r.$$

Decodificação

O processo de decodificação no sistema RSA consiste em obter F_i, $i = 1,2,\ldots,r$, de maneira que, se T_i é um bloco da mensagem original, então $F_i C_i = T_i$. O que queremos dizer é que, decodificando um bloco da mensagem codificada, esperamos obter um bloco correspondente da mensagem original. Para isso, precisamos de p e q. Portanto, é necessário fatorar n, mas, além de n, precisamos do inverso de e módulo $\phi(n)$ para codificar. Assim, calculamos d aplicando o algoritmo euclidiano estendido a e e $\phi(n)$. Logo, para decodificar, consideramos os números e e d.
Consideremos o bloco C_i. Usando a chave de decodificação (n,d), F_i será o bloco decodificado.Portanto,

$$F_i = \text{resto da divisão de } C_i^d \text{ por } n.$$

Em termos de aritmética modular, F_i é a forma reduzida de C_i^d módulo n.

Temos, então, n e e. Aplicando o algoritmo euclidiano estendido $(x\alpha + y\beta = z)$ para calcular d, obtemos

$$\phi(n) = e.m + 1 \Rightarrow 1 = \phi(n) + (-m).e.$$

Logo, o inverso de e módulo $\phi(n)$ é $-m$. Precisamos que d seja positivo. Portanto $d = \phi(n) - m$, que é o menor inteiro positivo congruente a $-m$ módulo $\phi(n)$. Efetuando a conta por meio do cálculo da forma reduzida de C_i^d módulo n, obtemos:

$$C_i^d \equiv F_i \ mod \ n \ ; \ i = 1,2,\ldots,r.$$

A mensagem fica, então, decifrada, retornando ao texto original.

Exemplo 4.2.2. *Vamos codificar e decodificar a seguinte mensagem:*

DEUS SOBERANO E SENHOR

Solução:

Realizaremos as três etapas da criptografia RSA.

Pré-codificação

D	E	U	S	∇	S	O	B	E	R	A
14	15	31	29	89	29	25	12	15	28	11
N	O	∇	E	∇	S	E	N	H	O	R
24	25	89	15	89	29	15	24	18	25	28

A mensagem dada fica convertida no seguinte número:

$$T_N = 14153129892925121528112425891589291524182528.$$

Podemos escolher parâmetros $p = 11$ e $q = 17$. Assim, $n = p.q = 11.17 \Rightarrow n = 187$.

Quebrando T_N em blocos, obtemos:

$$14-153-12-98-92-92-51-21-52-81-124-258-91-58-92-9-152-41-82-52-8$$

Observação: O texto numérico (T_N) é quebrado em blocos pelo fato de tornar o sistema ainda mais seguro, pois se os blocos codificados cair em mãos erradas, quem interceptar não saberá quais as letras que compõe a mensagem. O tamanho de um bloco B_i, pode variar de um algarismo até a quantidade de algarismo de n. Assim, $B_i \in \{1, \ldots, n\}$, onde, cada elemento do conjunto é o tamanho do bloco.

Codificação

Cálculo de $\phi(n) = (p-1)(q-1) = (11-1)(17-1) \Rightarrow \phi(n) = 160$.
Escolheremos e, tal que $(e, \phi(n)) = (e, 160) = 1$. Por exemplo, $e = 3$.
Com a chave $(187, 3)$ codificaremos os blocos da mensagem:

$$\begin{aligned}
T_1^e = 14^3 = 2744;\ 2744 = 187 \cdot 14 + 126 &\Rightarrow C_1 = 126 \\
T_2^e = 153^3 = 3581577;\ 3581577 = 187 \cdot 19152 + 153 &\Rightarrow C_2 = 153 \\
T_3^e = 12^3 = 1728;\ 1278 = 187 \cdot 6 + 156 &\Rightarrow C_3 = 156 \\
T_4^e = 98^3 = 941192;\ 941192 = 187 \cdot 5033 + 21 &\Rightarrow C_4 = 21 \\
\vdots & \\
T_{21}^e = 8^3 = 512;\ 512 = 187 \cdot 2 + 138 &\Rightarrow C_{21} = 138
\end{aligned}$$

Logo,os blocos da mensagem codificada são:

$$126-153-156-21-20-20-68-98-171-17-159$$
$$-180-148-71-20-168-135-105-92-171-138$$

Se quiséssemos a mensagem codificada e não em blocos, teríamos

$$126153156212020689817117159180148712016813510592171138,$$

o que torna a mensagem praticamente inquebrável pois quem tiver acessado o texto dessa forma não sabe o formato dos blocos e nem quantos blocos tem a mensagem.

Decodificação

Vamos determinar d para obter a chave privada.

Sabemos que $\phi(n) = e.m+1$ e $d = \phi(n) - m$.

Então, $160 = 3m+1 \Rightarrow m = \dfrac{160-1}{3} \Rightarrow m = 53$. Portanto, $d = 160-53 \Rightarrow d = 107$.

Também podemos obter d por meio do método utilizado no Exemplo 3.2.1 então teríamos

$$\frac{1+10l}{3} \in IN \text{ achando } l = 2 \text{ e } d = 107.$$

Agora que temos o valor de d, utilizando a chave $(187, 107)$, decodificaremos os blocos cifrados:

$$\begin{aligned} C_1^d = 126^{107};\ 126^{107} \equiv F_1\ mod\ 187 \Rightarrow F_1 = 14 \\ C_2^d = 153^{107};\ 153^{107} \equiv F_2\ mod\ 187 \Rightarrow F_2 = 153 \\ C_3^d = 156^{107};\ 156^{107} \equiv F_3\ mod\ 187 \Rightarrow F_3 = 12 \\ C_4^d = 21^{107};\ 21^{107} \equiv F_4\ mod\ 187 \Rightarrow F_4 = 98 \\ \vdots \\ C_{21}^d = 138^{107};\ 138^{107} \equiv F_{21}\ mod\ 187 \Rightarrow F_{21} = 8 \end{aligned}$$

Voltamos aos blocos da mensagem original:

$$F = 14-153-12-98-92-92-51-21-52-81-124-258-91-58-92-9-152-41-82-52-8$$

Temos, novamente, então:

$$T_N = 14153129892925121528112425891589291524182528$$

Realizando a conversão outra vez, obtemos

14	15	31	29	89	29	25	12	15	28	11
D	E	U	S	∇	S	O	B	E	R	A
24	25	89	15	89	29	15	24	18	25	28
N	O	∇	E	∇	S	E	N	H	O	R

Portanto, obtemos o texto:

DEUS SOBERANO E SENHOR.

4.2.4 Funcionamento e Segurança do RSA

Funcionamento

O sistema RSA só será útil, se decodificando um bloco já codificado, conseguirmos de volta um bloco correspondente ao original. Com os pares (n,e) de codificação e (n,d) de decodificação, necessitamos verificar que se T_i é um número inteiro positivo e $1 \leq T_i \leq n-1$, então $F_i(C_i) = T_i$, ou seja, queremos provar que $F_i(C_i) \equiv T_i \ mod \ n$. Sabemos que tanto T_i quanto $F_i(C_i)$ pertencem ao intervalo $[1, n-1]$. Por isso, são congruentes módulo n se são iguais. Por definição de T_i e C_i temos que $F_i(C_i) \equiv (T_i^e)^d \equiv T_i^{ed} \ mod \ n$. Temos, assim, $T_i^{ed} \equiv T_i^{1+\phi(n)l} \equiv (T_i^{\phi(n)l})T_i \ mod \ n$ e como $T^{\phi(n)} \equiv 1 \ mod \ n$, então
$T_i^{ed} \equiv T \ mod \ n$. Portanto $F_i(C_i) \equiv T_i \ mod \ n$. Porém, não podemos concluir ainda nada porque nem sempre $(T_i, n) = 1$ para que $T_i^{\phi(n)} \equiv 1 \ mod \ n$, uma vez que os números dos blocos pertencem ao intervalo $[1, n-1]$. De maneira que a solução pode ser dada com qualquer número desse intervalo. Desse modo, temos que calcular a forma reduzida de T_i^{ed} módulo p, módulo q. Vamos, então, obter a forma reduzida de T_i^{ed} módulo q.
Sabemos que

$$ed = 1 + l\phi(n) = 1 + l(p-1)(q-1)$$

e, daí,

$$T_i^{ed} \equiv T_i(T_i^{(p-1)(q-1)}) \ mod \ q.$$

Suponhamos que $q \nmid T_i$. Então $T_i^{q-1} \equiv 1 \ mod \ q$. Logo, $T_i^{ed} \equiv T_i \ mod \ q$. Como q é número primo, no caso em que $q \mid T_i \Rightarrow T_i \equiv 0 \ mod \ q$. Assim, $T_i^{ed} \equiv T_i \ mod \ q$ vale para qualquer valor de T_i. Para calcular $T_i^{ed} \equiv T_i \ mod \ p$ procedemos de maneira análoga. O que queremos dizer é que $q \mid T_i^{ed} - T_i$ e $p \mid T_i^{ed} - T_i$, e pelo fato de p e q serem números primos distintos, $(p,q) = 1$, e, por isso, $pq \mid T_i^{ed} - T_i$, para qualquer $T_i \in \mathbb{Z}$. Com isso, chegamos à conclusão de que o método RSA funciona.

