VINICIUS ROBERTO GOMES DOMINGUES

CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação do Mestrado Profissional em Matemática em Rede Nacional, para obtenção do título de *Magister Scientiae.*

VIÇOSA
MINAS GERAIS - BRASIL
2017

Ficha catalográfica preparada pela Biblioteca Central da Universidade Federal de Viçosa - Câmpus Viçosa

T
D671c
2017

Domingues, Vinícius Roberto Gomes, 1988-
Criptografia no Ensino Médio / Vinícius Roberto Gomes Domingues. – Viçosa, MG, 2017.
viii, 98f. : il. ; 29 cm.

Inclui apêndices.
Orientador: Mercio Botelho Faria.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f83-84.

1. Aritmética. 2. Matrizes (Matemática). 3. Criptografia - Ensino médio. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-graduação em Matemática. II. Título.

CDD 22 ed. 513

VINÍCIUS ROBERTO GOMES DOMINGUES

CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação do Mestrado Profissional em Matemática em Rede Nacional, para obtenção do título de *Magister Scientiae*.

APROVADA: 09 de fevereiro de 2017.

Diogo da Silva Machado

Anderson Tiago da Silva

Mercio Botelho Faria
(Orientador)

Agradecimentos

A Nossa Senhora, pela proteção em mais essa caminhada. E por manter os eternos Gu e Fabão sob seu manto, lá em cima, olhando por nós.

Aos meus pais Eustáquio e Ana, por sempre colocarem os sonhos dos filhos a frente de qualquer coisa, e por fazerem sacrifícios para que eles se tornem realidade. Amo vocês!

Ao meu padrinho Luiz, madrinhas Marilia e Íris, Tio Antônio, Tia Nice e Fernanda por me incentivarem a continuar os estudos, e acreditarem em meu potencial até mais do que eu. Amo vocês!

Aos Alunos do Ensino Fundamental por me ensinarem a ter, e demonstrarem, muita paciência. Aos do Ensino Médio por me permitirem participar de sua preparação para uma nova etapa.

Aos alunos da UFV, pelas risadas, conversas e ensinamentos. Principalmente aos meus "Engenheiros"

Aos Tchucos: Judas, DaLua, Liw, Diego, Pablito, Champs e Cava que mesmo distantes continuam me fazendo rir e chorar. Aos Manos: Laís, Migué, Jonas e Calouro, pela amizade de sempre.

Aos remanescentes Raul, Flavin, Nened, Bidão e Tim, por me aguentarem mais tempo na Cidade Educadora.

Ao Denis e Capelão, pelas conversas, risadas, danones e até conselhos.

Aos professores do Colégio Agostiniano Mendel, pois mesmo após anos, continuam sendo importantíssimos em minha formação. Suas aulas sempre servirão de inspiração.

Minha família de São Paulo, incluindo Marcela, Thaís, Pino, Gordo, Pongo, Wagnão, Marcinho e Huguinho.

Aos meus amigos Gramenses, os Cobras, Primos(Ademir, Erasmo, Haline, os Ribeiros), Curé (melhor time do mundo), junto com Candy, Zoião e Leonel.

A todos da E.E. Mariano Gomes (em especial Lelé, Maria Zinato, Ana Cláudia, De Lurdes), da E.E. Padre Alváro (em especial Noca, Tia Vania, Diana e Soraia), Pró Efeito Genesis (Polyane e D. Graça) e equipe da Comunex (especialmente Gabi, Ricardo, Patrick, Márcia e Kekel). Melhores profissionais dos melhores estabelecimentos de Ensino.

Ao Brendon,por me mostrar que o melhor presente que um professor pode receber é presenciar o sucesso de um ex-aluno; e por me ensinar que com esforço e dedicação conseguimos ir mais longe.

Aos meus anjos: Carol, Ana Luísa e Luana, alunas que sempre confiaram em mim e se tornaram o meu trio preferido.

Paulinho, Tadeu e André, por serem os maiores acadêmicos com quem tive o prazer de conviver. E consequentemente, servirem de exemplo para minha vida acadêmica.

Ao Leandro e Hugo, amigos do PROFMAT com quem pude contar quando mais precisei nessa caminhada.

À Lucy, sempre será minha orintadora, "mãe", exemplo profissional.

Aos professores do DMA/UFV pelos ensinamentos acadêmicos e profissionais

Ao meu orientador pela paciência e orientação, sem as quais essa dissertação não sairia.

Lista de Figuras

2.1 Relação Algorítmo e Chave 8
2.2 Histogramas de Frequência 13
2.3 Possibilidades com a mudança de Cabos 18
2.4 Alan Turing 20

5.1 Atribuições no Método RSA 49

7.1 Correspondência entre Letras e Números 74
7.2 Quadro Simplificado Relação Letras/Números 77

8.1 Correspondência entre Letras e Números 93

Lista de Tabelas

4.1 Dias e Datas do Ano 33

Resumo

DOMINGUES, Vinícius Roberto Gomes, M.Sc., Universidade Federal de Viçosa, fevereiro de 2017. **Criptografia no Ensino Médio**. Orientador: Mercio Botelho Faria.

Este trabalho trata aos conceitos de Aritmética Modular e Matrizes que são utilizados na Criptografia. Foram abordados fatos históricos para mostrar a importância da Criptografia. Apresentamos conteúdos que podem ser facilmente trabalhados em aula do Ensino Médio. Demonstramos dois métodos distintos de se criptografar mensagens utilizando tais conceitos, com sugestões de como podem ser utilizados.

Abstract

DOMINGUES, Vinícius Roberto Gomes, M.Sc., Universidade Federal de Viçosa, February, 2017. **Cryotography in High School.** Advisor: Mercio Botelho Faria.

This work is related to concepts of modular arithmetic and matrices, which are used in cryptography. Historical facts have been approached to show the importance of cryptography. We present contents that can be easilly applied in high school classes. We demonstrate two distinct methods of how to encrypt messages using these concepts, with suggestions on how they can be used.

Sumário

1 Introdução **1**

2 Contexto Histórico **5**

2.1 Antiguidade 6

2.2 Decifrando as Mensagens 9

2.3 Mais Recentemente 15

3 Os Livros **23**

3.1 Critérios Eliminatórios Comuns a Todas as Áreas 24

3.2 Princípios e critérios de avaliação para a área de Matemática 25

3.3 Critérios eliminatórios específicos para Matemática 26

3.4 A escolha dos livros 27

3.4.1 Livro 1 28

3.4.2 Livro 2 29

3.4.3 Livro 3 31

4 A base Matemática do método RSA **33**

4.1 Aritmética Modular 34

4.2 Propriedades da congruência modular 35

4.3 Resíduos 36

4.4 Inversos Modulares 39

4.5 Algoritmo do Resto Chinês 40

4.6 Potências 42

5 O Método RSA **43**

5.1 Codificar 44

5.2 Decodificar 47

6 Um pouco de Matrizes e Determinantes **51**

6.1 Filas: Linha, Coluna 53

6.2 Algumas Matrizes Especiais 55

6.2.1 Matriz Transposta 56

6.3 Igualdade e Operações . . . 56
6.3.1 Adição de Matrizes . . . 56
6.3.2 Subtração de Matrizes . . . 57
6.3.3 Multiplicação de um Número Real por Matriz . . . 57
6.3.4 Multiplicação de Matrizes . . . 58
6.4 Determinantes . . . 61
6.4.1 Matriz de Ordem 1 . . . 61
6.4.2 Matriz de ordem 2 . . . 62
6.4.3 Matriz de ordem 3 . . . 62
6.4.4 Abaixamento da Ordem . . . 64
6.4.5 Casos Especiais . . . 65
6.5 A Matriz Inversa . . . 69

7 Cifra de Hill **73**
7.1 Como Funciona . . . 73
7.2 Criptoanálise . . . 77

8 Considerações Finais **81**

Capítulo 1

Introdução

O aluno, normalmente, não tem atenção para conteúdos que necessitem de abstração ou generalização, o que muitas vezes acaba com a motivação em estudar determinado conteúdo.

Para motivar o aluno, costuma-se dizer que todo aparato tecnológico foi construído a partir de fundamentos matemáticos, porém isso não é suficiente. O aluno busca algo novo e, muitas vezes, não percebe que é necessário conhecer o que existe para poder construir algo novo.

O CBC sugere, como solução desse problema, que se deva

"Estabelecer conexões entre temas matemáticos de diferentes campos, e entre esses temas e conhecimentos de outras áreas curriculares...Isso significa que o projeto pedagógico para a Matemática deve ser elaborado de forma articulada com as outras disciplinas e que, sempre que possível, seja ressaltada a relação entre os conceitos abstratos com as suas aplicações e interpretações em situações concretas."[SEE 2010]

Ao longo dos anos os livros didáticos vêm mudando a maneira de apresentar seu conteúdo. Os mais recentes costumam apresentar, junto com o conteúdo, alguns textos e curiosidades relacionados, mas muitos dos livros didáticos privilegiavam a conceituação em detrimento das aplicações, o que alguns autores consideram ser o grande problema dos livros didáticos brasileiros [Lima 2001].

Por perceber essa carência de aplicações em algumas coleções, buscamos abordar um assunto o qual além de estar presente no cotidiano ainda pudesse fazer uma relação com alguns conteúdos matemáticos do Ensino Médio, escolhendo assim a criptografia.

Diferente de outras aplicações que requerem um grande conteúdo matemático pode-se iniciar os estudos de criptografia com conceitos elementares como a contagem. Porém o

embasamento matemático não fica apenas em conteúdos básicos, partindo desta aplicação, o professor pode atingir os maiores problemas da atualidade, que são estudados nos departamentos de matemática pura.

Nesse trabalho serão apresentados alguns métodos de criptografia, porém o enfoque será nos métodos RSA e a Cifra de Hill, os quais conseguimos fazer elos com conteúdos trabalhados no Ensino Médio seguindo a orientação :

> Aprender Matemática de uma forma contextualizada, integrada e relacionada a outros conhecimentos traz em si o desenvolvimento de competências e habilidades que são essencialmente formadoras, à medida que instrumentalizam e estruturam o pensamento do aluno, capacitando-o para compreender e interpretar situações, para se apropriar de linguagens específicas, argumentar, analisar e avaliar, tirar conclusões próprias, tomar decisões, generalizar e para muitas outras ações necessárias à sua formação.[Brasil 2002]

O que queremos alcançar?

O objetivo geral desse trabalho é propor a implementação de uma sequência didática do tema criptografia, utilizando Teoria de Números e Matrizes.

Para tanto, foram planejados alguns objetivos mais específicos; tais como, investigar como os conteúdos necessários para o tema são abordados em algumas coleções; observar se essas coleções trazem aplicações, entre elas a criptografia; sugerir um sequencia didática, com conceitos e aplicações, que envolva Teoria dos Números, Matrizes e Criptografia.

Desenvolvimento

Após analisar o que o CBC e PCN sugeriam para o desenvolvimento de qualquer conteúdo matemático, foi feita uma pesquisa bibliográfica para verificar se algumas coleções utilizadas fazem uma abordagem prática desses conteúdos.

Foram escolhidas três coleções para serem analisadas, uma voltada apenas para o Ensino Médio, outra que é utilizada tanto no Ensino Médio quanto em cursos de graduação, e por fim uma para capacitação de professores que pode ser utilizada em cursos de graduação.

Após verificarmos que nenhuma delas seguia exatamente as sugestões do CBC ou PCN, desenvolvemos toda a parte teórica e uma parte prática com aplicações para os conteúdos.

Para a elaboração da parte teórica foram utilizadas essas coleções por serem amplamente adotadas entre os seguimentos que queremos atingir: professores e alunos do Ensino Médio e Graduação. Apesar de serem as principais fontes, também foram utilizados outros livros muito utilizados em cursos de Graduação, e algumas Dissertações que abordassem parte do conteúdo.

Estrutura

No próximo capítulo desse trabalho será feito uma abordagem histórica do uso da criptografia, desde seus primórdios, que se tem registros, até a era computacional. Essa contextualização histórica é outra sugestão do CBC para estimular o desenvolvimento de novas habilidades.

> As metodologias utilizadas devem priorizar um papel ativo do aluno, estimulando a leitura de textos matemáticos e os recursos didáticos de caráter lúdico como jogos, exposições, mural de problemas e curiosidades matemáticas" [SEE 2010]

O Capítulo três será dedicado ao entendimento rápido do Plano Nacional do Livro Didático (PNLD) [Brasil 2016], e de como são avaliados os livros para o Ensino Médio, e quais observações podemos fazer com base em três livros: um do Ensino Médio inscrito no PNLD, outro que transita no Ensino Médio e Superior, e outro que costuma ser utilizado apenas para nivel Superior e aperfeiçoamento de professores.

No capítulo quatro abordaremos todo o conteúdo matemático necessário para o entendimento do método RSA; definindo, exemplificando e apresentando propriedades dos números primos e da congruência. Serão apresentadas também outras aplicações dessa teoria, que estão presentes no cotidiano.

No capítulo cinco o Método RSA será minuciosamente detalhado de modo que possa ser utilizado por professores e alunos em sala de aula.

O sexto capítulo será destinado para o conteúdo de matrizes e determinantes destacando as definições propriedades e principais teoremas; tudo o que consideramos essencial para o entendimento da cifra de Hill.

O sétimo, analogamente ao quinto, terá uma explicação detalhada do Método de Hill; de modo que possa servir como uma cartilha para ser utilizada em sala.

Capítulo 2

Contexto Histórico

Durante a história, códigos decidiram o resultado de batalhas, provocando a morte de autoridades; os quais dependeram de comunicações eficientes para governar seus países ou comandar seus exércitos.

Foi a constante ameaça da interceptação dessas comunicações que motivou o desenvolvimento de códigos e cifras, que são técnicas para encobrir uma mensagem de modo que só o destinatário pudesse ler seu conteúdo.

A história da criptografia, possivelmente, nunca será definitiva, pois a batalha entre criadores e decifradores de códigos é contínua, desta forma, a teoria dos códigos deve estar em constante evolução. Esse é um dos pontos levantados em um dos livros que foram fonte de pesquisa para esse capítulo, [Singh 2008]

> E evolução é um termo bem adequado, porque o desenvolvimento de códigos pode ser visto como uma luta evolutiva, já que qualquer código está sempre sob o ataque dos decifradores. Quando se desenvolve uma nova arma, revelando a fraqueza de um código, este deixa de ser útil. Ou ele se torna extinto ou evolui e transforma num código novo e mais forte.

A batalha secular entre criptógrafos e decifrados, inspirou muitas descobertas científicas notáveis, uma vez que os codificadores têm buscado sempre criar códigos cada vez mais fortes, enquanto os decifradores devem inventar sempre métodos mais poderosos para ataca-los. Durante essa guerra ambos lados se apoiam numa variedade de disciplinas e tecnologias que acabaram enriquecendo essas áreas (matemática à linguística, teoria da informação à teoria quântica).

A criptografia sempre será importante, uma vez que a informação é uma mercadoria cada vez mais valiosa. Assim o processo de codificação de mensagens desempenha um

processo cada vez maior na vida diária.

Grande parte dessa história continua desconhecida, pois muitos registros ainda não foram trazidos à tona, e muitos dos heróis nunca receberam, em vida, o reconhecimento, por seu trabalho, afinal para que pudesse ter alguma vantagem sobre o inimigo suas contribuições não podiam ser publicadas enquanto ainda tinham valor diplomático ou militar.

2.1 Antiguidade

As guerras entre Grécia e Pérsia, contribuiram com dois dos primeiros incidentes nos quais a escrita secreta foi fundamental, em um tempo no qual não existia muita preocupação com o tempo que a mensagem demoraria para chegar ao destinatário.

Heródoto relatou o primeiro caso quando escreveu "As Histórias", nas quais consta que um espião raspou a cera de tabuletas de madeira e escreveu o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera, podendo assim ser transportada em segurança.

A história de Histaeu que queria encorajar uma traição contra o rei persa, pode ser considerada o segundo caso. Para transmitir suas instruções em segurança, ele raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo voltasse a crescer para passar sem que ninguém notasse.

Outros tipos de registro nos quais a mensagem era ocultada podem ser observados quando antigos chineses escreviam mensagens em seda fina, que era então amassada formando uma pequena bola e coberta com cera, a qual o mensageiro engolia; ou então no século XVI quando Giovani Porta descreveu como esconder uma mensagem dentro de um ovo cozido fazendo uma tinta com uma onça de alume e um quartilho de vinagre e então escrevendo na casca do ovo. Para ler a mensagem basta retirar a casca do ovo.

Apesar de criativos, esses métodos não são muito seguros, pois a interceptação da mensagem escondida compromete toda a sua segurança. O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder seu significado-um processo conhecido como encriptação.

A vantagem de se criptografar uma mensagem é que, caso o inimigo a intercepte, ela será ilegível, pelo menos em um primeiro momento, sem conhecer o algoritimo e chaves

utilizados para cifragem.

A criptografia pode ser dividida em dois ramos, não independentes: transposição e substituição.

Na transposição, as letras da mensagem são simplesmente reordenadas, gerando um anagrama[1]. Para mensagens muito curtas este método pode ser considerado inseguro, já que existe um número limitado de maneira de rearranjarem poucas letras.

Uma transposição ao acaso das letras oferece um nível de segurança altíssimo, porque não será possível que o interceptador consiga recompor até mesmo uma frase curta. Mas há uma desvantagem tão grande quanto o nível de segurança, pois se as letras forem misturadas ao acaso, sem fundamento, a decodificação do anagrama se tornará impossível até mesmo pro destinatário.

O primeiro aparelho criptográfico militar de que se tem registro, envolve uma forma de transposição, o Citale Espartano, datado do século cinco antes de cristo. O Citale consiste em um cilindro de madeira em volta do qual é enrolado uma tira. O remetente escreve a mensagem ao longo do comprimento do Citale e depois desenrola a tira, para decodificar a mensagem, o destinatário enrola a tira em outro cilindro de mesmo diâmetro usado pelo remetente.

Em uma das guerras entre Esparta e Pérsia, o Citale teve importante participação. Com o auxilio de tal artefato Lisandro de Esparta conseguiu alertar seus aliados e se preparar para repelir o ataque do persa Farnabazo.

A alternativa para tentar diminuir as fraquesas da transposição é a substituição.

A diferença entre transposição e substituição é que a transposição faz com que cada letra mantenha sua identidade, mas muda sua posição (o A continua significando A), enquanto a substituição faz com que as letras mudem de identidade, retendo a posição (dependendo do emparelhamento o A pode significar O).

Num texto escrito no século IV pelo brâmane Vatsyayana, o Kama-Sutra, aparece uma das primeiras descrições de código por substituição. O texto que recomenda que as mulheres devem estudar 64 artes. A arte listada no número 45 da lista é mlecchita-vikalpa, a arte da escrita secreta. Uma das técnicas recomendadas envolve o emparelhamento ao acaso das letras do alfabeto, substituindo-se cada letra por seu par.

Outro autor a mencionar técnicas de criptografia foi Seutonio, em “Guerras da Gália

[1]substantivo masculino; transposição de letras de palavra ou frase para formar outra palavra ou frase diferente

de Júlio César". Diferente dos mencionados anteriormente, ele trata da substituição. Cesar substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo. Outros escritos do mesmo autor indicam que Cesar, as vezes, substituía cada letra da mensagem por outra que estivesse três casas à frente. Esse processo ficou conhecido como Cifra de César.

Seutonio menciona apenas que César deslocava as letras em três casas, porém podemos observar que efetuando qualquer deslocamento entre um a 25 casas, é possível criar 25 códigos distintos. Esse número é considerado pequeno levando-se em conta a importância da mensagem codificada. Esse problema de segurança pode ser resolvido se não nos limitarmos a apenas mover as letras do alfabeto, permitindo que o alfabeto cifrado seja qualquer rearranjo do alfabeto original, então poderemos gerar um números ainda maior de cifras: 26! (a letra A pode ocupar qualquer uma das 26 posições do alfabeto, a letra B qualquer um dos 25 espaços restantes, e assim por diante), aproximadamente 400.000.000.000.000.000.000.000.000 de possibilidades.

Independente do método escolhido, é crucial um acordo entre destinatário e remetente para definição da Chave e Algoritmo que serão utilizados.

O relacionamento entre algoritmo[2] e chave é ilustrado na figura:

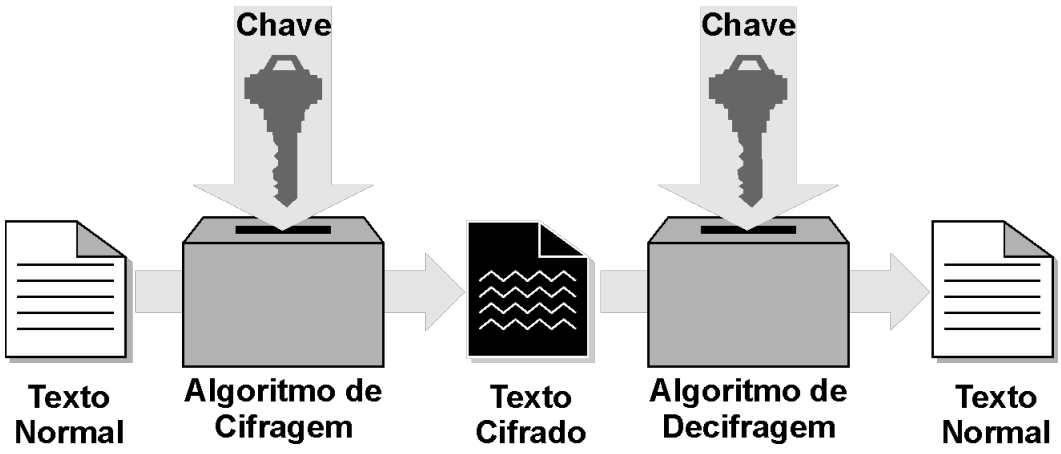


Figura 2.1: Relação Algorítmo e Chave

Cada conjunto formado por algoritmo (iguais ou diferentes) e chave diferentes é considerado uma cifra diferente. No caso citado o algoritmo consiste em substituir cada letra do alfabeto original por uma letra do alfabeto cifrado; enquanto a chave define o

[2]sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas.

alfabeto exato que será usado em uma codificação em particular.

