Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Curso de Pós-Graduação em Matemática em Rede Nacional - PROFMAT

Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula. [†]

por

Thiago Valentim Marques

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Trabalho de conclusão apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Abril/2013
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES

M357c Marques, Thiago Valentim.
Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula / Thiago Valentim Marques.- João Pessoa, 2013.
82f. : il.
Orientador: Bruno Henrique Carvalho Ribeiro
Dissertação (Mestrado) – UFPB/CCEN
1. Matemática. 2. Criptografia. 3. Protocolo Diffie-Hellman. 4. Logaritmos discretos. 5. Raízes primitivas.

UFPB/BC CDU: 51(043)

Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula.

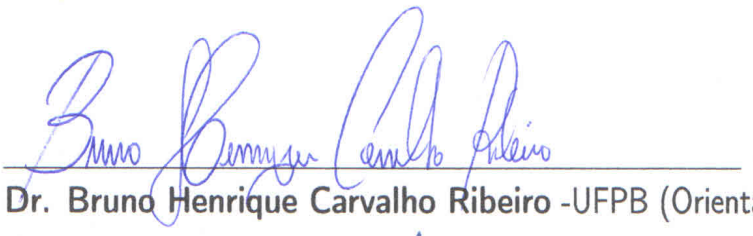
por

Thiago Valentim Marques

Trabalho de conclusão apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

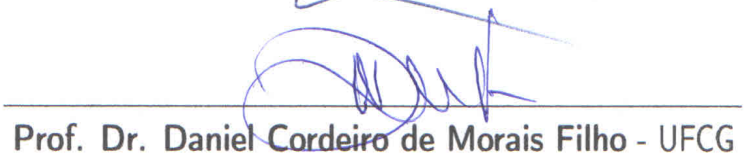
Área de Concentração: Matemática.

Aprovada por:



Prof. Dr. Bruno Henrique Carvalho Ribeiro -UFPB (Orientador)

Prof. Dr. Antônio de Andrade e Silva - UFPB



Prof. Dr. Daniel Cordeiro de Morais Filho - UFCG

Abril/2013

Agradecimentos

A Deus, que sempre está iluminando o meu caminho me ajudando a conquistar vitórias.

À minha família, pela formação, amor e incentivo nos meus estudos. Em especial, meus pais Ilo Marques (in memoriam) e Francisca Valentim, minha irmã Flávia e meus sobrinhos João Paulo, Sarah Karoline e Isaac Newton.

A Alyne Rayane cuja companhia me faz o homem mais feliz do mundo, sendo minha amiga e ao mesmo tempo minha namorada, sempre propiciando momentos maravilhosos.

Ao meu grande amigo, na verdade irmão, Thiago Antônio, pela sua amizade e companheirismo em todos os momentos, sempre discutindo propostas que tornem o ensino da Matemática cada vez mais proveitoso.

Ao meu orientador, Professor Bruno Henrique Carvalho Ribeiro que propôs o tema desse trabalho, acompanhou o seu desenvolvimento, fez as devidas correções sempre disponibilizando tempo para ajudar. Enfim, pela sua excelente orientação.

Aos professores Antônio de Andrade e Silva e Daniel Cordeiro de Morais Filho pelas excelentes contribuições que foram fundamentais para a melhoria deste trabalho.

A todos os professores que ministraram aulas no PROFMAT na UFPB, pela dedicação destinada ao ensino e aprendizagem nas disciplinas ministradas, em especial os professores Bruno Ribeiro e Napoleon Caro Tuesta.

Ao professor Carlos Alexandre Gomes pelas aulas ministradas em Natal e João Pessoa que foram importantíssimas para a minha aprovação nas disciplinas e no exame de qualificação do PROFMAT.

Aos meus amigos de Mestrado na UFPB, que estiveram junto comigo nessa caminhada durante os dois últimos anos, pelo companheirismo e amizade, em especial a Aldrin Rufino, Sandro Godeiro e Andreilson Oliveira por enfrentar a estrada todos os sábados na ida de Natal a João Pessoa.

Aos colegas do PROFMAT da UFRN e UFERSA, em especial Emanuel Gomes, Fellipe Arrais, Leonardo Andrade, Gilberto Fernandes, Thiago Pardo, Jorge Pontes e Luciano Nóbrega que sempre estavam presentes nas aulas do Professor Carlos Alexandre Gomes.

Aos Professores Aldrin Rufino e Edilson, pelos ensinamentos na minha educação básica e inspiração para ser um professor de matemática.

Aos professores da graduação na UFRN: André Gustavo, Benedito Tadeu, Gurgel de Melo, Antônio Roberto, Marcelo Gomes e Gabriela Lucheze, pela enorme contribuição na minha formação.

Aos colegas de graduação na UFRN, em especial Dayvid Marques, Daniel Teixeira, José Carlos e Marconio da Silva pelos excelentes momentos de discussão matemática e colaboração.

A Professora Teresa Paula pela sua amizade e pela correção ortográfica desse trabalho, ao Professor Paulo Eduardo pela correção do abstract deste trabalho e ao Professor Daniel Teixeira pelas correções em latex.

Ao pessoal do PET de Matemática da UFRN e ao professor Marcelo Gomes.

À Sociedade Brasileira de Matemática (SBM) pela criação do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) dando oportunidade para que professores da educação básica possam melhorar os seus conhecimentos matemáticos.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pela bolsa concedida.

Dedicatória

Dedico este trabalho às duas pessoas que foram fundamentais no apoio aos meus estudos: meu pai, Ilo Marques Bezerra (in memoriam) e minha mãe, Francisca Valentim da Silva Bezerra, que, desde 2004, assumiu, com extremo amor e responsabilidade, o papel de ambos.

Epígrafe

"Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real." (Lobachevsky)

Resumo

Neste trabalho, vamos estudar a evolução da criptografia ao longo da história; analisar a diferença entre as criptografias simétricas e assimétricas; enunciar definições e teoremas sobre relações binárias, teoria dos grupos, raízes primitivas e logaritmos discretos; entender o procedimento do protocolo da troca de chaves de Diffie-Hellman; e, na parte final deste trabalho, iremos propor três atividades para serem aplicadas em sala de aula.

Palavras chaves: criptografia, sigilo, Diffie-Hellman, logaritmos discretos, raízes primitivas, matemática, segurança.

Abstract

In this paper we are studying cryptography's evolution throughout history; analyzing the difference between symmetric and asymmetric cryptographies; enunciating definitions and theorems about binary relations, group theories, primitive roots and discrete logarithms; understanding the procedure of Diffie-Hellman's key change protocol. In the last part in this work, we are proposing three activities to be applied in classroom.

Keywords: cryptography; secrecy; Diffie-Hellman; discrete logarithms; primitive roots; mathematics; safety.

Sumário

Lista de Figuras

Introdução

O computador tornou-se indispensável no nosso dia a dia, pois está presente nos ambientes que frequentamos, seja em casa, na escola ou no trabalho. A utilização deste recurso para a comunicação via internet é de suma importância na sociedade, pois diariamente enviamos e-mails, utilizamos redes sociais ou escrevemos mensagens para celulares utilizando aplicativos em sites. A partir disso, surgem as seguintes perguntas: será que temos privacidade ao enviar essas mensagens? Se alguém interceptar essas mensagens, elas serão lidas ou elas estarão codificadas? Perguntas como essas são o interesse do nosso estudo.

Desde os tempos antigos, por vários motivos, imperadores, generais e reis procuravam obter modos eficientes de comunicação entre seus exércitos. A necessidade de as informações não serem descobertas motivou a elaboração de técnicas para ocultar o real significado delas por meio de códigos, possibilitando que somente o remetente e o destinatário pudessem entender o que a mensagem dizia, dificultando o trabalho de eventuais intrusos na tentativa de desvendá-la. Essa técnica é chamada criptografia, cuja evolução deve-se, em boa parte, ao longo dos anos, a Matemática.

A força de um código está relacionada à dificuldade de um intruso decifrá-lo e, dessa forma, tem-se uma "guerra" entre cifradores e decifradores de mensagens. Na medida em que a informação se torna mais valiosa, o processo de codificação das mensagens tem um papel cada vez mais importante na sociedade.

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. (SINGH, 2007, p.13)

A importância da criptografia está relacionada com a proteção de dados sigilosos de caráter pessoal ou profissional. Por exemplo: na comunicação de dois países aliados na criação de uma nova tecnologia que deve ser mantida em segredo. Através da Ciência da Computação, tendo a ajuda da Matemática, essas informações são transmitidas de modo extremamente rápido e seguro. Hoje em dia vemos isso acontecer claramente quando fazemos uma transação bancária via internet, pois é preciso um meio de encriptar a senha dos usuários para que hackers não possam obtê-la e ter acesso à conta do usuário. Vários bancos têm um sistema diferenciado de proteção de senhas dos usuários, que é feito utilizando criptografia.

O problema fundamental e quase axiomático durante muitos anos foi o "problema da distribuição de chaves", ou seja, dois usuários devem se comunicar utilizando um algoritmo, mas, para isso ser feito, eles precisam de uma chave para codificar e decodificar as mensagens. Como essa chave pode ser distribuída de modo seguro? A Matemática entra em cena com os números primos e os logaritmos discretos. Iremos aprender que estes são fundamentais para resolver o problema da troca de chaves, pois o intruso terá uma dificuldade imensa, já que não existe um algoritmo eficiente que possa calcular esses logaritmos discretos para números primos muito grandes. Isso foi feito por Diffie e Hellman nos anos 70, causando um avanço imenso na criptografia.

Partindo do princípio que a criptografia é um assunto importante e interessante no contexto atual, acredita-se que a sua utilização em sala de aula possa ser um fator que motive os alunos, já que a informática está presente de maneira intensa na vida dos jovens. Trazendo a criptografia para a sala de aula, poderemos associá-la com conteúdos de Matemática, vistos na educação básica, fazendo com que o aluno sinta motivação no momento de aprender ou aplicar tal conteúdo.

Partindo do princípio que a criptografia é um assunto importante e interessante no contexto atual, acredita-se que a sua utilização em sala de aula possa ser um fator que motive os alunos, já que a informática está presente de maneira intensa na vida dos jovens. Trazendo a criptografia para a sala de aula, poderemos associá-la com conteúdos de Matemática, vistos na educação básica, fazendo com que o aluno sinta motivação no momento de aprender ou aplicar tal conteúdo.

O objetivo geral deste trabalho é fornecer um conhecimento sobre Criptografia de modo que o Professor de Matemática possa introduzi-la em sala de aula, relacionando este tema com assuntos do ensino básico, tornando a prática docente mais dinâmica e motivante, pois os alunos ficarão frente a frente com atividades de codificação e decodificação.

Os objetivos específicos são:

- Introduzir a definição de criptografia;
- Relatar a evolução histórica da criptografia;
- Diferenciar as criptografias simétrica e assimétrica;
- Compreender a definição de relações, grupos, raízes primitivas e logaritmos discretos bem como os teoremas e demonstrações;
- Saber a importância dos logaritmos discretos na troca de chaves de Diffie-Hellman;
- Relacionar a criptografia com assuntos de matemática vistos no ensino básico.

A fim de proporcionar uma visão geral do nosso trabalho, apresentamos uma breve descrição dos assuntos que iremos tratar em cada um dos capítulos.

No capítulo um, vamos mostrar a evolução histórica da criptografia apresentando como Heródoto relatou o aparecimento da Esteganografia; a Cifra de César; os criptoanalistas árabes; a cifra de Vigenère, as máquinas de cifragem e a criptografia na atualidade, descrevendo a criptografia simétrica e a assimétrica.

No capítulo dois, faremos um estudo resumido de Álgebra, apresentando várias definições e teoremas importantes que são utilizados na criptografia. Os assuntos que veremos são: relações binárias, Grupos, Raízes Primitivas e Logaritmos Discretos.

No capítulo três, uma abordagem histórica sobre a criptografia Diffie-Hellman será apresentada e, em seguida, descreveremos o problema da troca de chaves junto com a sua solução utilizando Logaritmos Discretos.

No último capítulo, vamos propor três atividades que relacionam a criptografia com funções polinomiais do primeiro grau, matrizes e divisibilidade, respectivamente.

Capítulo 1

A evolução da criptografia ao longo da história

Neste capítulo vamos fazer uma abordagem histórica da criptografia, mostrando a evolução dos métodos de cifragem, fornecendo dados para que o Professor de Matemática possa ter ideias de como introduzir este assunto no ensino básico. As referências utilizadas na escrita deste capítulo foram SINGH [20]; STALLINGS [21]; MALAGUTTI [13]; TÁBARA [22] e OLIVEIRA [15].