Segurança

Como o RSA é um método de chave pública, o par (n,e) é acessível a qualquer usuário. Então o RSA só será seguro se, mesmo conhecendo n e e, for difícil calcular d, pois só calcularemos d se tivermos $\phi(n)$ e e. Porém, só obteremos $\phi(n)$ se fatorarmos n para termos p e q. Mas, se n for um número grande, a fatoração será difícil.

O que queremos é que conhecendo $n = p.q$ e $\phi(n) = (p-1)(q-1)$ determinemos p e q com essas informações. Entretanto, $\phi(n) =)(p-1)(q-1) = pq - (p+q) + 1$, de forma

que $p+q = n+1-\phi(n)$. Contudo,

$$(p+q)^2 - 4n = p^2 + q^2 - 2pq = (p-q)^2 \Rightarrow |p-q| = \sqrt{(p-q)^2 - 4n}.$$

Conhecendo $p+q$ e $p-q$, calculamos facilmente p e q, ou seja, fatoramos n. Porém, não temos $\phi(n)$. Então esse tipo de fatoração só aconteceria se tivéssemos um algoritmo rápido para calcular $\phi(n)$ partindo de n e e. Poderíamos imaginar que fosse possível conseguir T_i com base na forma reduzida de T_i^e módulo n, sem tentar obter d. Só que, quando n é grande, isso se torna complicado. Dessa forma, quebrar o RSA e fatorar n são problemas equivalentes, embora isso ainda não tenha sido demonstrado.

4.2.5 Assinaturas Eletrônicas

Para garantir a segurança de textos (mensagens) eletrônicos é preciso autenticá-los, ou seja, assinar de alguma forma para que o receptor saiba que eles foram enviados pelo remetente autorizado. Uma vez que o RSA está sendo usado, os dados de codificação são públicos, de maneira que qualquer um pode mandar um texto codificado. Por isso, uma fonte precisa de garantia da outra, ou seja, o texto tem que ser "assinado": uma assinatura eletrônica. Vamos ver como se assina um texto (mensagem).

Sejam C_e e F_e as funções de codificação e decodificação de uma fonte A, respectivamente, C_b e F_b as funções correspondentes a fonte B. Para enviar um bloco T_i, em vez de A enviar $C(T_i)$ para B normalmente, ele manda assinada e envia $C_b(F_e(T_i))$. Primeiro A aplica a função de decodificação a T_i e só depois codifica usando a função de codificação de B. Ao receber o bloco $C_b(F_e(T_i))$, B decodifica para obter $F_e(T_i)$, e depois codifica para obter T_i, que é o bloco original, lembrando que C_e é público, por isso, é conhecido por B.

Quando B aplica aos blocos a sequência de funções C_eF_b, o texto deve fazer sentido para ter certeza de que a mensagem enviada foi codificada utilizando as funções C_bF_e. Como F_e é conhecido somente por A, ele deve ter sentido. Dessa maneira, B pode estar seguro de que o texto é legítimo, isto é, foi enviado por A.

5 PROPOSTA DE ATIVIDADES PARA ENSINO MÉDIO

Apresentaremos, aqui, uma proposta de aplicação da Criptografia Simétrica no Ensino Médio. Para trabalhar a Cifra Assimétrica é recomendado que se trabalhe com estudantes que possuem uma maior familiaridade com a Matemática (alunos que já estejam na $3^{\underline{a}}$ série do ensino médio, ou aqueles que possuem mais talento em matemática em qualquer série), já que a criptografia assimétrica requer aplicação de conceitos mais avançados de Teoria dos Números.

Para cada método de Criptografia apresentaremos uma atividade na qual será possível trabalhar com conteúdos do currículo da Educação Básica.
O Método 4.1.1 pode ser trabalhado em qualquer turma do Ensino Médio. Os métodos 4.1.3, 4.1.4 devem ser trabalhados nas turmas da $1^{\underline{a}}$ série do Ensino Médio como aplicação do conteúdo de *função afim, e função linear*. Já os métodos 4.1.2, 4.1.7 e 4.1.8 devem ser trabalhados nas turmas da $2^{\underline{a}}$ série do Ensino Médio como aplicação dos conteúdos *Matrizes e Determinantes*. O método 4.1.5 deve ser aplicado após o conteúdo de *Análise Combinatória*, e o método 4.1.6 pode ser aplicado em qualquer turma de Ensino Médio.

5.1 Aplicações da Criptografia no Ensino Médio

Iremos apresentar alguns exemplos de métodos de Criptografia Simétrica, fazendo um paralelo com os conteúdos do currículo do Ensino Médio. Para a proposta de atividades, usaremos a seguinte tabela de Pré-Codificação:

Tabela 6 – Conversão para Atividades Básicas

♯	Â	Á	Ê	É	Î	Í	Ô	Ó	Ú
00	01	02	03	04	05	06	07	08	09
Ã	Ẽ	Õ	Ç	A	B	C	D	E	F
10	11	12	13	14	15	16	17	18	19
G	H	I	J	K	L	M	N	O	P
20	21	22	23	24	25	26	27	28	29
Q	R	S	T	U	V	W	X	Y	Z
30	31	32	33	34	35	36	37	38	39

O professor pode utilizar uma tabela menor, porém usaremos essa tabela e trabalharemos com congruências módulo 40, pois ela tem letras acentuadas e o cedilha (ç), e o espaço será representado por ♯.

O professor deverá explicar ao aluno que, para se estabelecer uma chave a, é necessário que a e m sejam coprimos, pois só assim a terá inverso multiplicativo módulo

m.

Forneceremos exemplos de alguns métodos (exceto o método da cifra de César).

Exemplo 5.1.1. *Utilizando as chaves $a = 13$ e $b = 21$, vamos cifrar a palavra: EDUCAÇÃO.*

Solução:

Como $(13, 40) = 1$, concluímos que 13 tem inverso multiplicativo módulo 40.

A congruência de codificação é da forma $c \equiv (13t + 21)\ mod\ 40$. Essa congruência tem uma aparência peculiar com a função afim $(f(x) = ax + b)$, $c(t) = 13t + 21$. Observe que assim procedendo, estamos realizando uma analogia com um conteúdo do ensino médio. Agora, o professor pode utilizar o conceito de função afim para criptografar a mensagem.

Vamos, pois, codificar e decodificar a mensagem dada:

E	D	U	C	A	Ç	Ã	O
18	17	34	16	14	13	10	28

Aqui para codificar basta aplicar o algoritmo da divisão para obter resultados módulo 40.

Segue os resultados:

$$
\begin{aligned}
c(18) = 13.18 + 21 = 255 &\Longrightarrow 255 = 40.6 + 15 \Longrightarrow c(18) = 15,\\
c(17) = 13.17 + 21 = 242 &\Longrightarrow 242 = 40.6 + 02 \Longrightarrow c(17) = 02,\\
c(34) = 13.34 + 21 = 463 &\Longrightarrow 463 = 11.6 + 23 \Longrightarrow c(34) = 23,\\
c(16) = 13.16 + 21 = 229 &\Longrightarrow 229 = 40.5 + 29 \Longrightarrow c(16) = 29,\\
c(14) = 13.14 + 21 = 203 &\Longrightarrow 203 = 40.5 + 03 \Longrightarrow c(14) = 03,\\
c(13) = 13.13 + 21 = 190 &\Longrightarrow 190 = 40.4 + 30 \Longrightarrow c(13) = 30,\\
c(10) = 13.10 + 21 = 151 &\Longrightarrow 151 = 40.3 + 31 \Longrightarrow c(10) = 31,\\
c(28) = 13.28 + 21 = 385 &\Longrightarrow 385 = 40.9 + 25 \Longrightarrow c(18) = 25.
\end{aligned}
$$

Que nos fornecem a mensagem codificada: BÁJPÊQRL.

Para decodificar a mensagem, precisamos determinar o inverso multiplicativo de 13, e para calcular usaremos a congruência $13X \equiv 1\ mod\ 40$.

Para determinar o inverso de 13 módulo 40 sem usar congruências, o professor pode recorrer ao algoritmo da divisão e obter a seguinte equação $13X = 40Q + 1$, é equivalente a $13X - 40Q = 1$. Sabemos que $x \in \{7, 17, 27, 37\}$, pois são os únicos números módulo 40, que multiplicados por 13, produzem números que têm último algarismo 1. Dentre esses números, o que satisfaz a equação acima é 37, pois $13 \cdot 37 - 40 \cdot 12 = 1$. Concluímos, assim, que 37 é o único inverso multiplicativo de 13 módulo 40. Para calcular o simétrico aditivo de 21 módulo 40, basta resolver a equação $21 + d = 40$. Assim, $d = 19$.

Logo, a congruência que decodifica a mensagem é $t \equiv 37(c+19)\ mod\ 40$. Podemos também obter a função inversa e decodificar a mensagem, para isso basta que $c(t)$ seja invertível. Mas $c(t)$ é invertível, cuja a inversa de $c(t)$ é : $t(c) = \dfrac{c-21}{13}$. Considerando, agora, o simétrico de 21 e o inverso multiplicativo de 13, temos $c(t) = 37(c+19)$, algo semelhante à congruência de decodificação.

Aplicando o mesmo procedimento que usamos para codificar, decodificamos a mensagem e obtemos a mensagem original.

Na cifra Linear deve-se determinar o inverso multiplicativo da chave.