De modo geral, ele até pode suspeitar qual seja o algoritmo, mas não conhece a chave exata. Essa expectativa é chamada de Principio de Kerckhoff , enunciada por Auguste Kerckhoff von Nieuwenhof em seu livro La Cryptographie Militaire.

"A segurança de um criptossitema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave"

Um sistema de código seguro necessita, além de manter a chave em segredo, possuir um amplo número de chaves em potencial, afim de confundir o inimigo ou trocá-la quando necessário.

Uma maneira de conseguir uma chave mais simples de memorizar do que um alfabeto inteiro é escolher uma palavra chave ou frase chave. Retira-se as letras repetidas e então use o resultado no início do alfabeto cifrado. O restante é meramente uma mudança que começa onde a frase termina, omitindo-se as letras que já existem na frase chave. Apesar da vantagem, o número de chaves potencial diminui.

Apesar de gregos e romanos utilizarem diferentes métodos séculos antes de Cristo, a civilização que mais contribuiu para a criptografia foi a árabe. Além de empregar cifras, os estudiosos árabes foram capazes de quebra-las. Eles inventaram a criptoanalise, a ciência que permite decifrar uma mensagem sem conhecer a chave.

Foram encontrados documentos que comprovam que no antigo mundo árabe, os segredos de Estado eram codificados, bem como registro dos impostos, demonstrando um uso amplo e rotineiro da criptografia. Manuais administrativos, que resistiram às ações do tempo e chegaram até os dias atuais, são outra forte evidência de que os árabes dominavam a criptografia; como exemplo pode ser citado o Adab al-kuttab (o manual dos secretários) do século X que inclui uma seção especifica sobre o assunto.

2.2 Decifrando as Mensagens

Várias disciplinas são necessárias para a criptoanálise, incluindo matemática, estatística e linguística. O Conhecimento dessas áreas foi capaz devido a prosperidade do mundo árabe, na qual a civilização atingiu um nível bem sofisticado de estudo.

Estudiosos árabes buscavam entender e catalogar de maneira cronológica as palavras

do Profeta. Para isso estudavam as palavras e também começaram analisar as letras individualmente e, em especial, descobriram que algumas letras são mais comuns que outras.

Não há um registro específico de quem foi o primeiro a perceber que as frequências podiam ser exploradas de modo a quebrar os códigos. A mais antiga descrição conhecida desta técnica nos vem de um cientista do século IX, Abu Yusef Yafiqub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi. Autor de 290 livros e diferentes áreas de conhecimento, teve o que é considerado seu maior tratado, "Um manuscrito sobre a decifração de mensagens criptigrafadas"redescoberto em 1987 em Istambul.

Esse tratado contém detalhes sobre estatística, fonética e sintaxe arábicas, mas seu sistema inovador de criptoanalise pode ser resumido em dois parágrafos.

- "Um meio de se decifrar uma mensagem codificada, quando conhecemos seu idioma, é encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma pagina. Então contamos a frequência que cada letra aparece. A letra que aparece com maior frequência chamamos de primeira, equanto a segunda mais frequente recebe o nome de segunda e assim por diante até contarmos todas as letras diferentes do texto. "

- "Em seguida examinamos o criptograma que desejamos decifrar e também classificamos seus símbolos. Descobrimos qual símbolo que aparece com maior frequência e o transformamos na primeira letra do texto que usamos como amostra, até convertermos todos os símbolos do criptograma que desejamos decifrar."

Em um texto muito curto, esse sistema mencionado não é muito útil, pois um texto curto tem maior probabilidade de se desviar significativamente das frequências padrão, por exemplo: se houver menos de cem letras, a decodificação será extremamente difícil.

Provavelmente no mesmo período que al-Kindi descrevia a invenção da criptoanalise, os europeus ainda lutavam com os elementos básicos da criptografia; sendo os monges os únicos que se destacavam na área. Eles estudavam a bíblia em busca de significados ocultos, ficando intrigados com o fato de que o Velho Testamento continha exemplos óbvios e deliberados de criptografia, como o atbash.

O assunto despertava tanto interesse que foi um monge, no século XIII, Roger Bacon, o autor do primeiro livro europeu a descrever o uso da criptografia. O livro "Epistle on the

secret Works of Art and the Nullity of Magic"inclui sete métodos para manter mensagens em segredos.

Foi graças ao período renascentista que a criptografia europeia se desenvolveu ao longo do século XV. O renascimento das artes, ciências e da educação produziam o conhecimento, enquanto as articulações políticas forneceram a motivação para a criptografia. Nesse período a Itália fornecia ambiente favorável para o desenvolvimento; ela era o coração da Renascença e tinha inúmeras cidades-estado independentes umas das outras. Para manter contato com seus embaixadores em outras cidades, os governantes precisavam criptografar suas mensagens, mantendo sigilo sobre seu conteúdo e possivelmente levando vantagem sobre os outros governantes.

O avanço da criptoanálise se fez necessário graças ao rápido, e imprensinvel, desenvolvimento da criptografia. Ninguém sabe ao certo se essas ideias surgiram independentemente na Europa ou foram trazidas do mundo árabe.

Giovanni Soro, o primeiro grande criptoanalista europeu não poderia ser de outro lugar a não ser da Itália, mais especificamente de Veneza, uma das mais importantes cidade-estado e o principal entreposto comercial da época. Nomeado secretário de cifras em 1506, sua reputação era tão grande que estados aliados enviavam para seu escritório as mensagens interceptadas para serem criptoanalisadas. Alguns historiadores afirmam que até mesmo o Vaticano, considerado o segundo maior centro de criptoanalise da Europa na época, enviava para Soro mensagens aparentemente indecifráveis que tinha caído em suas mãos.

Para não ficar para trás a França também começou a formar escritórios especializados em criptoanálise, empregando alguns dos mais habilidosos criptoanalistas, como o criptoanalista do rei Francisco I da França, Philibert Babou; e consolidando-se ao final do século XVI com a chegada de François Viète, que tinha um prazer especial em quebrar códigos espanhóis.

Com tantos escritórios e consequentes avanços na criptoanálise, era extremamente necessário que melhorias fossem feitas nas cifras. Uma das mais simples para a segurança da cifra de substituição monoalfabetica foram os nulos, símbolos e letras que não eram equivalentes às letras verdadeiras, ou seja, não representavam nada. Outra, foi que as vezes os criptógrafos, propositalmente, escreviam as palavras com grafia errada dificultando, mas não evitando, a analise de frequência.

Essas técnicas apenas atrasavam a análise, portanto uma nova tentativa de reforçar a cifra de substituição monoalfabética era necessária, a introdução de palavras-codigo. Apesar do nível muito mais alto de segurança, esse método também é uma substituição, na qual cada palavra pode ser representada por outra palavra ou símbolo. O alto nível de segurança gera outra grande dificuldade: criar uma grande quantidade de códigos; pois caso fosse possível seria necessário um expeço livro contendo todos os códigos, o qual seria muito difícil de distribuir ou substituir durante uma grande batalha; e caso esse livro caísse nas mãos inimigas toda a comunicação estaria comprometida.

Os Nomenclatores foram criados, para tentar diminuir essas dificuldades, tentando manter um nível elevado de segurança. Esse é um sistema que utiliza um alfabeto cifrado, o qual é usado para misturar grande parte da mensagem e uma lista limitada de palavras código. Porém como a maior parte da mensagem poderá ser decifrada usando-se a análise de frequência, as palavras em códigos restantes poderão ser deduzidas a partir do contexto, essa técnica não é muito mais segura que uma cifra simples.

Maria, da Escócia, não percebeu essas fragilidades dos Nomenclatores enquanto se correspondia com seus simpatizantes na tentativa de tomar o trono da Inglaterra ocupado pela rainha Elizabeth no século XVI.

Diante de tantos sistemas falhos, uma nova cifra precisava ser criada. Suas origens podem ser traçadas até Leon Battista Alberti, nativo de Florença, embora esta cifra só viesse a surgir, definitivamente, no final do século XVI. Destaque na Renascença, Alberti, nascido em 1404, foi reconhecido principalmente como arquiteto, tendo projetado a primeira Fonte de Trevi em Roma e escrito o primeiro livro impresso sobre arquitetura, "De re aedificadora".

O principal problema apresentado até então era a análise de frequencia, e para solucioná-lo Alberti propôs o uso de dois ou mais alfabetos, usados alternadamente. Sua principal vantagem é que a mesma letra do texto original não aparece necessariamente como uma única letra no texto cifrado.

Esse certamente foi o maior avanço no assunto num período de mil anos, porém Alberti não conseguiu desenvolve-lo, transformando-o num sistema completo de cifragem. Essa tarefa foi realizada por vários intelectuais que aperfeiçoaram a ideia original de maneira separada. Primeiro apareceu Johannes Trithemius, um abade alemão nascido em 1562, depois Giovanni Porta, um cientista italiano nascido em 1535, e finalmente o diplomata

francês, que recebeu maior reconhecimento, Blaise de Vigenère, nascido em 1523.

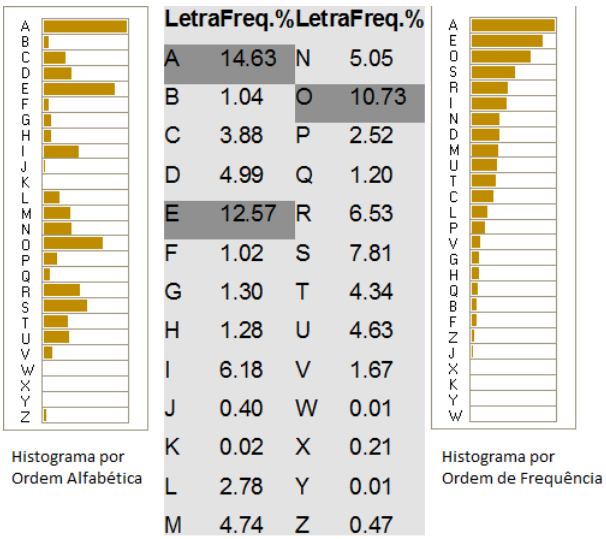
Conhecida como cifra de Vigenère em honra ao homem que a desenvolveu em sua forma final, a força dessa cifra consiste em que ela não usa apenas um, e sim 26 alfabetos cifrados distintos para cifrar a mensagem cifrada.

As formas de cifra de substituição que eram empregadas até então, eram chamadas de cifras de substituição monoalfabéticas, por usarem apenas um alfabeto cifrado por mensagem. A cifra de Vigenère pertence a uma classe conhecida como polialfabética, porque emprega vários alfabetos cifrados por mensagem.

A natureza polialfabética é responsável por sua força, mas também torna seu uso muito mais complicado; o que acabou desestimulando a maioria das pessoas a utilizá-la.

A substituição monoalfabética era rápida, fácil de ser usada e mantinha o segredo da mensagem contra pessoas que não conheciam a criptoanalise; o que a fez reinar por séculos, porém se mostrava inadequada para aplicações mais sérias, tais como comunicações militares e governamentais.

Em consequência disso, os criptógrafos buscaram uma cifra intermediária, mais segura do que a cifra monoalfabética direta, mas mais simples que a polialfabética. Entre várias candidatas surgiu a cifra de substituição homofônica (mesmo som). Nela cada letra é substituída por uma variedade de substitutivos, seu número potencial sendo proporcional a frequência



Letra	Freq.%	Letra	Freq.%
A	14.63	N	5.05
B	1.04	O	10.73
C	3.88	P	2.52
D	4.99	Q	1.20
E	12.57	R	6.53
F	1.02	S	7.81
G	1.30	T	4.34
H	1.28	U	4.63
I	6.18	V	1.67
J	0.40	W	0.01
K	0.02	X	0.21
L	2.78	Y	0.01
M	4.74	Z	0.47

Figura 2.2: Histogramas de Frequência

Por exemplo: Criamos 15 símbolos para representar a letra A, pois essa corresponde

a aproximadamente 15% de todas as letras que aparecem em um texto em português. O objetivo é equilibrar as frequências dos símbolos no texto cifrado.

Essa cifra porém pode ser quebrada, pois existem algumas peculiaridades das letras: como a letra Q (rara, ou seja, provavelmente um único símbolo) que só pode ser seguida pela letra U (4,63%) representada por no máximo 5 símbolos. Localizando duas letras as outras ficam mais fáceis.

Essa analise demonstra que a cifra homofônica nada mais é que uma cifra monoalfabética. Uma letra pode ser representada por vários símbolos, mas cada símbolo pode representar uma única letra. Já na cifra polialfabética uma letra será representada por símbolos diferentes, mas estes símbolos poderão representar letras diferentes durante a cifragem, o que torna tudo mais confuso.

Buscando reforçar uma determinada cifra ou criar outra intermediária, ao mesmo tempo decifrar mensagens e reunir informações cada potencia europeia tinha a sua Câmara Negra; cuja a mais famosa e eficiente era a dos Geheime Kabinets-Kanzlei em Viena.

No mesmo período que as Câmaras Negras foram implantadas, tivemos o desenvolvimento do telégrafo. Milhares de telegramas eram transportados diariamente, e alguns continham mensagens que não poderiam ser interceptadas; o que obrigou os criptógrafos a adotar a cifra de Vigenère, uma vez que os criptoanalistas praticamente excluíram o uso das cifras monoalfabeticas.

Essa cifra polialfabética apresenta duas grandes vantagens: possui um número enorme de chaves, e é imune a análise de frequencia. Para decifrar a mensagem, o destinatário precisa saber que linha do quadrado Vigenère foi usada para a cifragem de cada letra, o que seria muito dificil de descobrir se não existisse um sistema previamente combinado para a mudança entre linhas.

Mesmo com todas as dificuldades, a cifra de Vigenére não era intransponível. Claro que para ser quebrada era necessária um mente muito hábil, como a de Charles Babbage, o precursor dos computadores modernos. Ao invés de se utilizar de cáluculos mecânnicos ou computações complexas, ele percebeu que o cifragem era cíclica. Dependendo da palavra ou frase chave usada as repetições aparecem muitas vezes em um texto grande; isso dá uma ideia de frequência das letras semelhante a cifra monoalfabetica. Por exemplo se a palavra tiver 7 letras distintas serão usados apenas 7 alfabetos, então devemos analisar as letras em intervalos de sete em sete.

Existem registros que levam a crer que essa criptoanalise foi feita provavelmente em 1854, porém foi revelada apenas no século XX. Ninguém sabe ao certo o porquê dessa demora, existem algumas teorias sobre o motivo de ter ficado desconhecida tanto tempo: uma sugere que não foi revelada para que os inimigos não soubessem que tal cifra poderia ser quebrada, dando assim vantagem aos britânicos; outra refere a fama de displicente do autor, já que não costumava terminar ou divulgar seus projetos.

A maneira de resolver a cifra não recebeu o nome de Babbage,assim como a cifra não recebeu o nome de quem a idealizou. O homenageado foi o oficial da reserva do exercito prussiano Friedrich Wilhelm Kasiski que a publicou em 1863, de maneira independente aos avanços de Babbage; ela é conhecida como Teste de Kasiski.

Todo esse desenvolvimento da criptoanálise e de novas cifras ficou muito restrito ao Governo e Militares, afinal demandava tempo e dinheiro. Buscando novas alternativas para enviar mensagens sem precisar pagar caro nas mensagens telegrafadas, o interesse do público pela criptografia também cresceu significativamente, assim mensagens criptografadas eram enviadas através de colunas em jornais locais que eram enviados gratuitamente.

Com o crescente interesse do público pelas técnicas criptográficas, não demorou muito para que códigos e cifras aparecessem na literatura do século XIX, como no romance de Julio Verne “Viagem ao Centro da Terra”, ou em contos do Sherlock Holmes escritos por Sir Arthur Conan Doyle, ou no melhor exemplo de literatura de ficção sobre o assunto “O besouro dourado”de Edgar Allan Poe.

2.3 Mais Recentemente

O telegrafo motivou o uso da cifra de Vigènere, mas depois que Babbage e Kasiski destruíram sua segurança, criptógrafos precisavam desenvolver uma nova cifra. Tal necessidade foi potencializada no inicio do século XX quando o físico italiano Guglielmo Marconi inventou um aparelho que revolucionaria a telecomunicação e consequentemente a criptogrfia,o rádio.

Como não eram mais necessárias gigantescas linhas de transmissão, uma mensagem poderia chegar a qualquer lugar com o rádio. Contudo o que muita gente via como uma vantagem, também era sua principal fraqueza militar, já que as mensagens poderiam

alcançar seu destinatário e também o inimigo; afinal estavam "espalhadas"pelo ar.

Durante o inicio da Primeira Guerra Mundial, o rádio foi uma arma importantíssima. Antes do advento do rádio as mensagens interceptadas eram raras e preciosas, contudo na Grande Guerra a quantidade de mensagens era enorme demandando muito tempo dos criptoanalistas. Mesmo assim os alemães tentaram se precaver e desenvolveram a cifra ADFGVX, sendo uma mistura de substituição e transposição; o que deixavam seus criadores confiantes em sua segurança. Porém por se tratar apenas de uma variação ou combinações das cifras dos séculos anteriores, essa confiança era ilusória, afinal poderiam ser decifradas caso houvesse tempo para isso.

"nada deve ser mais estimado do que a informação, mais bem pago do que a informação e nada deve ser mais confidencial do que o trabalho de coleta de informações"(Sun-Tzu, A arte da Guerra)

O poder do rádio e a quebra da cifra foram cruciais para o desenrolar da Grande Guerra, mesmo com a falta de tempo para decifrar todas as mensagens, uma em especial mudou o rumo da história, o Telegrama Zimmerman. Esse telegrama revelava a proposta de uma futura aliança entre Alemanha e México, bem como a estratégia alemã de afundar navios americanos que levavam suprimentos para a Inglaterra, fazendo assim os Estados Unidos, até então neutros no conflito, entrarem no lado Aliado decidindo o curso na guerra.

Para manter a vantagem sobre os alemães, fazendo-os acreditar que sua comunicação continuava segura, a informação de que houve uma quebra na cifra não foi revelada por muito tempo. Assim o Eixo continuava revelando todos seus passos e segredos "espontaneamente".

Para corrigir os erros cometidos e substituir os sistemas de criptografia inadequados usados na Primeira Guerra, Arthur Scherbius utilizou uma ideia de um instrumento do século XV, considerado a primeira máquina criptográfica inventada por Leon Alberti, disco de cifras.

O Disco de Cifras é formado por dois discos de cobre, um maior que o outro, nos quais estavam gravados um alfabeto em cada um. Alberti sugeriu que se mudasse a disposição do disco durante uma mensagem, o que, na verdade gera uma cifra polialfabética. O disco de cifras acelera o trabalho e reduz os erros, comparado ao quadrado de Vigenère. Scherbius criou sua versão elétrica do disco, a mais poderosa máquina de cifragem da

história até então, a Máquina Enigma.

A máquina Enigma consiste de três elementos básicos conectados por fios: um teclado para a entrada de cada letra do texto original, uma unidade misturadora, e um mostrador com lâmpadas que indicam o texto cifrado.

A unidade misturadora, a principio, era formada por três discos. A ideia era de que cada disco misturador girasse automaticamente após cada letra ser digitada no teclado, como foi sugerido por Alberti. Com esta regulagem giratória o misturador define, essencialmente, 26 alfabetos cifrados e máquina é utilizada para implementar uma cifra polialfabética.

A característica mais importante do projeto é a rotação do disco. Após 26 giros do primeiro disco o segundo disco gira uma vez, proporcionando mais 26 giros no primeiro disco; e após as 26 rotações do segundo disco o terceiro disco faz uma rotação. Dessa maneira temos 26 x 26 x 26 combinações com apenas três discos.

Mesmo com uma quantidade considerável de chaves, dispondo de membros habilidosos, uma equipe consequiria analisar todas as chaves em um dia. Então Scherbius decidiu reforçar a segurança aumentando o numero de ajustes inicias; primeiro ele fez com que os misturadores pudessem ser removidos e trocados de lugar(6!); a segunda característica implementada foi a introdução de um painel de tomadas entre o teclado e o misturador, esse painel produz o efeito de trocar algumas das letras antes que elas entrem no misturador.

A Máquina Enigma revolucionou a criptografia assim como a cifra de Vigènere, e assim como essa também não recebeu os devidos méritos no inicio, neste caso o alto custo da máquina desencorajou os compradores em potencial, militares e homens de negócio.

O interesse foi despertado quando os britânicos revelaram a verdadeira história do telegrama Zimmermam. A partir de então houve uma explosão no número de pedidos e Scherbius começou a produção em massa, em 1925, chegando a 30 mil maquinas para os militares nas duas décadas seguintes.

Os militares precisavama de um nível extremamente elevado de segurança, então Scherbiu fez novos ajustes em sua máquina: adicionou mais dois rotores, totalizando 5 dos quais três eram usados (os exemplares da marinha alemã chegavam a ter até 8 rotores); adicionou cabos que ligavam duas letras, podem ser usados de 0 a 13 cabos, mas normalmente utilizavam 10 cabos. O resultado dessas mudanças pode ser observado na

figura 2.3:

Cabos (n)	Combinações possíveis
0	1
1	325
2	44.850
3	3.453.450
4	164.038.875
5	5.019.589.575
6	100.391.791.500
7	1.305.093.290.000
8	10.767.019.640.000
9	53.835.098.190.000
10	150.738.274.900.000
11	205.552.193.100.000
12	102.776.096.500.000
13	7.905.853.580.550
Total	532.985.208.200.000

Fonte: CRYPTO, 2012.