1.1 Heródoto

Um dos primeiros textos sobre códigos secretos foi escrito pelo geógrafo e historiador grego Heródoto (485 a.C. - 420 a.C.). Ele foi o primeiro não só a escrever sobre o passado, mas também a considerar o passado como um problema filosófico ou um projeto de pesquisa que podia revelar conhecimento do comportamento humano. Por esse motivo ele recebeu o título de "o pai da História". Na sua principal obra, conhecida por "as histórias de Heródoto", é retratada a história dos conflitos entre a Pérsia e a Grécia no início do século V a.C; atribuiu, pois, à habilidade da escrita secreta a causa de a Grécia não ter sido conquistada por Xerxes, cuja intenção, à época, era formar um grande exército para invadir a Grécia. Para a infelicidade de Xerxes, o plano da invasão foi testemunhado por Demarato, um grego que foi expulso da sua terra natal e vivia em uma cidade persa chamada Susa. Mesmo sendo um exilado, ele ainda tinha um sentimento de lealdade com a Grécia e decidiu enviar uma mensagem para advertir os espartanos dos planos de invasão de Xerxes. O principal desafio era como enviar essa mensagem sem que ela fosse interceptada pelos guardas. Vejamos a história contada nas palavras de Heródoto:

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os gregos. (SINGH, 2007, p. 20)

Assim, os gregos, que não estavam se preparando para uma batalha, começaram a se armar. Como exemplo, podemos citar o lucro das minas de ouro, antes compartilhada pelos cidadãos, começou a ser entregue à marinha para a construção de duzentos navios de guerra. Curiosidade: os gregos foram vencedores da futura batalha. Note que a estratégia de Demarato foi, apenas, ocultar a mensagem.

Heródoto também narra outro incidente no qual a ocultação foi suficiente para garantir a transmissão segura da mensagem. É a história de Histaeu, que queria encorajar Aristágora de Mileto a se revoltar contra o rei persa. Para transmitir suas instruções de segurança, Histaeu raspou a cabeça do mensageiro, escreveu a mensagem no couro cabeludo e aguardou até que o cabelo voltasse a crescer. O mensageiro partiu e, quando chegou ao seu destino, raspou a cabeça e exibiu a mensagem ao destinatário.

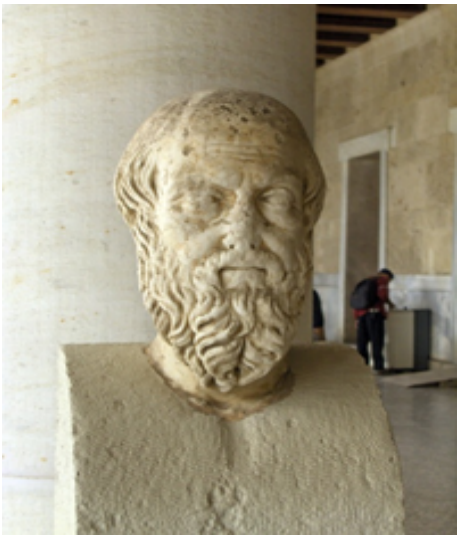


Figura 1.1: Busto de Heródoto
Fonte: http://commons.wikimedia.org/wiki/File:AGMA_Herodotus_7307.jpg

As duas histórias contadas por Heródoto não são consideradas comunicações secretas, pois foram obtidas através da ocultação da mensagem. A arte ou ciência de ocultar mensagens é chamada de *estenografia*, nome derivado das palavras gregas *estenos*, cujo significado é "escondido" e *graphein* que que significa "escrever". Várias formas de estenografias foram utilizadas durante muitos séculos. Entre alguns exemplos estão a escrita de uma mensagem secreta em uma tira de seda fina, que era amassada formando uma pequena bola, coberta com cera e engolida por um mensageiro; a tinta invisível usada na escrita que, após um suave aquecimento, adere a cor marrom; e a mensagem no ovo cozido que baseava-se em escrever uma mensagem sobre a casca desse ovo com uma tinta especial que penetrava essa casca e estampava o ovo.

1.2 A cifra de César

Em paralelo com o desenvolvimento da estenografia, houve a evolução da *criptografia*, derivada da palavra grega *kriptos*, que significa oculto, escondido, secreto. O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado - um processo conhecido como *encriptação*. A vantagem da criptografia: a mensagem codificada interceptada pelo inimigo será ilegível e seu conteúdo não poderá ser percebido. O primeiro código secreto que se tem notícia foi utilizado pelo militar e governante romano Júlio César (100 a.C. - 44 a.C.), na época da transição do final do período republicano da Roma Antiga.

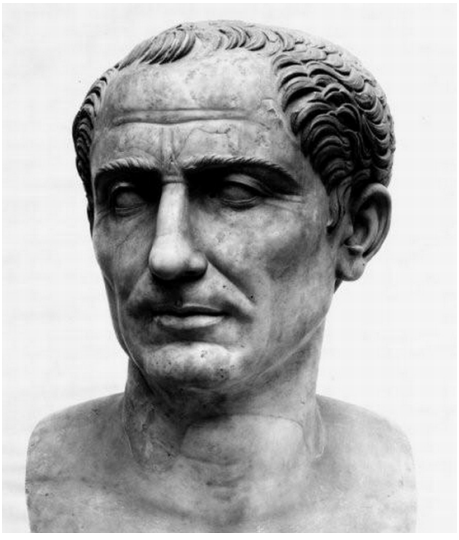


Figura 1.2: Cabeça colossal do imperador Júlio César
Fonte: http://sp-arte.aonde.org/wp-content/uploads/2012/01/exposicao-roma.jpg

Júlio César é considerado por muitos o maior gênio militar da história. Um dos motivos que pode justificar esse adjetivo é o fato dele utilizar um recurso para codificar mensagens com o objetivo de manter segredos de natureza militar. No livro "*As vidas dos Césares*", escrito no século II por Suetônio, um dos recursos utilizados por César consistia numa substituição de cada letra do alfabeto por outra, três posições adiante, a partir do que as três últimas letras do alfabeto fazem corresponder às três primeiras. Na prática, a letra "a" é substituída pela letra "d"; a letra "b", pela "e"; a letra "c", pela "f" e assim sucessivamente.

Qualquer forma de substituição criptográfica, a partir da qual cada letra é substituída por outra letra ou símbolo é chamada de cifra. Dessa forma, o alfabeto da língua portuguesa após a "*cifra de César*" é:

a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P

n	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figura 1.3: Cifra de César

Por exemplo, no lugar de escrever **atacar pelo norte**, o remetente escreveria **DWDFDU SHOR QRUWH**.

Antes de prosseguirmos, vamos definir congruência modular para entendermos a notação utilizada por STALLINGS [21]:

Definição 1 *Seja $m \in \mathbb{N}$ com $m > 1$. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais.*

$$a \equiv b \ mod \ m$$

Exemplo: Note que $12 \equiv 7 \bmod 5$, pois os restos da divisão de 12 e de 7 por 5 são iguais a 2.

A teoria das congruências também é importante para calcularmos o resto da divisão entre dois números. Se $0 \leq b < m$, então b é o resto da divisão de a por m, por exemplo 8 deixa resto 3 na divisão por 5:

$$8 = 1 \cdot 5 + 3$$

Então, $8 \equiv 3 \bmod 5$.

Com base nessa definição, vamos atribuir um equivalente numérico a cada letra do alfabeto $a = 0$, $b = 1$, $c = 2$, $d = 3$, ..., $z = 25$:

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

Podemos expressar um algoritmo da seguinte maneira: para cada letra no texto original, que vamos chamar de texto p, substitua-a pela letra do texto cifrado, que vamos chamar de C. Aplicando a notação utilizada na aritmética modular, temos:

$$C \equiv (p + 3) \bmod 26$$

Embora Suetônio só mencione que César deslocava as letras em três casas, fica claro que podemos fazer um deslocamento de qualquer quantidade, de modo que o algoritmo de César fica representado por

$$C \equiv (p + k) \bmod 26, \text{ com } k \in \mathbb{Z} \text{ fixo e } 1 \leq k \leq 25$$

No que diz respeito a decodificar o texto, basta fazer, no máximo, 25 tentativas, pois o texto não é o original, por isso uma possibilidade é excluída, ou seja, quando $k = 0$, STALLINGS [21] chama esse método de decodificação utilizando a "força bruta".

O método de César mais geral é aquele em que efetuamos uma permutação arbitrária das 26 letras do alfabeto. Como existem 26! permutações distintas de um conjunto de 26 elementos, existe uma grande quantidade de cifras distintas. Para tentar decodificar um texto utilizando a força bruta devemos descrever os 26! textos distintos (um para cada permutação) e, seguramente, um desses textos terá a mensagem original. Na prática, este método é totalmente inviável, pois existem mais de 400.000.000.000.000.000.000.000.000 rearranjos do alfabeto original e, por isso, durante séculos este foi o método mais eficiente para codificar mensagens.

1.3 Criptoanalistas árabes

No século IX um matemático árabe, que trabalhava na "Casa da sabedoria de Bagdad", escreveu um livro manuscrito sobre o deciframento de mensagens criptográficas. O nome deste árabe é Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi, mas nos referimos simplesmente como Al-Kindi, conhecido como "o filósofo dos árabes". Autor de 290 livros sobre Medicina, Astronomia, Matemática, Linguística e Música, seu maior tratado só foi descoberto em 1987, no Arquivo Otomano Sulaima-

niyyah em Istambul, e se intitula: "*Um manuscrito sobre a decifração de mensagens criptográficas*".

Figura 1.4: Imagem artística de Al-Kindi
Fonte: http://muslimheritage.com/topics/default.cfm?ArticleID=691

Nesse livro é descrito o método da análise das frequências, o qual permite "romper" todas as cifras de substituição monoalfabéticas, ou seja, cifras de substituição a partir das quais cada letra do texto claro é substituída por outra letra no texto cifrado, de forma constante.

O método de Al-Kindi consiste em decifrar uma mensagem codificada, quando se conhece o idioma. Para isso, deve-se encontrar um texto diferente, na mesma língua, suficiente longo para preencher uma página e fazer essa análise das frequências. A letra que aparecer com maior frequência no texto é chamada de "primeira", a segunda mais frequente recebe o nomes e "segunda" e assim por diante, até todas as letras do texto serem contadas. Em seguida, examina-se o texto cujo deciframento será feito e os símbolos também são classificados com relação à frequência. O símbolo que aparecer com maior frequência é substituído pela "primeira", o segundo símbolo mais frequente é substituído pela "segunda" e assim por diante, até todos os símbolos serem convertidos.

Para poder aplicar a análise das frequências, precisamos conhecer qual é a porcentagem de aparição de cada letra nos textos de uma determinada língua. A frequência média de cada letra na Língua Portuguesa está apresentada na tabela a seguir:

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

Figura 1.5: Frequência das letras na língua portuguesa

Para decodificar o texto cifrado, basta contar a frequência de cada símbolo no texto para descobrir a que letra correspondem os símbolos mais frequentes. Isto geralmente é suficiente para quebrar o código e ler toda a mensagem. Observe, entretanto, que este método de quebra do código só funciona bem se a mensagem for longa. É fácil escrever uma mensagem curta cuja contagem de frequência seja totalmente diferente da contagem de frequência média do português. Por exemplo, na frase "O rato roeu a roupa do rei de Roma" a letra R aparece 5 vezes e a letra A aparece 4 vezes. De um modo geral, textos curtos têm maior probabilidade de se desviarem significativamente das frequências padrão; caso haja menos de cem letras, a decodificação será muito difícil.

Por exemplo, MALAGUTTI [13] apresenta o seguinte texto para ser decodificado:

urtklm tr dqapuakcftr ltr iasqtr aj nmqsuouar lacfdqa t jakrtoaj tetfxm a cmjniasa t steait ntqt qaofrsqtq tr ruersfsufcmar akcmksqtltr

Analisando a frequência de cada letra no texto, temos:

Letra	Frequência(%)	Letra	Frequência(%)
a	13,91	n	2,61
b	0,00	o	2,61
c	4,35	p	0,87
d	0,87	q	7,83
e	2,61	r	11,30
f	5,22	s	6,96
g	0,00	t	15,65
h	0,00	u	5,22
i	2,61	v	0,00
j	3,48	w	0,00
k	4,35	x	0,87
l	3,48	y	0,00
m	5,22	z	0,00

Figura 1.6: Frequência das letras no texto cifrado

Note que a letra que aparece com maior frequência é a letra t e há uma grande possibilidade de ela ser a letra A no texto original. A segunda letra que aparece na segunda colocação das frequência é a letra a e, como fizemos anteriormente, há uma grande possibilidade de ela ser a letra E. Vale a pena ressaltar que isso é apenas um estudo, ou seja, estamos fazendo uma especulação. Substituindo essas informações no texto, temos:

UrAklm Ar dqEpuEkcfAr lAr iEsqAr Ej nmqsuouEr lEcfdqE A jEkrAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofrsqAq Ar ruersfsufcmEr EkcmksqAlAr.

Diferenciamos em maiúsculas as letras do alfabeto original e minúsculas as do alfabeto cifrado. A letra r é a terceira letra com maior frequência, então ela pode estar codificando as letras O,R ou S. Vamos substituir essa letra por cada uma das letras que estamos especulando para ver se algum texto faz sentido.

Substituindo a letra r por O:

UOAklm AO dqEpuEkcfAO lAO iEsqAO Ej nmqsuouEO lEcfdqE A jEkOAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofOsqAq AO OueOsfsufcmEO EkcmksqAlAO.

Substituindo r por R, temos:

URAklm AR dqEpuEkcfAR lAR iEsqAR Ej nmqsuouER lEcfdqE A jEkRAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofRsqAq AR RueRsfsufcmER EkcmksqAlAR.