O próximo exemplo trata de cifras por meio de matrizes.

Exemplo 5.1.2. *Com a matriz-chave* $A = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}$, *vamos criptografar a palavra AMOR.*

Solução:

A congruência de codificação de qualquer mensagem é dada por: $C \equiv AT\ mod\ 40$, ou seja,

$$\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \equiv \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} . \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix}\ mod\ 40.$$

Inicialmente, observamos que $det(A) = 1$, e assim, A é uma matriz invertível. Podemos, agora, pré-codificar a palavra dada, como segue:

$$T = \begin{bmatrix} A & O \\ M & R \end{bmatrix} \Longrightarrow T = \begin{bmatrix} 14 & 28 \\ 26 & 31 \end{bmatrix}.$$

Obtenhamos agora a matriz criptografada correspondente ao produto da matriz-chave A pela matriz de códigos T, isto é,

$$C = A \cdot T = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} . \begin{bmatrix} 14 & 28 \\ 26 & 31 \end{bmatrix} = \begin{bmatrix} 92 & 121 \\ 210 & 273 \end{bmatrix} = \begin{bmatrix} 12 & 1 \\ 10 & 33 \end{bmatrix},$$

que nos dá a palavra codificada: ÕÃÂT.

Para decodificar a palavra que acabamos de obter, precisamos usar um processo semelhante, porém com a matriz C e a matriz $D = A^{-1}$, que é a inversa de A:

$$A \cdot D = I \Longrightarrow \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} . \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Obtemos, assim, os seguintes sistemas lineares.

$$\begin{cases} x_1 + 3y_1 = 1 \\ 2x_1 + 7y_1 = 0 \end{cases} \text{ e } \begin{cases} x_2 + 3y_2 = 0 \\ 2x_2 + 7y_2 = 1 \end{cases}.$$

Resolvendo esses sistemas eobtemos as soluções $x_1 = 7$, $x_2 = -3$, $y_1 = -2$ e $y_2 = 1$.

Temos, então, a matriz inversa de A, $D = A^{-1} = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix}$.

Logo,

$$T = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix} . \begin{bmatrix} 12 & 1 \\ 10 & 33 \end{bmatrix} = \begin{bmatrix} 54 & -92 \\ -14 & 31 \end{bmatrix} = \begin{bmatrix} 14 & 28 \\ 26 & 31 \end{bmatrix},$$

e obtemos a palavra original: AMOR.

Nesse método, usamos como conteúdo do Ensino Médio matrizes e determinantes, as operações de multiplicação de matrizes, o cálculo do determinante e determinação de matriz inversa, além de sistemas lineares.

O próximo exemplo aborda os mesmos conteúdos do Exemplo 5.1.2 e também a operação de adição de matrizes.

Exemplo 5.1.3. *Por me do método de Cifra em Blocos, usando como chave o par de matrizes* $A = \begin{bmatrix} 3 & 2 \\ 13 & 9 \end{bmatrix}$ *e* $B = \begin{bmatrix} 5 \\ 7 \end{bmatrix}$*, vamos codificar a palavra MESTRE.*

Solução:

Para codificar a palavra, precisamos saber se A é uma matriz invertível. Como $det(A) = 1$, a matriz A é invertível.

Podemos obter a codificação pela congruência:

$$\begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \equiv \left(\begin{bmatrix} 3 & 2 \\ 13 & 9 \end{bmatrix} . \begin{bmatrix} t_{11} \\ t21 \end{bmatrix} + \begin{bmatrix} 5 \\ 7 \end{bmatrix} \right) \ mod\ 40.$$

Fazendo a pré-codificação, temos os blocos:

$$\begin{bmatrix} M \\ R \end{bmatrix}; \begin{bmatrix} S \\ T \end{bmatrix}; \begin{bmatrix} R \\ E \end{bmatrix} \Longrightarrow \begin{bmatrix} 26 \\ 18 \end{bmatrix}; \begin{bmatrix} 32 \\ 33 \end{bmatrix}; \begin{bmatrix} 31 \\ 18 \end{bmatrix}.$$

Aplicando a congruência acima, obtemos os blocos:

$$\begin{bmatrix} 39 \\ 27 \end{bmatrix}; \begin{bmatrix} 07 \\ 02 \end{bmatrix}; \begin{bmatrix} 14 \\ 12 \end{bmatrix} \Longrightarrow \begin{bmatrix} Z \\ N \end{bmatrix}; \begin{bmatrix} \hat{O} \\ \acute{A} \end{bmatrix}; \begin{bmatrix} A \\ \tilde{O} \end{bmatrix},$$

que nos fornece a palavra codificada: ZNÔÁAÕ.

Para decodificar a palavra que acabamos de obter, precisamos de calcular a matriz inversa ($D = A^{-1}$) da matriz A e a matriz simétrica (H) da matriz B. Temos, então

$$\begin{bmatrix} 5 \\ 7 \end{bmatrix} + \begin{bmatrix} h_{11} \\ h_{21} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Longrightarrow H = \begin{bmatrix} 35 \\ 33 \end{bmatrix},$$

lembrando que essa operação é feita módulo 40. Para obtermos a inversa, devemos efetuar operações análogas àquelas do Exemplo 5.1.2 sobre cálculo da inversa. Assim, temos

$$D = \begin{bmatrix} 9 & 13 \\ -2 & 3 \end{bmatrix}.$$

A congruência que fornece a decodificação da dada é:

$$\begin{bmatrix} t_{11} \\ t_{21} \end{bmatrix} \equiv \begin{bmatrix} 9 & 13 \\ -2 & 3 \end{bmatrix} \left(\begin{bmatrix} 35 \\ 33 \end{bmatrix} + \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \right) \ mod\ 40$$

que nos fornece a palavra original: MESTRE.

O exemplo a seguir usa cifra permutacional.

Exemplo 5.1.4. *Vamos codificar a palavra CRIADO, permutando 6 apenas posições no alfabeto.*

Solução:

Para criptografar essa palavra deslocaremos na tabela a seguir 6 posições de cada letra da palavra que queremos criptografar.

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

Que nos fornece a palavra codificada: IXGJU.

Para decodificar a palavra IXGJU, basta voltarmos 6 posições na tabela, ou então, resolvermos a seguinte congruência $6 + p \equiv 0\ mod\ 26$ (fazermos a seguinte conta $6 + P = 26 \Longrightarrow P = 20$), e assim, ao invés de voltarmos, iremos 20 posições a diante, e obtemos a mensagem original.

Observe que nesse exemplo, é trabalhado com módulo 26, e não 40 como nos demais exemplos.

O próximo exemplo trabalha com vetores de duas componentes. O professor de matemática não terá dificuldade em trabalhar esse método, mesmo não tendo o conteúdo de vetor no currículo de matemática. Pois, no currículo de física tem esse conteúdo, lógico que do ponto de vista geométrico e como grandeza física, basta que o professor faça a tranposição da ideia de vetor, para a parte algébrica.

Exemplo 5.1.5. *Usando como chave o vetor* $\vec{a} = (23, 18)$*, vamos codificar a palavra*

CONGREGADO.

Solução:

Pré-codificando a mensagem, temos a tabela,

C	O	N	G	R	E	G	A	D	O
16	28	27	20	31	18	20	14	17	28

.

Temos então os seguintes vetores,

$$\vec{t_1} = (16, 28),\ \vec{t_2} = (27, 20),\ \vec{t_3} = (31, 18),\ \vec{t_4} = (20, 14)\ e\ \vec{t_5} = (17, 28).$$

A congruência que nos fornece a codificação da palavra dada é

$$\vec{c_i} \equiv (\vec{a} + \vec{t_i})\ mod\ 40 \Longrightarrow (c_{1_i}, c_{2_i}) \equiv ((t_{1_i}, t_{2_i}) + (23, 18))\ mod\ 40.$$

Podemos reescrever essa congruência como sendo $(c_{1_i}, c_{2_i}) = (t_{1_i} + 23, t_{2_i} + 18)$, e quando a soma de qualquer uma das componentes passar 40 (módulo que está sendo trabalhado), efetuamos a divisão euclidiana, e pegamos o resto.

Assim, temos

$(c_{1_1}, c_{2_1}) = (16 + 23, 28 + 18) = (39, 46) \Longrightarrow (c_{1_1}, c_{2_1}) = (39, 06)$

Que nos fornece os seguintes vetores

$$\vec{c_1} = (39, 06),\ \vec{c_2} = (10, 38),\ \vec{c_3} = (14, 36),\ \vec{c_4} = (03, 32)\ e\ \vec{c_5} = (00, 06).$$

Assim, temos os vetores códigos,

(Z,Í); (Ã,Y); (A,W); (Ê,S) e (♯,Í).

Obtemos então o seguinte código: ZÍÃYAWÊS♯Í.

Essa mensagem pode ser decodificada pela congruência $\vec{t_i} \equiv (\vec{c_i} + (17, 22))\ mod\ 40 \Longrightarrow (t_{1_i}, t_{2_i}) \equiv ((c_{1_i}, c_{2_i}) + (17, 22))\ mod\ 40$, que pode ser representada por $\vec{t_i} = \vec{c_i} + (17, 22)$,

que é a expressão $(t_{1_i}, t_{2_i}) = (c_{1_i} + 17, c_{2_i} + 22)$, lembrando que aqui é trabalhado módulo 40.