Figura 2.3: Possibilidades com a mudança de Cabos

Com tantas mudanças a quebra da cifra Enigma era um enorme desafio, principalmente nas décadas de 1920 a 1940, pois não existiam computadores que auxiliavam os cálculos. E foi justamente essa força que motivou o desenvolvimento de muitos dispositivos que serviram como base para a computação moderna.

> Se a necessidade é a mãe das invenções, então a adversidade é a mãe da criptoanálise [Singh 2008]

Mesmo sem conseguir grandes avanços durante muito tempo, a Polônia continuou monitorando as comunicações alemãs, chegando a criar uma agência de cifras em 1919 para concentrar os trabalhos; essa agência mais tarde incorporou outra e foi formado o Biuro Szyfrow, departamento de cifras e códigos dos serviços secretos da Polonia.

Todo esse esforço só teve resultado quando um alemão resolveu trair seu país. Ele era irmão do chefe de comunicações seguras do exercito e entregou cópia de dois documentos, “Manual de operação da máquina de cifragem Enigma”e “Instruções de uso das chaves da máquina Enigma”. Em 1932 os poloneses construíram sua primeira réplica da máquina Enigma baseados nssas informações, que permitiram deduzir o conjunto de conexões, bem como entender o esquema dos livros de códigos usados.

Em algumas momentos os poloneses conseguiram decifrar o código, em outros, os alemães aperfeiçoavam a máquina dificultando a criptoanálise e com isso teve início uma intensa batalha, até que um grupo de brilhantes matemáticos projetaram as bombas criptográficas. Essas bombas eram uma versão mecanizada de um sistema de catalogação que poderia procurar automaticamente os ajustes corretos dos misturadores.

Todo esse esforço, porém, era minado por eventos isolados que acabavam dificultando cada vez mais o trabalho dos cripanalistas:a adição de novos elementos a máquina Enigma; o custo de construir bombas para verificar em tempo hábil todas essas possibilidades; o rompimento de relações entre as agências de inteligência francesa e polonesa; e principalmente, a invasão da Polônia, obrigando a equipe de inteligência destruir qualquer documento que pudesse revelar no que trabalhavam.

Buscando ajuda nesse arduo trabalho e temendo a invasão alemã, o diretor da agência polonesa compartilhou os avanços de sua equipe e duas réplicas da Enigma com franceses e britânicos; sendo que os últimos conseguiram quebrar definitivamente a cifra da maquina Enigma.

Para conseguir quebrar a cifra, os britânicos criaram um local considerado, até hoje, uma referencia em criptoanálise, Escola de Cifras e Códigos do Governo localizada em Bletchley Park.

A rotina desse local era exaustiva: os avanços feitos em um dia eram descartados à meia noite, quando os operadores alemães mudavam as chaves da máquina Enigma para novas; assim a cada novo dia, o trabalho de identificação da chave era recomeçado.

Com o tempo, a equipe de Bletchley Park percebeu algumas fraquezas da máquina Enigma e no modo em que era operada. Essa percepção só foi possivel pois os opreadores eram passiveis de erros e hábitos que se tornaram rotineiros, favorecendo um pouco o trabalho dos decifradores que conseguiram perceber padrões nesses hábitos.

A equipe de criptoanalistas que se dedicavam a quebra da Enigma era extremamente talentosa, destacando-se entre esses o matemático Alan Turing[3], responsável por identificar a maior fraqueza da máquina Enigma. Ele percebeu que era possível prever parte do conteúdo de mensagens ainda não decifradas baseando-se em quando e onde elas eram enviadas, por exemplo: logo após as seis horas da manhã os alemães enviavam

[3]Tratando-se de contexto histórico um bom material que pode ser utilizado é o filme Jogo de Imitação que tem como enredo principal o trabalho de Turing e da equipe de Bletchley Park

Figura 2.4: Alan Turing

relatórios cifrados sobre a previsão do tempo, logo continham a palavra Wetter(tempo, em alemão).

Novamente um comportamento que os alemães julgavam ser destacável acabou sendo uma de suas maiores fraquezas em uma guerra. A disciplina alemã gerou uma situação que acabou auxiliando Turing, uma vez que a maior parte das mensagens eram muito parecidas em seu estilo, de modo que se podia até mesmo ter uma ideia da posição que estaria a palavra Wetter dentro de uma mensagem cifrada, como por exemplo: as seis primeiras letras de um certo texto cifrado correspondiam a Wetter.

Mesmo com todas essas "dicas"alemãs, diariamente era necessário testar aproximadamente $1,03.10^{23}$ chaves. Para simprlificar o problema, Turing tentou seguir a estratégia de Marian Rejewsi criando, assim, as bombas britânicas, cada uma consistia em doze conjuntos de rotores conectados eletricamente, capazes de lidar com elos mais longos.

Para procurar uma chave, era necessário um informação muito importante que antes, parecia ser impossivel de conseguir: os cribs, relação entre algumas letras codificadas e um texto sem codificar. Foram necessários dois protótipos diferentes de bombas e algum esforço para conseguir decifrar o que antes ninguém acreditava que seria capaz, a cifra da máquina Enigma.

Claro que todos esses avanços ficaram encobertos por muito tempo, até mesmo depois que a Segunda Guerra acabou. Como em outros casos já citados, isso foi feito para manter em segurança os envolvidos e, principalmente, tentar alguma vantagem sobre o inimigo que não sabia que suas mensagens podiam ser lidas. Mesmo sem termos certeza dos

métodos empregados e de toda a história, podemos afirmar que os avanços obtidos em Bletchley Park foram de enorme valor para a Ciência da Computação.

Em todos os casos citados até então, as chaves eram mantidas em segredo o tempo todo; porém em 1976, Bailey Whitfield e Martin Edward Hellman mudaram esse panorama ao publicarem um artigo denominado "New Directions in Cryptography", no volume 22 da revista IEEE Transactions on Information Theory. Neste artigo descreveram o primeiro método para trocar uma chave usando um canal público, abrindo as portas para a criptografia de Chave Pública, muito popular atualmente.

O mais conhecido dos métodos de criptografia de chave pública foi inventado em 1978, o RSA. As letras RSA correspondem as iniciais dos inventores do código: Rivest, Shamir e Adleman. Existem outros códigos de chave pública, mas o RSA é o mais utilizado em aplicações comerciais [Coutinho 2011].

Por ser um método bastante utilizado e que se baseia em uma das áreas mais clássicas da matemática, a Teoria do números, ele será melhor detalhado mais adiante nesse trabalho.

Atualmente, a criptografia é amplamente utilizada na internet e em segurança, a fim de autenticar os usuários para lhes fornecer acesso aos sites e possibilitar proteção de transações financeiras e em comunicação. Essa necessidade de manter uma informação sigilosa, em oposição a ânsia de descobri-las foi fundamental para o estudo mais profundo de algumas áreas da matemática, auxiliando assim seu desenvolvimento, bem como outras tecnologias.

Neste capítulo, listamos alguns episódios históticos nos quais a criptografia foi fundamental. Porém ,é evidente que essa história não se restringe apenas a esses eventos. Muitos outros conhecidos não foram citados, e deve existir uma vasta quantidade que permanece, e permanecerá, desconhecida com o intuito de tentar manter algum tipo de vantagem sobre quem envia mensagens criptografadas, ou até mesmo para não abalar relações diplomáticas. Uma coisa é certa: conhecidos ou não, criptógrafos e criptoanalistas foram decisivos em muitos momentos da história e continuarão sendo, seja interferindo em grandes eventos ou assessorando o desenvolvimento de tecnologias presentes no nosso cotidiano.

Capítulo 3

Os Livros

Este Capítulo é dedicado a analisar alguns livros quanto a seus conteúdo e aplicações apresentadas. Para tanto tomaremos como base as diretrizes do Plano Nacional do Livro Didático. Esse trata mais especificamente dos livros que serão empregados no Ensino Médio das escolas públicas; mas será utilizado por esse trabalho ter como foco os alunos dessa escolaridade e os professores que lecionam para tais.

Durante a pesquisa sobre como são feitas as avaliações dos livros didáticos, podemos entender que ao longo de quase duas décadas que é aplicado, o processo sofreu diversas mudanças no sentido de aperfeiçoar/melhorar tanto a qualidade dos livros didáticos recomendados pelo Programa Nacional do Livro Didático (PNLD), quanto à eficiência do próprio programa.

Constata-se que ao longo do período de 1996 a 2016 o MEC investiu na qualidade, por meio da avaliação de livros didáticos distribuídos às escolas da rede escolar pública. De uma edição do PNLD para outra, os critérios de avaliação sofreram modificações, mesmo que, em muitas vezes, essas não foram substanciais. Mas é evidente que com a implementação do sistema de avaliação dos livros didáticos, esses materiais aumentaram seu nível de qualidade tanto no aspecto gráfico-editorial quanto nas correções conceituais.

Os programas de material didático compostos pelo Programa Nacional Biblioteca da Escola (PNBE) e o Programa Nacional do Livro Didático (PNLD) , tem como objetivos oferecer , as escolas de educação básica da rede escolar pública , obras didáticas, pedagógicas e literárias, além de outros materiais de apoio ao trabalho docente , de forma sistemática, regular e gratuita.

O PNLD foi implementado na década de 1980, porém o primeiro Guia do Livro

Didático ocorreu em (1996), quando os Livros didáticos eram classificados em quatro categorias:

Excluídos: livros que apresentavam erros conceituais, indução a erros, desatualização, preconceitos ou discriminações de qualquer tipo;

Não recomendados: Livros nos quais a dimensão conceitual apresentava insuficiência, sendo encontradas impropriedades que comprometessem significativamente sua eficácia didático pedagógica;

Recomendados com ressalvas: livros que possuíam qualidades mínimas que justificassem sua recomendação, embora apresentassem problemas que, se levados em conta pelo professor, poderiam não comprometer sua eficácia;

Recomendados: livros que atendessem, satisfatoriamente, aos critérios de análise comuns e específicos utilizados pelo Programa.

No Guia de 1998 apenas as duas últimas categorias foram mantidas, acrescentando - se a categoria recomendados com distinção, sendo os livros não - recomendados relacionados no final do documento. Além dessa mudança, também se adotou uma convenção gráfica, em que os livros eram classificados por números de "estrelas", seguindo a seguinte classificação: - Recomendados com distinção - Recomendados - Recomendados com ressalvas Nas edições seguintes dos Guias do Livro Didático, 2001 e 2004, a categoria não recomendados foi extinta, mantendo - se as demais categorias

A partir do Guia de Livro Didático de 2004 é introduzida a avaliação da obra completa e não mais livros isolados, o que reflete no processo de seleção de livro didático por parte dos professores, uma vez que não poderão mais escolher livros isolados e sim, a coleção completa. Caso um volume da coleção não se enquadre nos crítérios de avaliação e seja excluído do processo, toda a coleção também será excluida.

Essa mudança não será considerada em nosso estudos, por tratarmos de um tema especifico e não de todo conteúdo proposto para o Ensino Médio .

3.1 Critérios Eliminatórios Comuns a Todas as Áreas

Para que todas as áreas sigam um padrão mínimo, alguns critérios são aplicados a todas, e tem carater eliminatório, antes mesmo de chegarem aos critérios específicos de cada área.

Os critérios eliminatórios comuns a serem observados na avaliação são os seguintes:

a) respeito à legislação, às diretrizes e às normas oficiais relativas ao ensino médio;

b) observância de princípios éticos e democráticos necessários à construção da cidadania e ao convívio social republicano;

c) coerência e adequação da abordagem teórico - metodológica assumida pela obra no que diz respeito à proposta didático - pedagógica explicitada e aos objetivos visados;

d) respeito à perspectiva interdisciplinar na abordagem dos conteúdos;

e) correção e atualização de conceitos, informações e procedimentos;

f) observância das características e finalidades específicas do manual do professor e adequação da obra à linha pedagógica nela apresentada;

g) adequação da estrutura editorial e do projeto gráfico aos objetivos didático - pedagógicos da obra.

Caso qualquer livro não obedeça a qualquer um desses critérios, será considerado incompatível com os objetivos estabelecidos para o ensino médio, levando a sua exclusão do PNLD do ano vigente.

3.2 Princípios e critérios de avaliação para a área de Matemática

Como cada área tem suas peculiaridades, todas não poderiam ser julgadas pelos mesmos critérios; então uma nova lista para cada área especifica foi elaborada.

Segue a lista dos critérios que, juntamente com os anteriores, devem ser observados durante a avaliação:

a) planejar ações e projetar soluções para problemas novos, que exijam iniciativa e criatividade;

b) compreender e transmitir ideias matemáticas, por escrito ou oralmente, desenvolvendo a capacidade de argumentação;

c) interpretar matematicamente situações do dia - a - dia ou do mundo tecnológico e científico e saber utilizar a Matemática para resolver situações - problema nesses contextos;

d) avaliar os resultados obtidos na solução de situações - problema;

e) fazer estimativas mentais de resultados ou cálculos aproximados;

f) saber usar os sistemas numéricos, incluindo a aplicação de técnicas básicas de cálculo, regularidade das operações etc.;

g) saber empregar os conceitos e procedimentos algébricos, incluindo o uso do conceito de função e de suas várias representações (gráficos, tabelas, fórmulas etc.) e a utilização das equações;

h) reconhecer regularidades e conhecer as propriedades das figuras geométricas planas e sólidas, relacionando - as com os objetos de uso comum e com as representações gráficas e algébricas dessas figuras, desenvolvendo progressivamente o pensamento geométrico;

i) compreender os conceitos fundamentais de grandezas e medidas e saber utilizá - los em situações - problema;

j) utilizar os conceitos e procedimentos estatísticos e probabilísticos, valendo - se, entre outros recursos, da combinatória;

k) estabelecer relações entre os conhecimentos nos campos da aritmética, álgebra, geometria, grandezas e medidas, combinatória, estatística e probabilidade, para resolver problemas, passando de um desses quadros para outro, a fim de enriquecer a interpretação do problema, encarando - o sob vários pontos de vista.

No processo de avaliação das obras de Matemática, serão consideradas as observações acima, os critérios eliminatórios comuns indicados na seção anterior e os critérios eliminatórios específicos abaixo discriminados.

3.3 Critérios eliminatórios específicos para Matemática

Para o componente curricular Matemática será observado se a obra:

a) inclui todos os campos da Matemática escolar, a saber, números, álgebra, geometria (incluindo trigonometria), estatística e probabilidade;

b) privilegia a exploração dos conceitos matemáticos e de sua utilidade para resolver problemas;

c) apresenta os conceitos com encadeamento lógico, evitando: recorrer a conceitos ainda não definidos para introduzir outro conceito, utilizar - se de definições circulares, confundir tese com hipótese em demonstrações matemáticas, entre outros;

d) propicia o desenvolvimento, pelo estudante , de competências cognitivas básicas, como: observação, compreensão, argumentação, organização, análise, síntese, comunicação de ideias matemáticas e memorização.

3.4 A escolha dos livros

Foram escolhidos três livros para fazer uma avaliação critrica.

Para tal escolha, buscamos um que seja adotado por uma Escola Pública do Ensino Médio, outro de uma coleção reconhecida nacionalmente, que costuma estar presente em referências bibliográficas; e um terceiro que é utilizado para cursos de graduação e para aperfeiçoamento de professores.

Para a análise dos conteúdos foram selecionados pontos mais importantes, de acordo com o objetivo do nosso trabalho e recomendações dos parâmetros governamentais. Os livros escolhidos são:

a) **Livro 1:** Matemática, Uma nova abordagem: Progressões: 2º ano. [Giovanni, Giovanni Jr, Bonjorno e Câmara]

   Faz parte de uma coleção de três livros e é adotado como pelo Colégio de Aplicação da Universidade Federal de Viçosa (CAP-COLUNI-UFV).

b) **Livro 2:** Fundamentos da Matemática Elementar: sequências, matrizes, determinante, sistemas.[Iezzi 2005]

   Faz parte de uma coleção com 11 volumes e é adotado como livro complementar pelo CAP-COLUNI-UFV, e pela disciplinas de Introdução a Algebra Linear da UFV.

c) **Livro 3:** Álgebra Linear [Boldrini, 1984]

Volume único adotado nas referencias bibliográficas dos cursos de Algebra Linear da UFV.

3.4.1 Livro 1

Introdução

Apresenta uma definição rapida e sucinta, e parte para exemplos númericos sem muita relação com exemplos utilizados no dia a dia.

Conteúdo

Falta uma aplicação prática das operações com matrizes. A maneira como é definida estas operações através da forma reduzida costuma ficar confuso para um aluno do Ensino Médio, pois não oferece uma visão da matriz, ficando muito abstrato. São colocados exemplos após cada propriedade, as quais não costumam ser demonstradas. Esses exemplos são muito importantes para que o aluno perceba o que poderá ou não fazer. Porém nenhum teorema ou propriedade é devidamente provado de forma literal, apenas são apresentados exemplos para utilização desses.

Contextualização

Singulariza o uso em "quase todos os ramos da ciência e da engenharia". O livro poderia ter reforçado que além disso é usada constantemente por todos em muitas outras atividades, mas que seu uso as vezes é feito de forma inconsciente e informal, por exemplo quando observamos a tabela de um campeonato de futebol. Ao final do capítulo existe uma seção chamada "Leitura e Compreensão", na qual é abordado um texto com algum conteúdo matemático. São apresentados alguns textos muito interessantes, porém as perguntas feitas ao final desse não costumam ter nenhuma abordagem matemática, apenas de interpretação.

Aplicações

Ao final de cada Capítulo o livro traz duas seções "Retomando e Pesquisando"e em alguns aparece a seção "Tecnologia". Na primeira um texto e uma pesquisa ou atividade

são propostos aos alunos, mas de maneira superficial, sem utilizar muitas propriedades estudas. Já na segunda, são exercícios que o aluno pode realizar com computadores ou calculadoras, porém não especifica em momento algum qual o processo empregado; apenas apresenta um roteiro do que deve ser feito.

Exercícios

Não apresenta muitos exercícios nos quais os alunos devem mostrar ou provar alguma propriedade. Dessa maneira é recomendado para os alunos de uma turma não tão avançada. Os exercícios se concentram apenas em aplicar os conteúdos vistos durante o capítulo, e existe uma seção no final do livro chamada "Aprofundamento"no qual são trabalhado exercícios com nível de dificuldade maior e de Vestibulares.

Considerações

O livro 1 é o que mais apresenta textos e atividades para os alunos, porém não servem de maneira enfática para uma boa contextualização e motivação dos alunos.

Para aplicar prontamente os conteúdos aprendidos e propriedades o livro apresenta bons exercícios e conteúdos, porém é insuficiente para os professores, visto que esses, sempre que possível, devem demonstrar as propriedades para melhor entendimento dos alunos.

3.4.2 Livro 2

Introdução

Inicialmente o livro restringe as matrizes à tabelas de números reais. Uma matriz não está restrita à números reais. Ela pode se estender além do conjunto de números complexos, a qualquer outro tipo de objetos matemáticos, como por exemplo funções, etc. Além de não colocar uma tabela para o melhor entendimento do aluno, a identificação de elementos, linhas e colunas é feita de forma muito direta, faltando esmiuçar mais.

Conteúdo

A grande maioria dos teoremas e propriedades são demonstrados ao longo dos capítulos. Alguns tem sua demonstração simplificada, ou apenas indicada; enquanto

outros estão na parte dos exercícios, ficando a critério dos alunos demonstrarem alguns.

Contextualização

Entre um capítulo e outro, existem alguns textos históricos, nos quais apresentam a vida de alguns matemáticos e algumas de suas contribuições, porém tudo de maneira resumida.

Creio que da maneira que são apresentados não motivam o aluno para estudarem esse conteúdo ou qualquer outro; e também não são ideais para serem utilizados por professores para introduzirem um conteúdo.

Aplicações

O livro não apresenta nenhuma aplicação prática dos conteúdos abordados, ficando a critério dos alunos e professores buscarem em outros livros.

Exercícios

Apresenta exercícios de todos os níveis, desde a fixação até os que necessitam de algum conteúdo visto anteriormente, ou demonstrações. Todos com qualidade muito boa. Em relação a quantidade, creio que sejam mais do que suficientes; além dos apresentados nos capítulos (número próximo a 100 em cada capítulo), ainda existem os exercícios de Vestibulares que são aproximadamente 300.

Considerações

O livro II por não ter muitos textos para contextualização ou exercícios com aplicações, sua utilização em uma sala de aula no Ensino Médio deveria ser acompanhada de material de apoio que contenha esses aspectos.

Este livro serve muito bem de complemento para o Ensino Superior e professores, principalmente por trazer e cobrar demonstrações completas de partes do conteúdo.

3.4.3 Livro 3

Introdução

O livro fala de maneira sucinta uma das importâncias das matrizes, sem explorar muito esses aspectos. Apresenta um exemplo numérico que pode ser encontrado em situações do dia a dia, e depois começa a generalizar, até a definição formal de matrizes.

Conteúdo

Grande parte dos Teoremas e propriedades são provados, apenas algumas que são deixadas como exercícios para os alunos.

Contextualização

Não existem textos ou apresentações de situações que instiguem os alunos a buscarem novos conhecimentos.

Aplicação

Ao final do capítulo são apresentados algumas aplicações ligadas a outras áreas do conhecimento, no caso as Biológicas.

Existe uma breve explicação, e depois adentra com exemplos numéricos e depois com as generalizações.

Exercícios

Apresenta exercícios de todos os níveis, desde a fixação até os que necessitam de algum conteúdo visto anteriormente, ou demonstrações. Todos com qualidade muito boa. Em relação a quantidade, creio que não sejam suficientes; ainda mais por se tratar de um livro presente em referencias de cursos superiores.