Finalmente, substituindo r por S, a mensagem fica:

USAklm AS dqEpuEkcfAS lAS iEsqAS Ej nmqsuouES lEcfdqE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofSsqAq AS SueSsfsufcmES EkcmksqAlAS.

Diante das três possibilidades, a que mais faz sentido é a terceira, ou seja, quando trocamos r por S. A quarta letra é a q, então, provavelmente ela será O ou R. Assim:

Se a letra q foi substituída por O, obtemos:

USAklm AS dOEpuEkcfAS lAS iEsOAS Ej nmOsuouES lEcfdOE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nAOA OEofSsOAO AS SueSsfsufcmES EkcmksOAlAS.

Se a letra q foi substituída por R,

USAklm AS dREpuEkcfAS lAS iEsRAS Ej nmRsuouES lEcfdRE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nARA REofSsRAR AS SueSsfsufcmES EkcmksRAlAS.

Na primeira opção temos algo que se torna absurdo na Língua Portuguesa. Isso se dá pelo fato da palavra **nAOA** aparecer no texto. Logo, iremos optar pela segunda possibilidade. Note que a palavra **Ej** pode ser EM, ou seja, a letra j pode ter sido substituída pela letra M no momento da codificação. Assim:

USAklm AS dREpuEkcfAS lAS iEsRAS EM nmRsuouES lEcfdRE A MEkSAoEM AeAfxm E cmMniEsE A sAeEiA nARA REofSsRAR AS SueSsfsufcmES EkcmksRAlAS.

Realmente isso faz muito sentido, pois apareceu a palavra **MEkSAoEM**, haja vista, claramente, que ela representa a palavra MENSAGEM, ou seja, no texto cifrado, a letra k foi trocada por N e a letra o foi substituída por G. Analisando mais uma vez o texto:

USANlm AS dREpuENcfAS lAS iEsRAS EM nmRsuGuES lEcfdRE A MENSAGEM AeAfxm E cmMniEsE A sAeEiA nARA REGfSsRAR AS SueSsfsufcmES ENcmNsRAlAS.

Podemos observar que apalavra **lEcfdRE** deve ser DECIFRE, **REGfSsRAR** deve ser REGISTRAR e **USANlm** deve ser USANDO. Desta forma, percebemos que l é D, f é I, d é F, s é T e m é O.

USANDO AS FREpuENCIAS DAS iETRAS EM nORTuGuES DECIFRE A MENSAGEM AeAIxO E COMniETE A TAeEiA nARA REGISTRAR AS SueSTITuICOES ENCONTRADAS.

Note que **SueSTITuICOES** é SUBSTITUIÇÕES, **FREpuENCIAS** é FREQUÊNCIAS, **iETRAS** é LETRAS. Assim, u é U, e é B, p é Q e i é L. Logo:

USANDO AS FREQUENCIAS DAS LETRAS EM nORTUGUES DECIFRE A MENSAGEM ABAIxO E COMnLETE A TABELA nARA REGISTRAR AS SUBSTITUICOES ENCONTRADAS.

Finalmente, note que a letra n é a letra P e a letra x é X. Logo chegamos a mensagem original:

USANDO AS FREQUENCIAS DAS LETRAS EM PORTUGUES DECIFRE A MENSAGEM ABAIXO E COMPLETE A TABELA PARA REGISTRAR AS SUBSTITUICOES ENCONTRADAS.

Note que não foi tão difícil descriptografar a mensagem, visto que foi possível manter a estrutura da Língua Portuguesa, só omitindo acentos e trocando ç por c. Poderíamos ter juntado os artigos, preposições entre outros nas próximas palavras. Isso já tornaria o texto mais difícil de ser decifrado. Apesar de ser um método que requer muito tempo para ser decifrado, os chamados "criptoanalistas" foram evoluindo nos seus métodos tanto no mundo árabe quanto na Europa, destruindo a segurança deste método, ou seja, qualquer um que enviasse uma mensagem codificada tinha que aceitar a possibilidade de que um especialista inimigo poderia interceptá-la e conhecer os segredos mais preciosos.

1.4 A cifra de Vigenère

O italiano Leon Battista Alberti (1404 - 1472) nasceu em Génova e foi pintor, compositor, poeta, filósofo e, sobretudo, conhecido como arquiteto. Alberti teve grande destaque na Renascença, pois, em meados de 1440, ele escreveu um ensaio do que acreditava ser um novo tipo de cifra. Alberti propôs a utilização de dois ou mais alfabetos cifrados, usados alternadamente, para confundir os criptoanalistas. Observe:

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado 1	X	F	O	R	I	H	J	K	N	G	M	E	Z	B	Y	P	A	L	Q	D	C	T	U	S	V	W
Alfabeto cifrado 2	F	R	O	A	L	M	E	G	H	I	J	K	N	P	Y	Z	B	C	D	Q	S	T	U	V	W	X

O avanço principal do método de Alberti consiste em não permitir que a mesma letra do texto original apareça como uma única letra do alfabeto cifrado, ou seja, ele é o primeiro personagem que se tem notícia que utilizou a cifra de substituição polialfabética. Nesse método ele utilizava alternadamente dois alfabetos de César, causando uma enorme dificuldade para os criptoanalistas, pois a análise das frequências era insuficiente para decifrar as mensagens. Ele não conseguiu desenvolver a sua ideia num sistema completo de cifragem, sistema que fora aperfeiçoado por Johannes Trithemius (1462 - 1516), depois pelo italiano Giovanni Porta (1541 - 1615), e, por fim, pelo nosso próximo personagem: Blaise de Vigenère (1523 - 1596).

Segundo TÁBARA [22], Blaise de Vigenère foi um diplomata francês do século XVI. Em razão da diplomacia, entrou em contato com o mundo da criptografia e,

quando encerrou sua carreira, dedicou grande parte do seu tempo a esta arte. Em 1586, publicou o livro *Traité des chiffres où secrètes manières d'escrire* no qual expôs seu novo método de criptografar mensagens, baseado na cifra de César, a partir das ideias de Alberti.

Vamos imaginar que ciframos a primeira letra utilizando o método de César, deslocando três unidades; a segunda letra, deslocando 7; e assim por diante, deslocando arbitrariamente. Este método resiste à análise de frequências, pois cada letra se codifica de muitas formas distintas. Mas, se trocarmos arbitrariamente a cifra de César, nem nós mesmos seremos capazes de decifrá-la. Para não se perder na própria encriptação, Vigenère utilizou o conceito de *palavra chave*. Vamos imaginar que nos dão a chave de **VIGENERE**. Se quisermos cifrar uma mensagem com esta chave procederemos do seguinte modo: para cifrar a primeira letra, utilizamos o alfabeto de César que começa por V, ou seja, quando $k = 21$ na cifra de César; para cifrar a segunda letra, utilizamos o alfabeto que começa por I, isto é, quando $k = 8$; a terceira com G, quando $k = 6$ e assim por diante, até chegar à oitava letra. Para a nona letra voltamos a utilizar o alfabeto na letra V. Neste exemplo, utilizamos seis alfabetos diferentes. Caso sejam escolhidas outras palavras (ou frases) chave, podemos variar muito o resultado do criptograma.

Figura 1.7: Blaise de Vigenère
Fonte: http://algorithinking.blogspot.com.br/2011/07/vigenere-cipher.html

Para a realização prática deste método utiliza-se uma tabela que contém todos os alfabetos possíveis de serem utilizados. Para complicar ainda mais os criptoanalistas do método de Vigenère, basta elencar chaves bem mais longas e com poucas letras repetidas. Quanto mais alfabetos empregarmos, mais difícil será realizar a criptoanálise.

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

Figura 1.8: Cifra de Vigenère

Na cifra de Vigenère, uma linha diferente do quadrado é utilizada para codificar letras diferentes da mensagem. Para decifrar a mensagem, o destinatário precisa saber que linha do quadrado de Vigenère foi usada para a cifragem, e, para isso, utiliza-se uma palavra-chave. Por exemplo, vamos utilizar a palavra-chave **ROMA** para o texto **INVADIR A CIDADE**. A letra "I" será substituída pela letra correspondente no alfabeto que começa pela letra "R", ou seja, a letra "Z"; a letra "N" será substituída pela letra correspondente no alfabeto que começa pela letra "O", ou seja, a letra "B" e assim por diante, até chegarmos ao texto cifrado **ZBHAUWD R OIUOPE**.

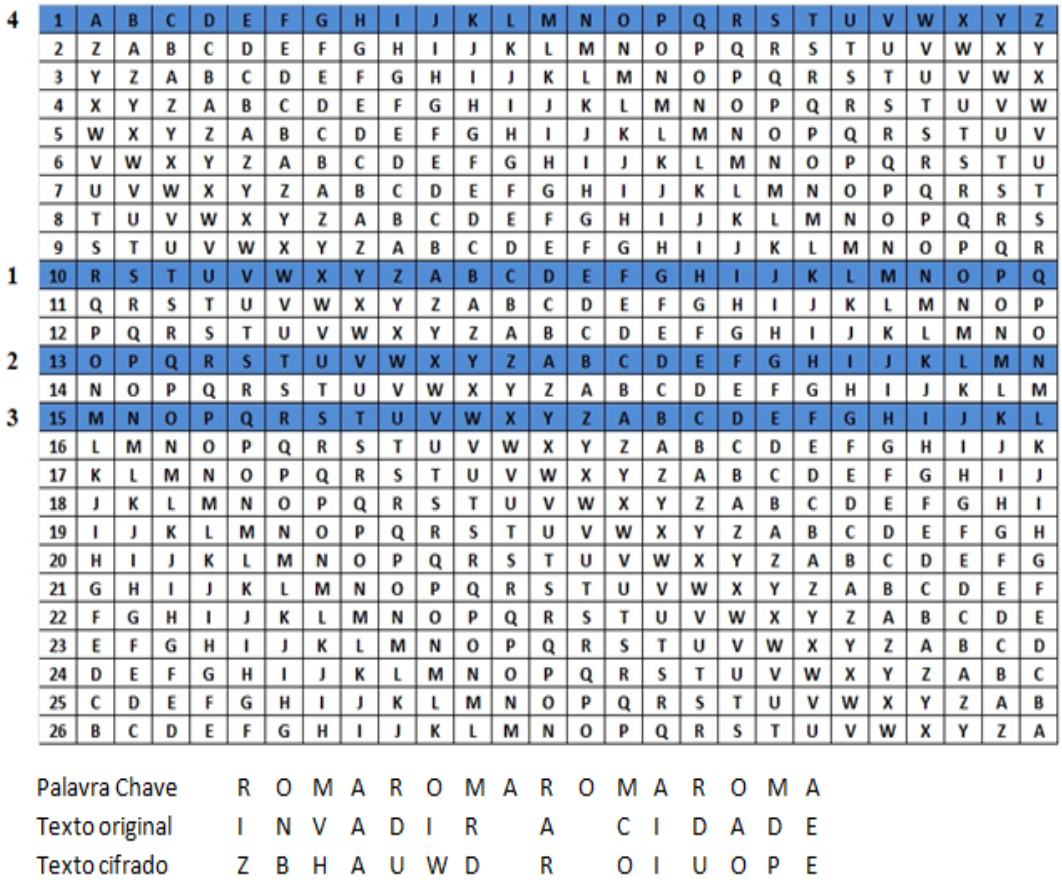


Figura 1.9: Cifragem da frase "invadir a cidade"

A aplicação deste método no computador ou no seu estudo matemático é feita utilizando-se aritmética modular. A partir da palavra chave, aplicamos os números associados e cada letra do texto original deve adicionar, modularmente, as letras da chave. Apesar da potência deste método, ele veio a ser utilizado muito tarde, devido à complexidade do mesmo. Além disso ele resistiu durante muitos séculos às tentativas dos criptoanalistas quebrá-lo, tanto que chegou a ser conhecido como "*Le chiffre indéchiffrable*" que significa a cifra indecifrável.

1.5 Máquinas de cifragem

De acordo com SINGH [20], a primeira máquina criptográfica que se tem registro foi inventada no século XV pelo arquiteto italiano Leon Alberti, um dos criadores da cifra polialfabética. A máquina era composta de dois discos de cobre. O maior era fixo e o outro, o menor, era móvel. Cada disco continha o alfabeto ao longo da sua borda; no disco maior, o alfabeto original em letras maiúsculas e, no menor, o alfabeto cifrado em letras minúsculas. O disco menor poderia ser girado e, com isso,

poderia ser usado para cifrar uma mensagem utilizando a cifra de César. Embora fosse um dispositivo muito básico, o disco de cifras possibilitava o trabalho de cifragem e foi utilizado por séculos. A figura 1.9 mostra o disco utilizado na Guerra Civil americana.

Figura 1.10: Disco de cifras utilizado na guerra civil americana
Fonte: http://www.cryptomuseum.com/crypto/usa/ccd/index.htm

Em 1918 o inventor alemão Arthur Scherbius e seu amigo Richard Ritter fundaram uma empresa, a Scherbius&Ritter. Um de seus projetos era substituir os sistemas de Criptografia inadequados, usados na Primeira Guerra Mundial, a partir da troca de cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. Engenheiro eletricista de formação, ele patenteou uma invenção de uma máquina de cifra mecânica, basicamente uma versão elétrica do disco de Alberti, mais tarde vendida como a máquina Enigma.