Aplicando essa expressão na palavra codificada, voltamos a palavra original.

5.2 Propostas de Metodologias para o ensino da Criptografia

Metodologia é uma palavra que tem origem grega (*methodos + logia*), sendo (*meta* = objetivo, finalidade; e *hodos* = caminho, intermediação) ***methodos*** *o caminho para conseguir atingir um objetivo* e ***logia*** *o conhecimento, ciência, estudo.* Podemos então definir ***metodologia:*** *como sendo o estudo do caminho para atingir um objetivo.*

Ensino é ação, maneira de transmitir conhecimento. O ensino é desenvolver a aprendizagem, e só há aprendizagem quando as informações sobre determinado conteúdo são transformadas em conhecimento, com todos os requisitos necessário para a definição de conhecimento. Assim, podemos dizer que ***Metodologia de Ensino*** é o estudo do caminho para atingir o aprendizado de alguém (ajudar a desenvolver conhecimento).

Na prática educativa uma metodologia de ensino é a maneira de como se é transmitido o conhecimento, com objetivo de alcançar a aprendizagem.

5.2.1 Metodologias de Ensino de Criptografia

Faremos sugestões de Metodologias para que professores do Ensino Médio trabalhem Criptografia nas séries em que são regentes de aulas.

Para ensinar Criptografia o professor deverá:

1. Explicar o conteúdo do currículo básico do Ensino Médio de acordo com cada série de ensino.
2. Após desenvolver as atividades de fixação de aprendizagem, falar da importância da aplicação da Matemática em diversas áreas de conhecimento.
3. Conceituar Congruências Módulo m, e falar de suas aplicações.
4. Falar sobre a importância da segurança da informação.
5. Conceituar Criptografia, falar sobre Sistema Criptográfico.
6. Trabalhar os métodos de Criptografia que melhor se adequam ao conteúdo trabalhado, como uma aplicação do conteúdo.

7. Desenvolver atividades de métodos de Criptografia, para que os estudantes entendam o funcionamento dos métodos.

8. Elaborar exercícios para que os alunos fixem os métodos, esses exercícios podem ficar para ser feito em casa.

9. Construir aparatos que ajudam a criptografar mensagens.

10. Fazer uma avaliação sobre os métodos de Criptografias trabalhados.

Ao realizar as atividades o professor deverá seguir as três etapas do processo de Criptografia. Além disso, deve deixar claro a necessidade da segurança, assim, é aconselhável que se divida a turma em grupos, isso após o professor trabalhar os seis primeiros itens acima.

5.2.2 Sugestões de atividades de Criptografia

Aqui sugerimos algumas atividades para trabalhar Criptografia em sala de aula. Inicialmente proporemos duas atividades sobre o algoritmo da Divisão Euclidiana e outra(s) atividade(s) sobre Congruências Módulo m.

Atividade 5.2.1 (Algoritmo da Divisão)**.** *Efetuar a divisão de dois números a e b por um número m, determinar o resto da divisão e depois escrever na forma do Algoritmo da Divisão.*

Atividade 5.2.2. *(Par ou Impar) Desenvolva uma explicação usando a definição do Algoritmo da Divisão para determinar quando um número é par ou quando um número é impar.*

Atividade 5.2.3 (Congruência Módulo m)**.** *Verificar se os números a e b são congruentes módulo m, e se os números c e d são congruentes módulo m. Em caso de serem congruentes explique $a+c \equiv b+d \ mod \ m$ e $a \cdot c \equiv b \cdot d \ mod \ m$. Caso não serem congruentes, justifique $a+c \not\equiv b+d \ mod \ m$ e $a \cdot c \not\equiv b \cdot d \ mod \ m$*

Atividade 5.2.4 (Determinando Algarismo)**.** *Determinar o algarismo das unidades na representação decimal do número $N = (2014^{2015} + 2013 \cdot 2017^{2015})^{2015}$.*

Atividade 5.2.5 (Dia da semana)**.** *8 de março de 2015 foi um dia de domingo. Que dia da semana será 27 de setembro de 2019?*

Para as atividades de Criptografia usaremos a tabela a seguir, o professor pode escolher outra tabela, para desenvolver suas atividades.

Tabela 7 – Pré-Codificação de Mensagens

♯	A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	♯
14	15	16	17	18	19	20	21	22	23	24	25	26	00

Atividade 5.2.6 (Criptografia: Pré-Codificação)**.** *Usando a tabela 7 pré-codifique a mensagem*

VIDA BOA É VIDA FELIZ

Atividade 5.2.7 (Cifra de César)**.** *Ainda usando a Tabela 7 para pré-codificação, criptografe a mensagem,*

VIVER EM PAZ,

usando a Cifra de César (Método 4.1.1). A chave ou será uma escolha sua.

Atividade 5.2.8 (Aplicação em Grupo)**.** *Monte um grupo com três pessoas (X, Y e Z) e escolham um método de Criptografia. Agora siga os seguintes passos.*

1. *As Pessoas X e Y combinam uma chave de cifragem, sem que Z saiba;*
2. *X entrega codifica a mensagem, e entrega para Z entregar para Y;*
3. *Antes de entregar a mensagem para Y, Z deve tentar quebrar o código e decifrar o conteúdo da mensagem;*
4. *Z devolve a mensagem para Y, mesmo se não tiver conseguido decodificar a mensagem;*
5. *X, Y e Z devem relatar sobre o método utilizado e sua segurança.*

Atividade 5.2.9 (Aplicação em Grupo)**.** *Monte um grupo com três pessoas (X, Y e Z) e sigam os seguintes passos*

1. *X e Y escolhem um método de Criptografia, e a chave do método sem que Z saiba;*
2. *X codifica a mensagem através do método combinado, e entrega para Z entregar a mensagem cifrada para Y;*
3. *Z deve tentar quebrar a mensagem, antes de entregar para Y;*
4. *Z entrega a mensagem para Y, mesmo se não conseguir quebrar o código da mensagem;*

5. *X, Y e Z devem relatar sobre o método utilizado e sua segurança.*

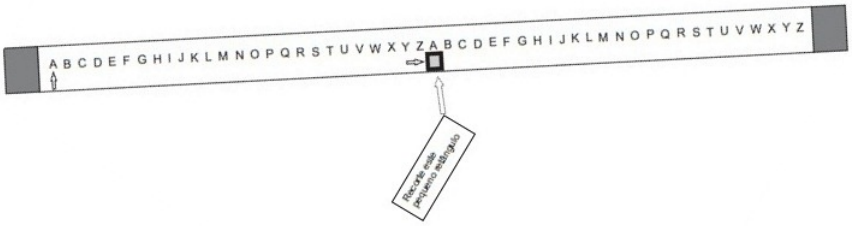
Atividade 5.2.10 (Régua Cifrante)**.** *Essa atividade é simples e permite aplicar a Cifra de César facilmente. Para Fazer uma régua Cifrante precisamos de poucos materiais, e seguir os seguintes passos:*

1. *Recorte dois retângulos, uma mais largo e menor que o outro, escrevendo o alfabeto nos dois retângulos;*

Figura 7 – Régua Cifrante 1

FONTE: Apostila 10 do Programa PIC da OBMEP (dezembro 2015)

Figura 8 – Régua Cifrante 2



FONTE: Apostila 10 do Programa PIC da OBMEP (dezembro 2015)

2. *Encaixe os retângulos conforme a figura a seguir;*

Figura 9 – Régua Cifrante Pronta

FONTE: Apostila 10 do Programa PIC da OBMEP (dezembro 2015)

3. *Escolha o texto a ser codificado e deslize a fita mais fina para obter as letras codificadas correspondentes.*

Atividade 5.2.11 (Várias Chaves)**.** *Pode-se dividir a turma em vários grupos, onde dois a dois trocam mensagens usando a Cifra One-Time-Pad para cifrar uma palavra. O grupo que interceptar a mensagem do destinatário deve tentar quebrar o código. Ao fim da atividade, o professor pode fazer um explanação do motivo da Cifra OTP ser inviável.*

Atividade 5.2.12 (Relacionando Conteúdos)**.** *Ao fim de aplicar um método de Criptografia, pode-se pedir ao alunos, que relacione as ferramentas matemáticas utilizadas no processo do Método com os conteúdos estudados em sala de aula.*

Atividade 5.2.13 (Analisando Frequências)**.** *Pode-se passar um texto cifrado para os alunos e pedir que eles tentem decifrar, usando apenas o análise da frequência de cada letra no texto, fazendo com que os alunos percebam que sempre um texto cifrado de cifra simétrica sempre há uma letra que aparece mais que a demais. Depois utilizando a Tabela 3 (Frequência média de cada letra na língua Portuguesa), explicar como tentar decodificar uma menagem utilizando apenas essa tabela.*

Trabalhando Congruências Módulo m

Para trabalhar Congruências Módulo m, o professor poderá abordar primeiro o fato da ocorrência de fenômenos cíclicos (aqueles se repetem regularmente em períodos iguais). Além disso, poderá falar da importância de aprender Congruência, mostrando depois que esse conteúdo está relacionado com o Algoritmo da Divisão Euclidiana.