Considerações

O livro 3 por não ter muitos textos para contextualização ou exercícios com aplicações, sua utilização em uma sala de aula no Ensino Médio não é recomendada.

Este livro é excelente para o Ensino Superior e para aprimoramento de professores.

Percebemos que os livros, separadamente, apresentam algumas restrições para serem adotados em uma sala do Ensino Médio ou para Professores, porém caso os três sejam adotados para preparação das aulas e das atividades, acreditamos que teremos uma aula na qual os alunos terão todo o conteúdo proposto, fazendo exercícios de fixação e outros que os estimule a provarem alguns resultados, com textos para contextualização e aplicações do conteúdo, ou seja, uma aula completa.

Claro que não existem apenas esses citados, como citado anteriormente, tomamos esses como base pois um deles é do PNLD, outro pode ser utilizado no Ensino Médio e Superior, e o terceiro é referência nas disciplinas de nível superior que trabalham com Matrizes e Sistemas Lineares.

Outros que podemos citar que podem auxiliar na preparação dessas aulas são [Hefez e Fernandes 2012] e [Howard e Rorres 2001]; ressaltado que sempre devem ser utilizados juntos, ou para adaptar a linguagem para os alunos do Ensino Médio ou para utilização das aplicações.

Capítulo 4

A base Matemática do método RSA

Antes de apresentarmos definições e propriedades, introduziremos um exemplo usado em um vídeo do Programa de Iniciação Cientifica da OBMEP (PIC-OBMEP) e que utiliza conceitos básicos e intuitivos de divisão e resto.

Exemplo: O ano de 2013 começou em uma terça-feira. Em que dia da semana cairá o ultimo dia desse ano?

Solução: Como o ano de 2013 não é um ano bissexto ele possui 365 dias.

Sabemos que o dia 1º de janeiro é uma terça-feira assim como dia 8 e 15 de janeiro. Podemos contar e marcar os dias que serão terça-feira manualmente, porém seria um trabalho cansativo.

A tabela a seguir mostra como esse método poderia ser feito:

domingo	segunda-feira	terça-feira	quarta-feira	quinta-feira	sexta-feira	sábado
-	-	01/01	02/01	03/01	04/01	05/01
06/01	07/01	08/01	09/01	10/01	11/01	12/01
13/01	14/01	15/01	16/01	17/01	18/01	19/01
20/01	21/01	22/01	23/01	24/01	25/01	26/01
27/01	28/01	29/01	30/01	31/01	01/02	02/01

Tabela 4.1: Dias e Datas do Ano

Podemos perceber que o 1º, 8º, 15º, 22º,...64º...211º dias caem todos em uma terça-feira, ou seja, todos os dias que divididos por 7 tenham resto 1 caem na terça feira. Assim dividiremos 365 por 7:

$$365 = 7 \cdot 52 + 1$$

Como o resto dessa divisão é 1, então o ultimo dia do ano cairá também em uma terça-feira.

O exemplo acima é feito rapidamente em nosso dia a dia pela maioria das pessoas quando querem marcar um compromisso e saber em que dia da semana cai determinada data próxima; mesmo que desconhecidos pela maioria das pessoas são utilizados principios matemáticos, e a aritmética desse fenômeno cíclico é denomidada aritmética modular.

4.1 Aritmética Modular

Definição 4.1 *Seja n um inteiro não nulo. Dois inteiros a e b serão ditos congruentes módulo n se os restos da divisão de a e b por n forem iguais. Quando a e b são congruentes módulo m, escrevemos* $a \equiv b(mod\, n)$*, caso contrário, escrevemos* $a \not\equiv b(mod\, n)$.

Uma forma mais simples de verificar se dois números são congruentes é dada pela seguinte proposição:

Proposição 4.2 *Se a e b são números inteiros, então diremos que a é congruente a b módulo n se a-b é um múltiplo de n; ou seja; se n divide (a-b) (**Notação:** $m|(a-b)$).*

Demonstração: Se $a \equiv b(mod\, n)$, então existem inteiros r, q e q' tais que $a = nq + r$ e $b = nq' + r$, logo $a - b = n(q - q')$ e consequentemente $n|(a - b)$. Reciprocamente, suponha que $n|(a - b)$. Pela divisão euclidiana temos que $a = nq + r$ e $b = nq' + r'$ com $0 \leq r, r' < n$ logo $a - b = n(q - q') + r - r'$. Como $n|n(q - q')$, segue que $n|(r - r')$, logo $r = r'$ pois $|r - r'| < n$. Portanto $a \equiv b(modn)$

■

Exemplo: Os números 65 e 9 são congruentes módulo 7, $65 \equiv 9(mod\, 7)$, pois ambos os números deixam o mesmo resto quando divididos por 7.

Ou, utilizando a proposição anterior, temos que 65-9 é divisível por 7.

4.2 Propriedades da congruência modular

A congruência modular satisfaz algumas propriedades que a tornam muito semelhante à igualdade usual. As propriedades mais elementares da igualdade são as seguintes:

Reflexiva: todo número é igual a si próprio;

Simétrica: se $a = b$ então $b = a$;

Transitiva: se $a = b$ e $b = c$, então $a = c$.

Na verdade, costumamos usar estas propriedades da igualdade sem ter sequer consciência que as fazemos.

No caso da congruência modular não é assim tão óbvio que estas propriedades são satisfeitas, mas podemos verificá-las sem muito trabalho como faremos adiante. Antes porém, convém perguntarmos: para que fazer o esforço de provar que estas propriedades valem para a congruência modular? Será mera curiosidade?

A resposta, naturalmente, é que não se trata apenas de curiosidade: precisamos dessas propriedades para poder utilizar de forma correta a congruência modular nas contas que faremos nas próximas seções, incluindo-se a codificação de uma mensagem pelo RSA. É para isto que vamos provar que a congruência modular satisfaz propriedades análogas às enunciadas, mais precisamente:

Proposição 4.3 *Sejam a, b, c, d e n inteiros com* $n > 1$.

(i) Reflexiva: todo número é congruente módulo n a si próprio $(a \equiv a(mod n))$;

(ii) Simétrica: se $a \equiv b(mod n)$ *então* $b \equiv a(mod n)$;

(iii) Transitiva: se $a \equiv b(mod n)$ *e* $b \equiv c(mod n)$ *então* $a \equiv c(mod n)$;

Demonstração:

(i) Temos que $n|0$ ou $n|(a-a)$, então $a \equiv a(mod n)$.

(ii) Se $a \equiv b(mod n)$, então $a - b = kn$, k inteiro. Portanto, $b - a = -(kn) = (-k)n$, então $b \equiv a(mod n)$.

(iii) Se $a \equiv b(mod n)$ e $b \equiv c(mod n)$, então $n|(a-b)$ e $n|(b-c)$, logo $n|(a-b+b-c)$, donde $n|(a-c)$ e portanto $a \equiv c(mod n)$.

■

4.3 Resíduos

Antes de prosseguir, precisamos estudar em mais detalhes a relação entre a congruência módulo n e a divisibilidade de inteiros, já que é isto que torna a congruência tão útil.

Para começar, observe que a propriedade reflexiva da congruência módulo n é equivalente à afirmação de que zero é divisível por n. Por sua vez, a propriedade simétrica equivale a dizer que se um dado número é divisível por n então, ao multiplicá-lo por -1, obtemos outro múltiplo de n. Finalmente, a transitiva nos diz apenas que a soma de múltiplos de n também é um múltiplo de n. Em outras palavras, as três propriedades que provamos correspondem às propriedades dos múltiplos.

Mas podemos ir bem mais longe que isto. Digamos que a seja um inteiro positivo. Dividindo a por n temos:

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

com $0 \leq r < n$.

Assim

$$a - r = nq$$

que equivale a dizer que

$$a - r \equiv q(modn)$$

Verificamos com isto que todo inteiro *positivo* é congruente módulo n ao resto de sua divisão por n, que é um número entre 0 e n.

Em geral, se $a \equiv r(modn)$ e $0 \leq r < n$, dizemos que r é o *resíduo* de a módulo n. Note que usamos o artigo definido ao definir resíduo: *o resíduo* e não *um resíduo*. Isto porque cada número só pode ter um resíduo módulo n. De fato, se

$$a \equiv r(modn), 0 \leq r \leq n-1;$$

$$a \equiv r'(modn), 0 \leq r' \leq n-1;$$

então, pelas propriedades simétrica e transitiva, temos que $r \equiv r'(modn)$. Digamos que $r \geq r'$. Pela definição da congruência, isto significa que $r - r'$ é um múltiplo de n. Mas tanto r, quanto r' são menores que n, de modo que $0 \leq r - r' < n$. Isto significa que $r - r'$ só pode ser múltiplo de n se o co-fator correspondente for zero; o que nos dá

$r = r'$, mostrando que os dois resíduos, r e r' têm que ser iguais.

Aparentemente a única coisa que fizemos ao introduzir os resíduos foi inventar um nome novo para o resto, mas não é bem assim. Note que o termo resíduo se aplica a qualquer inteiro, positivo ou negativo, ao passo que o resto geralmente é usado quando dividimos um inteiro positivo por n. O que ocorre, então, se a for negativo?

Para tratar o caso geral, podemos seguir as etapas do exemplo acima. Primeiramente, como estamos supondo que a é negativo, então - a deve ser positivo. Dividindo-o por n,

$$-a = nq + r, 0 \leq r < n;$$

onde q e r são o quociente e o resto da divisão, respectivamente. Multiplicando esta equação por - 1, obtemos

$$a = n(-q) - r, 0 \leq r < n;$$

isto é

$$a \equiv -r(modn), 0 \leq r < n.$$

Se $r = 0$, então $a \equiv 0(modn)$ e já achamos o resíduo. Se $r \neq 0$, então $(n-r)-(-r) = n$ nos diz que $-r \equiv (n-r)(modn)$ de modo que a transitividade da congruência nos permite concluir que

$$a \equiv (n - r)(modn).$$

Ainda precisamos nos certificar que n - r é um resíduo, mas para isto, basta verificar que está entre 0 e n - 1. Como $r \geq 0$ e $r \neq 0$, temos que $r > 0$. Logo $n - r < n$. Entretanto, $r < n$, donde concluímos que $n - r > 0$.

Proposição 4.4 *Sejam a e $n > 1$ números inteiros e r o resto da divisão de $|a|$ por n, então o resíduo de a módulo n é igual a*

i) 0, se $r = 0$;

ii) r, se $r \neq 0$ e $a \geq 0$;

iii) $n - r$, se $r \neq 0$ e $a < 0$.

Proposição 4.5 *Se $p > 3$ é primo, então p só pode ter resíduos iguais a 1 ou a 5 módulo 6.*

Há uma outra maneira de dizer que a deixa resíduo r módulo n que, apesar de às vezes produzir alguma confusão, é usual e muito conveniente. Como $a \equiv r(modn)$significa que, para algum inteiro k,

$$a = k.n + r;$$

dizemos simplesmente que a é da forma $kn+r$. Usando esta terminologia, o enunciado da proposição passaria a ser todo primo $p > 3$ é da forma $6k + 1$ ou da forma $6k + 5$.

Proposição 4.6 *Se $a \equiv a'(modn)$ e $b \equiv b'(modn)$, então:*

(i) $a + b \equiv a' + b'(modn)$;

Exemplo: *A divisão de 9 por 6, gera resto 3. A divisão de 13 por 6, gera resto 1. Já a divisão de 22 = (9 + 13) por 6, gera resto 4 =(3 + 1).*

(ii) $ab \equiv a'b'(modn)$.

Exemplo: *A divisão de 9 por 6, gera resto 3. A divisão de 13 por 6, gera resto 1. Já a divisão de* $117 = (9 \times 13)$ *por 6, gera resto* $3 = (3 \times 1)$.

Exemplo: *Nesse caso é só escolhermos números iguais no exemplo anterior, pois multiplicação de números iguais podemos transformá-la em potencias.*

Demonstração:

(i) Se $a \equiv a'(modn)$ e $b \equiv b'(modn)$, segue que $n|(a-a')$ e $n|(b-b')$, logo $n|(a-a'+b-b')$ e portanto $a + b \equiv a' + b'(modn)$;

(ii) Se $a \equiv a'(modn)$ e $b \equiv b'(modn)$, segue que $n|(a - a')$ e $n|(b - b')$. Como

$$ab - a'b' = a(b - b') + b'(a - a')$$

temos $n|(ab - a'b')$ e consequentemente $ab \equiv a'b'(modn)$.

■

Classes Residuais: Dado n natural, qualquer inteiro a é equivalente, módulo n, a exatamente um dos inteiros $0, 1, 2, 3, ..., n - 1$. Este inteiro é um representante da Classe Resídual determinada por a, e é chamado resíduo de a módulo n e denotamos por

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{n-1}\}$$

Exemplo: $\overline{1} = \{k \in \mathbb{Z}/k \equiv 1(mod\, n)\}$

4.4 Inversos Modulares

Definição 4.7 *Dado um elemento a em $\mathbb{Z}_n$, dizemos que um elemento a' em $\mathbb{Z}_n$ é um recíproco, ou inverso multiplicativo de a módulo n se*

$$a'a = aa' \equiv 1(modn).$$

Neste caso, também dizemos que a' é o inverso de a módulo n, e vice-versa.

Exemplo: O inverso modular de 5 módulo 8 é o próprio 5; pois $5 \cdot 5 \equiv 1(mod 8)$

Observação: Esse resultado independe do representante dentro da classe.

Teorema 4.8 *Sejam $a < n$ inteiros positivos. O resíduo a tem inverso módulo n se, e somente se, a e n não têm fatores primos em comum.*

Outra maneira de se referir a esse Teorema é dado pela seguinte proposição:

Proposição 4.9 *Seja a um elemento não nulo de $\mathbb{Z}_n$. Então a é inversível se, e somente se, $mdc(a, n) = 1$*

Exemplo: Verifiquemos quais os inversos modulares utilizando $n = 7$.

Número	1	2	3	4	5	6
Inverso	1	4	5	2	3	6

Observamos que todos os números menosres do que 7 possuem inverso modular, isto deve-se ao fato de que 7 é um número primo; o que implica não ter nenhum fator em comum com os números que o antecedem.

Exemplo: Quais os inversos modulares utilizando $n = 10$?

Número	1	2	3	4	5	6	7	8	9
Inverso	1	-	7	-	-	-	3	-	9

Observamos que os números pares e o número 5 não possuem inverso modular quando $n = 10$, pois possuem fatores primos em comum com este.

Nos dois casos em que fizemos a tabela para mostrar os inversos de um número de acordo com determinado módulo, fizemos por tentativas, ou seja, multiplicamos o número

a por inteiros maiores ou iguais a a de modo a alcançar a congruencia desejada. Esse método é utilizada quando o valor de n é considerado baixo.

Teorema 4.10 *Suponha que a tem inverso módulo n. Se* $ab \equiv ac(modn)$*, para* $b, c \in \mathbb{Z}$*, então* $b \equiv c(modn)$*.*

Corolário 4.11 *Sejam* $a < n$ *inteiros positivos sem fatores primos comuns. Se* $ab \equiv ac(modn)$*; para* $a, b \in \mathbb{Z}$*, então* $b \equiv c(modn)$*.*

4.5 Algoritmo do Resto Chinês

Teorema 4.12 ***(Teorema Chinês do Resto)*** *Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema*

$$\begin{cases} x \equiv a(modm) \\ x \equiv b(modn) \end{cases}$$

sempre tem solução e qualquer uma de suas soluções pode ser escrita na forma

$$a + m(m' \cdot (b - a) + n.t)$$

onde t é um inteiro qualquer e m' *é o inverso de m módulo n.*

Demonstração:

Vamos supor que x_0 é a solução do sistema apresentado, logo utilizando a primeira equação do sistema temos

$$x_0 = m \cdot k + a, k \in \mathbb{Z}$$

Substituindo x_0 na segunda equação do sistema obtemos:

$$m \cdot k + a \equiv b(modn)$$

ou seja,

$$m.k \equiv b - a(modn) \tag{4.1}$$

Supondo que m e n sejam primos entre si, concluímos que m é inversível módulo n. Digamos que m' é o inverso de m módulo n. Multiplicando a equação 4.1 por m', obtemos

$$k \equiv m'(b-a)(modn)$$

Logo concluímos que

$$k = n \cdot t + m'(b-a), \text{ com } t \text{ inteiro.}$$

Se substituirmos o valor de k na equação 4.5 obteremos

$$x_0 = m \cdot (n \cdot t + m'(b-a)) + a, \text{ com } k \text{ inteiro}$$

■

Devemos ficar atentos para não confundir e achar que $m \cdot m' = 1, 1 \in \mathbb{Z}$, já que m e m' são inversos um do outro. De fato os números são inversos, mas são inversos modulares, ou seja, $\overline{m} \cdot \overline{m'} = \overline{1}, \overline{1} \in \mathbb{Z}_n$.

Assim a relação correta é $mm' \equiv 1(modn)$; que não simplifica a fórmula da solução geral.

Outro cuidado que devemos ter é que obtivemos uma fórmula para a solução de sistemas de duas congruências, porém isso tem a restrição de que os módulos são primos entre si. Isso foi utilizado para que conseguissemos isolar o valor de k na equação 4.1

Quando os módulos *não* são primos entre si, o sistema pode ou não ter solução, dependendo dos coeficientes constantes que aparecem nas congruências.

Considerando o sistema:

$$\begin{cases} x \equiv a(modm) \\ x \equiv b(modn) \end{cases}$$

Se o mdc entre m e n for d, e aplicarmos os mesmos procedimentos de substituição encontraremos que

1. se d divide $b-a$ então o sistema tem solução;

2. se d **não** divide $b-a$ então o sistema **não** tem solução.

4.6 Potências

Começaremos essa seção com o seguinte exemplo numérico.

Exemplo: Calcular o resto da divisão de 2^{123} por 31.

Calculando algumas potências de 2 módulo 31 obtemos os seguintes resultados:

$$2^1 \equiv 2(mod 31)$$

$$2^2 \equiv 4(mod 31)$$

$$2^3 \equiv 8(mod 31)$$

$$2^4 \equiv 16(mod 31)$$

$$2^5 \equiv 1(mod 31)$$

Ou seja, sempre que tivermos a potência 2^5 teremos resto 1 módulo 31. Assim vamos fatorar o expoente 123.

$$2^{123} = 2^{5 \cdot 24} \cdot 2^3 = (2^5)^{24} \cdot 2^3$$

$$2^{123} \equiv (2^5)^{24} \cdot 2^3 \equiv 1 \cdot 2^3 (mod 31)$$

Portanto o resto da divisão de 2^{123} por 31 é 8.

Podemos generalizar de acordo com a seguinte proporsição:

Proposição 4.13 *Se $a \equiv a'(mod n)$ e $b \equiv b'(mod n)$, então:*

$a^k \equiv [(b)]^k (mod n)$; *para qualquer $k \geq 0$.*

Demonstração: Por indução a proposição é verdadeira para $k = 1$, suponha verdadeira para um inteiro positivo k, temos $a^k \equiv [(b)]^k (mod n)$ e $a \equiv b(mod n)$.

Portanto, já vimo que é possível: $a^k.a \equiv [(b)]^k.b(mod n)$ ou $a^{k+1} \equiv [(b)]^{k+1}(mod n)$. Logo a proposição é verdadeira para o inteiro positivo $k + 1$. Portanto, a proposição é verdadeira para todo inteiro positivo k ■

Capítulo 5

O Método RSA

Esse método foi inspirado em um artigo publicado em 1976 por Whitfield Diffie e Martin Hellman, que sugeria que com o desenvolvimento das redes computacionais, algumas informações deveriam ser encriptadas antes de serem enviadas. Eles propuseram um método para a chave ser enviada de forma segura, com todas as informações necessárias disponibilizadas publicamente. Isso seria possível com uma função que fosse facil de ser calculada, mas dificil de ser invertida, mesmo que com o auxílio de computadores.

Após a publicação do artigo, três estudantes do Massachusetts Institute of Technology (MIT) passaram a tentar desenvolver um método de encriptação como o sugerido pelos autores do artigo. Para otimizarem seu tempo e verificarem a eficácia dos métodos que propunham, dois deles ficaram incubidos de criar ideias para esconder a mensagem, enquanto outro dedicava-se a descobrir a técnica.

Diversos métodos foram descartados até que foi apresentado um método que não conseguiu ser quebrado, e veio a ser chamado de RSA; em homenagem aos seus criadores: Ronald Rivest, Adi Shamir e Leonard Adleman.

Esse método tem sido analisado durante 40 anos, e apesar de descobertas algumas fraquezas, que são sempre corrigidas, permanece inviolado até hoje. Justamente por ser o primeiro exemplar de um criptossistema de chave pública e por resistir um tempo considerável, o RSA se tornou um dos algoritmos mais seguros de encriptação de informações.

Antes de iniciarmos a codificação da mensagem precisamos definir a Chave Pública e a Chave Privada. Para tanto devemos providenciar algumas coisas:

- uma relação entre letras e números;

Para o método RSA normalmente é utilizada a relação ilustrada na tabela abaixo, com o espaço entre palavras determinado pelo número 99.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

- dois números primos distintos, p e q; denominados parâmetros RSA;
- módulo RSA, $n = pq$;
- definir $\varphi(n)$ que determina a quantidade de co-primos, ou primos entre si , com n, e que são menores que ele.

$$\varphi(n) = (p-1)(q-1)$$

- escolher $e \in \mathbb{N}$ de modo que $mdc(\varphi(n), e) = 1$
- blocos cujos valores sejam menores que n. Esses blocos são oriundos da separação do número, encontrado a partir da conversão da mensagem em números.
- determinar d de modo que $d \in \mathbb{N}$ é o inverso de e módulo $\varphi(n)$.