Em 1925, Scherbius produziu a Enigma em grande escala, pois as autoridades alemãs acreditavam na segurança absoluta que ela proporcionava. Trinta mil máquinas foram adquiridas e utilizadas, nas duas décadas seguintes, pelo exército alemão. A Enigma era extremamente forte e, por aproximadamente treze anos, os criptoanalistas franceses e britânicos acreditaram que mensagens cifradas por ela eram indecifráveis sem o conhecimento da chave. Até que após um árduo trabalho, o criptoanalista Alan Turing conseguiu quebra-la na primeira metade da década de 40. Isso foi feito em Bletchley Park, onde ficava a sede da Escola de Cifras e Códigos do Governo (GC&CS) da Inglaterra, a partir do desenvolvimento dos criptoanalistas poloneses. Essa identificação se deu pelo desenvolvimento de máquinas chamadas "bombas". A quebra das cifras da Enigma deu aos Aliados uma vantagem fundamental, que, de acordo com historiadores, encurtou a guerra por mais dois anos, salvando muitas vidas.

Figura 1.11: Enigma - Maquina alemã
Fonte: http://www.ilord.com/enigma.html

Outro aparelho que tinha como finalidade decifrar mensagens foi desenvolvido na Inglaterra com base nas ideias de Turing. Denominado de "Colossus", foi utilizado para decifrar as codificações feitas pela máquina Lorenz, empregada nas comunicações de Hitler e seus generais. O Colossus apresentou duas vantagens em relação às bombas: a primeira era que ele era constituído de válvulas eletrônicas bem mais rápidas do que os antigos eletromecânicos utilizados nas bombas e a segunda é o fato de serem programáveis, ou seja, esse fato fez com que ele seja considerado o precursor do computador moderno. em razão disto, podemos dizer que o computador teve origem na criptoanálise.

1.6 Criptografia nos computadores

1.6.1 Criptografia simétrica

A criptografia simétrica (ou de chave privada) transforma um texto claro em um texto cifrado, usando uma chave secreta e um algoritmo de criptografia. A partir da mesma chave e com o auxílio de um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado. Ela é conhecida também por secret-key ou symmetric-key encryption. Esta chave pode ser uma palavra, frase ou uma sequência aleatória de números e/ou símbolos. O tamanho da chave é medido em bits e, por regra, quanto maior for a chave, mais seguro será o documento codificado. O esquema dessa criptografia pode ser resumido na figura 1.12.

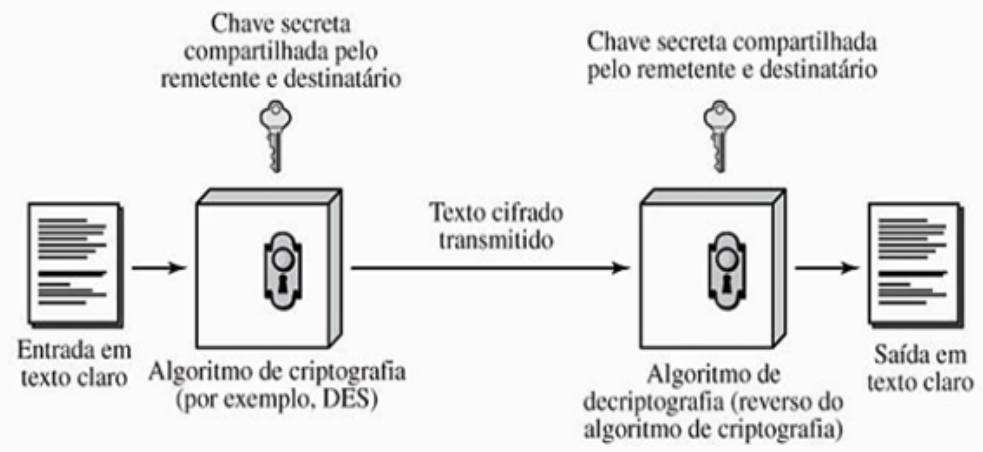


Figura 1.12: Modelo simplificado de Criptografia simétrica
Fonte: STALLINGS [21], p. 18

Para um remetente e um destinatário se comunicarem utilizando este método, eles têm que concordar quanto ao valor da chave e têm que manter isso em segredo. Se eles estão em localizações físicas diferentes, deverão confiar em um mensageiro, telefone, SMS, e-mail, pessoalmente ou outro meio seguro de comunicação para prevenir a revelação da chave secreta antes da transmissão. Como fazer que destinatário receba a chave sem alguém interceptá-la? Veremos mais adiante que isto se tornou um problema quase axiomático na informática, conhecido como "o problema da troca de chaves".

Os principais algoritmos de chave privada são, conforme OLIVEIRA [15]:

DES - O Data Encryption Standard (DES) foi o algoritmo simétrico mais disseminado no mundo, até a padronização do AES. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações, seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na internet.

AES - O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo NIST em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão pelo governo dos Estados Unidos, é um dos algoritmos mais populares, desde 2006, usado para Criptografia de chave simétrica, sendo considerado como o padrão substituto do DES. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.

IDEA - O International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para Criptografia de e-mail pessoal mais disseminado no mundo.

Outros algoritmos de chave privada são 3DES, Blowfish, Twofish, RC4 e CAST.

1.6.2 Criptografia assimétrica

A criptografia assimétrica (ou de chave pública) transforma um texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado. A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. Para ilustrar essa situação, vamos utilizar o esquema dos cadeados em que Alice deseja enviar uma carta a Bob. Bob distribui milhares de cadeados abertos iguais pelas agências de correios do mundo todo, mas somente ele tem a chave que abre esses cadeados. Assim, Alice vai até uma agência dos correios, pede o cadeado referente a Bob e tranca a carta com esse cadeado. Note que ela não pode mais abrir o cadeado, somente Bob pode fazer isso. Assim, mesmo que outra pessoa tente interceptar a mensagem, somente Bob pode abri-lo.

Esse modelo de criptografia foi criado na década de 70 pelo matemático Clifford Cocks, que trabalhava no serviço secreto inglês, porém, como o seu trabalho não foi divulgado, a primeira evidência pública foi em 1976 com Diffie e Hellman. Eles mudaram os rumos da criptografia desenvolvendo a criptografia assimétrica na tentativa de solucionar o problema da troca de chaves. Conforme foi dito por Diffie: "Afinal, qual é a vantagem de desenvolver criptossistemas impenetráveis, se seus usuários forem forçados a compartilhar suas chaves com um Centro de Distribuição de Chaves - CDC - que pode estar sujeito a roubo ou suborno?". A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Deve-se destacar que na criptografia assimétrica, o tempo de processamento de mensagens é muitas vezes maior do que a criptografia simétrica, dando maior dificuldade para o criptoanalista que deseja decifrar a mensagem. A figura 1.13 mostra, de forma simplificada, a criptografia assimétrica.

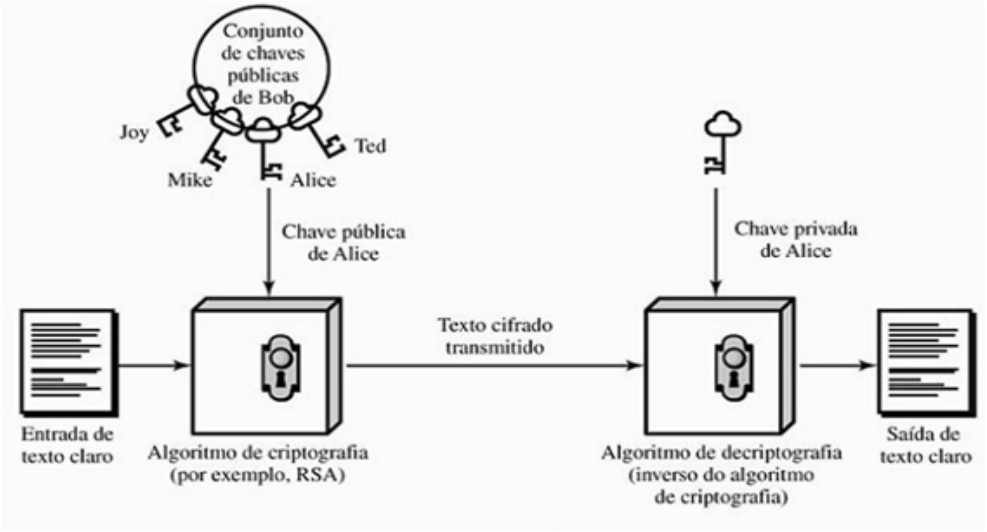


Figura 1.13: Modelo simplificado de Criptografia assimétrica
Fonte: STALLINGS [21], p. 184

Os principais algoritmos de chave pública, conforme OLIVEIRA [15] são:

RSA - É um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no Massachusetts Institute of Technology (MIT). Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes.

ElGamal - É outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.

Diffie-Hellman - Também baseado no problema do logaritmo discreto; trata-se do criptossistema de chave pública mais antigo ainda em uso. O conceito de

chave pública, aliás, foi introduzido pelos autores deste criptossistema em 1976. O problema desse método é que ele não permite ciframento, o sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.

Curvas Elípticas - Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie-Hellman e o ElGamal podem ser implementados em curvas elípticas sobre corpos finitos.

No nosso trabalho vamos focar como funciona a criptografia utilizando o protocolo Diffie-Hellman para a troca de chaves. Para isso devemos ter conhecimento sobre Grupos, assunto estudado na disciplina de Álgebra Abstrata nas universidades, para compreendermos melhor o problema do logaritmo discreto.

Capítulo 2

Das relações binárias aos logaritmos discretos

Neste capítulo vamos estudar várias definições e teoremas relacionados à Álgebra. Este estudo será feito para que possamos entender, nos demais capítulos, o protocolo da troca de chaves de Diffie-Hellman. Mesmo que a maioria desses assuntos não estejam presentes no currículo do ensino básico, o Professor de Matemática pode fazer algumas adaptações nos resultados para que estes fiquem mais acessíveis aos alunos. As referências utilizadas para a elaboração deste capítulo foram ARAÚJO [2], DOMINGUES Domingues-Iezzi, FIGUEIREDO [9], FILHO [10], HEFEZ [11] e KAKUTA [12], ORE [16], SHOKRANIAN [19], SANTOS [18] e STALLINGS [21].

2.1 Relações binárias

Definição 2 *Dados dois elementos x e y, chama-se par ordenado um terceiro elemento que se indica por (x, y), em que o elemento x é chamado de primeira coordenada e o elemento y é chamado de segunda coordenada*

Definição 3 *Dados dois conjuntos não vazios A e B, chama-se produto cartesiano de A por B, denotado por $A \times B$, o conjunto formado por todos os pares ordenados (x, y), onde $x \in A$ e $y \in B$.*

$$A \times B = \{(x, y) \mid x \in A \text{ e } y \in B\}$$

Exemplo: Considere os conjuntos $A = \{-1, 0, 1\}$ e $B = \{1, 2, 3, 4\}$.

a) $A \times B = \{(-1,1), (-1,2), (-1,3), (-1,4), (0,1), (0,2), (0,3), (0,4), (1,1), (1,2), (1,3), (1,4)\}$

b) $B \times A = \{(1,-1), (1,0), (1,1), (2,-1), (2,0), (2,1), (3,-1), (3,0), (3,1), (4,-1), (4,0), (4,1)\}$

Definição 4 *Dados dois conjuntos não vazios A e B, chama-se relação binária ou simplesmente relação de A em B a todo subconjunto R do produto cartesiano $A \times B$.*

$$R \text{ é relação de } A \text{ em } B \Leftrightarrow R \subset A \times B$$

O conjunto A recebe o nome de *conjunto de partida* e o conjunto B recebe o nome de *conjunto de chegada*. Para indicar que $(x, y) \in \mathbb{R}$, escrevemos xRy e lemos "x erre y" ou "x se relaciona com y por R". Caso $(x, y) \notin R$, escrevemos $x \not R y$ e lemos "x não erre y" ou "x não se relaciona com y por R".

Exemplo: Com base no exemplo anterior, temos alguns exemplos de relações:

$$\begin{aligned} R_1 &= \{(-1,1),(-1,2),(0,2),(1,3)\} \\ R_2 &= \{(0,1),(0,2),(0,3)\} \\ R_3 &= \{(1,4)\} \end{aligned}$$

2.2 Domínio, imagem e relação inversa

Definição 5 *Seja R uma relação de A em B. Chama-se domínio de R e denota-se por $D(R)$ o subconjunto de A formado pelos elementos x para os quais existe algum y em B tal que xRy.*

$$D(R) = \{x \in A \mid \exists y \in B \text{ com } xRy\}$$

Exemplo: Utilizando as relações R_1, R_2 e R_3 utilizadas na seção anterior, temos que seus respectivos domínios são:

$$\begin{aligned} D(R_1) &= \{-1, 0, 1\} \\ D(R_2) &= \{0\} \\ D(R_3) &= \{1\} \end{aligned}$$

Definição 6 *Seja R uma relação de A em B. Chama-se imagem de R e denota-se por $Im(R)$ o subconjunto de B formado pelos elementos y para os quais existe algum x em A tal que xRy.*

$$Im(R) = \{y \in B \mid \exists x \in A \text{ com } xRy\}$$

Exemplo: Novamente utilizando R_1, R_2 e R_3, obtemos:

$$\begin{aligned} Im(R_1) &= \{1,2,3\} \\ Im(R_2) &= \{1,2,3\} \\ Im(R_3) &= \{4\} \end{aligned}$$

Definição 7 *Seja R uma relação de A em B. Chama-se relação inversa de R e denota-se por R^{-1} a seguinte relação de B em A:*

$$R^{-1} = \{(y,x) \in B \times A : \ (x,y) \in R\}$$

Exemplo: Dados os conjuntos $A = \{1,2,3\}$ e $B = \{-3,0,2\}$. A relação inversa de $R = \{(1,-3),(2,0),(3,2)\}$ em $B \times A$ é $R^{-1} = \{(-3,1),(0,2),(2,3)\}$.