O professor pode trabalhar a divisão de dois números inteiros a e b por um mesmo número natural m e comparar seus restos, das respectivas divisões por m, antes de introduzir o conceito e a notação de congruência. Após isso separar alguns fenômenos cíclicos a aplicar usando a divisão. Por exemplo, analisando um ângulo de 4865°, qual será seu correspondente menor que 360°? Observe que $4865 = 360.13 + 5$, logo o ângulo de 4865° corresponde ao ângulo de 5° na circunferência (círculo trigonométrico).

Depois de fazer esse comparativo, o professor poderá trabalhar a definição de Congruência Módulo m, e suas propriedades básicas, sempre mostrando exemplos numéricos, antes de ir a qualquer demonstração, para facilitar a compreensão e abstração do aluno em relação ao conteúdo estudado.

6 PROGRAMAS EXECUTÁVEIS EM LINGUAGEM C

Apresentaremos, neste capítulo, alguns programas executáveis que servem de apoio nas aulas, pois facilitam a compreensão dos alunos quando veem o programa funcionando, também, podendo eles mesmos executarem no computador o que estudaram.

Os programas aos quais nos referimos acima são alguns dos métodos de criptografia simétrica, aqueles que condizem mais com os conteúdos abordados em sala de aula, durante um ano letivo do Ensino Médio. Também apresentaremos o algoritmo da divisão, pois ele é usado em todo o nosso trabalho.

Esses programas foram escritos em códigos da linguagem **C**.

A Linguagem **C** foi criada por Dennis M. Ritchie e Ken Thompson no laboratório Bell, em 1972, sendo uma evolução da antiga linguagem BCPL. C é uma ferramenta poderosa na programação de qualquer tipo de sistema, como sistemas operacionais, planilhas, banco de dados, sistemas de transmissão de dados e telefonia, dentre outros.

A linguagem C é vantajosa, pois é uma linguagem de alto nível com uma sintaxe bastante estruturada e flexível tornando sua programação bastante simplificada. Seus programas são compilados, gerando programas executáveis. Pode-se fazer em C programação de baixo nível, quanto de alto nível.

Alguns compliadores para programar em C são: Dev C++, CodeBlocks, Microsoft Visual C++, dentre outros.

Um compilador é um programa no qual são feitos os programas na linguagem da máquina (computador).

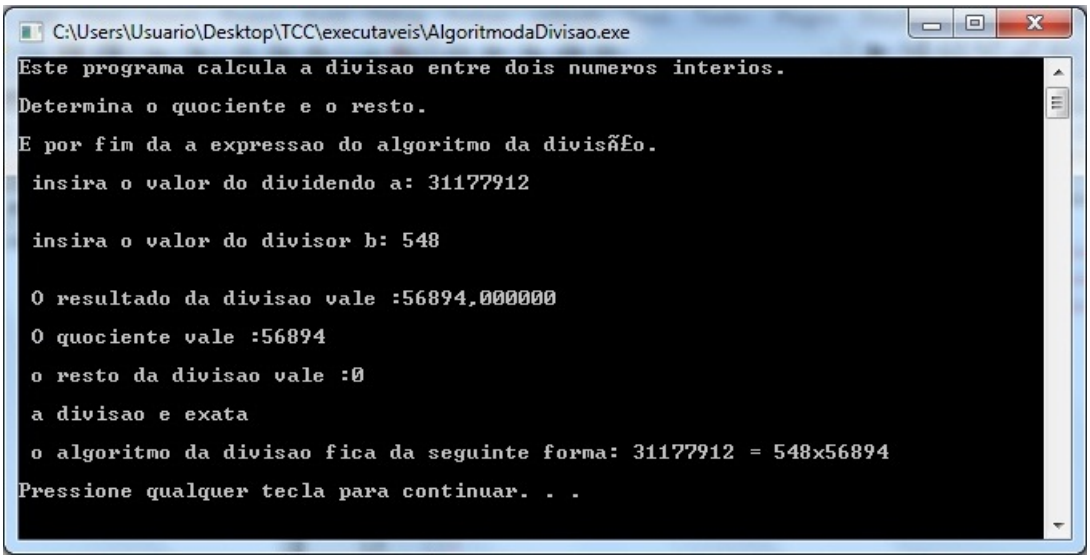
Sobre programação em linguagem C, o leitor pode encontrar mais informação em (MIZRAHI, 2008) e (SOFFNER, 2013)

Faremos execução de duas divisões por um programa executável criado na linguagem C. Esse programa efetua a divisão, determina o quociente, o resto e os escreve na forma do algoritmo da divisão de Euclides.

As divisões a serem feitas são $31177912 \div 548$ e $758493231 \div 762$. Ao executar temos duas opções:

A primeira divisão é exata.

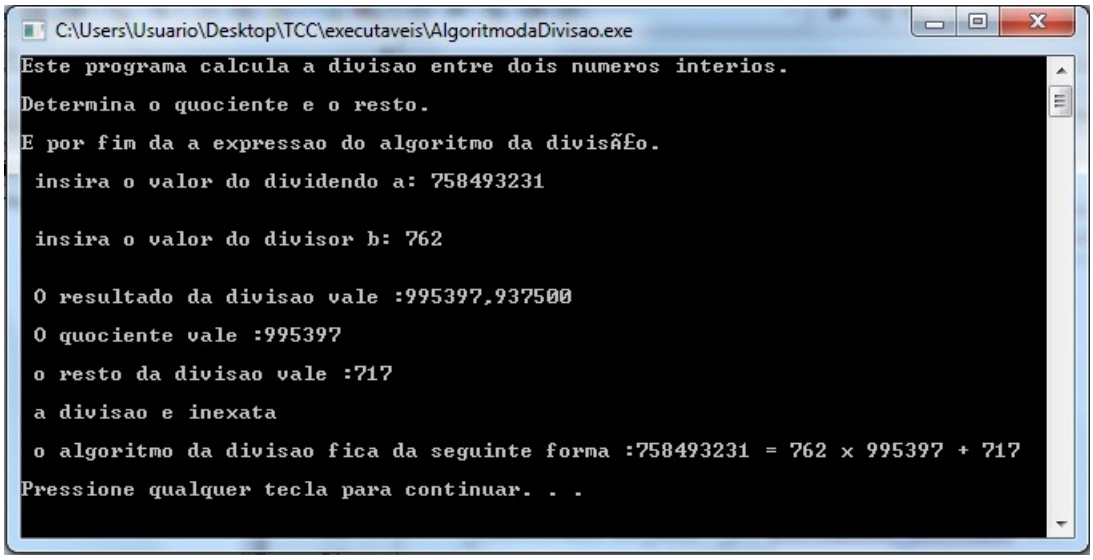
Figura 10 – Divisão exata



FONTE: criado no codeblocks (2015)

A segunda divisão é inexata.

Figura 11 – Divisão inexata



FONTE: criado no codeblocks (2015)

Imagine o trabalho para fazer essas divisões apenas com lápis, papel e borracha. A função do programa é trazer facilidade ao usuário, pois, se a divisão fosse com números de poucos algarismos, poderia ser feita no papel. Porém como são números de uma quantidade significativa de algarismos, o programa é o indicado para essa tarefa.

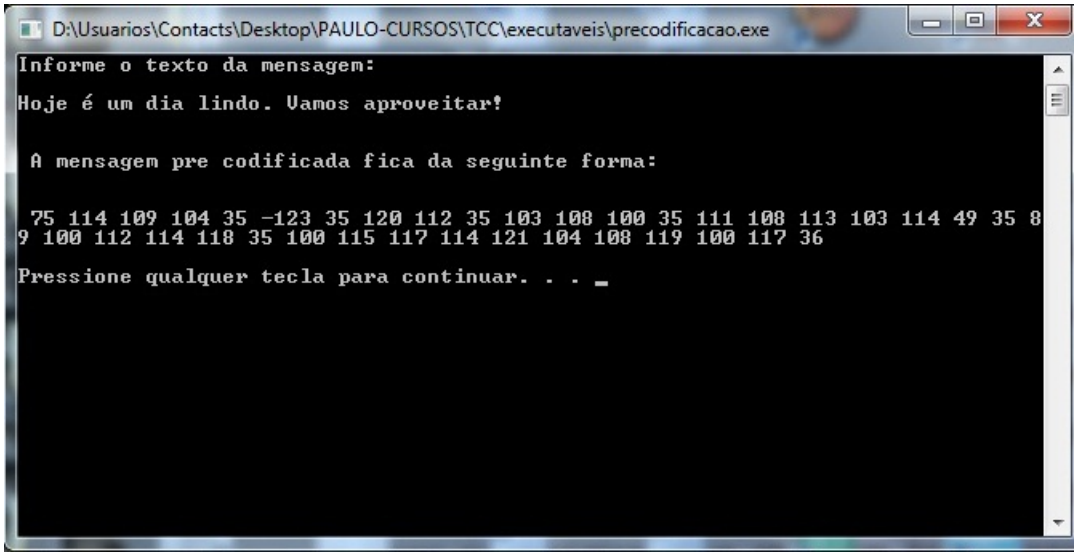
Para os programas de Criptografia, usaremos para pré-codificação a tabela ASCII, que é uma tabela de codificação, desenvolvida a partir de 1960. Vale lembrar que a tabela ASCII, não é um método de Criptografia. Ela é uma tradução dos símbolos mais frequentes

para a linguagem binária. Ela atribui significados específicos para os $2^7 = 128$ números binários (formados por 0 e 1) de sete dígitos.