Devemos ter alguns cuidados nesses procedimentos, como escolheremos $e \neq 1$ por motivos de segurança; sendo $e > 2$ e impar toda vez que p ou q não forem iguais a 2.

O valor de e não pode ser 2 ou outro número par sempre que p ou q não forem iguais a 2, pois $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ é par.

Outro cuidado a ser tomado é que não devemos começar um bloco com zero, pois isto traria problemas na hora de montar a seqüência recebida; mas a maneira de escolher os blocos não é única e não precisa ser homogênea.

5.1 Codificar

Chamaremos (n, e) de chave de codificação RSA.

Considerando b um bloco que foi separado anteriormente, ele será codificado separadamente, transformando-se em um bloco $C(b)$ da seguinte maneira:

$$C(b) \equiv b^e (mod\, n)$$

ou seja, é o resto da divisão de b^e por n.

A mensagem que será enviada para o destinatário é a sequencia dos blocos codificados.

Exemplo:

Seja $p = 11$, $q = 13$ e $e = 7$, então temos $n = 143$, $\varphi(143) = (11-1)(13-1) = 120$.

O Remetente deseja enviar a frase "VOVÓ, PAGUE OS CINQUENTA CENTAVOS", para tanto a transforma na seguinte sequencia:

312431249925101630149924289912182326301423291099121423291031242 8

Uma das configurações de separação de blocos que pode ser feita é:

31 24 31 24 99 25 10 16 30 14 99 24 28 99 121 82 32 6 30 14 23 29 10 99 121 42 32 9 10 31 24 28

Esses blocos poderão ser codificados da seguinte maneira

$$C(31) \equiv 31^7 (mod\, 143) \Longrightarrow C(31) \equiv 125 (mod\, 143)$$

$$C(24) \equiv 24^7 (mod\, 143) \Longrightarrow C(24) \equiv 106 (mod\, 143)$$

$$C(99) \equiv 99^7 (mod\, 143) \Longrightarrow C(99) \equiv 44 (mod\, 143)$$

$$C(25) \equiv 25^7 (mod\, 143) \Longrightarrow C(25) \equiv 64 (mod\, 143)$$

$$C(10) \equiv 10^7 (mod\, 143) \Longrightarrow C(10) \equiv 10 (mod\, 143)$$

$$C(16) \equiv 16^7 (mod\, 143) \Longrightarrow C(16) \equiv 3 (mod\, 143)$$

$$C(30) \equiv 30^7 (mod\, 143) \Longrightarrow C(30) \equiv 134 (mod\, 143)$$

$$C(14) \equiv 14^7 (mod\, 143) \Longrightarrow C(14) \equiv 53 (mod\, 143)$$

$$C(28) \equiv 28^7 (mod\, 143) \Longrightarrow C(28) \equiv 63 (mod\, 143)$$

$$C(121) \equiv 121^7 (mod\, 143) \Longrightarrow C(121) \equiv 121 (mod\, 143)$$

$$C(82) \equiv 82^7 (mod\, 143) \Longrightarrow C(82) \equiv 69 (mod\, 143)$$

$$C(32) \equiv 32^7 (mod\, 143) \Longrightarrow C(32) \equiv 98 (mod\, 143)$$

$$C(6) \equiv 6^7 (mod\, 143) \Longrightarrow C(6) \equiv 85 (mod\, 143)$$

$$C(23) \equiv 23^7 (mod\, 143) \Longrightarrow C(23) \equiv 23 (mod\, 143)$$

$$C(29) \equiv 29^7 (mod\, 143) \Longrightarrow C(29) \equiv 94 (mod\, 143)$$

$$C(42) \equiv 42^7 (mod\, 143) \Longrightarrow C(42) \equiv 81 (mod\, 143)$$

$$C(9) \equiv 9^7 (mod\, 143) \Longrightarrow C(9) \equiv 48 (mod\, 143)$$

Assim a sequencia enviada será:

125 106 125 106 44 64 10 3 134 53 44 106 63 44 121 69 98 85 134 53 23 94 10 44 121 81 98 48 10 125 106 63

No exemplo acima explicitamos os valores de p, q e $\varphi(n)$ de modo a ficar mais didático e para que o aluno aconpanhe melhor os resultados obtidos. Em um caso real seriam

fornecidos apenas n e e.

5.2 Decodificar

A chave de decodificação do sistema RSA é definida como (n, d).

Seja a um dos blocos codificados $C(b)$, então $D(a)$ é o resultado do processo de decodificação dado por:

$$D(a) \equiv a^d (mod n)$$

Sabendo a relação estabelecida entre as letras e números, o destinatário consegue ler a mensagem.

Exemplo:

Continuando o exemplo anterior, temos $d = 103$; pois $1 = 120 \cdot 1 + 7 \cdot (-17)$.

Decodificando os blocos recebidos teremos os seguintes resultados:

$$D(125) \equiv 125^{103} (mod 143) \Longrightarrow D(125) \equiv 31 (mod 143)$$

$$D(106) \equiv 106^{103} (mod 143) \Longrightarrow D(106) \equiv 24 (mod 143)$$

$$D(44) \equiv 44^{103} (mod 143) \Longrightarrow D(44) \equiv 99 (mod 143)$$

$$D(64) \equiv 64^{103} (mod 143) \Longrightarrow D(64) \equiv 25 (mod 143)$$

$$D(10) \equiv 10^{103} (mod 143) \Longrightarrow D(10) \equiv 10 (mod 143)$$

$$D(3) \equiv 3^{103} (mod 143) \Longrightarrow D(3) \equiv 16 (mod 143)$$

$$D(134) \equiv 134^{103} (mod 143) \Longrightarrow D(134) \equiv 30 (mod 143)$$

$$D(53) \equiv 53^{103}(mod143) \Longrightarrow D(53) \equiv 14(mod143)$$

$$D(63) \equiv 63^{103}(mod143) \Longrightarrow D(63) \equiv 28(mod143)$$

$$D(121) \equiv 121^{103}(mod143) \Longrightarrow D(121) \equiv 121(mod143)$$

$$D(69) \equiv 69^{103}(mod143) \Longrightarrow D(69) \equiv 82(mod143)$$

$$D(98) \equiv 98^{103}(mod143) \Longrightarrow D(98) \equiv 32(mod143)$$

$$D(85) \equiv 85^{103}(mod143) \Longrightarrow D(85) \equiv 6(mod143)$$

$$D(23) \equiv 23^{103}(mod143) \Longrightarrow D(23) \equiv 23(mod143)$$

$$D(94) \equiv 94^{103}(mod143) \Longrightarrow D(94) \equiv 29(mod143)$$

$$D(81) \equiv 81^{103}(mod143) \Longrightarrow D(81) \equiv 42(mod143)$$

$$D(48) \equiv 48^{103}(mod143) \Longrightarrow D(48) \equiv 9(mod143)$$

Dessa maneira o remetente terá a seguinte sequencia:

312431249925101630149924289912182326301423291099121423291031242 8

Ignorando o número 99, que significa espaço, e fazendo a correspondencia inversa dos números com suas respectivas letras o remetemte chega a seguinte frase

VOVO PAGUE OS CINQUENTA CENTAVOS

O quadro a seguir ilustra as atribuições do remetente e destinatário durante o processo de encriptação RSA.

	DESTINATÁRIO	REMETENTE
Criação das chaves	Escolhe os números primos *p* e *q*, calcula *n*, escolhe *e*; e divulga *(n,e)*	
Codificação		Separa a mensagem em blocos *b*, calcula *C(b)* e os envia para o destinatário
Decodificação	Calcula *d* e *D(a)*. Obtém a mensagem	

Figura 5.1: Atribuições no Método RSA

Os números primos escolhidos para compor n e o atribuido a e nos exemplos acima são considerados pequenos e mesmo assim percebemos que os cálculos não foram tão triviais apesar da ajuda de calculadoras científicas.

Então se escolhermos números primos cada vez maiores a segurança aumenta exponencialmente, afinal não é tão simples fatorarmos, mesmo com ajuda de computadoress, um número composto por números primos muito grandes. Essa é a base na qual a segurança do Sistema RSA se sustenta.

Capítulo 6

Um pouco de Matrizes e Determinantes

Mesmo que não percebamos, sempre nos deparamos com sistemas lineares, e as Matrizes acabam por nos auxiliar na resolução desses.

Registros indicam que os chineses representavam os sistemas lineares por meio de seus coeficientes escritos com barras de bambu; e os resolviam utilizando o método de eliminação, que consiste em anular coeficientes por meio de operações elementares, algo bem próximo do que chamamos de escalonamento atualmente.

Atribui-se ao japonês Seki Kowa (1637-1708) um dos primeiros aparecimentos de Matrizes em 1683. Contudo, são outros dois matemáticos quem utilizaram implicitamente a noção de matriz e a nomearam pela primeira vez, Joseph Louis Lagrange (1736-1813), em 1790; e Augustin-Louis Cauchy (1789-1857) que as chamou de tabelas, respectivamente.

Somente em 1850 essa configuração numérica recebeu o nome de Matriz com o matemático inglês James Joseph Sylvester (1814-1897). O nome foi dado de acordo com o significado original da palavra Matriz, local onde se gera ou cria algo, como o próprio Sylvester explicou em um artigo publicado na Philosophical Magazine: "(...) um bloco retangular de termos... o que não representa um determinante, mas é como se fosse uma matriz a partir da qual podemos formar vários sistemas de determinantes, ao fixar um número p e escolher à vontade p linhas e p colunas (...)"

Ainda em 1850 Arthur Cayley (1821-1895) passou a divulgar amplamente o nome, Matriz, inclusive através de sua obra Memoir on the Theory of Matrices (1858), na qual apresentava demonstrações de sua utilidade. Devido a esse fato Cayley é considerado por

muitos o pai das Matrizes.

Apesar de Cayley ser reconhecido dessa maneira, alguns resultados já eram conhecidos anteriormente, nos séculos XVIII e XIX passaram a investigar a Teoria das Formas Quadráticas.

Existem registros que apontam que o primeiro curso de Teoria das Matrizes foi voltado ao Teorema Espectral. No caso o curso era uma versão mais abstrata da Teoria de Matrizes, a Álgebra Linear.

Chama-se **matriz** de ordem $m \times n$, lê-se m por n, a tabela de $m \cdot n$ números reais dispostos em m linhas e n colunas. Representa-se por letras maíusculas (A ou $A_{m\times n}$, B ou $B_{m\times n}$, ...) e escreve-se a matriz utilizando os símbolos

$$\left(\quad\right) \text{ ou } \left[\quad\right]$$

Exemplos

$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 5 \end{pmatrix}$, $B_{3\times 2} = \begin{bmatrix} 1 & 2 \\ 0 & -1 \\ \pi & \sqrt{3} \end{bmatrix}$ etc.

Seja $A = \begin{pmatrix} h & k & p \\ x & y & z \end{pmatrix}$ uma matriz genérica de ordem 2×3.

O elemento **h**, situado na 1ª linha e na 1ª coluna pode ser representado pelo símbolo a_{11}. Lê-se **a um um**.

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

O elemento **k**, situado na 1ª linha e na 2ª coluna pode ser representado pelo símbolo a_{12}. Lê-se **a um dois**.

$$A = \begin{pmatrix} \cdots & a_{12} & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

O elemento **z**, situado na 2ª linha e na 3ª coluna pode ser representado pelo símbolo a_{23}. Lê-se **a dois três**.

$$A = \begin{pmatrix} \cdots & \cdots & \cdots \\ \cdots & \cdots & a_{23} \end{pmatrix}$$

De modo análogo **p** é o elemento a_{13}, **x** é o elemento a_{21} e **y** é o elemento a_{22}. Assim sendo, uma matriz A de ordem 2×3 pode ser assim representada:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

De modo geral. indicando por a_{ij} o elemento da linha i e da coluna j, pode-se representar a matriz A de ordem $m \times n$ como se segue:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Escrevemos simplesmente $A = (a_{ij})_{mxn}$ com $i \in \{1, 2, 3, ..., m\}$ e $j \in \{1, 2, 3, ..., n\}$.

Observação: Ao representar uma matriz como "tabela", estamos dando uma noção intuitiva de matriz. Formalmente, matriz é uma função que a cada par *(i,j)*, de números narurais, não nulos, associa o número real a_{ij}.

6.1 Filas: Linha, Coluna

a) **Linha** de uma matriz é uma n-upla de elementos com o mesmo primeiro índice.

Exemplo:a segunda linha de uma matriz $A = (a_{ij})_{2\times4}$ é:

$$A = \begin{pmatrix} \cdots & \cdots & \cdots & \cdots \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix}$$

b) **Coluna** de uma matriz é uma n-upla de elementos com o mesmo segundo índice.

Exemplo: a terceira coluna de uma matriz $A = (a_{ij})_{3\times 4}$ é

$$A = \begin{pmatrix} \cdots & \cdots & a_{13} & \cdots \\ \cdots & \cdots & a_{23} & \cdots \\ \cdots & \cdots & a_{33} & \cdots \end{pmatrix}$$

c) **Fila** de uma matriz significa linha ou coluna, indistintamente.

d) A matriz $A_{m\times n}$ é chamada *quadrada*, quando o número de linhas é igual ao número de colunas. Nos demais casos, é chamada retangular.

Simbolicamente, a matriz $A_{m\times n}$ pode ser:

- Quadrada $\Leftrightarrow m = n$
- Retangular $\Leftrightarrow m \neq n$

e) A matriz $A_{m\times n}$ é chamada matriz linha, quando tem uma única linha; e matriz coluna quando se tem uma única coluna.

Simbolicamente, a matriz $A_{m\times n}$ pode ser:

- Matriz Linha $\Leftrightarrow m = 1$
- Matriz Coluna $\Leftrightarrow n = 1$

Exemplos:

$A = \begin{pmatrix} 1 & 5 & 0 \\ 2 & -4 & 7 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 5 \\ 2 & -4 \end{pmatrix}$,

$C = \begin{pmatrix} 1 \\ 2 \\ -6 \end{pmatrix}$,

$D = \begin{pmatrix} 1 & 5 \end{pmatrix}$

Podemos dizer que:

- A é uma matriz retangular
- B é uma matriz quadrada

- C é uma matriz coluna e também retangular
- D é uma matriz linha e é também retangular

6.2 Algumas Matrizes Especiais

Matriz Nula

Matriz Nula é aquela que tem todos os elementos iguais a *zero*.

Representa-se por $0_{m\times n}$.

Exemplos:

$$0_{2\times 3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \; 0_{3\times 2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Matriz Identidade

A matriz quadrada $A(a_{ij})_{n\times n}$ definida por

$$\begin{cases} a_{ij} = 1 \Leftrightarrow i = j \\ a_{ij} = 0 \Leftrightarrow i \neq j \end{cases}$$

é chamada matriz identidade de ordem n, ou matriz unidade de ordem n, e é representada pelo símbolo I_n.

Assim sendo:

$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ é a matriz identidade de ordem 4

Matriz Oposta

A matriz oposta de $A = (a_{ij})_{m\times n}$ é a matriz $-A = (-a_{ij})_{m\times n}$.

Exemplo:

$$A = \begin{pmatrix} 1 & 0 & 10 \\ -4 & 1 & 5 \\ 1 & 7 & 1 \\ 0 & 3 & -2 \end{pmatrix} \Leftrightarrow -A = \begin{pmatrix} -1 & 0 & -10 \\ 4 & -1 & -5 \\ -1 & -7 & -1 \\ 0 & -3 & 2 \end{pmatrix}$$

6.2.1 Matriz Transposta

A matriz transposta da matriz $A = (a_{ij})_{m\times n}$ é a matriz $A^t = (a_{ji})_{n\times m}$, tal que

$$b_{ji} = a_{ij}; \forall i \in \{1, 2, 3, ..., m\}, \forall j \in \{1, 2, 3, ..., n\}$$

Exemplo

$$A = \begin{pmatrix} -1 & 0 & -10 \\ 4 & -1 & -5 \end{pmatrix} \Leftrightarrow A^t = \begin{pmatrix} -1 & 4 \\ 0 & -1 \\ -10 & -5 \end{pmatrix}$$

Propriedades da transposta:

Se A e B forem matrizes conformes para a operação indicada e k um número real, então:

- $A = B \Longleftrightarrow A^t = B^t$
- $(A + B)^t = A^t + B^t$
- $(AB)^t = B^t \cdot A^t$
- $(A^t)^t = A$
- $(kA)^t = kA^t$

6.3 Igualdade e Operações

Igualdade de Matrizes

Duas Matrizes de mesma ordem $A_{m\times n}$ e $B_{m\times n}$, são iguais se, e somente se, todos os elementos correspondentes são iguais.

Se $A = B$, então cada elemento a_{ij} de A é igual ao correspondente elemento b_{ij} de B

$$A = B \Longleftrightarrow a_{ij} = b_{ij},$$

com $i \in \{1, 2, 3, ..., m\}$ e $j \in \{1, 2, 3, ..., n\}$

6.3.1 Adição de Matrizes

Dadas duas matrizes de mesma ordem, $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$, define-se soma de A e B como sendo a matriz $C = (c_{ij})_{m\times n}$ tal que cada elemento de C é a soma dos elementos correspondentes de A e B.

$$C = A + B \Longleftrightarrow c_{ij} = a_{ij} + b_{ij}$$

com $i \in \{1, 2, 3, ..., m\}$ e $j \in \{1, 2, 3, ..., n\}$

Exemplo:

$$\begin{pmatrix} 1 & 0 & 10 \\ -4 & 1 & 5 \\ 1 & 7 & 1 \\ 0 & 3 & -2 \end{pmatrix} + \begin{pmatrix} 2 & 3 & 10 \\ -4 & 3 & 5 \\ 4 & 7 & 5 \\ 0 & 3 & -6 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 20 \\ -8 & 4 & 10 \\ 5 & 14 & 6 \\ 0 & 6 & -8 \end{pmatrix}$$

6.3.2 Subtração de Matrizes

Dadas duas matrizes de mesma ordem, $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$, define-se diferença de A e B como sendo a matriz $C = (c_{ij})_{m\times n}$ tal que cada elemento de C é a soma dos elementos correspondentes de A e $-B$. Em outras palavras:

$$C = A + (-B) = A - B \iff c_{ij} = a_{ij} - b_{ij}$$

6.3.3 Multiplicação de um Número Real por Matriz

Dada uma matriz $A = (a_{ij})_{m\times n}$ e o número real α, define-se o produto de α por A como sendo a matriz $B = (b_{ij})_{m\times n}$ tal que cada elemento b_{ij} de B é igual ao produto do número α pelo correspondente elemento da matriz A, ou seja,

$$B = \alpha.A \iff b_{ij} = \alpha.a_{ij}$$

com $i \in \{1, 2, 3, ..., m\}$ e $j \in \{1, 2, 3, ..., n\}$

Observação: Essa operação também é pode ser chamada de Multiplicação de Matriz por um escalar **Exemplo:** Sejam $A = \begin{pmatrix} 1 & 0 & 10 \\ -4 & 1 & 5 \\ 1 & 7 & 1 \\ 0 & 3 & -2 \end{pmatrix}$ e $\alpha = 3$. Temos:

$$3.\begin{pmatrix} 1 & 0 & 10 \\ -4 & 1 & 5 \\ 1 & 7 & 1 \\ 0 & 3 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 30 \\ -12 & 3 & 15 \\ 3 & 21 & 3 \\ 0 & 39 & -6 \end{pmatrix}$$

6.3.4 Multiplicação de Matrizes

A matriz produto $A \cdot B$ existe se, e somente se, o número de colunas da matriz A for igual ao número de linhas da matriz B. Seguindo essa regra para afirmarmos se existe o produto entre as matrizes A e B, é fácil perceber que a existencia de $A \cdot B$ não garante a existência de $B \cdot A$ Se existir,a matriz $A \cdot B$ tem o mesmo número de linhas da matriz A e o mesmo número de colunas da matriz B.

Exemplo: Se $A = (a_{ij})_{2\times 7}$ e $B = (b_{jk})_{7\times 5}$, então existe $A \cdot B$ pois o número de colunas de A (sete) é igual ao número de linhas de B (sete).

$$A_{2\times 7} \cdot B_{7\times 5} = C_{2\times 5}$$

Podemos observar também que não existe matriz $D = B \cdot A$, pois o número de colunas de B (cinco) é diferente do número de linhas de A (dois).

Exemplo: Se $A = (a_{ij})_{2\times 3}$ e $B = (b_{jk})_{3\times 2}$, então existe AB e BA. De fato

$$A_{2\times 3} \cdot B_{3\times 2} = C_{2\times 2}$$

$$B_{3\times 2} \cdot A_{2\times 3} = D_{3\times 3}$$

Esse último exemplo mostra que mesmo que exista AB e BA não é garantido que sejam iguais. Mostraremos outros exemplos disso mais a frente.

O produto da matriz $A = (a_{ik})_{m\times p}$ pela matriz $B = (b_{kj})_{p\times n}$ é a matriz $C = (c_{ij})_{m\times n}$ tal que cada elemento c_{ij} de C é igual à soma dos produtos dos elementos da i-ésima linha de A pelos correspondentes elementos da j-ésima coluna de B.

$$C = A \cdot B \Longleftrightarrow c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + a_{i3} \cdot b_{3j} + ... + a_{ip} \cdot b_{pj}$$

Exemplo: Dadas as matrizes $A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 1 \end{pmatrix}_{2\times 3}$ e $B = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}_{3\times 3}$, obteremos a matriz AB que será uma matriz 2×3.