Note que:

i) $D(R^{-1}) = Im(R)$

ii) $Im(R^{-1}) = D(R)$

iii) $(R^{-1})^{-1} = R$

Definição 8 *Quando $A = B$ e R é uma relação de A em B, diz-se que R é uma relação sobre A ou, ainda, R é uma relação em E.*

2.3 Relações de equivalência

Definição 9 *Uma relação R sobre um conjunto não vazio A é chamada relação de equivalência sobre A quando R é relexiva, simétrica e transitiva, ou seja, quando são verdadeiras as seguintes propriedades:*

i) *Se $x \in A$, então xRx (reflexiva)*

ii) *Se $x, y \in A$ e xRy, então yRx (simétrica)*

iii) *Se $x, y, z \in A$ e xRy e yRz, então xRz (transitiva)*

Quando R é uma relação de equivalência sobre um conjunto A, costumamos representar $(x, y) \in R$ (ou xRy) por

$$x \equiv y \bmod R \text{ ou } x \sim y \bmod R$$

Antes de irmos para o próximo exemplo, vamos utilizar uma definição equivalente a **definição 1** de congruência modular. Assim:

Definição 10 *Dados $a, b \in \mathbb{N}$ e m um número natural fixo, com $m > 1$, dizemos que a é congruente a b módulo m se, e somente se, m dividir a diferença $a - b$. Em símbolos:*

$$a \equiv b \ m \Leftrightarrow m \,|\, (a - b)$$

A prova da equivalência das duas definições é feita de maneira imediata.

Exemplo: A relação de congruência módulo m (em que $m \in \mathbb{Z}$ e $m > 1$) sobre $\mathbb{Z}$, é uma relação de equivalência, pois:

i) Se $x \in \mathbb{Z}$, então $x \equiv x \bmod m$

De fato, $a \equiv b$ m, pois $m \,|\, 0$.

ii) Se $x, y \in \mathbb{Z}$ e $x \equiv y \bmod m$, então $y \equiv x \bmod x$

Com efeito, se $m \,|\, (a-b)$, então m divide o negativo, ou seja, $m \,|\, -(a-b)$, ou ainda, $m \,|\, b - a$.

iii) Se $x, y, z \in \mathbb{Z}$ e $x \equiv y \bmod m$ e $y \equiv z \bmod m$, então $x \equiv z \bmod m$

Note que $m \,|\, (a - b)$ e $m \,|\, (b - c)$, então $m \,|\, (a - b) + (b - c)$, ou seja, $m \,|\, (a - c)$.

2.4 Classes de equivalência e conjunto quociente

Definição 11 *Seja R uma relação de equivalência sobre um conjunto A. Dado $a \in A$, chama-se classe de equivalência determinada por a módulo R (ou segundo R) e indica-se por $[a]$, o subconjunto de A constituído por todos os elementos x tais que xRa,*

$$[a] = \{x \in A \mid xRa\} \ \ ou \ \ [a] = \{x \in A \mid x \equiv a \ mod \ R\}$$

Neste caso, o elemento $a \in [a]$ é chamado um representante de classe $[a]$.

Exemplo: Seja $A = \{x \in \mathbb{Z} : |\, x \,| \leq 10\}$ e consideremos a relação R sobre A definida por:

$$aRb \Leftrightarrow a^2 + 2a = b^2 + 2b$$

Note que R é uma relação de equivalência, pois:

i) aRa, pois $a^2 + 2a = a^2 + 2a$, $\forall a \in A$.

ii) $aRb \Leftrightarrow a^2 + 2a = b^2 + 2b \Leftrightarrow b^2 + 2b = a^2 + 2a \Leftrightarrow bRa$.

iii) aRb e $bRc \Leftrightarrow a^2 + 2a = b^2 + 2b$ e $b^2 + 2b = c^2 + 2c \Rightarrow a^2 + 2a = c^2 + 2c \Leftrightarrow aRc$.

Proposição 1 *Seja R uma relação de equivalência sobre A e sejam $a, b \in A$. As seguintes proposições são equivalentes:*

i) aRb

ii) $a \in [b]$

iii) $b \in [a]$

iv) $[a] = [b]$

Demonstração: Devemos provar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.
$(i) \Rightarrow (ii)$: É decorrência da definição de classe de equivalência.
$(ii) \Rightarrow (iii)$: Como $a \in [b]$, então aRb. Daí, pela simetria de R, bRa e, portanto, $b \in [a]$.
$(iii) \Rightarrow (iv)$: Por hipótese, $b \in [a]$, ou seja, bRa. Logo, aRb. Temos que provar que $[a] \subset [b]$ e $[b] \subset [a]$.
De fato, para provar a primeira das inclusões, seja $x \in [a]$. Então, xRa e, levando em conta que aRb, concluímos, por transitividade de R, que xRb. Assim, $x \in [b]$ e $[a] \subset [b]$.
A prova de $[b] \subset [a]$ é feita de modo análogo.
$(iv) \Rightarrow (i)$: Como $a \in [a]$ e $b \in [b]$, os conjuntos $[a]$ e $[b]$ não são vazios. Considere um $x \in [a] = [b]$. Então, xRa e xRb. Assim, pela simetria em R, valem aRx e xRb. A transitividade em R garante, então, que aRb. ■

Nota: A propriedade (ii) nos motra que se $x \in [a]$, então $[x] = [a]$, isto é, todo elemento de uma classe de equivalência é um representante desta classe.

Exemplo: Utilizando a relação de congruência módulo m ($m \in \mathbb{N}$ e $m > 1$) sobre $\mathbb{Z}$, as classes de equivalência $[0], [1], [2], [3], ..., [m-1]$ são denominadas *classes residuais módulo m* e são dadas por

$$\begin{aligned}
[0] &= \{x \in A \mid x \equiv 0 \bmod m\} \\
[1] &= \{x \in A \mid x \equiv 1 \bmod m\} \\
[2] &= \{x \in A \mid x \equiv 2 \bmod m\} \\
[3] &= \{x \in A \mid x \equiv 3 \bmod m\} \\
&\vdots \\
[m-1] &= \{x \in A \mid x \equiv m-1 \bmod m\}
\end{aligned}$$

Note que paramos em $[m-1]$, pois $[m] = [0]$.

Definição 12 *O conjunto de todas as classes de equivalência módulo R será indicado por A/R e chamado conjunto quociente de A por R, termo que justifica o fato que R "particiona" o conjunto A em subconjuntos não vazios e disjuntos.*

Exemplo: Note que podemos particionar o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, em que cada um deles possuem os números inteiros que possuem o mesmo resto na divisão por m, ou seja, R é a operação $\equiv \bmod m$. Assim, podemos particionar o conjunto $\mathbb{Z}$ utilizando todos os conjuntos de classes residuais módulo m.

$$\mathbb{Z}/R = \{[0], [1], [2], [3], ..., [m-1]\}$$

Denotaremos o conjunto quociente $\mathbb{Z}/R$, em que R é a operação $\equiv \bmod m$ por $\mathbb{Z}_m$.

Definição 13 *Dadas duas classes residuais $[a]$ e $[b] \in \mathbb{Z}_m$ chama-se soma $[a] + [b]$ a classe $[a+b]$.*

Definição 14 *Dadas duas classes residuais $[a]$ e $[b] \in \mathbb{Z}_m$ chama-se produto $[a] \cdot [b]$ a classe $[a \cdot b]$.*

Evidentemente, é necessário garantir que estas operações estão *bem definidas* no sentido de que uma soma ou um produto de classes residuais independem do particular representante da classe que foi utilizado. Isto significa que devemos provar que se $x \in [a]$ e $y \in [b]$, então $[x] + [y] = [a] + [b]$ e $[x] \cdot [y] = [a] \cdot [b]$. Dessa forma, se $x \in [a]$ e $y \in [b]$ implicam que $x \equiv a \bmod m$ e $y \equiv b \bmod m$ e, então, é imediato que, $x + y \equiv a + b \bmod m$ e $x \cdot y \equiv a \cdot b \bmod m$.

Exemplo: Vamos construir as tabelas da adição e multiplicação em $\mathbb{Z}_4$.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

x	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

2.5 Funções

Definição 15 *Seja f uma relação de A em B. Dizemos que f é uma função de A em B quando*

i) $D(f) = A$;

ii) *Dado $a \in D(f)$, existe um único elemento $b \in B$ tal que $(a, b) \in f$.*

Se f é uma função de A em B, vamos escrever $b = f(a)$ para denotar que $(a, b) \in f$ e $f : A \to B$ será uma maneira simbólica de dizermos que f é uma função de A em B. O conjunto B será chamado de *contradomínio* de f.

Definição 16 *Sendo A um conjunto não vazio, toda função $f : A \times A \to A$ recebe o nome de operação sobre A ou lei de composição interna em A.*

Exemplo: A função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $f(x, y) = x^y$ é a operação de potenciãção sobre $\mathbb{N}$.

Definição 17 *Seja $\otimes$ uma operação sobre um conjunto não vazio A. Seja B um subconjunto não-vazio de A. Dizemos que B é uma parte fechada de A para a operação $\otimes$ se, e somente se, temos*

$$x \in B \text{ e } y \in B \Rightarrow x \otimes y \in B, \forall x, y \in B$$

2.6 Grupos

Definição 18 *Seja G um conjunto não vazio e $\otimes : G \times G \to G$ uma operação. Dizemos que $(G, \otimes)$ é um grupo se satisfaz as seguintes condições:*

i) *A operação é associativa:* $a \otimes (b \otimes c) = (a \otimes b) \otimes c, \forall a, b, c \in G$;

ii) *Existe um elemento neutro:* $\exists e \in G$ *tal que* $a \otimes e = e \otimes a = a, \forall a \in G$;

iii) *Existência do elemento simétrico:* $\forall a \in G, \exists a' \in G \mid a \otimes a' = a' \otimes a = e$.

Da definição de grupos seguem algumas propriedades imediatas:

- A unicidade do elemento neutro de $(G, \otimes)$;
- A unicidade do simétrico de cada elemento de G;
- Se e é o elemento neutro, então $e' = e$;
- $(a')' = a$ para qualquer que seja $a \in G$;
- $(a \otimes b)' = b' \otimes a'$;
- Todo elemento de G é regular para a operação $\otimes$, ou seja, vale a "lei do corte":

$$a \otimes x = a \otimes y \Rightarrow x = y.$$

Definição 19 *Dizemos que um grupo* $(G, \otimes)$ *é abeliano ou comutativo se a operação* $\otimes : G \times G \to G$ *é comutativa, isto é,*

$$a \otimes b = b \otimes a, \forall a, b \in G.$$

Caso a operação de um grupo seja representada pelo símbolo $+$, então a identidade do grupo é chamada zero, o inverso de um elemento a é denotado por $-a$ e o grupo é dito *grupo aditivo*. Por outro lado, se a operação é representada pelo símbolo $\times$, então a identidade do grupo é chamada um, o inverso de um elemento a é a^{-1} e o grupo é chamado de *grupo multiplicativo*.

Definição 20 *Um grupo finito é um grupo* $(G, \otimes)$ *no qual o conjunto* G *é finito. O número de elementos de* G *denotado por* $o(G)$ *é chamado de ordem do grupo* G.

Para representar todos os elementos de um grupo finito costuma-se utilizar a tabela (ou tábua) da operação associada ao grupo. A primeira linha da tabela é chamada de *linha fundamental* e a primeira coluna à esquerda é chamada de *coluna fundamental*. Por exemplo, observe a tabela do grupo $(G, \otimes)$, em que $G = \{g_1, g_2, g_3, ..., g_n\}$.

$\otimes$	g_1	...	...	g_i	...	g_j	...	...	g_n
g_1	$g_1 \otimes g_1$	...	...	$g_1 \otimes g_i$	...	$g_1 \otimes g_j$	...	...	$g_1 \otimes g_n$
...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...
g_i	$g_i \otimes g_1$	...	...	$g_i \otimes g_i$	...	$g_i \otimes g_j$	...	...	$g_i \otimes g_n$
...	...	...	...	...	...	...	...	...	...
g_j	$g_j \otimes g_1$	...	...	$g_j \otimes g_i$	...	$g_j \otimes g_j$	...	...	$g_j \otimes g_n$
...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...
g_n	$g_n \otimes g_1$	...	...	$g_n \otimes g_i$	...	$g_n \otimes g_j$	...	...	$g_n \otimes g_n$

Observe que

- A operação $\otimes$ é comutativa se a tabela é simétrica em relação a diagonal principal;
- Existe um elemento neutro, se existirem uma linha e uma coluna idênticas às fundamentais;
- Seja L_i a linha iniciada por g_i. Se nesta linha o elemento neutro e, se situa na coluna C_j, então o simétrico de g_i' inicia na coluna C_j.