Mostraremos, agora, alguns programas executáveis de Criptografia, cujos algoritmos são os métodos de cifragem apresentados neste trabalho.

O próximo programa executável mostrará como fica uma mensagem quando pré-codificada.

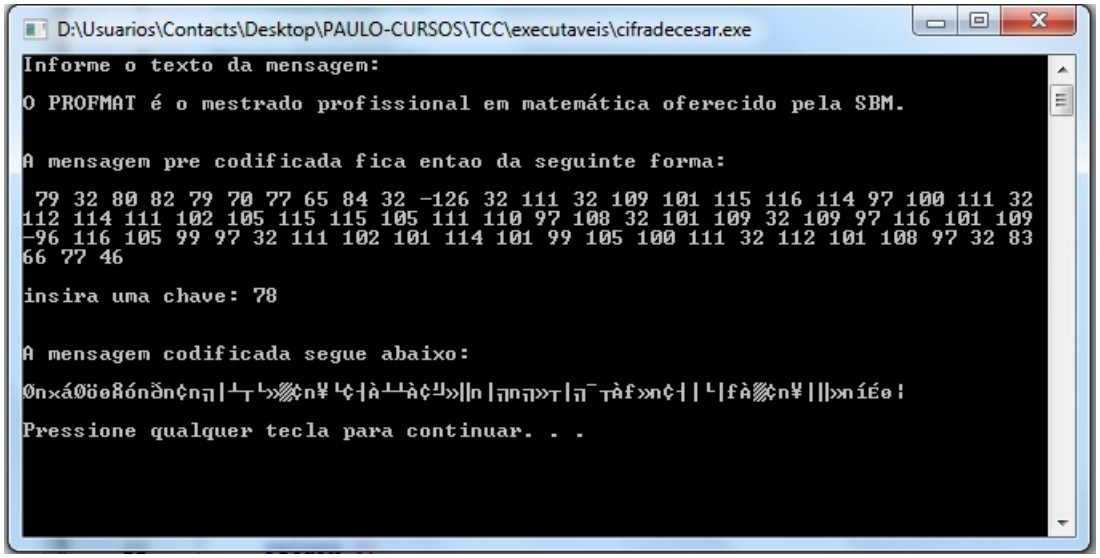
Figura 12 – Pré-codificação de mensagem



FONTE: criado no codeblocks (2015)

O programa a seguir é a *Cifra de César*, apenas com a codificação do texto mensagem.

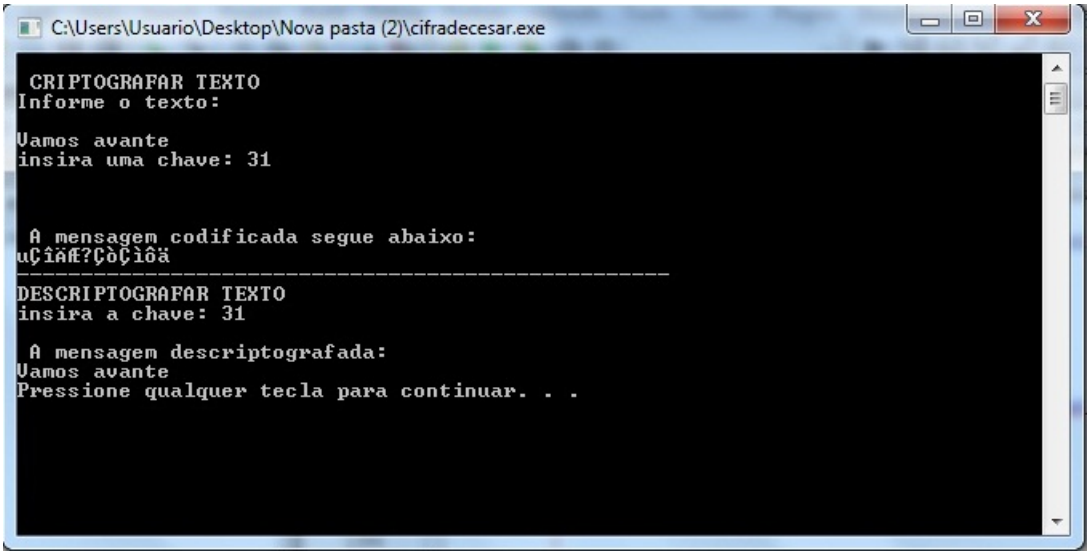
Figura 13 – Cifra de César



FONTE: criado no codeblocks (2015)

O programa a seguir mostra a *Cifra de César*, executando as etapas da criptografia.

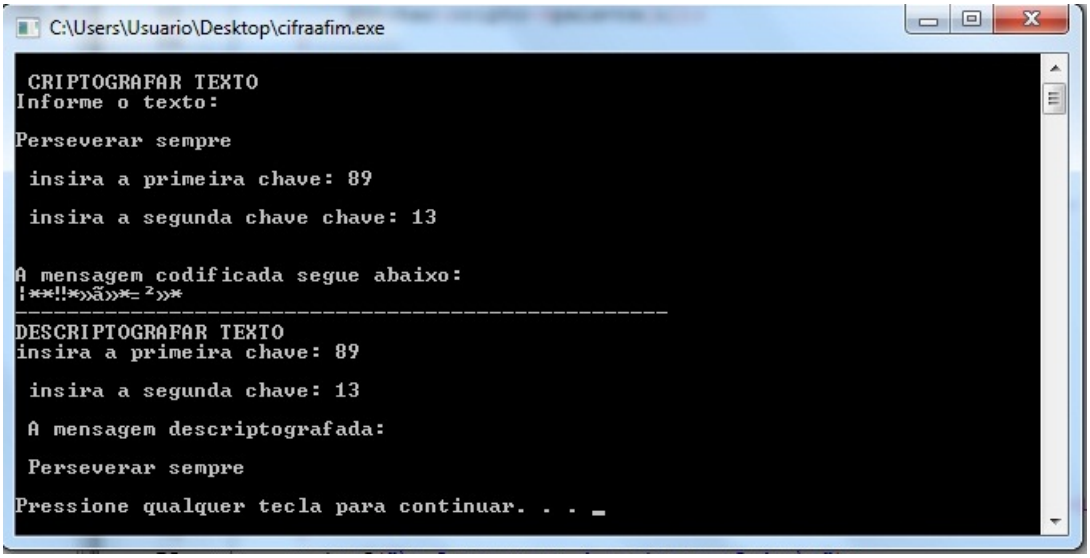
Figura 14 – Cifra de César



FONTE: criado no codeblocks (2015)

O próximo programa mostra uma mensagem que é codificada na *Cifra Afim*

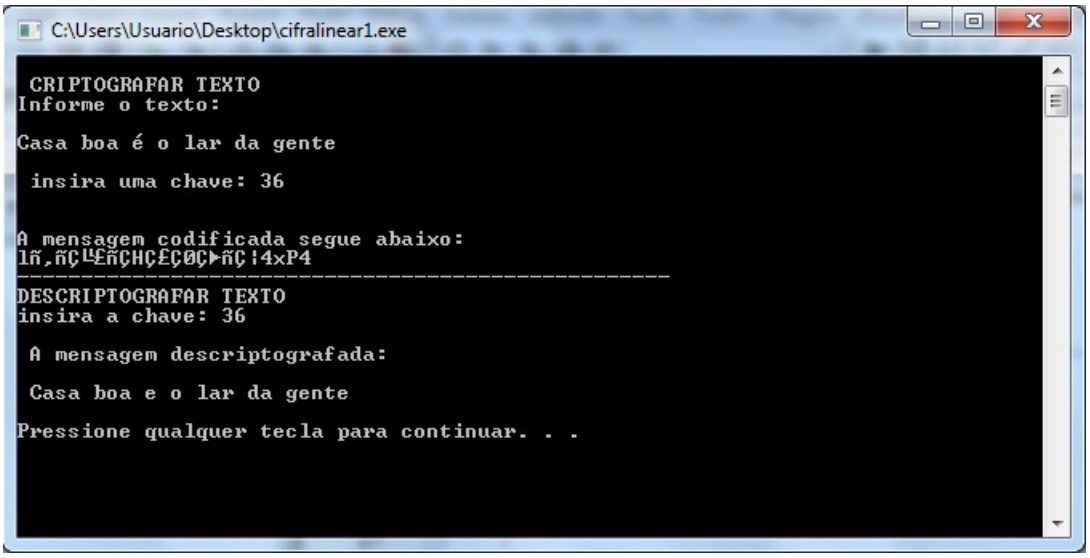
Figura 15 – Cifra Afim



FONTE: criado no codeblocks (2015)