Resolução:

- O elemento c_{11} da matriz produto AB é obtido utilizando a primeira linha de A e a primeira coluna de B e é igual a 7, pois:

$$\begin{pmatrix} 1 & 3 & 2 \\ \square & \square & \square \end{pmatrix} \cdot \begin{pmatrix} 2 & \square & \square \\ 1 & \square & \square \\ 1 & \square & \square \end{pmatrix} = \begin{pmatrix} 1.2 + 3.1 + 2.1 & \square & \square \\ \square & \square & \square \end{pmatrix} = \begin{pmatrix} 7 & \square & \square \\ \square & \square & \square \end{pmatrix}$$

- O elemento c_{12} da matriz produto AB é obtido utilizando a primeira linha de A e a segunda coluna de B e é igual a 3, pois:

$$\begin{pmatrix} 1 & 3 & 2 \\ \square & \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & 1 & \square \\ \square & 0 & \square \\ \square & 1 & \square \end{pmatrix} = \begin{pmatrix} 7 & 1.1 + 3.0 + 2.1 & \square \\ \square & \square & \square \end{pmatrix} = \begin{pmatrix} 7 & 3 & \square \\ \square & \square & \square \end{pmatrix}$$

- O elemento c_{13} da matriz produto AB é obtido utilizando a primeira linha de A e a terceira coluna de B e é igual a 9, pois:

$$\begin{pmatrix} 1 & 3 & 2 \\ \square & \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square & 3 \\ \square & \square & 2 \\ \square & \square & 0 \end{pmatrix} = \begin{pmatrix} 7 & 3 & 1.3 + 2.2 + 2.0 \\ \square & \square & \square \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ \square & \square & \square \end{pmatrix}$$

- O elemento c_{21} da matriz produto AB é obtido utilizando a segunda linha de A e a primeira coluna de B e é igual a 6, pois:

- O elemento c_{22} da matriz produto AB é obtido utilizando a segunda linha de A e a segunda coluna de B e é igual a 3, pois:

$$\begin{pmatrix} \square & \square & \square \\ 2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \square & 1 & \square \\ \square & 0 & \square \\ \square & 1 & \square \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ 6 & 2.1 + 1.0 + 1.1 & \square \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ 6 & 3 & \square \end{pmatrix}$$

- O elemento c_{23} da matriz produto AB é obtido utilizando a segunda linha de A e a terceira coluna de B e é igual a 8, pois:

$$\begin{pmatrix} \square & \square & \square \\ 2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \square & \square & 3 \\ \square & \square & 2 \\ \square & \square & 0 \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ 6 & 3 & 2.3 + 1.2 + 1.0 \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ 6 & 3 & 8 \end{pmatrix}$$

Assim sendo, $AB = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 1 \end{pmatrix}_{2\times 3} \cdot \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}_{3\times 3} = \begin{pmatrix} 7 & 3 & 9 \\ 6 & 3 & 8 \end{pmatrix}_{2\times 3} = C$

$$\begin{pmatrix} \square & \square & \square \\ 2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & \square & \square \\ 1 & \square & \square \\ 1 & \square & \square \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ 2.2 + 1.1 + 1.1 & \square & \square \end{pmatrix} = \begin{pmatrix} 7 & 3 & 9 \\ 6 & \square & \square \end{pmatrix}$$

PROPRIEDADES QUE NÃO VALEM

a) A multiplicação de matrizes **não** é comutativa, ou seja, AB e BA não são obrigatoriamente iguais. Existem, portanto, matrizes A e B tais que $AB \neq BA$.

Exemplo: Sejam $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ e $C = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, temos:

- $AB = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}$ e $BA = \begin{pmatrix} 4 & 1 \\ 2 & 1 \end{pmatrix}$, logo $AB \neq BA$
- $AC = \begin{pmatrix} 2 & 0 \\ 4 & 2 \end{pmatrix}$ e $CA = \begin{pmatrix} 2 & 0 \\ 4 & 2 \end{pmatrix}$, logo $AC = CA$

b) Na multiplicação de matrizes, não vale a "lei do anulamento do produto", ou seja, o produto de duas matrizes pode ser nulo, mesmo que ambas não sejam nulas. Existem, portanto, matrizes A e B tais que $A \neq 0$, $B \neq 0$ e $AB = 0$.

Exemplo: Sejam $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, temos:

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Longrightarrow AB = 0$$

c) Na multiplicação de matrizes, não vale a "lei do cancelamento", ou seja, na igualdade $AB = AC$, não se pode "cancelar" A e concluir que $B = C$. Existem, portanto, matrizes A, B e C tais que $AB = AC$ e $B \neq C$.

Exemplo: Sejam $A = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & 0 \\ -1 & 4 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -1 \\ 2 & 2 & 2 \end{pmatrix}$ e $C = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$, temos:

$$AB = AC = \begin{pmatrix} 3 & 4 & 1 \\ 2 & 3 & 2 \\ 3 & 2 & -7 \end{pmatrix} \text{ apesar de } B \neq C.$$

6.4 Determinantes

Submetendo os elementos de uma matriz quadrada a operações, mediante uma definição, obtem-se como resultado um número que é chamado determinante dessa matriz.

O determinante de uma matriz A

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

é indicado por

$$det \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

ou det A

ou simplesmente $\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{vmatrix}$.

O cálculo de determinante da matriz quadrada A de ordem n será feito da seguinte maneira:

- pela definição apenas para $n = 1$;
- utilizando regras práticas para $n = 2$ e $n = 3$;
- pelo abaixamento da ordem para $n > 1$.

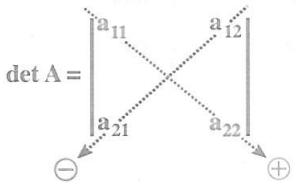
6.4.1 Matriz de Ordem 1

Se $A = a_{11}$, então, por definição,

$$detA = a_{11}$$

6.4.2 Matriz de ordem 2

Se $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, então detA será caldulado pelo seguinte dispositivo prático



$$detA = a_{11}.a_{22} - a_{12}.a_{21}$$

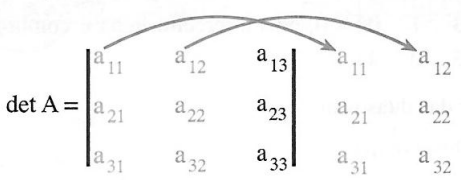
Exemplo:

$A = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \Longrightarrow detA = 2 \cdot 5 - 3 \cdot 1 = 7$

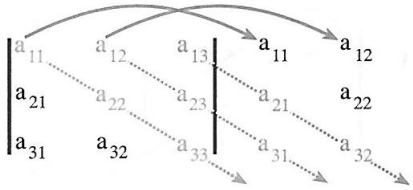
6.4.3 Matriz de ordem 3

Se $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, então detA será calculado por um dispositivo prático chamado Regra de Sarrus, que consiste em:

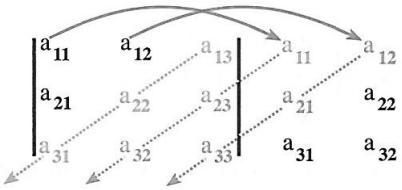
I) Repetir as duas primeiras colunas ao lado da terceira coluna



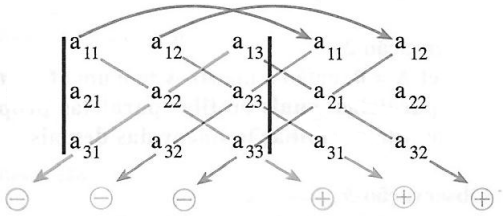
II) Obter os produtos $a_{11} \cdot a_{22} \cdot a_{33}$, $a_{12} \cdot a_{23} \cdot a_{31}$ e $a_{13} \cdot a_{21} \cdot a_{32}$



III) Obter os produtos $a_{13} \cdot a_{22} \cdot a_{31}$, $a_{11} \cdot a_{23} \cdot a_{32}$ e $a_{12} \cdot a_{21} \cdot a_{33}$



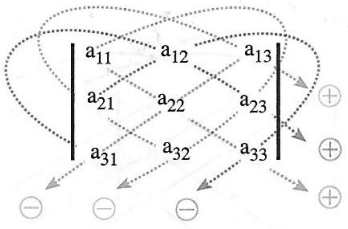
IV) Obter o $detA$ fazendo a diferença entre a soma das parcelas do item (II) e a soma das parcelas do item (III)



Em resumo, pela Regra de Sarrus, temos

$$detA = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - (a_{13} \cdot a_{22} \cdot a_{31} + a_{11} \cdot a_{23} \cdot a_{32} + a_{12} \cdot a_{21} \cdot a_{33})$$

Pode ser usada, ainda, sem repetir colunas. Observe o esquema e confirme o resultado.



Exemplo:

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 & 2 & 1 \\ 3 & 2 & 4 & 3 & 2 \\ 2 & 5 & -2 & 2 & 5 \end{vmatrix}$$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

6.4.4 Abaixamento da Ordem

Essa técnica permite calcular o determinante de uma matriz de ordem n utilizando o determinante de matrizes de ordem $n-1$.

Permite, pois, abaixar a ordem.

Para utlizarmos essa técnica precisamos definir duas coisas:

- Menor Complementar: O menor complementar D_{ij} do elemento a_{ij} da matriz quadrada M, é o determinante que se obtém de M eliminando-se a linha i e a coluna j.

- Cofator ou Complemento Algébrico: O cofator do elemento a_{ij} da matriz quadrada M é

  $$A_{ij} = (-1)^{i+j} \cdot D_{ij}$$

  em que D_{ij} é o menor complementar de a_{ij}.

  Definidos esses elementos podemos aplicar o Teorema de Laplace o qual garante que o determinante de qualquer matriz quadrada M de ordem n é igual à soma dos produtos dos elementos de uma fila pelos seus respectivos cofatores,

  então:

  $$detM = a_{1j} \cdot A_{1j} + a_{2j} \cdot A_{2j} + a_{3j} \cdot A_{3j} + ... + a_{nj} \cdot A_{nj}$$

  ou

  $$detM = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + a_{i3} \cdot A_{i3} + ... + a_{nj} \cdot A_{nj}$$

6.4.5 Casos Especiais

- Fila Nula: o determinante de uma matriz quadrada se anula quando a matriz possui uma fila nula.

  Exemplo: $A = \begin{pmatrix} 2 & 0 & 7 \\ 3 & 0 & 3 \\ 5 & 0 & 1 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 0 & 7 \\ 3 & 0 & 3 \\ 5 & 0 & 1 \end{vmatrix}$

  $$2 \cdot 0 \cdot 1 + 0 \cdot 3 \cdot 5 + 7 \cdot 3 \cdot 0 - 5 \cdot 0 \cdot 7 - 0 \cdot 3 \cdot 2 - 1 \cdot 3 \cdot 0 = 0$$

- Filas Paralelas Proporcionais: o determinante de uma matriz quadrada se anula quando a matriz possui duas filas paralelas proporcionais.

  Exemplo:

  $A = \begin{pmatrix} 5 & 2 & 3 \\ 15 & 6 & 9 \\ 1 & 2 & 5 \end{pmatrix}$ com a primeira e segunda linha proporcionais ($L_2 = 3L_1$)

  $$detA = \begin{vmatrix} 2 & 0 & 7 \\ 3 & 0 & 3 \\ 5 & 0 & 1 \end{vmatrix} = 5 \cdot 6 \cdot 2 + 2 \cdot 9 \cdot 1 + 3 \cdot 15 \cdot 5 - 1 \cdot 6 \cdot 3 - 5 \cdot 9 \cdot 5 - 2 \cdot 15 \cdot 2 = 0$$

- Fila Combinação Linear[1]: o determinante de uma matriz quadrada se anula quando a matriz possui uma fila que é combinação linear das demais filas paralelas.

  Exemplo: $\begin{pmatrix} 1 & 1 & 2 \\ 3 & 1 & 0 \\ 5 & 3 & 4 \end{pmatrix}$ com a terceira linha sendo combinação linear das duas primeiras ($L_3 = 2L_1 + L_2$).

  $$detA = \begin{vmatrix} 1 & 1 & 2 \\ 3 & 1 & 0 \\ 5 & 3 & 4 \end{vmatrix} = 1.1.4 + 1.0.5 + 2.3.3 - 5.1.2 - 3.0.1 - 4.3.1 = 0$$

Casos em que determinante se altera

[1]Combinação Linear é uma expressão construída a partir de um conjunto de termos, multiplicando cada termo por uma constante. Por exemplo, uma combinação linear de x e y seria qualquer expressão da forma ax + by, onde a e b são constantes

- Trocando Filas Paralelas: o determinante de uma matriz quadrada muda de sinal, quando duas filas paralelas trocam entre si de posição.

  Exemplo:

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 & 2 & 1 \\ 3 & 2 & 4 & 3 & 2 \\ 2 & 5 & -2 & 2 & 5 \end{vmatrix}$$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

Trocando a 1ª e 2ª colunas obtemos $B = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 3 & 4 \\ 5 & 2 & -2 \end{pmatrix} \Longrightarrow detB = \begin{vmatrix} 1 & 2 & -3 \\ 2 & 3 & 4 \\ 5 & 2 & -2 \end{vmatrix}$

$$= 1 \cdot 3 \cdot (-2) + 5 \cdot 4 \cdot 2 + (-3) \cdot 2 \cdot 2 - 3 \cdot 5 \cdot (-3) - 1 \cdot 4 \cdot 2 - (-2) \cdot 2 \cdot 2 = 67$$

- Multiplicando uma fila por α: o determinante de uma matriz quadrada fica multiplicado por α, quando os elmentos de uma fila são multiplicados por α.

  Exemplo:

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 & 2 & 1 \\ 3 & 2 & 4 & 3 & 2 \\ 2 & 5 & -2 & 2 & 5 \end{vmatrix}$$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

Multiplicando a 1ª linha por 2 temos: $B = \begin{pmatrix} 4 & 2 & -6 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detB = \begin{vmatrix} 4 & 2 & -6 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{vmatrix}$

$$= 4 \cdot 2 \cdot (-2) + 2 \cdot 4 \cdot 2 + (-6) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-6) - 5 \cdot 4 \cdot 4 - (-2) \cdot 3 \cdot 2 = -134$$

- Multiplicando a Matriz por α: o determinante de uma matriz quadrada de ordem n fica multiplicado por α^n, quando a matriz é multiplicada por α.

  Exemplo:

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 & 2 & 1 \\ 3 & 2 & 4 & 3 & 2 \\ 2 & 5 & -2 & 2 & 5 \end{vmatrix}$$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

Multiplicando a matriz por 2 temos: $B = \begin{pmatrix} 4 & 2 & -6 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detB = \begin{vmatrix} 4 & 2 & -6 \\ 6 & 4 & 8 \\ 4 & 10 & -4 \end{vmatrix}$

$$= 4 \cdot 4 \cdot (-4) + 2 \cdot 8 \cdot 4 + (-6) \cdot 6 \cdot 10 - 4 \cdot 4 \cdot (-6) - 10 \cdot 8 \cdot 4 - (-4) \cdot 6 \cdot 2 = -536$$

$$-536 = 8 \cdot (-67) = 2^3 \cdot (-67) = 2^3 \cdot detA$$

Casos em que determinante não se altera

- Trocando linhas por colunas: o determinante de uma matriz quadrada não se altera quando trocamos ordenadamente as linhas pelas colunas.

$$detA = detA^t$$

Exemplo:

$A = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 & 2 & 1 \\ 3 & 2 & 4 & 3 & 2 \\ 2 & 5 & -2 & 2 & 5 \end{vmatrix}$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

Temos $A^t = \begin{pmatrix} 2 & 3 & 2 \\ 1 & 2 & 5 \\ -3 & 4 & -2 \end{pmatrix} \Longrightarrow detA^t = \begin{vmatrix} 2 & 3 & 2 \\ 1 & 2 & 5 \\ -3 & 4 & -2 \end{vmatrix}$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

- Somando uma combinação linear: Se a uma fila de uma matriz quadrada M somarmos uma combinação linear das demais filas paralelas, obteremos uma nova matriz N com o mesmo determinante. (**Teorema de Jacobi**)

$$detN = detM$$

Exemplo:

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 2 & 5 & -2 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 & 2 & 1 \\ 3 & 2 & 4 & 3 & 2 \\ 2 & 5 & -2 & 2 & 5 \end{vmatrix}$$

$$= 2 \cdot 2 \cdot (-2) + 1 \cdot 4 \cdot 2 + (-3) \cdot 3 \cdot 5 - 2 \cdot 2 \cdot (-3) - 5 \cdot 4 \cdot 2 - (-2) \cdot 3 \cdot 1 = -67$$

Somando $2L_1 + L_2$ à L_3 temos $B = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 9 & 9 & -4 \end{pmatrix} \Longrightarrow detA = \begin{vmatrix} 2 & 1 & -3 \\ 3 & 2 & 4 \\ 9 & 9 & -4 \end{vmatrix}$

$$= 2 \cdot 2 \cdot (-4) + 1 \cdot 4 \cdot 9 + (-3) \cdot 3 \cdot 9 - 2 \cdot 9 \cdot (-3) - 9 \cdot 4 \cdot 2 - (-4) \cdot 3 \cdot 1 = -67$$

Propriedades Complementares

- Teorema de Binet: Se A e B forem matrizes quadradas de mesma ordem, então:

$$det(A \cdot B) = detA \cdot detB$$

- Determinante de Vandermonde: A matriz abaixo é chamada matriz de Vandermonde ou matriz das potências da linha $(a_1, a_2, a_3, ..., a_n)$.

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ (a_1)^2 & (a_2)^2 & \cdots & (a_n)^2 \\ \vdots & \vdots & \ddots & \vdots \\ (a_1)^{n-1} & (a_2)^{n-1} & \cdots & (a_n)^{n-1} \end{pmatrix}$$

O determinante dessa matriz é igual ao produto de todas as diferenças possiveis entre um elemento qualquer da sua linha $(a_1, a_2, a_3, ..., a_n)$ e todos os anteriores

$$detA = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ (a_1)^2 & (a_2)^2 & \cdots & (a_n)^2 \\ \vdots & \vdots & \ddots & \vdots \\ (a_1)^{n-1} & (a_2)^{n-1} & \cdots & (a_n)^{n-1} \end{vmatrix} = \Pi(a_i - a_k) \text{ para } 1 \leq k < i \leq n$$

Exemplo:

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = (b-a)(c-a)(c-b)$$

- Zero de um dos lados da diagonal principal: Se numa matriz quadrada forem nulos todos os elementos situados de um mesmo lado da diagonal principal, o seu determinante será igual ao produto dos elementos dessa diagonal.

Exemplo:

Seja $A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 5 \\ 0 & 0 & 7 \end{pmatrix}$ uma matriz triangular inferior.

Então $detA = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 3 & 5 \\ 0 & 0 & 7 \end{vmatrix} = 1{\cdot}3{\cdot}7+1{\cdot}5{\cdot}0+2{\cdot}0{\cdot}0-0{\cdot}3{\cdot}2-0{\cdot}5{\cdot}1-0{\cdot}1{\cdot}7 = 1{\cdot}3{\cdot}7 = 21$

6.5 A Matriz Inversa

A Matriz Inversa é um tipo de matriz que poderia estar inserida na seção Algumas Matrizes Especias 6.2, porém ela foi deixada em uma seção a parte pois podemos utilizar conceitos de determinantes.

Definição 6.1 *Dada uma matriz A, tal que $detA \neq 0$. A matriz B é dita inversa de A se*

$$A \cdot B = B \cdot A = I$$

Denotamos a matriz inversa de A por A^{-1}.

Ou seja, nem toda matriz A possui uma matriz inversa A^{-1}. Para que possua uma inversa a matriz deve obedecer algumas condições:

- A Matriz A deve ser quadrada
- A Matriz A deve ter determinante não nulo, ou seja, $detA \neq 0$

Definida uma matriz A que atenda as condições descritas, podemos determinar A^{-1} de modo que

$$A \cdot A^{-1} = I$$

Desse modo se aplicarmos o Teorema de Binet, temos que $detA^{-1} = \frac{1}{detA}$. De fato:

$$A \cdot A^{-1} = I$$

Aplicando *det* de ambos os lados da igualdade

$$det(A \cdot A^{-1}) = detI$$

Pelo Teorema de Binet temos:

$$detA \cdot detA^{-1} = detI$$

$$detA \cdot detA^{-1} = 1$$

Como $detA \neq 0$ então:

$$detA^{-1} = \frac{1}{detA}$$

Exemplo:

A Matriz $\begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \end{pmatrix}$ não tem inversa pois não é uma matriz quadrada.

E a matriz $\begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 5 & 18 & 1 \end{pmatrix}$ não tem inversa pois seu determinante é igual a zero.

Já a matriz $A = \begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 14 & 15 & 0 \end{pmatrix}$ possui inversa pois é uma matriz quadrada e tem $detA \neq 0$.

Para calcularmos a matriz inversa A^{-1} podemos supor uma matriz $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ e multiplicarmos por A de modo que o resultado seja a matriz identidade I.

$$A = \begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 14 & 15 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Essa multiplicação irá gerar um sistema linear de fácil resolução visto que a maior parte dos resultados é igual a zero, facilitando o isolamento de uma das letras e substituição nas outras equações.

Com a resolução desse sistema obteremos a seguinte matriz $A^{-1} = \begin{pmatrix} \frac{15}{429} & \frac{-30}{429} & \frac{21}{429} \\ \frac{-14}{429} & \frac{28}{429} & \frac{9}{429} \\ \frac{177}{429} & \frac{75}{429} & \frac{-267}{429} \end{pmatrix}$

Ressaltamos que esse não é a única maneira de obtermos a matriz inversa de uma determinada matriz. Existem métodos que utilizam conceitos não vistos nesse trabalho, outra que utiliza determinantes e outro que envolve escalonamento de sistemas lineares. Fica a critério dos professores pesquisarem os métodos que abordarão com seus alunos.