Exemplo: $G = \{-1, 1\}$ é um grupo em relação à multiplicação usual. Ele é um grupo finito de ordem 2. Observe a tabela:

x	-1	1
-1	1	-1
1	-1	1

Exemplo: Vamos construir as tabelas de $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ e $\mathbb{Z}_5$ com relação as operações de adição e multiplicação usuais.

Note que $(\mathbb{Z}_m, +)$ é sempre um grupo e o representamos como o *grupo aditivo das classes residuais módulo m*. Porém $(\mathbb{Z}_m, \times)$ só será o o *grupo multiplicativo das classes residuais módulo m* se, e somente se, m for um número primo. Note que $(\mathbb{Z}_4, \times)$ não é um grupo, pois [2] não possui elemento simétrico, mas $(\mathbb{Z}_2, \times)$, $(\mathbb{Z}_3, \times)$ e $(\mathbb{Z}_5, \times)$ são grupos.

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

x	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

x	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

x	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

x	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Definição 21 *Seja $(G, \otimes)$ um grupo. Diz-se que um subconjunto não vazio $H \subset G$ é um subgrupo de G se:*

i) *H é fechado para a operação $\otimes$ (isto é, se $a, b \in H$, então $a \otimes b \in H$);*

ii) *$(H, \otimes)$ também é um grupo.*

Note que se e indica o elemento neutro de G, então $\{e\}$ é um subgrupo de G. É imediato, também, que o próprio G é um subgrupo de si mesmo. Esses dois subgrupos, ou seja, $\{e\}$ e G, são chamados de subgrupos triviais de G.

Proposição 2 *Seja $(G, \otimes)$ um grupo. Para que um subconjunto não vazio $H \subset G$ seja um subgrupo de G, é necessário e suficiente que $(a \otimes b')$ seja um elemento de H sempre que a e b pertencerem a esse conjunto.*

Demonstração:

Vamos indicar por e e e_h, respectivamente, os elementos neutros de G e H. Como

$$e_h \otimes e_h = e_h = e_h \otimes e$$

e todo elemento do grupo é regular em relação a $\otimes$, então $e = e_h$.
Agora, vamos tomar um elemento $b \in H$ e indiquemos por b' e b'_h seus simétricos em G e H, respectivamente. Como,

$$b'_h \otimes b = e_h = e = b' \otimes b \Rightarrow b'_h = b'$$

Novamente pelo fato de todos os elementos do grupo serem regulares para sua operação. Finalmente, se $a, b \in H$, então $a \otimes b'_h \in H$, pois temos da hipótese que $(H, \otimes)$ é um grupo. Mas, $b'_h = b'$ e, portanto, $a \otimes b' \in H$.

Reciprocamente, sabemos que, por hipótese, H não é vazio, então podemos considerar um elemento $x_0 \in H$. Juntando esse fato a hipótese: $x_0 \otimes x'_0 = e \in H$. Considerando um elemento $b \in H$, da hipótese e da conclusão anterior segue que:

$$e \otimes b' = b' \in H$$

Mostremos agora que H é fechado para a operação $\otimes$. De fato, se $a, b \in H$, então levando em conta a conclusão anterior, $a, b' \in H$. Usando a hipótese, temos:

$$a \otimes (b')' = a \otimes b \in H$$

Agora, só falta mostrar a associatividade em H. De fato, se $a, b, c \in H$, então $a, b, c \in G$ e, portanto, $a \otimes (b \otimes c) = (a \otimes b) \otimes c$, já que essa propriedade vale em G.
■

Quando estivermos tratando de grupos multiplicativos, denotaremos ab para indicar que $a \cdot b$, então a condição de subgrupo dada pela proposição, em termos de grupos multiplicativos, apresenta-se assim:

$$a, b \in H \Rightarrow ab^{-1} \in H$$

Definição 22 *Seja G um grupo multiplicativo. Se $a \in G$ e m é um número inteiro, a potência m-ésima de a, ou potência de a de expoente m, é o elemento de G denotado por a^m e definido da seguinte maneira:*

i) *Se $m \geq 0$, por recorrência, da seguinte forma*

$$a^0 = e \text{ elemento neutro de } G$$

$$a^m = aa^{m-1}, \text{ se } m \geq 1$$

ii) *Se $m < 0$*

$$a^m = \left(a^{-m}\right)^{-1}$$

A definição por recorrência no caso $m \geq 0$ deve ser interpretada assim:

$$\begin{aligned} a^1 &= a^{1-1}a = a^0 a = ea = a \\ a^2 &= a^{2-1}a = a^1 a = aa \\ a^3 &= a^{3-1}a = a^2 a = aaa \end{aligned}$$

E assim por diante.

Exemplo: No grupo multiplicativo $\mathbb{Z}_5^*$ das classes de resíduos módulo 5, seja $a = [2]$. Então:

$$\begin{aligned} [2]^0 &= [1] \\ [2]^1 &= [2] \\ [2]^2 &= [2]\,[2] = [4] \\ [2]^3 &= [4]\,[2] = [3] \\ [2]^{-1} &= [3] \\ [2]^{-2} &= \left([2]^2\right)^{-1} = ([4])^{-1} = [4] \end{aligned}$$

Note que $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$ foi gerado pelas potências de $[2]$.

Proposição 3 *Seja G um grupo multiplicativo. Se m e n são números inteiros e $a \in G$, então:*

i) $a^m a^n = a^{m+n}$;

ii) $a^{-m} = (a^m)^{-1}$;

iii) $(a^m)^n = a^{mn}$.

Demonstração:

i) Inicialmente vamos demonstrar por indução sobre n o caso particular, em que $n \geq 0$ e $m + n \geq 0$. De fato,

$$n = 0 \Rightarrow a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$$

Logo, a propriedade é válida quando $n = 0$.

Agora, seja $r \geq 0$ e suponhamos que, para qualquer inteiro m tal que $m + r \geq 0$, seja válida a igualdade $a^{m+r} = a^m a^r$, ou seja, a nossa hipótese de indução, então:

$$a^m a^{r+1} \overset{*}{=} a^m (a^r a) = (a^m a^r) a \overset{**}{=} a^{m+r} a \overset{*}{=} a^{(m+r)+1}$$

Note que nas passagens assinaladas por $*$ usamos a definição de potência, o que é possível por que $r+1 \geq 1$ e $m+r+1 \geq 1$; e na passagem assinalada por $**$ usamos a hipótese de indução.

Para o caso geral, sejam m e n inteiros quaisquer. Tomemos um número inteiro $p > 0$ tal que $p+n > 0$ e $p+m+n > 0$, o que claramente é possível. Da definição, temos:

$$a^p a^{-p} = a^p (a^p)^{-1} = e$$

Então,

$$\begin{aligned} a^{m+n} &= a^{m+n}\left(a^p a^{-p}\right) = \left(a^{m+n} a^p\right) a^{-p} \overset{*}{=} a^{(m+n)+p} a^{-p} = \\ &= a^{m+(n+p)} a^{-p} \overset{*}{=} \left(a^m a^{n+p}\right) a^{-p} = \left[a^m \left(a^n a^p\right) a^{-p}\right] = \\ &= \left[\left(a^m a^n\right) a^p a^{-p}\right] = \left(a^m a^n\right)\left(a^p a^{-p}\right) = a^m a^n e = a^m a^n \end{aligned}$$

Note que nas passagens $*$ utilizamos a conclusão anterior.

ii) Note que, devido ao primeiro item,

$$a^{-m} a^m = a^{(-m)+m} = a^0 = e$$

De modo análogo,

$$a^m a^{-m} = e$$

Logo, cada uma dessas potências é inversa da outra, ou seja,

$$a^{-m} = (a^m)^{-1}$$

Como queríamos demonstrar nesse item.

iii) Para provar a veracidade dessa equação, vamos provar por indução o caso em que $n \geq 0$. Para $n = 0$, temos:

$$(a^m)^0 = e = a^0 = a^{m.0}$$

Vamos supor que exista $r \geq 0$ que satisfaça a igualdade $(a^m)^r = a^{mr}$ (hipótese de indução). Vamos provar que é valida a igualdade $(a^m)^{r+1} = a^{m(r+1)}$. De fato,

$$(a^m)^{r+1} = (a^m)^r (a^m)^1 = a^{mr} a^m = a^{mr+m} = a^{m(r+1)}$$

e, por fim, vamos supor que $n < 0$. Assim:

$$(a^m)^n \overset{*}{=} \left[(a^m)^{-n}\right]^{-1} = \left(a^{-mn}\right)^{-1} \overset{**}{=} a^{mn}$$

Em $*$ usamos a definição e $**$ usamos (ii). ■

Definição 23 *Se a é um elemento de um grupo multiplicativo G, denotaremos por $\langle a \rangle$ o subconjunto de G formado pelas potências inteiras de a, ou seja,*

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

.

Proposição 4 *(i) o subconjunto $\langle a \rangle$ é um subgrupo de G; (ii) se H é um subgrupo de G ao qual a pertence, então $\langle a \rangle \subset H$.*

Demonstração:

i) Note que $\langle a \rangle \neq \phi$, pois e, o elemento neutro de G, pertence a ele, uma vez que $e = a^0$. Considere u e v elementos de $\langle a \rangle$. Dessa forma:

$$u = a^m \text{ e } v = a^n$$

Para convenientes inteiros m e n, utilizando a proposição anterior, temos:

$$uv^{-1} = a^m (a^n)^{-1} = a^m a^{-n} = a^{m-n}$$

Isso mostra que $uv^{-1} \in \langle a \rangle$, ou seja, $\langle a \rangle$ é um subgrupo de G.

ii) Se $a \in H$, então toda potência de a também pertence a H e, portanto, $\langle a \rangle \subset H$. ■

2.7 Grupos Cíclicos

Definição 24 *Um grupo multiplicativo G será chamado de grupo cíclico se, para algum elemento $a \in G$, se verificar a igualdade $G = \langle a \rangle$. Nessas condições, o elemento a é chamado gerador do grupo G.*

$$G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

Exemplo: O grupo multiplicativo $(\mathbb{Z}_5^*, \cdot)$ é um grupo cíclico, pois

$$\mathbb{Z}_5^* = \left\{[2]^1, [2]^2, [2]^3, [2]^4\right\} = \{[2], [4], [3], [1]\} = \{[1], [2], [3], [4]\} = \langle 2 \rangle$$

Proposição 5 *Seja $G = \langle a \rangle$ um grupo cíclico que $a^r = a^s$ para algum par de inteiros distintos r e s. Então, existe um inteiro $h > 0$ tal que:*

i) $a^h = e$

ii) $a^r \neq e$ *sempre que* $0 < r < h$.

Neste caso,

$$G = \langle a \rangle = \left\{e, a, a^2, ..., a^{h-1}\right\}$$

o grupo é chamado de grupo cíclico finito e o expoente h, período ou ordem de a, cuja notação é $ord(a) = h$.

Demonstração: Sem perda de generalidade, vamos supor que $r > s$. Então,

$$a^r \left(a^s\right)^{-1} = a^s \left(a^s\right)^{-1} = e$$

E,

$$a^{r-s} = e$$

Em que $r - s > 0$. Isso mostra que há potências de a, com expoentes estritamente positivos, iguais ao elemento neutro e. Portanto, pelo princípio da boa ordenação, é possível fazer a seguinte escolha: seja h o menor número inteiro estritamente positivo tal que $a^h = e$. Então,

$$\begin{aligned} a^h &= e \\ a^{h+1} &= a^h a = ea = a \\ a^{h+2} &= a^{h+1} a = aa = a^2 \end{aligned}$$

Ou seja, a partir do expoente h as potências de a se repetem ciclicamente. Vamos provar a unicidade das potências a seguir:

$$\begin{aligned} a^0 &= e \\ a^1 &= a \\ a^2 & \\ \vdots & \\ a^{h-1} & \end{aligned}$$

De fato, suponhamos que $a^i = a^j$, com $0 \leq i < j < h$. Então, $0 < j - i < h$ e

$$a^{j-i} = a^j \left(a^i\right)^{-1} = a^j \left(a^j\right)^{-1} = e$$

Ora, mas isso gera um absurdo, pois dada a escolha de h, não podemos ter simultaneamente $0 < j - i < h$ e $a^{j-i} = e$.