O programa a seguir mostra a *Cifra Linear*

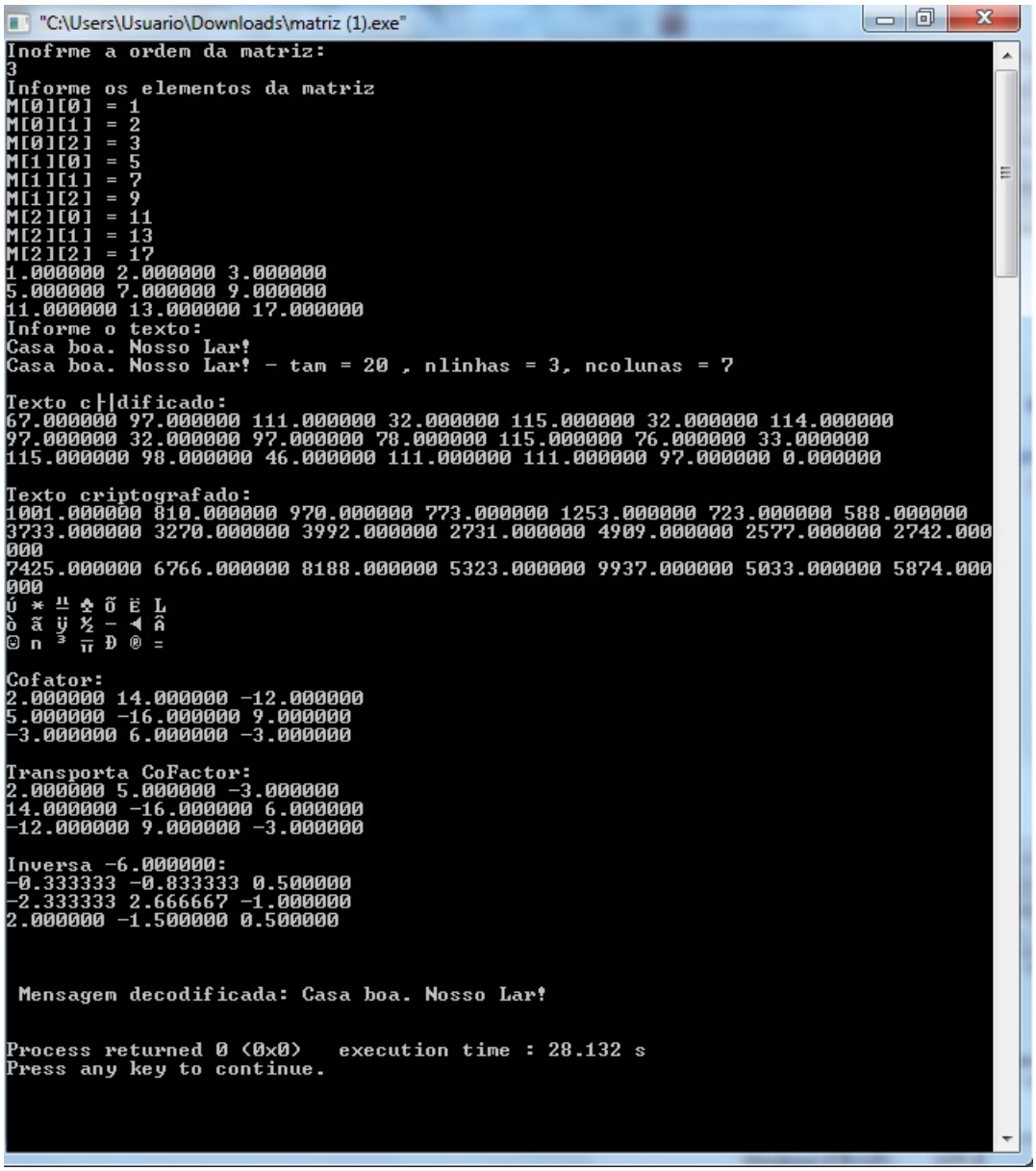
Figura 16 – Cifra Linear



FONTE: criado no codeblocks (2015)

O próximo programa mostra a *Cifra por Meio de Matriz*, mostra também o tamanho do texto, a matriz dos cofatores e a matriz inversa antes da mensagem decodificada.

Figura 17 – Cifra Por Meio de Matriz



FONTE: criado no codeblocks (2015)

7 CONCLUSÃO

Neste trabalho, apresentamos um estudo de Criptografia, inciando por um breve histórico, apresentando a teoria necessária para aplicar os métodos criptográficos aqui estudados, conceituando Criptografia e definido o que é um sistema criptográfico de chave simétrica e sistema criptográfico de chave assimétrica, ou seja, chave pública e, finalmente, aplicação de alguns métodos para o ensino médio, e mostrado alguns programas executáveis, para melhor compreensão dos métodos de Criptografia.

Esperamos que este trabalho tenha utilidade para estudo e aplicação de conteúdos no Ensino Médio, uma vez que o ensino no Brasil está precisando de propostas para que professores façam aulas com mais contextualização e interdisciplinaridade nos conteúdos ensinados, para trazer mais próximo a realidade do aluno.

Assim, tratando de alguns dos conteúdos da Educação Básica, mostramos que é possível trabalhar Criptografia nesse nível. Sendo aplicado de acordo com a realidade de cada turma, o professor pode escolher o método que melhor julgue que deva ser trabalhado.

REFERÊNCIAS

AABOE, A. **Episódios da História da Matemática Antiga.** Tradução Professor João Bosco Pitombeira. 3. ed. São Paulo: SBM, 2013.

BOLDRINI SUELE I. RODRIGUES COSTA, V. L. F. H. G. W. J. L. **Álgebra Linear**. 7. ed. São Paulo: Harbra, 1980.

BURNETTS S., P. S. **Criptografia**: O guia oficial do rsa. São Paulo: Campus, 2002.

COUTINHO, S. C. **Números inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2003.

DANTE, L. R. **Matemática**: Contexto e aplicações. São Paulo: Atual, 2010. vol. 2.

EVES, H. **Introdução à História da Matemática**. Tradução Higyno H. Domingues. São Paulo: Unicamp, 2004.

FERREIRA, J. **A construção dos Números**. Rio de Janeiro: SBM, 2010.

HALMOS, P. R. **Teoria ingênua dos conjuntos**. Rio de Janeiro: Ciência Moderna, 2001.

HEFEZ, A. **Elementos de Aritmética**. Rio de Janeiro: SBM, 2003.

_____. **Curso de Álgebra**. 5. ed. Rio de Janeiro: IMPA, 2013.

_____. **Aritmética**. Rio de Janeiro: SBM, 2014.

HEFEZ, A.; FERNANDEZ, C. de S. **Introdução à Álgebra Linear**. Rio de Janeiro: SBM, 2013.

IEZZI, S. H. G. **Fundamentos de Matemática Elementar**: sequências, matrizes, determinantes e sistemas. São Paulo: Atual, 2004. vol. 4.

LANDAU, E. **Teoria elementar dos Números**. Rio de Janeiro: Ciência Moderna, 2013.

LEMOS, M. **Criptografia, Números Primos e Algoritmos**. 5. ed. Rio de Janeiro: IMPA, 2001.

MIZRAHI, V. V. **Treinamento em Linguagem C**. 2. ed. São Paulo: Pearson, 2008.

MORGADO, A. C.; CARVALHO, J. B. P. de; CARVALHO, P. C. P.; FERNANDEZ, P. **Análise Combinatória e Probabilidade**. 9. ed. Rio de Janeiro: SBM, 2006.

NUMABOA. **História da Criptografia**. 2015. Disponível em: <http://www.numaboa.com.br/criptografia/historia>. Acesso em: ago. 2015.

SA, J. R. Carlos Correia de. **Treze Viagens pelo Mundo da Matemática**. 2. ed. Rio de Janeiro: SBM, U.PORTO editorial, 2012.

SHOKRANIAN MARCUS SOARES, H. C. S. **Teoria dos Números**. 3. ed. Brasília: UNB, 1999.

SHOKRANIAN, S. **Criptografia para iniciantes**. Brasília: UNB, 2005.

SOFFNER, R. **Algoritmos e programação em linguagem C**. São Paulo: Editora Saraiva, 2013.

ANEXOS

ANEXO: UM POUCO SOBRE MATRIZES

Falaremos nesse anexo sobre o cálculo do determinante de uma matriz quadrada através do *Teorema de Laplace* e a determinação da matriz inversa.

Cálculo de Determinante

Iremos mostrar uma regra prática para cálculo de determinantes de uma matriz quadrada A de ordem $n \times n$.

Os resultados aqui expostos podem também ser encontrados em: (HEFEZ; FERNANDEZ, 2013), (DANTE, 2010), (IEZZI, 2004)

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

Uma matriz A_{ij} é denominada submatriz da matriz $A_{n\times n}$ quando todos elementos de A_{ij} são obtidos através da escolha de um elemento a_{ij} de $A_{n\times n}$. A partir da escolha do elemento a_{ij} elemina-se os elementos da linha e da coluna que a_{ij} pertence, os elementos restantes formam a submatriz A_{ij}.