Capítulo 7

Cifra de Hill

A "cifra de Hill"é um cripto-sistema de substituição polialfabética, introduzido em 1929 por Lester S. Hill, baseado em transformações matriciais. Porém, a segurançaa oferecida por essa cifra não era grande e um método para quebrá-la foi rapidamente desenvolvido.

Apesar de não apresentar muita segurança ela pode ser bem trabalhada no Ensino Médio como uma aplicação prática da multiplicação de matrizes.

Vimos que as cifras de substituição tem a grande desvantagem de preservarem as frequencias de letras individuais. Porém na Cifra de Hill conseguimos contornar um pouco esse problema.

Uma maneira de superar este problemas é dividir o texto em grupos de letras e criptografar o texto comum por grupo, em vez de uma letra de cada vez. Por isso é chamado de Sistema Poligrafico: sistema de criptografia no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituido por um conjunto de n letras cifradas.

7.1 Como Funciona

Vejamos como podemos aplicar esse método da maneira mais geral.

- Inicialmente devemos estabelecer uma relação entre as letras do alfabeto, caracteres mais utilizados e os números, como no quadro a seguir

  Essa configuração apresentada no quadro não é a única possível, mas recomenda-se que seja seguida uma ordem lógica para facilitar a memorização por parte dos

	a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
o	p	q	r	s	t	u	v	w	x	y	z	à	á	â
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
ã	ç	é	ê	í	ó	ô	õ	ú	ü	A	B	C	D	E
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
U	V	W	X	Y	Z	À	Á	Â	Ã	Ç	É	Ê	Í	Ó
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
Ô	Õ	Ú	Ü	0	1	2	3	4	5	6	7	8	9	:
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
;	<	=	>	?	@	!	"	#	$	%	&	'	(	)
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
*	+	,	-	.	/	[	\	]	_	{	|	}		
105	106	107	108	109	110	111	112	113	114	115	116	117		

Figura 7.1: Correspondência entre Letras e Números

interlocutores. Por exemplo, podemos estabelecer que a letra corresponde ao número 7, a letra B ao número 8 e assim por diante.

O quadro mostra a diferenciação entre letras maiúsculas e minúsculas, ela não é obrigatória; mas essa técnica aumenta o poder da cifra, dificultando mais a análise de frequencia.

- Após estabelecermos a relação, devemos escrever a frase escolhida como o conjunto de números correspondentes

- Devemos escolher uma matriz quadrada A de ordem n de modo que essa matriz A tenha uma inversa A^{-1}, ou seja, $detA \neq 0$. Podemos também escolher uma palavra chave, que será transformada em uma matriz com as mesmas caracteristicas descritas acima.

- Escolhida a matriz, dividimos a frase em blocos de tamanho n. Caso o total de letras não seja divisível por n devemos completar a frase com alguma letra ou símbolo préviamente escolhido.

- Multipliquemos cada bloco de tamanho n pela matriz A, transformando-os em novos números.

  São esses novos números que deverão ser enviados ao destinatário.

- Ao receber a mensagem codificada, o destinatário deverá dividir esses novos números em blocos de tamanho n

- Para interpretá-los o destinatário deverá utilizar a matriz A^{-1}; multiplicando cada bloco pela matriz A^{-1}; obtendo os números originais.

Exemplo:

Utilizaremos um quadro de relações menos sofisticado que o mostrado anteriormente.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	X	W	Y	Z	É	.	,	-
16	17	18	19	20	21	22	23	24	25	26	27	28	29	0

A frase escolhida para ser criptografada é "O São Paulo é o maior clube do Brasil", e a palavra de referância é SOBERANO, que pode ser transformada na seguinte matriz:

$$A = \begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 14 & 15 & 0 \end{pmatrix}$$

A frase pode ser transformada no seguinte conjunto de números:

15 0 19 1 15 0 16 1 21 12 15 0 27 0 15 0 13 1 9 15 18 0 3 12 21 2 5 0 4 15 0 2 18 1 19 9 12

Como a matriz escolhida é uma matriz de ordem 3, dividiremos a frase em blocos de tamanho três:

Bloco 1: 15 0 19
Bloco 2: 1 15 0
Bloco 3: 16 1 21
Bloco 4: 12 15 0
Bloco 5: 27 0 15
Bloco 6: 0 13 1
Bloco 7: 9 15 18
Bloco 8: 0 3 12
Bloco 9: 21 2 5
Bloco 10: 0 4 15
Bloco 11: 0 2 18
Bloco 12: 1 19 9
Bloco 13: 12 0 0

Transformaremos cada bloco em uma matriz coluna e multiplicaremos pela matriz A, temos:

$$A.B_1 = \begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 14 & 15 & 0 \end{pmatrix} . \begin{pmatrix} 15 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 323 \\ 94 \\ 210 \end{pmatrix} = X_1$$

O resultado das outras multiplicações são:

$$X_2 = \begin{pmatrix} 244 \\ 275 \\ 239 \end{pmatrix} \qquad X_3 = \begin{pmatrix} 361 \\ 119 \\ 239 \end{pmatrix} \qquad X_4 = \begin{pmatrix} 453 \\ 330 \\ 393 \end{pmatrix}$$

$$X_5 = \begin{pmatrix} 543 \\ 150 \\ 378 \end{pmatrix} \qquad X_8 = \begin{pmatrix} 69 \\ 66 \\ 45 \end{pmatrix} \qquad X_{11} = \begin{pmatrix} 66 \\ 54 \\ 30 \end{pmatrix}$$

$$X_6 = \begin{pmatrix} 197 \\ 235 \\ 195 \end{pmatrix} \qquad X_9 = \begin{pmatrix} 439 \\ 146 \\ 324 \end{pmatrix} \qquad X_{12} = \begin{pmatrix} 322 \\ 356 \\ 299 \end{pmatrix}$$

$$X_7 = \begin{pmatrix} 432 \\ 333 \\ 351 \end{pmatrix} \qquad X_{10} = \begin{pmatrix} 90 \\ 87 \\ 60 \end{pmatrix} \qquad X_{13} = \begin{pmatrix} 228 \\ 60 \\ 168 \end{pmatrix}$$

Após a multiplicação de todos os blocos obteremos a seguinte sequencia de números

323 94 210 244 275 239 361 119 239 453 330 393 543 150 378 197 235 195 432 333 351 69 66 45 439 146 324 90 87 60 66 54 30 322 356 299 228 60 168

A divisão em blocos de tamanho três será feita com essa sequencia. Esses blocos poderão ser transformados em matrizes coluna.

Essas matrizes X_n foram obtidas da seguinte maneira $A \cdot B_n = X_n$, então dado X_n se multiplicarmos A^{-1} obteremos B_n.

De fato:

$$A \cdot B_n = X_n$$

$$A^{-1} \cdot A \cdot B_n = A^{-1} \cdot X_n$$

$$I \cdot B_n = A^{-1} \cdot X_n$$

$$B_n = A^{-1} \cdot X_n$$

Então fazendo essa operação com cada bloco obteremos por exemplo:

$$A^{-1} \cdot X_8 = \begin{pmatrix} \frac{15}{429} & \frac{-30}{429} & \frac{21}{429} \\ \frac{-14}{429} & \frac{28}{429} & \frac{9}{429} \\ \frac{177}{429} & \frac{75}{429} & \frac{-267}{429} \end{pmatrix} \cdot \begin{pmatrix} 69 \\ 66 \\ 45 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 12 \end{pmatrix} = B_8$$

Assim retornaremos à sequencia:

15 0 19 1 15 0 16 1 21 12 15 0 27 0 15 0 13 1 9 15 18 0 3 12 21 2 5 0 4 15 0 2 18 1 19 9 12 0 0

E utilizando o quadro de relação temos:

O - SAO - PAULO - É - O - MAIOR - CLUBE - DO - BRASIL –

7.2 Criptoanálise

A criptoanálise da cifra de Hill é baseada no conhecimento das letras originais de partes do texto cifrado, como vimos que foi feito com todas as cifras polialfabéticas durante a história.

Para ilustrar como ela é feita, consideraremos um ciframento realizado dividindo-se a mensagem em blocos de duas letras; considerando o seguinte quadro:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figura 7.2: Quadro Simplificado Relação Letras/Números

Um criptoanalista deve saber que a mensagem foi cifrada em blocos de 2 letras, com um quadro de n elementos e que alguns pares como (m_1, m_2) e (m'_1, m'_2), correspondam, respectivamente, aos pares (c_1, c_2) e (c'_1, c'_2) do texto cifrado. Isso pode ser feito associando-se os digramas mais frequentes do texto cifrado aos digramas mais comuns no idioma da mensagem.

Escrevendo esses blocos como matrizes coluna e considerando a relação

$$M = A^{-1}C$$

, temos

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = A^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

ou seja,

$$\begin{pmatrix} m_1 & m'_1 \\ m_2 & m'_2 \end{pmatrix} = A^{-1} \begin{pmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{pmatrix}$$

Se a matriz

$$C = \begin{pmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{pmatrix}$$

for inversível em $M_2(Z_{26})$, isto é, se $mdc(det(C), 30) = 1$, o criptoanalista poderá multiplicar ambos os lados da última igualdade por

$$C^{-1} = \begin{pmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{pmatrix}^{-1}$$

,

obtendo a matriz A^{-1}, que possibilitará a decifração completa da mensagem.

Por outro lado, se a matriz C não for invertível, a criptoanálise não será tão rápida.

Suponha, por exemplo, que os digramas NS e HI sejam, nessa ordem, os mais frequentes num texto, criptografado pela cifra de Hill, que desejamos criptoanalisar. Caso a mensagem original seja em português, como os digramas DE e RA são os mais comuns nesse idioma, podemos supor que NS corresponde a DE e HI corresponde a RA.

Dessa forma, os pares (3,4) e (17,0) foram transformados em (13,18) e (7,8), respectivamente.

Assim, temos

$$\begin{pmatrix} 3 & 17 \\ 4 & 0 \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} 13 & 7 \\ 18 & 8 \end{pmatrix}$$

Como a matriz

$$C = \begin{pmatrix} 13 & 7 \\ 18 & 8 \end{pmatrix}$$

não é invertível em $M_2(\mathbb{Z}_{26})$, pois $det(C) = 4$ e $mdc(4, 26) = 2$, podemos tentar obter uma matriz invertível através de outro par de letras. Caso não seja possível, uma outra alternativa consiste em reduzir o número de possibilidades para essa matriz.

Isso será feito considerando as seguintes matrizes:

$$\overline{A}^{-1}, \overline{M} = \begin{pmatrix} 3 & 4 \\ 4 & 0 \end{pmatrix} e \overline{C} = \begin{pmatrix} 0 & 7 \\ 5 & 8 \end{pmatrix}$$

que são, respectivamente, as reduções das matrizes $A^{-1}, M, C \in M_2(\mathbb{Z}_{26})$ em $M_2(\mathbb{Z}_{13})$.

Dessa forma, a partir da relação

$$\overline{M} = \overline{A}^{-1}\overline{C}$$

e da inversa de $\overline{C}$ em $M_2(\mathbb{Z}_{13})$ podemos obter

$$\overline{A}^{-1} = \overline{MC}^{-1} = \begin{pmatrix} 3 & 4 \\ 4 & 0 \end{pmatrix} . \begin{pmatrix} 2 & 8 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 11 \\ 8 & 6 \end{pmatrix}$$

Assim, como as entradas da matriz $\overline{A}^{-1}$, pertencentes a $\mathbb{Z}_{13}$, são reduções das entradas da matriz A^{-1}, pertencentes a $\mathbb{Z}_{26}$, temos duas possibilidades para cada entrada de A^{-1}. Assim, temos $2^4 = 16$ possibilidades para a matriz A^{-1}.

Como A^{-1} é invertível, temos que $mdc(det(A^{-1}), 26) = 1$, podemos eliminar 10 das 16 possibilidades para A^{-1}.

Além disso, como

$$A^{-1}. \begin{pmatrix} 13 & 7 \\ 18 & 8 \end{pmatrix} = \begin{pmatrix} 3 & 17 \\ 4 & 0 \end{pmatrix}$$

ficam apenas duas possibilidades:

$$A^{-1} = \begin{pmatrix} 1 & 11 \\ 8 & 19 \end{pmatrix} \text{ ou } A^{-1} = \begin{pmatrix} 1 & 24 \\ 8 & 19 \end{pmatrix}$$

Finalmente, poderemos determinar a matriz correta realizando a decifragem da mensagem codificada com ambas, e verificando qual delas fornece o resultado satisfatório.

No geral, para criptoanalisar mensagens criptografadas pela cifra de Hill, operando com blocos de n letras, podemos nos basear na frequencia de ocorrência de poligramas (blocos de n letras) no idioma da mensagem original. Porém esse método é viável, apenas para pequenos valores de n. Note que para $n = 10$, por exemplo, existem 26^{10} poligramas, o que torna a análise de frequencia dos mesmos praticamente impossível.

Escolher blocos de tamanhos cada vez maiores nos obriga a escolhermos matrizes quadradas desse mesmo tamanho n que pode dificultar a obtenção de sua inversa, como

podemos perceber no exemplo que utilizamos uma matriz 3×3, isso também é uma maneira de aumentar a segurança da Cifra de Hill.

Capítulo 8

Considerações Finais

Com esse trabalho podemos observar que alguns livros não seguem a risca o que é sugerido pelo PCN e CBC. Apesar de serem bons livros em relação aos conteúdos apresentados, não trazem muitas aplicações práticas dos conteúdos, inclusive relacionados a Criptografia.

Neste trabalho, apresentamos aplicações para conteúdos que podem ser trabalhados em uma sala de aula do Ensino Médio, com o objetivo de mostrar como podemos criar uma interação dos alunos com os conteúdos apresentados. As Diretrizes nacionais e estaduais, indicam que o conteúdo de Matemática deve despertar o interesse dos alunos, incentivando-os a estudar outros conteúdos; e promover a percepção do uso da matemática em assuntos da vida moderna.

Durante o desenvolvimento do trabalho, fica evidente que o tema tem um vasto contexto histórico e tecnológico, ao mesmo tempo que pode ser vinculado a conceitos matemáticos que podem ser desenvolvidos com alunos do Ensino Médio, possibilitando o ensino e aprendizado da matemática com aplicações mais "palpáveis". Devido a essa característica, acreditamos que a Criptografia possa servir de motivação para o estudo da matemática por parte desses alunos, não apenas dos conteúdos que envolvam a criptografia; mas esperamos que percebam que a matemática é extremamente importante em nossos aparatos tecnológicos e busquem novos conhecimentos.

As propostas pedagógicas relacionadas à Criptografia apresentadas nesse trabalho, tanto utilizando a Aritmética modular quanto Matrizes, mostram ser excelentes ferramentas para o ensino-aprendizagem da matemática, pois priorizam o papel ativo do aluno trabalhando situações nas quais o raciocínio e aplicação de conceitos são

desenvolvidos com a prática.

Espera-se que este trabalho possa gerar reflexões e estímulos em professores, que por diversos motivos, não tem o hábito de trabalhar conteúdos matemáticos dentro de contextos ou com aplicações. Existe a expectativa que esses professores percebam o quão valioso é um processo de ensino-aprendizagem no qual o aluno seja o articulador de seu próprio conhecimento, enquanto o professor comporta-se como um mediador e auxiliador nessa construção.

Pensando em possíveis trabalhos futuros, sugerimos a utilização da ferramenta moderna nas qual as Matrizes tem presença maciça: a computação; para criação de algum tipo de aplicativo que possa facilitar a codificação e decodificação de mensagens utilizando matrizes. Outra sugestão é tentarmos levar o tema Criptografia até alunos do Ensino Fundamental, adaptando linguagens e buscando novas maneiras de introduzirmos alguns conceitos.

Referências Bibliográficas

[Boldrini, 1984] BOLDRINI, José L. et al.: Álgebra Linear, Ed Harbra, 3a edição, São Paulo, SP, 1984.

[Brasil 1998] BRASIL. Secretaria de Educação Fundamental. Parâmetros curriculares nacionais : Matemática / Secretaria de Educação Fundamental. Brasília : MEC, 1998.

[Brasil 2002] BRASIL. Parâmetros curriculares nacionais: Matemática-PCN+. Brasília: MEC/SEF, 2002

[Brasil 2016] BRASIL. Programa Nacional do Livro Didático. Brasília: MEC/SEF, 2016

[Coutinho 2011] COUTINHO, S. C. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA, 2001.

[Coutinho 2007] COUTINHO S.C. Programa de Iniciação Científica da OBMEP 2007 - Imprinta Express Gráfica e Editora Ltda.

[De Menezes 2003] DE MENEZES, R. Criptografia e Álgebra. Belo Horizonte, UFMG, 17 de março de 2003.

[Giovanni, Giovanni Jr, Bonjorno e Câmara] GIOVANNI, José Ruy; GIOVANNI JR, José Ruy; BONJORNO, José Roberto; CÂMARA, Paulo Roberto de Souza. Matemática, Uma nova abordagem: Progressões: 2º ano. FTD. 3 ed. São Paulo, 2013

[Hefez e Fernandes 2012] HEFEZ, Abramo; FERNANDES, Cecília de Souza. Introdução a Álgebra Linear. 2. ed. Rio de Janeiro, SBM, 2012

[Howard e Rorres 2001] HOWARD, Anton; RORRES, Chris. Álgebra Linear com Aplicações. 8. ed. Porto Alegre: Bookman, 2001.

[Iezzi 2005] IEZZI, Gelson, HAZZAN, Samuel. Fundamentos da Matemática Elementar: sequências, matrizes, determinante, sistemas. Atual Editora Ltda: 4 ed. São Paulo, 2005

[Lemos 2008] LEMOS, M. Criptografia, Números Primos e Algoritmos, Rio de Janeiro, RJ: Editora do IMPA.

[Leon 2008] LEON, Steven J. Álgebra Linear com Aplicações. Rio de Janeiro: LTC, 2008.

[Lima 2001] LIMA, E. Exame de Textos - Análise de Livros de Matemática para o Ensino Médio. Rio de Janeiro: IMPA/SBM, 2001.

[Santos 2001] SANTOS, R. J. Geometria analítica e álgebra linear. Belo Horizonte, UFMG, 2001.

[SEE 2010] SECRETARIA DE ESTADUAL DE EDUCAÇÃO. Currículo Básico Comum. Minas Gerais, 2010

[Singh 2008] SINGH, Simon. O Livro dos Códigos: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: Record, 2008.

[Terada 1988] TERADA, R. Criptografia e a importância das suas aplicações. Revista do professor de matemática, São Paulo, 12: 1 ? 7, 1988.

Primeiro Apêndice

Proposta Pedagógica do Método RSA

Para auxiliar a aplicação da criptografia utilizando o método RSA elaboramos uma proposta pedagógica que pode ser aplicada a alunos do Ensino Médio, alunos de Graduação e capacitação de professores.

A proposta elaborada com esta dissertação é dividida em seis aulas com duração de 1 hora cada, de maneira que não fique cansativo nem para os participantes nem para quem for ministra-las, podendo assim tirar o máximo de proveito possível do conteúdo apresentado.

O objetivo é mostrar a importância da criptografia desde os tempos antigos até os dias atuais e também mostrar o mais conhecido método de criptografia atual, o RSA, e o mais importante, mostrar aos alunos e professores uma aplicação da Teoria de Números. Afinal muitos conceitos são utilizados intuitivamente por alunos do ensino Fundamental e Médio, enquanto os alunos de Graduação em Matemática aprendem esse conteúdo mais profundamente ao longo do curso e que, muitas vezes, não é trabalhado de forma eficiente, fazendo com que os alunos não dêem a importância devida ao tema.

Voltado para estudantes do Ensino Médio também pode ser direcionado à pessoas com certo interesse pelo assunto, uma vez que a proposta para as primeiras aulas é de fazer uma revisão dos conteúdos que são pré-requisitos para o andamento desta proposta.

As aulas serão mais expositivas, com apresentações de slides. Assim, o material utilizado será lápis, borracha, papel, quadro-negro, projetor multimídia, computador. Além desses recursos, na primeira aula, podem ser apresentados aparelhos criptográficos, tais como o Citale Espartano, com o intuito de mostrar aos participantes o funcionamento deste.

As atividades sugeridas foram baseadas nos seguintes livros [Coutinho 2007],

[Coutinho 2011] e [Lemos 2008], que tratam específicamente do Método RSA.

AULA 1: INTRODUÇÃO À CRIPTOGRAFIA

Nessa aula será apresentada a abordagem histórica da Criptografia. Serão tratados os significados, a história, os contextos em que a criptografia é importante. De forma a aumentar ainda mais a curiosidade dos alunos. Essa parte é de grande importância, pois trata de como surgiu a Criptografia, qual a necessidade de se inventar um método para mandar mensagens.

Os alunos serão levados a discutir sobre os métodos e pensar na validade deles, como, por exemplo, por que a Cifra de César não deu certo? Além disso, após a contextualização de Criptografia, serão levados a pensar em quantas vezes já usaram de algum meio criptográfico ao longo da vida, etc.

Essa aula é finalizada com uma atividade do Código de César, para mostrar o início da Criptografia, uma forma mais simples de criptografar uma mensagem. Nesta ATIVIDADE 1, os participantes terão que codificar uma frase escolhida por eles, de acordo com a cifra de César, o jeito de transladar o alfabeto ficará a cargo de cada um, após feita a codificação e com base na tabela de freqüência das letras no português, cada um terá que analisar se este tipo de codificação é seguro para a frase escolhida ou se com a ajuda da tabela é possível decodificar o que foi escrito. Deste modo, será possível aos participantes analisar, com as próprias mãos, o motivo da Cifra de César ter falhado.

ATIVIDADE 1: Considere a tabela de freqüência das letras no português:

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		

Cada aluno deve codificar uma frase de sua escolha. Peça aos alunos que verifiquem se a tabela de freqüência das letras no português é válida para suas frases.