Agora, vamos provar que os únicos elementos no grupo cíclico são e, a, a^2, a^3, ..., a^{h-1}. De fato, seja x um elemento de $G = \langle a \rangle$. Então, $x = a^m$ para algum inteiro m. Usando-se o algoritmo de Euclides colocando m como dividendo e h como divisor, temos:

$$m = hq + r \ (0 \leq r < h)$$

Então,

$$a^m = a^{hq+r} = \left(a^h\right)^q a^r = e^q a^r = ea^r = a^r$$

Como os valores possíveis de r são $0, 1, 2, 3, ..., h-1$, então as possibilidades para a^m são $e, a, a^2, a^3, ..., a^{h-1}$. Isso mostra que $\langle a \rangle \subset \left\{a^0 = e, a^1 = a, a^2, a^3, ..., a^{h-1}\right\}$. Note que, devido a definição de $\langle a \rangle$, vale a inclusão contrária, ou seja, $\langle a \rangle = \left\{a^0 = e, a^1 = a, a^2, a^3, ..., a^{h-1}\right\}$ e a ordem desse grupo é h. ■

2.8 Raízes primitivas

Definição 25 *Designaremos por $\phi(m)$ à quantidade de números naturais entre 0 e $m-1$ que são primos com m.*

Teorema 26 (*Euler*) *Sejam $m, a \in \mathbb{N}$ com $m > 1$ e $mdc(a, m) = 1$. Então:*

$$a^{\phi(m)} \equiv 1 \ mod \ m$$

Teorema 27 *Se* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ *é a decomposição de* m *em fatores primos, então*

$$\phi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

Em particular, quando m *é primo* $\phi(m) = m - 1$.

Para calcular o resto da divisão de uma potência a^n por um número natural $m > 1$, é conveniente achar um expoente h de modo que a potência $a^h \equiv 1 \bmod m$. Pelo teorema de Euler existe $h = \phi(m)$ tal que a^h deixa resto 1 na divisão por m. Como o conjunto formado por esses elementos h é não-vazio, podemos utilizar o princípio da boa ordenação para a seguinte definição:

Definição 28 *Suponha que* $a, m \in \mathbb{N}^*$, *com* $m > 1$ *e* $mdc(a, m) = 1$, *define-se ordem de* a *com respeito a* m *como sendo o número natural*

$$ord_m(a) = min\left\{i \in \mathbb{N}^*; a^i \equiv 1 \ mod\ m\right\}.$$

Exemplo:

a) A ordem de 7 com respeito a 15 é igual a 4.

Com efeito,

$$\begin{aligned} 7^1 &\equiv 7 \bmod 15 \\ 7^2 = 49 &\equiv 4 \bmod 15 \\ 7^3 = 343 &\equiv 13 \bmod 15 \\ 7^4 = 2401 &\equiv 1 \bmod 15 \end{aligned}$$

Note que poderíamos ter utlizado as propriedades da aritmética modular, mas preferimos calcular as potências na "força bruta". Ao calcular $7^4 \equiv 1 \bmod 15$ percebemos que nenhuma potência de 7 menor que 4 é congruente a 1 módulo 15. Logo, $ord_{15}(7) = 4$.

Agora, vamos calcular $\phi(15)$:

$$\phi(15) = 3.5\left(1 - \frac{1}{3}\right).\left(1 - \frac{1}{5}\right) \Rightarrow \phi(15) = 3.5.\frac{2}{3}.\frac{4}{5} \Rightarrow \phi(15) = 8.$$

Logo, a ordem de 7 com respeito a 15 é igual 4 e $\phi(15) = 8$.

b) A ordem de 4 com respeito a 9 é igual a 3.

De fato,

$$\begin{aligned} 4^1 &\equiv 4 \bmod 9 \\ 4^2 = 16 &\equiv 7 \bmod 9 \\ 4^3 = 64 &\equiv 1 \bmod 9 \end{aligned}$$

Por curiosidade, vamos calcular $\phi(9)$:

$$\phi(9) = 3^2.\left(1 - \frac{1}{3}\right) \Rightarrow \phi(9) = 9.\frac{2}{3} \Rightarrow \phi(9) = 6.$$

Nos dois casos percebe-se que a $ord_m(a) \mid \phi(m)$. Isso será enunciado no corolário do teorema a seguir.

Teorema 29 *Temos que $a^n \equiv 1$ mod m se, e somente se, $ord_m(a) \mid n$.*

Demonstração: Inicialmente vamos fazer $ord_m(a) = k \in \mathbb{N}^*$. Seja n um inteiro tal que existe um único par de inteiros q e r, $0 \leq r < k$ tal que

$$n = qk + r$$

Dessa forma,

$$a^n = a^{qk+r} = \left(a^k\right)^q a^r \equiv a^r \bmod m$$

Como $a^n \equiv 1 \bmod m$, acabamos de mostrar que $a^r \equiv 1 \bmod m$. Sendo $r < k$, r deve ser zero, pois k é, por definição, o menor inteiro positivo para o qual $a^k \equiv 1 \bmod m$. Logo, $r = 0$ e $n = qk$. A recíproca é demonstrada de maneira análoga. ■

Corolário 5.1 *Sejam $a, m \in \mathbb{N}$, com $mdc(a, m) = 1$. Temos que $ord_m(a) \mid \phi(m)$.*

Definição 30 *Quando $\phi(m)$ é a ordem de a com respeito a m, então dizemos que a é uma raiz primitiva módulo m.*

$$a \text{ é raiz primitiva com respeito a } m \Leftrightarrow ord_m(a) = \phi(m)$$

Exemplo: Vamos calcular a ordem de 2 com respeito a 9. Note que não precisamos calcular todas as potências do número 2, pois vimos que $ord_9(2) \mid \phi(9) = 6$. Assim:

$$2^1 \equiv 2 \bmod 9$$
$$2^2 = 4 \equiv 4 \bmod 9$$
$$2^3 = 8 \equiv 8 \bmod 9$$
$$2^6 = 64 \equiv 1 \bmod 9$$

Dessa forma, o inteiro 2 é uma raiz primitiva módulo 9, pois a ordem de 2 com respeito a 9 é 6 e $\phi(9) = 6$.

Teorema 31 *Seja $ord_m(a) = k \in \mathbb{N}^*$, então $a^t \equiv a^h$ mod m se, e somente se, $t \equiv h$ mod k.*

Demonstração: Vamos supor que $a^t \equiv a^h \bmod m$. Sem perda de generalidade podemos supor que $t \geq h$. Logo, como $a^t \equiv a^h a^{t-h} \bmod m$ e $a^t \equiv a^h \bmod m$ temos $a^h \equiv a^h a^{t-h} \bmod m$. Como $\text{mdc}(a, m) = 1$ temos $(a^h, m) = 1$, podemos cancelar a^h nesta última congruência, obtendo

$$1 \equiv a^{t-h} \bmod m.$$

Dessa forma, $k \mid (t - h)$ o que equivale a dizer que $t \equiv h \bmod k$.

A recíproca é uma consequência do algoritmo da divisão de Euclides. Se $t \equiv h \bmod k$, então existe um inteiro n tal que $t = h + nk$. Logo:

$$a^t = a^{h+nk} = a^h \left(a^k\right)^n \equiv a^h \bmod m$$

Pois k é a ordem de a módulo m, o que conclui a demonstração. ■

Corolário 5.2 *Seja p um número primo e a uma raiz primitiva módulo p, então $a^t \equiv a^h$ mod m se, e somente se, $t \equiv h$ mod $(p - 1)$.*

Demonstração: Com efeito, se p é um número primo, então pelo teorema anterior, sabemos que $a^t \equiv a^h \bmod m \Leftrightarrow t \equiv h \bmod (ord_p(a))$. Como a é raiz primitiva, então $ord_p(a) = \phi(p) = p - 1$ e, consequentemente, $a^t \equiv a^h \bmod m \Leftrightarrow t \equiv h \bmod (p - 1)$.
■

Por curiosidade, somente os números naturais da forma 1, 2, 4, p^t e $2p^t$ (p primo impar e t inteiro positivo) possuem raízes primitivas. A demonstração desse teorema é feita por SANTOS [18].

Teorema 32 $\langle a \rangle = \mathbb{Z}_m^*$ *se, e somente se, a é raiz primitiva módulo m.*

O resultado desse teorema é muito importante, pois somente raízes primitivas geram grupos cíclicos módulo m, STALLINGS [21].

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Figura 2.1: Potência dos inteiros módulo 19
Fonte: STALLINGS [21], p. 176

2.9 Logaritmos discretos

Definição 33 *Para um número natural b co-primo com m, e a uma raiz primitiva módulo m, definimos como índice de b módulo m na base a ou logaritmo discreto de b módulo m na base a denotado por* $dlog_{a,m}(b)$ *como o único número* $j \in \{1, 2, 3, 4, \cdots, \phi(m)\}$ *tal que* $a^j \equiv b \ mod \ m$.

O índice ou logaritmo discreto de b módulo m na base a foi denotado por $dlog_{a,m}(b)$, mas alguns autores denotam esse fato por $dlog_{a,m}(b)$.

A principal aplicação dos logaritmos discretos é feita em algoritmos de chave pública, como por exemplo na troca de chaves de Diffie-Hellman e no ElGamal. Esse assunto é conhecido como problema do logaritmo discreto, em que é considerado um número primo p ao invés de um inteiro qualquer m ($m > 1$).

Exemplo: As potências de 2 com expoentes positivos módulo 11 são:

$$\begin{aligned} 2^1 = 2 &\equiv 2 \bmod 11 \\ 2^2 = 4 &\equiv 4 \bmod 11 \\ 2^3 = 8 &\equiv 8 \bmod 11 \\ 2^4 = 16 &\equiv 5 \bmod 11 \\ 2^5 = 32 &\equiv 10 \bmod 11 \\ 2^6 = 64 &\equiv 9 \bmod 11 \\ 2^7 = 128 &\equiv 7 \bmod 11 \\ 2^8 = 256 &\equiv 3 \bmod 11 \\ 2^9 = 512 &\equiv 6 \bmod 11 \\ 2^{10} = 1024 &\equiv 1 \bmod 11 \end{aligned}$$

Note que 2 é raiz primitiva módulo 11, pois $\phi(11) = 11 - 1 = 10$ e, portanto, $\mathbb{Z}_{11}^* =< 2 >= \{2^1, 2^2, 2^3, \cdots, 2^{10}\}$.

Esses resultados que obtivemos das potências de 2 módulo 11, nos fornecem os valores de $dlog_{2,11}(x)$. Por exemplo, $dlog_{2,11}(1) = 0$, pois $2^0 \equiv 1 \bmod 11$ e $dlog_{2,11}(6) = 9$, pois $2^9 \equiv 6 \bmod 11$.

Vamos construir uma tabela com $dlog_{2,11}(x)$ para todos os valores de x de 1 a 10.

x	1	2	4	8	5	10	9	7	3	6	1
$dlog_{2,11}(x)$	0	1	2	3	4	5	6	7	8	9	10

Na verdade a função $dlog_{2,11}(x)$, em que $x \in \mathbb{N}^*$, satisfaz propriedades semelhantes às propriedades dos logaritmos. As propriedades são:

i) $dlog_{a,p}(1) = 0$;

ii) $dlog_{a,p}(a) = 1$;

iii) $dlog_{a,p}(xy) \equiv dlog_{a,p}(x) + dlog_{a,p}(y) \bmod (p-1)$;

iv) $dlog_{a,p}(x^r) \equiv r.dlog_{a,p}(x) \bmod (p-1)$;

Demonstração:

i) Da definição, temos que $dlog_{a,p}(1) = 0$, pois $a^0 = 1 \equiv 1 \bmod p$.

ii) Da definição, temos que $dlog_{a,p}(a) = 1$, pois $a^1 = a \equiv a \bmod p$.

iii) Considere $a^{dlog_{a,p}(x)} \equiv x \bmod p$ e $a^{dlog_{a,p}(y)} \equiv y \bmod p$, multiplicando as duas congruências, temos:

$$a^{dlog_{a,p}(x)+dlog_{a,p}(y)} \equiv xy \equiv a^{dlog_{a,p}(xy)} \bmod p$$

Mas, como a é raiz primitiva módulo p, então

$$dlog_{a,p}(xy) \equiv dlog_{a,p}(x) + dlog_{a,p}(y) \bmod (p-1)$$

iv) Seja r um inteiro não-negativo. Podemos escrever x^r como $x.x.x.x.x.x \cdots x$ com r fatores iguais a x. Considere $a^{dlog_{a,p}(x)} \equiv x \bmod p$, multiplicando essa congruência por ela mesmo r vezes, temos:

$$a^{dlog_{a,p}(x)+dlog_{a,p}(x)+\cdots+dlog_{a,p}(x)} \equiv x^r \equiv a^{dlog_{a,p}(x^r)} \bmod p$$

De maneira análoga ao que fizemos no item anterior, temos:

$$dlog_{a,p}(x^r) \equiv r.dlog_{a,p}(x) \bmod (p-1)$$

■

Capítulo 3

Criptografia Diffie-Hellman

Neste capítulo estudaremos os fatos históricos que foram importantes para o sergimento do protocolo Diffie-Hellman; o problema da distribuição das chaves e a troca de chaves de Diffie-Hellman. As referências bibliográficas utilizadas foram: SINGH [20], ALMEIDA [1], COUTINHO [5], DIÁZ [6], FIARRESGA [8], ODLYZKO [14], RAYMOND [17] e VERISSIMO [23].

3.1 Um pouco de história

Whitfield Diffie - nascido em 1944, Queens, Nova York, EUA - é muito conhecido pela sua descoberta do conceito de criptografia de chave pública (com Martin Hellman). Desde os tempos de criança tinha especial fascínio pela Matemática; leu livros que iam do *Manual de tabelas matemáticas da Companhia Química da Borracha até o Curso de matemática pura* de G. H. Hardy. Justamente por isso, Diffie decidiu estudar Matemática no Massachusetts Instituteof Technology - MIT; formou-se em 1965. Depois disto, trabalhou com segurança de computadores até que, no início dos anos 70, adquirira o amadurecimento necessário para se tornar um criptógrafo de pensamento livre. Seus cabelos longos e a sua maneira de ser fazem dele uma espécie de *hippie* da alta tecnologia.