Exemplo .0.1. *Dada a matriz*

$$A = \begin{bmatrix} 2 & 5 & 9 & 13 \\ 11 & 0 & 4 & 1 \\ 3 & 31 & 77 & 6 \\ 15 & 8 & 21 & 2 \end{bmatrix}.$$

Vamos obter a submatriz A_{12} da matriz A. Para isso tomamos o elemento $a_{12} = 5$ e eliminamos da sua linha da sua coluna obtendo assim:

$$A_{12} = \begin{bmatrix} 11 & 4 & 1 \\ 3 & 77 & 6 \\ 15 & 21 & 2 \end{bmatrix}.$$

O número Δ_{ij} é o determinante afetado pelo sinal $(-1)^{i+j}$ da submatriz A_{ij}, obtida de A retirando-se a *i-ésima* linha e a *j-ésima coluna*, chamamos (Δ_{ij}) de cofator ou complemento algébrico do elemento a_{ij}.

$$\Delta_{ij} = (-1)^{i+j} det(A_{ij})$$

Por exemplo o cofator Δ_{12} da matriz A é:

$$\Delta_{12} = (-1)^{1+2} det(A_{12}) = -488$$

Teorema .0.1 (Teorema de Laplace)**.** *O determinante de uma matriz A, de ordem $n \geq 2$, é a soma dos produtos dos elementos de uma fila qualquer (linha ou coluna) pelos respectivos cofatores. Isto é,*

(a) Se escolhermos a coluna j da matriz A

$$A = \left[\begin{array}{ccc|c|cc} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{array}\right]$$

então:

$$det(A_{n\times n}) = a_{1j}\Delta_{1j} + a_{2j}\Delta_{2j} + \ldots + a_{nj}\Delta_{nj}$$
$$det(A_{n\times n}) = \sum_{j=1}^{n} a_{ij}\Delta_{ij}$$

(b) Se escolhermos a linha i da matriz A

$$A = \left[\begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ \hline a_{i1} & a_{i2} & \dots & a_{in} \\ \hline \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array}\right]$$

então:

$$det(A_{n\times n}) = a_{i1}\Delta_{i1} + a_{i2}\Delta_{i2} + \ldots + a_{in}\Delta_{in}$$
$$det(A_{n\times n}) = \sum_{i=0}^{n} a_{ij}\Delta_{ij}$$

Protanto, para calcularmos um determinante, não precisamos necessariamente dos elementos da $1^{\underline{a}}$ coluna (linha) e seus cofatores; qualquer outra coluna (linha) e seus cofatores permitem seu cálculo.

Observação: Para calcular o determinante através do Teorema .0.1, é aconselhável procurar a linha ou coluna que tiver mais elementos zeros (se houver elemento zero), pois ficará mais fácil o cálculo do determinante, diminuindo a quantidade de operações.

Exemplo .0.2. *Vamos calcular o determinante da matriz A através do Teorema .0.1.*

Solução:
Escolheremos a coluna 2 para calcular o determinante. Obtendo assim as seguintes submatrizes.

$$A_{12} = \begin{bmatrix} 11 & 4 & 1 \\ 3 & 77 & 6 \\ 15 & 21 & 2 \end{bmatrix}; A_{22} = \begin{bmatrix} 2 & 9 & 13 \\ 3 & 77 & 1 \\ 15 & 21 & 2 \end{bmatrix};$$

$$A_{32} = \begin{bmatrix} 2 & 9 & 13 \\ 11 & 4 & 1 \\ 15 & 21 & 2 \end{bmatrix}; A_{42} = \begin{bmatrix} 2 & 9 & 13 \\ 11 & 4 & 1 \\ 3 & 77 & 6 \end{bmatrix};$$

Temos

$$det(A) = 5.\Delta_{12} + 0.\Delta_{22} + 31.\Delta_{32} + 8.\Delta_{42}$$

$$det(A) = -2440 + 0 - 66154 + 81456$$

$$det(A) = 17542.$$

Matriz inversa

Vamos mostrar como calcular a inversa de uma matriz quadrada de ordem n.

Sabemos que a matriz $A_{n\times n}$ só será inversível se o determinante de $A_{n\times n}$ for diferente de zero.

Seja A uma matriz quadrada de ordem n. Dizemos que $A_{n\times n}$ é uma matriz inversível se existir uma matriz $X_{n\times n}$ tal que $(A.X)_{n\times n} = (X.A)_{n\times n} = I_{n\times n}$. Se $A_{n\times n}$ não é inversível, dizemos que A é uma matriz singular.

Se $A_{n\times n}$ é inversível, então é única a matriz $X_{n\times n}$ tal que $(A.X)_{n\times n} = (X.A)_{n\times n} = I_{n\times n}$.

Por exemplo a matriz $A_{2\times 2} = \begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix}$ possui inversa $X_{2\times 2} = \begin{bmatrix} 4 & -1 \\ -7 & 2 \end{bmatrix}$.

Observe que:

$$\begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix} . \begin{bmatrix} 4 & -1 \\ -7 & 2 \end{bmatrix} = \begin{bmatrix} 4 & -1 \\ -7 & 2 \end{bmatrix} . \begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Dada uma matriz inversível $A_{n\times n}$, chama-se inversa de A a matriz A^{-1} (que é única) tal que $A.A^{-1} = A^{-1}.A = I_n$.

Observe que para determinar a inversa de uma matriz inversível, seria suficiente apenas calcular seu determinante e montar um sistema linear para descobrir os elementos da inversa, porém se a matriz que desejamos obter a inversa for de ordem muito grande, o trabalho para resolver o sistema é imenso. Para isso iremos trabalhar um método que possibilita determinar a inversa sem precisar de multiplicar duas matrizes.

Dada uma matriz A, denominamos *matriz dos cofatores* (Δ) de A a matriz obtida com todos os cofatores da matriz A

$$\Delta = \begin{bmatrix} \delta_{11} & \delta_{12} & \dots & \delta_{1n} \\ \delta_{21} & \delta_{22} & \dots & \delta_{2n} \\ \vdots & \vdots & & \vdots \\ \delta_{n1} & \delta_{n2} & \dots & \delta_{nn} \end{bmatrix} \text{ é a matriz dos cofatores de } A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

Exemplo .0.3. *A matriz do cofatores de* $A = \begin{bmatrix} 2 & 5 & 9 & 13 \\ 11 & 0 & 4 & 1 \\ 3 & 31 & 77 & 6 \\ 15 & 8 & 21 & 2 \end{bmatrix}$. *É a matriz*

$$\Delta = \begin{bmatrix} -21 & 448 & -287 & 1379 \\ -469 & -13384 & 5285 & 1561 \\ -409 & -2134 & 1093 & 127 \\ 1598 & 10182 & -4056 & -1354 \end{bmatrix}.$$

Dada uma matriz quadrada, chamaremos de *matriz adjunta* ($\bar{A}'$) *de* A à transposta da matriz dos cofatores de A.

$$adj(A) = \bar{A}'.$$

No exemplo anterior temos

$$adj(A) = \begin{bmatrix} -21 & -469 & -409 & 1598 \\ 448 & -13384 & -2134 & 10182 \\ -287 & 5285 & 1093 & -4056 \\ 1379 & 1561 & 127 & -1354 \end{bmatrix}.$$

Enunciaremos um importante teorema cuja demonstração pode ser encontrada em (BOLDRINI SUELE I. RODRIGUES COSTA, 1980).

Teorema .0.2. $A.\bar{A}' = A.(adj(A)) = (det(A))I_n$

Para que uma matriz A possua inversa as seguintes condições precisam serem satisfeitas:

(i) Se A é uma matriz quadrada e existe uma matriz B tal que $A.B = I$, então A é inversível, ou seja A^{-1} existe e, além disso, $B = A^{-1}$
De fato, $B = B.I = B.(A.A^{-1}) = (B.A).A^{-1} = IA = A^{-1}$.

(ii) Se A é uma matriz quadrada, então A só será inversível se $det(A) \neq 0$.
De fato, suponha que $A_{n\times n}$ tenha inversa, isto é, existe A^{-1} tal que $A.A^{-1} = I_n$. Usando determinante temos

$$det(I_n) = det(A.A^{-1}) = det(A).det(A^{-1}) \text{ e } (I_n) = 1.$$

Então:
$det(A).det(A^{-1}) = 1$, logo o produto é diferente de zero. Assim, os dois números ($det(A)$ e $det(A_{-1})$) necessariamente devem ser diferente de zero, pois caso contrário o produto seria igual a zero. Daí se tem que $det(A) \neq 0$. E consequentemente $det(A^{-1}) = \dfrac{1}{det(A)}$.

Assim o $det(A) \neq 0$ é uma condição necessária para que A tenha uma inversa. Essa condição também é suficiente, já que de acordo com o Teorema .0.2 temos $A.\bar{A}' = (det(A)).I_n$. Observe que $A.\dfrac{1}{det(A)}.\bar{A}' = I$ e como a inversa é única, segue que $A^{-1} = \dfrac{1}{det(A)}.\bar{A}'$. Daí segue o seguinte Teorema:

Teorema .0.3. *Uma Matriz quadrada A admite uma inversa se, e somente se* $det(A) \neq 0$. *Neste caso:*

$$A^{-1} = \frac{1}{det(A)}.adj(A).$$

Assim pelo Teorema .0.3 a inversa da matriz $A = \begin{bmatrix} 2 & 5 & 9 & 13 \\ 11 & 0 & 4 & 1 \\ 3 & 31 & 77 & 6 \\ 15 & 8 & 21 & 2 \end{bmatrix}$. é a matriz

$$A^{-1} = \begin{bmatrix} -\frac{21}{17542} & -\frac{469}{17542} & -\frac{409}{17542} & \frac{1598}{17542} \\ \frac{448}{17542} & -\frac{13384}{17542} & -\frac{2134}{17542} & \frac{10182}{17542} \\ -\frac{287}{17542} & \frac{5285}{17542} & \frac{1093}{17542} & -\frac{4056}{17542} \\ \frac{1379}{17542} & \frac{1561}{17542} & \frac{127}{17542} & -\frac{1354}{17542} \end{bmatrix}.$$