AULAS 2 e 3: TEORIA DOS NÚMEROS

Nessa aula será feita uma revisão de Teoria dos Números, uma vez que é necessário dominar essa matéria para utilizar o algoritmo RSA.

Será feita uma breve explicação do conteúdo com diversos exempos numéricos.Logo

após essa revisão serão aplicadas atividades teóricas para a fixação do conteúdo.

Na ATIVIDADE 2, os alunos são convidados a encontrar o resto da divisão de um número por outro dado, assim, torna-se possível compreender melhor como se dá a resolução deste tipo de exercício, assim como na ATIVIDADE 3, já na ATIVIDADE 4, são apresentadas algumas equações, também com o intuito de que eles pratiquem a resolução de exercícios deste tipo.

É importante lembrar que, se houver algum tipo de dúvida no desenvolvimento de qualquer atividade, primeiro os participantes serão estimulados a discutir com os próprios colegas sobre a resolução, se continuar o impasse o ministrante poderá explicar novamente o processo, deste modo cada participante poderá compreender melhor o conteúdo.

ATIVIDADE 2: Para cada par de inteiros a, n abaixo ache um número inteiro b tal que $b \equiv a(mod n)$ e $0 \leq b < n$.

- a = 2351 e n = 2
- a = 50121 e n = 13
- a = 321671 e n = 14

ATIVIDADE 3: Calcule:

- $5^{20}(mod 7)$
- $7^{1001}(mod 11)$
- $2^{130}(mod 263)$
- $13^{1221}(mod 19)$

ATIVIDADE 4: Resolva as seguintes equações:

- $4x \equiv 3(mod 4)$
- $3x + 2 \equiv 0(mod 4)$
- $2x - 1 \equiv 7(mod 15)$

AULAS 4 e 5: O MÉTODO RSA. Nessas aulas, o método RSA será apresentado aos participantes. Sua aplicação e funcionamento. Como utilizá-lo para criptografar mensagens e a importância desse algoritmo nos dias atuais.

Esta é a fase mais importante de todo o desenvolvimento, pois é por meio dela que será mostrada a aplicação da Teoria dos Números na Criptografia, por isso, é essencial que cada etapa seja explicada com detalhes e que os participantes compreendam e assimilem o processo criptográfico.

Logo após essa explicação, serão apresentados exemplos do método para que os participantes possam se familiarizar com este. E poder utilizá-lo para criptografar o que desejam transmitir.

Com base na ATIVIDADE 5, deve-se colocar em prática os conceitos aprendidos a fim de fatorar n, para isto o participante deve lembrar o que n representa, além de recorrer a função $\varphi(n)$. Já nas ATIVIDADES 6 e 7, o participante é levado a colocar em prática o método, deste modo as possíveis dúvidas podem ser retiradas.

ATIVIDADE 5: Sabendo-se que $n = 3552377$ é igual ao produto de dois números primos e que $\varphi(n) = 3548580$; fatore n.

ATIVIDADE 6: A mensagem 6355-5075 foi codificada pelo método RSA usando a senha $n = 7597$ e $e = 4947$. Além disso, sabe-se que $\varphi(n) = 7420$. Decodifique a mensagem.

ATIVIDADE 7: A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte: $n = 10403$ e $e = 8743$. Recentemente os computadores do banco receberam, de local indeterminado, a seguinte mensagem: 4746 - 8214 - 9372 - 9009 - 4453 - 8198

O que diz a mensagem mandada ao Banco de Toulouse?

AULA 6: APLICAÇÃO DO MÉTODO RSA

Para finalizar será aplicado atividades sobre a Criptografia. Para fazer uma síntese do que foi exposto durante as aulas anteriores.

Para haver uma maior interação entre os participantes e desenvolver mais o trabalho em grupo, a turma será dividida em pequenos grupos com no máximo 4 integrantes cada. Nesta ATIVIDADE 8, os grupos são convidados a elaborar uma frase, de no máximo 4 palavras, após criada a frase terão que codificá-la, a importância do trabalho em grupo será vista neste momento, para criar a seqüência de blocos da frase codificada, os participantes terão que se organizar, uma vez que a seqüência inicial feita após a etapa de pré-codificação não pode ser mudada. Deste modo, o grupo deverá entrar em acordo e codificar a mensagem de modo que não percam a seqüência original.

Logo após, os grupos deverão trocar as frases codificadas e tentar decodificar a frase que recebeu do outro grupo. Após a decodificação a frase deve ser lida e então os grupos devem discutir os resultados alcançados, tanto com a atividade quanto com as aulas em si.

ATIVIDADE 8:

Neste momento, vamos formar grupos de no máximo 4 pessoas a fim de que possamos realizar a atividade.

Cada grupo deve montar uma frase de no máximo quatro palavras. Considerando $p = 5$e $q = 7$, o grupo deve codificar a frase escolhida.

Logo após, os grupos deverão trocar as frases codificadas e tentar decodificar a frase que recebeu do outro grupo. Após a decodificação a frase deve ser lida e então os grupos devem discutir os resultados alcançados.

Segundo Apêndice

Proposta Pedagógica para Cifra de Hill

A cifra de Hill pode ser compreendida com os conteúdos de Matrizes e Determinantes que costumam ser ensinados no Segundo Ano do Ensino Médio; e com o auxílio da Aritmética Modular que não costuma ser estuda profundamente nesse ciclo escolar. Portanto vamos nos concentrar nessa proposta apenas nos conteúdos que costumam ser ensinados no Ensino Médio, já que a Aritmética Modular é trabalhada na outra Proposta Pedagógica.

Buscamos organizar essa Proposta de maneira que possa ser utilizada comitantemente com o planejamento dos professores, sem precisar de aulas adicionais para sua aplicação.

AULA 1: INTRODUÇÃO A MATRIZES

Nessa aula serão mostrados aos alunos alguns exemplos de tabelas que são utilizadas no cotiadiano, e será definido o conceito de Matriz, apresentando suas principais caracteristicas.

As Matrizes Especiais (6.2) serão apresentadas ao alunos, sempre destacando suas principais propriedades.

ATIVIDADE 1: Nessa atividade pode ser proposto aos alunos que identifiquem algumas Matrizes Especiais, e também que construam matrizes de acordo com formúlas matemáticas.

AULA 2, 3 e 4: OPERAÇÕES COM MATRIZES

Grande parte do tempo no planejamento deve ser dedicado a essa parte, pois são muitos detalhes, principalmente quando trabalhamos Multiplicação de Matrizes

Acreditamos que deveemos iniciar a Multiplicação de um Número Real por Matriz (6.3.3) por ser mais intuitivo, podendo ser mais simples dos alunos compreenderem.

Passaremos para a Adição de Matrizes, que será utilizada quando trabalharmos

Subtração de Matrizes. Afinal essa última nada mais é que a Adição de uma matriz com uma Matriz Oposta (6.2)

ATIVIDADE 2: Nessa atividade o professor pode passar aos alunos diversos exemplos para que treinem tais operações, e identifiquem as propriedades comutativas e distributivas da adição e subtração de matrizes.

A Multiplicação de Matrizes pode ser introduzida com um exemplo simples que utilizamos diariamente.

ATIVIDADE 3: Sempre nos foi ensinado que devemos pesquisar os preços dos produtos em mais de um lugar buscando economizar. Portanto será entregue aos alunos uma lista de compras com diversos produtos e suas respectivas quantidades; e no quadro será colocada uma tabela de preços de, pelos menos, dois estabelicimentos que vendem tais produtos. Ao final será perguntado aos alunos: em qual dos dois estabelecimentos deve ser feita a compra de modo que pague o menor valor?

Após essa atividade podemos transformar a lista de compras e a tabela de preços em matrizes de modo que façamos a multiplicação das mesmas com os alunos.

Daí podemos formalizar a multiplicação de matrizes sempre com exemplos númericos pra facilitar o entendimento.

AULA 5: A Matriz Inversa.

Esse é um ponto de divergencia entre alguns professores, pois alguns compreendem que Matriz Inversa deve ser dada antes do conteúdo de Determinantes, enquanto outros acreditam que a ordem deva ser invertida.

Como pensamos em trabalhar com matrizes de ordem menor ou igual a 3, introduziremos Matriz Inversa antes de trabalharmos com Determinantes.

Deve ser definido o conceito de Matriz Inversa e apresentados diversos exemplos de modo que os alunos compreendam que existem matrizes que possuem inversa e que outras não.

ATIVIDADE 4: Essa atividade será um trabalho de repetição, pois serão apresentados diversas matrizes para que os alunos determinem suas inversas, caso existam.

AULA 6: Introdução à Criptografia

Para que um conteúdo tão importante como esse não fique apenas com a parte teórica e com exercícios de fixação que são feitos de maneira “mecânica”; é proposta uma atividade que é contextualizada e valoriza o papel ativo do aluno.

Nessa aula será apresentada a abordagem histórica da Criptografia, da mesma maneira que foi apresentada na Primeira Proposta Pedagógica. Inclusive com a mesma atividade.

AULA 7: A Cifra de Hill

Será explica e aplicada a Cifra de Hill.

- Inicialmente devemos estabelecer uma relação entre as letras do alfabeto, caracteres mais utilizados e os números, como no quadro a seguir

	a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
o	p	q	r	s	t	u	v	w	x	y	z	à	á	â
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
ã	ç	é	ê	í	ó	ô	õ	ú	ü	A	B	C	D	E
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
U	V	W	X	Y	Z	À	Á	Â	Ã	Ç	É	Ê	Í	Ó
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
Ô	Õ	Ú	Ü	0	1	2	3	4	5	6	7	8	9	:
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
;	<	=	>	?	@	!	"	#	$	%	&	’	(	)
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
*	+	,	-	.	/	[	\	]	_	{	|	}		
105	106	107	108	109	110	111	112	113	114	115	116	117		

Figura 8.1: Correspondência entre Letras e Números

Essa configuração apresentada no quadro não é a única possível, mas recomenda-se que seja seguida uma ordem lógica para facilitar a memorização por parte dos interlocutores. Por exemplo, podemos estabelecer que a letra corresponde ao número 7, a letra B ao número 8 e assim por diante.

O quadro mostra a diferenciação entre letras maiúsculas e minúsculas, ela não é obrigatória; mas essa técnica aumenta o poder da cifra, dificultando mais a análise de frequencia.

- Após estabelecermos a relação, devemos escrever a frase escolhida como o conjunto de números correspondentes

- Devemos escolher uma matriz quadrada A de ordem n de modo que essa matriz A tenha uma inversa A^{-1}, ou seja, $detA \neq 0$. Podemos também escolher uma palavra chave, que será transformada em uma matriz com as mesmas caracteristicas descritas acima.

- Escolhida a matriz, dividimos a frase em blocos de tamanho n. Caso o total de letras não seja divisível por n devemos completar a frase com alguma letra ou símbolo préviamente escolhido.

- Multipliquemos cada bloco de tamanho n pela matriz A, transformando-os em novos números.

  São esses novos números que deverão ser enviados ao destinatário.

- Ao receber a mensagem codificada, o destinatário deverá dividir esses novos números em blocos de tamanho n

- Para interpretá-los o destinatário deverá utilizar a matriz A^{-1}; multiplicando cada bloco pela matriz A^{-1}; obtendo os números originais.

Exemplo:

Utilizaremos um quadro de relações menos sofisticado que o mostrado anteriormente.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	X	W	Y	Z	É	.	,	-
16	17	18	19	20	21	22	23	24	25	26	27	28	29	0

A frase escolhida para ser criptografada é "O São Paulo é o maior clube do Brasil", e a palavra de referância é SOBERANO, que pode ser transformada na seguinte matriz:

$$A = \begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 14 & 15 & 0 \end{pmatrix}$$

A frase pode ser transformada no seguinte conjunto de números:

15 0 19 1 15 0 16 1 21 12 15 0 27 0 15 0 13 1 9 15 18 0 3 12 21 2 5 0 4 15 0 2 18 1 19 9 12

Como a matriz escolhida é uma matriz de ordem 3, dividiremos a frase em blocos de tamanho três:

Bloco 1: 15 0 19 Bloco 3: 16 1 21 Bloco 5: 27 0 15

Bloco 2: 1 15 0 Bloco 4: 12 15 0 Bloco 6: 0 13 1

Bloco 7: 9 15 18
Bloco 8: 0 3 12
Bloco 9: 21 2 5
Bloco 10: 0 4 15
Bloco 11: 0 2 18
Bloco 12: 1 19 9
Bloco 13: 12 0 0

Transformaremos cada bloco em uma matriz coluna e multiplicaremos pela matriz A, temos:

$$A.B_1 = \begin{pmatrix} 19 & 15 & 2 \\ 5 & 18 & 1 \\ 14 & 15 & 0 \end{pmatrix} . \begin{pmatrix} 15 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 323 \\ 94 \\ 210 \end{pmatrix} = X_1$$

O resultado das outras multiplicações são:

$$X_2 = \begin{pmatrix} 244 \\ 275 \\ 239 \end{pmatrix} \quad X_6 = \begin{pmatrix} 197 \\ 235 \\ 195 \end{pmatrix} \quad X_{10} = \begin{pmatrix} 90 \\ 87 \\ 60 \end{pmatrix}$$

$$X_3 = \begin{pmatrix} 361 \\ 119 \\ 239 \end{pmatrix} \quad X_7 = \begin{pmatrix} 432 \\ 333 \\ 351 \end{pmatrix} \quad X_{11} = \begin{pmatrix} 66 \\ 54 \\ 30 \end{pmatrix}$$

$$X_4 = \begin{pmatrix} 453 \\ 330 \\ 393 \end{pmatrix} \quad X_8 = \begin{pmatrix} 69 \\ 66 \\ 45 \end{pmatrix} \quad X_{12} = \begin{pmatrix} 322 \\ 356 \\ 299 \end{pmatrix}$$

$$X_5 = \begin{pmatrix} 543 \\ 150 \\ 378 \end{pmatrix} \quad X_9 = \begin{pmatrix} 439 \\ 146 \\ 324 \end{pmatrix} \quad X_{13} = \begin{pmatrix} 228 \\ 60 \\ 168 \end{pmatrix}$$

Após a multiplicação de todos os blocos obteremos a seguinte sequencia de números

323 94 210 244 275 239 361 119 239 453 330 393 543 150 378 197 235 195 432 333 351 69 66 45 439 146 324 90 87 60 66 54 30 322 356 299 228 60 168

A divisão em blocos de tamanho três será feita com essa sequencia. Esses blocos poderão ser transformados em matrizes coluna.

Essas matrizes X_n foram obtidas da seguinte maneira $A \cdot B_n = X_n$, então dado X_n se multiplicarmos A^{-1} obteremos B_n.

De fato:

$$A \cdot B_n = X_n$$

$$A^{-1} \cdot A \cdot B_n = A^{-1} \cdot X_n$$

$$I \cdot B_n = A^{-1} \cdot X_n$$

$$B_n = A^{-1} \cdot X_n$$

Então fazendo essa operação com cada bloco obteremos por exemplo:

$$A^{-1} \cdot X_8 = \begin{pmatrix} \frac{15}{429} & \frac{-30}{429} & \frac{21}{429} \\ \frac{-14}{429} & \frac{28}{429} & \frac{9}{429} \\ \frac{177}{429} & \frac{75}{429} & \frac{-267}{429} \end{pmatrix} \cdot \begin{pmatrix} 69 \\ 66 \\ 45 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 12 \end{pmatrix} = B_8$$

Assim retornaremos à sequencia:

15 0 19 1 15 0 16 1 21 12 15 0 27 0 15 0 13 1 9 15 18 0 3 12 21 2 5 0 4 15 0 2 18 1 19 9 12 0 0

E utilizando o quadro de relação temos:

O - SAO - PAULO - É - O - MAIOR - CLUBE - DO - BRASIL –

Existe outra maneira de aplicarmos o método descrito acima diminuindo os números com os quais trabalharemos.

Para isso devemos escolher a matriz chave A de maneira específica para que $mdc(det(A), m) = 1$, com m sendo o número de caracteres do quadro de relações entre Letras e Números.

Admitiremos o mesmo quadro utilizado para o exemplo anterior e $A = \begin{pmatrix} 6 & 11 \\ 1 & 2 \end{pmatrix}$.

Assim utilizando a mesma frase codificada no exemplo anterior, teríamos a mesma sequencia:

15 0 19 1 15 0 16 1 21 12 15 0 27 0 15 0 13 1 9 15 18 0 3 12 21 2 5 0 4 15 0 2 18 1 19 9 12 0

Devemos dividir, então, a sequencia em blocos de tamanho 2

Bloco 1: 15 0

Bloco 2: 19 1

Bloco 3: 15 0

Bloco 4: 16 1

Bloco 5: 21 12

Bloco 6: 15 0

Bloco 7: 27 0

Bloco 8: 15 0

Bloco 9: 13 1

Bloco 10: 9 15
Bloco 11: 18 0
Bloco 12: 3 12
Bloco 13: 21 2
Bloco 14: 5 0
Bloco 15: 4 15
Bloco 16: 0 2
Bloco 17: 18 1
Bloco 18: 19 9
Bloco 19: 12 0

Transformaremos cada bloco em uma matriz coluna e multiplicaremos pela matriz A, temos:

$$A \cdot B_1 = \begin{pmatrix} 6 & 11 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 0 \end{pmatrix} = \begin{pmatrix} 90 \\ 15 \end{pmatrix} = X_1$$

O resultado das outras multiplicações são:

$$X_2 = \begin{pmatrix} 125 \\ 21 \end{pmatrix} \quad X_3 = \begin{pmatrix} 90 \\ 15 \end{pmatrix} \quad X_4 = \begin{pmatrix} 197 \\ 18 \end{pmatrix} \quad X_5 = \begin{pmatrix} 258 \\ 45 \end{pmatrix} \quad X_6 = \begin{pmatrix} 90 \\ 15 \end{pmatrix} \quad X_7 = \begin{pmatrix} 162 \\ 27 \end{pmatrix}$$

$$X_8 = \begin{pmatrix} 90 \\ 45 \end{pmatrix} \quad X_9 = \begin{pmatrix} 89 \\ 15 \end{pmatrix} \quad X_{10} = \begin{pmatrix} 219 \\ 39 \end{pmatrix} \quad X_{11} = \begin{pmatrix} 108 \\ 18 \end{pmatrix} \quad X_{12} = \begin{pmatrix} 150 \\ 27 \end{pmatrix} \quad X_{13} = \begin{pmatrix} 148 \\ 25 \end{pmatrix}$$

$$X_{14} = \begin{pmatrix} 30 \\ 5 \end{pmatrix} \quad X_{15} = \begin{pmatrix} 189 \\ 34 \end{pmatrix} \quad X_{16} = \begin{pmatrix} 22 \\ 4 \end{pmatrix} \quad X_{17} = \begin{pmatrix} 119 \\ 20 \end{pmatrix} \quad X_{18} = \begin{pmatrix} 213 \\ 37 \end{pmatrix} \quad X_{19} = \begin{pmatrix} 72 \\ 12 \end{pmatrix}$$

Após a multiplicação de todos os blocos obteremos a seguinte sequencia de números

90 15 125 21 90 15 107 18 258 45 90 15 162 27 90 45 89 15 219 39 108 18 150 27 148 25 30 5 189 34 22 4 119 20 213 37 72 12

A sequencia acima pode ser mudada para uma sequencia menor. Essa nova sequencia seria o resto de cada número da sequencia original pelo número k de caracteres do quadro de relações:

0 15 5 21 0 15 17 18 18 15 0 15 12 27 0 15 29 15 9 9 18 18 0 27 28 25 0 5 9 4 22 4 29 20 3 7 12 12

A divisão em blocos de tamanho três será feita com essa sequencia. Esses blocos poderão ser transformados em matrizes coluna.

Essas matrizes X_n, como no exemplo anterior, foram obtidas da seguinte maneira: $A \cdot B_n = X_n$, então dado X_n se multiplicarmos A^{-1} obteremos B_n.

De fato:

$$A \cdot B_n = X_n$$

$$A^{-1} \cdot A \cdot B_n = A^{-1} \cdot X_n$$

$$I \cdot B_n = A^{-1} \cdot X_n$$

$$B_n = A^{-1} \cdot X_n$$

Para aplicarmos essa operação precisamos definir a matriz A^{-1}.

Teorema 8.1 *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, o residuo de det(A) módulo m tem um recíproco módulo m.*

Calculamos a matriz A^{-1} de uma matriz de ordem 2 da seguinte maneira:

$$A^{-1} = (detA)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

onde $(detA)^{-1}$ é o recíproco do resíduo *detA módulo m.*

Voltando a nosso exemplo (no qual $detA = 1$ e $(detA)^{-1}$ *módulo m* também é 1), aplicaremos a operação a cada bloco obteremos por exemplo:

$$A^{-1} \cdot X_1 = 1 \begin{pmatrix} 2 & -11 \\ -1 & 6 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 15 \end{pmatrix} = \begin{pmatrix} -165 \\ 90 \end{pmatrix} = B_1$$

Essa matriz $B_1 = \begin{pmatrix} -165 \\ 90 \end{pmatrix}$ é equivalente a matriz $B_1' = \begin{pmatrix} 15 \\ 0 \end{pmatrix}$, que são os restos da divisão dos números da matriz B_1 dividos por 30, número de caracteres do quadro que relaciona letras e números.

Conseguimos a sequencia:

15 0 19 1 15 0 16 1 21 12 15 0 27 0 15 0 13 1 9 15 18 0 3 12 21 2 5 0 4 15 0 2 18 1 19 9 12 0

E utilizando o quadro de relação temos novamente:

O - SAO - PAULO - É - O - MAIOR - CLUBE - DO - BRASIL –