O interesse de Diffie era a solução do problema da distribuição de chaves; apostava na crença de entrada na história daquele que encontrasse essa solução; posto que, nestas circunstâncias, surgiria a sumidade dos criptógrafos de todos os tempos. Ele acompanhou a evolução da organização de pesquisa ARPA (Advanced Research Projects Agency), fundada pelo Departamento de Defesa dos EUA, responsável por, em 1969, criar o sistema de comunicação em rede chamado de ARPANet; no transcurso do tempo, em seu processo evolutivo, esse método, em 1982, deu origem a internet. Enquanto a ARPANet ainda era uma criança, Diffie sentia que uma re-

volução digital estava prestes a acontecer e que o projeto abria as portas para o desenvolvimento de uma supervia de comunicação. Dessa forma, ele sabia que a criptografia se transformaria numa ferramenta essencial e que o problema da distribuição de chaves se tornaria especialmente agudo.

Diffie considerou duas situações. Na primeira, ele imaginou dois estranhos se comunicando via internet e se perguntou como eles poderiam trocar uma mensagem cifrada; e, na segunda, ele considerou uma pessoa que estava comprando um produto via internet. Como esta pessoa poderia mandar um e-mail contendo informações cifradas sobre o seu cartão de crédito, de modo que apenas o vendedor da internet pudesse decifrá-las? Note que nos dois casos as duas partes precisariam trocar uma chave, mas como isso poderia ser feito de modo seguro? Ele ficou obcecado pela solução do problema da troca de chaves.

Figura 3.1: Whitfield Diffie
Fonte: http://www.computerhistory.org/fellowawards/hall/bios/Whitfield,Diffie/

No ano de 1974, Diffie fez uma visita ao laboratório Thomas J. Watson da International Business Machine (IBM), onde foi convidado a dar uma palestra. Naquela ocasião, foram citadas várias estratégias para enfrentar o problema da distribuição de chaves, porém as suas ideias ainda eram muito experimentais. Um dos primeiros criptógrafos da IBM, Alan Kanheim, mencionou que outro palestrante falou sobre a questão da troca de chaves - referia-se a Martin Hellman, um professor da Universidade de Stanford, na Califórnia. Assim, Diffie começou uma viagem de cinco mil quilômetros até a Costa Oeste para falar com Hellman.

Martin Hellman nasceu em 1945 no Bronx, Nova York, EUA. Quando tinha apenas quatro anos de idade, sua família se mudou para um bairro cuja vizinhança era predominantemente formada por católicos irlandeses. Ser judeu mudou permanentemente a sua atitude frente à vida; na crença corrente, todo judeu é “Matador

de Cristo" e, em razão disto, apanhava dos demais meninos e sofria diversa outras formas de perseguições e discriminações ao longo da vida. Ele lembra que queria ser como os outros meninos com relação à árvore de Natal e presentes de fim de ano, mas percebeu que não poderia ser como os outros garotos e adotou uma atitude defensiva de "Quem é que deseja ser como todo mundo?". Ele conta que este foi um dos motivos pelos quais começou a se interessar por criptografia.

Os colegas chamaram-no de louco: como fazer pesquisa de criptografia, concorrer com a National Security Agency (NSA), uma agência de orçamento bilionário, e julgar que pudesse descobrir algo sem que eles soubessem? Sem falar que a NSA se apoderaria da descoberta e a classificaria como secreta. Até a visita inesperada de Diffie, em 1974, o famoso livro de David Kahn, The Codebreakers, tinha sido o seu livro de cabeceira e a única fonte de informação de Hellman.

Figura 3.2: Martin Hellman
Fonte: http://http://www.nndb.com/people/407/000028323/

Finalmente Diffie havia cruzado o país e, por meio de uma chamada telefônica, entrou em contato com Hellman, que não hesitou em encontrá-lo, embora o visitante fosse totalmente desconhecido. Depois de meia hora de conversa, um estava impressionado com o conhecimento do outro e perceberam que não estavam mais sozinhos na busca de uma solução que até então era impossível na prática. Apesar das evidentes diferenças de personalidade, travava-se ali começo de uma grande amizade e companheirismo. Imediatamente começaram a arquitetar um plano para poderem trabalhar juntos. Como Diffie não tinha condições de contratar o novo amigo como pesquisador, Hellman resolveu registrar Diffie como estudante graduado de Stanford. E, juntos, começaram a estudar o problema da distribuição de chaves, tentando encontrar uma alternativa para a cansativa tarefa de transportar fisicamente as chaves através de grandes distâncias.

3.2 O problema da distribuição das chaves

Se duas pessoas quiserem trocar mensagens secretas pelo telefone, o remetente deve cifrá-las e, para isso, ele usa uma chave, também secreta. Assim, surge o problema de transmitir uma chave secreta para o receptor, a fim de que seja possível transmiti-la. Em suma, antes que duas pessoas possam partilhar um segredo (a mensagem cifrada), é necessário partilhar outro segredo (a chave). Por mais complexa que fosse a cifra, se o "inimigo" interceptasse a chave, o sigilo iria por água a baixo.

Quando se estuda o problema da distribuição das chaves surgem três personagens fictícios que se tornaram um padrão nos debates sobre criptografia: Alice, Bob e Eva. Vamos à situação prática: Alice deseja enviar uma mensagem para Bob ou vice-versa e Eva está tentando interceptar esta mensagem. Se Alice está tentando enviar mensagens confidenciais para Bob, ela deve cifrá-las antes do envio usando uma determinada chave. Mas ela enfrenta sempre o problema de distribuição de chaves, visto que ela precisa mandar as chaves para Bob em segurança, pois, caso contrário, Bob não conseguirá decifrar as mensagens.

Uma alternativa para o problema seria Alice e Bob se encontrarem uma vez por semana e trocarem chaves suficientes para cobrirem todas as mensagens que possam ser enviadas durante os sete dias seguintes. Trocar chaves pessoalmente é certamente um modo seguro, mas, inconveniente, pois caso um dos dois ficasse doente, o sistema deixaria de funcionar, ou, ainda, se contratassem um mensageiro, isso seria menos seguro. De qualquer modo, a distribuição de chaves é inevitável e durante dois mil anos isso foi considerado um axioma da criptografia. Assim, surge um método que parece desafiar este axioma.

Suponha que Alice deseja enviar uma mensagem para Bob utilizando uma agência de correios, mas sabia que no trajeto desta carta alguém poderia abrir e ler a mensagem, então ela resolveu colocar a carta numa caixa de ferro trancada com um cadeado, ficando com a chave. Quando Bob recebe a caixa, ele não tem como abri-la, então ele coloca outro cadeado e mandou de volta para Alice. Após receber a caixa, ela remove o próprio cadeado, deixando apenas o cadeado de Bob para impedir a abertura da caixa. Por fim, ela envia novamente a caixa para Bob e, nesta circunstância, temos uma diferença crucial: Bob pode abrir a caixa porque ela está fechada apenas com o seu cadeado, para o qual só ele tem a chave, figura 3.3.

A mensagem chegou ao destinatário com segurança sem que as pessoas trocassem, necessariamente, as chaves. Será que a troca de chaves pode não ser uma parte inevitável na criptografia? Veremos que esse esquema é válido somente para cadeados, mas ele contribuiu muito para o avanço das pesquisas de Diffie e Hellman.

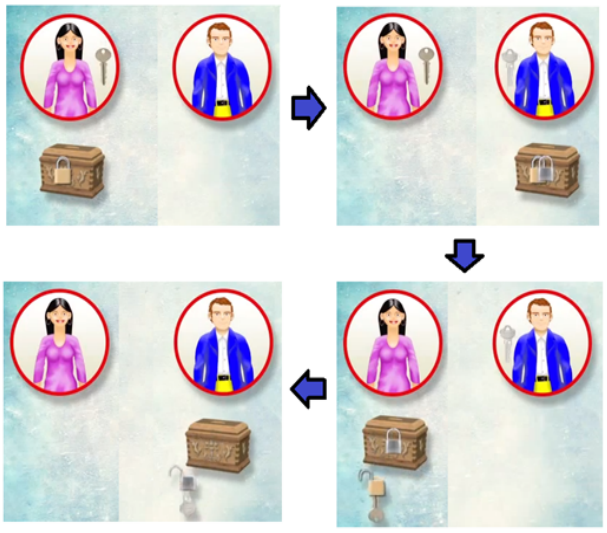


Figura 3.3: Esquema da troca de chaves ilustrada pelo exemplo dos cadeados
Fonte: http://www.youtube.com/watch?v=pEfEgCEKcJ0

3.3 O uso das funções na troca de chaves

Vamos interpretar o exemplo dos cadeados em termos de cifragem. Alice usa a sua própria chave para cifrar a mensagem e a envia para Bob. Ele codifica de novo a mensagem e a envia para Alice, daí ela recebe a mensagem, duplamente cifrada e retira a sua cifra e envia para Bob. Finalmente, Bob retira a sua cifra e ler a mensagem. Vejamos um exemplo:

Chave de Alice

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	W	S	J	A	M	K	Q	X	B	F	O	C	V	Z	H	E	U	Y	I	G	D	R	P	N	L

Chave de Bob

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Y	E	L	K	T	W	F	M	O	A	G	R	X	U	Z	B	H	N	C	V	D	Q	S	J	P	I

Mensagem	**eu amo estudar Criptografia**
Cifrada com a chave de Alice	AG TCZ AYIGJTU SUXHIZKUTMXT
Cifrada com a chave de Bob	YF VLI YPOFAVD CDJMOIGDVXJV
Decifrada com a chave de Alice	SK NZT SXLKENV MVDFLTUVNIDN
Decifrada com a chave de Bob	WD ROE WMCDBRT HTUGCENTRZUR

Note que a mensagem decifrada por Bob não faz sentido algum, ou seja, a ordem que o processo é realizado é muito importante. Por exemplo, se invertermos a ordem

em que foi decifrada, ou seja, primeiro Bob e depois Alice, obteremos a mensagem.

Decifrada com a chave de Bob	AG TCZ AYIGJTU SUXHIZKUTMXT
Decifrada com a chave de Alice	**eu amo estudar Criptografia**

Estamos diante de um problema: qual a ordem em que as cifragens devem ser feitas? De modo geral elas são feitas partindo do princípio "último dentro, primeiro fora". Por exemplo, pela manhã calçamos nossas meias e em seguida os nossos tênis. À noite nós retiramos os tênis primeiro e as meias por último. Seria impossível retirar as meias sem antes retirar os tênis. As pesquisas de Diffie e Hellman foram avançando e eles chegaram à conclusão de que deveriam utilizar funções matemáticas para resolver o problema das trocas de chaves.

Definição 34 *Uma função invertível $f(x)$ recebe o nome de função unidirecional se é "fácil" calcular $y = f(x)$ para todo x do seu domínio, mas é computacionalmente inacessível calcular $x = f^{-1}(y)$ para todos os elementos y da imagem de f.*

Essas funções apresentam uma propriedade em que elas e suas inversas são completamente assimétricas, quando nos referimos a termos de computação. Essas funções também são conhecidas como funções de "mão única". Para ilustrar isso de modo prático, a função que mistura tinta amarela com tinta azul para produzir tinta verde é unidirecional, pois é impossível desfazer essa mistura. A figura 3.4 representa como seria o esquema da troca de chaves utilizando o exemplo das tintas.

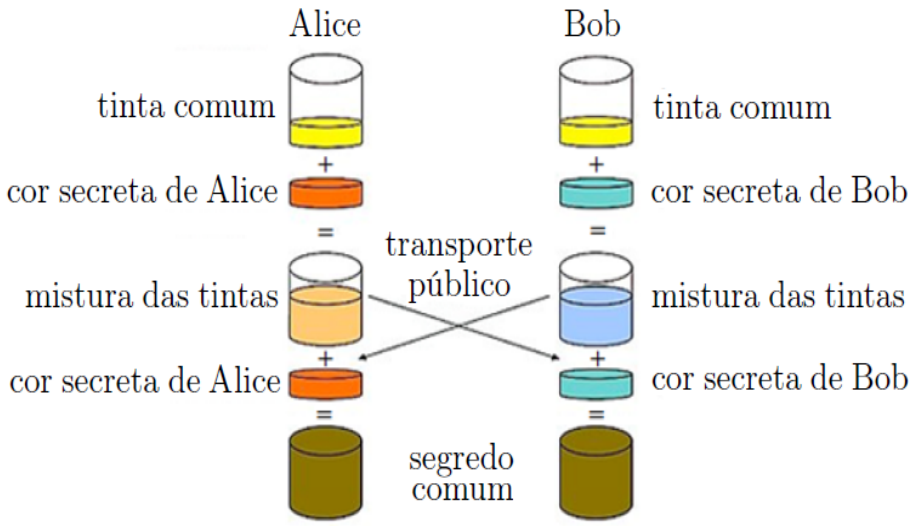


Figura 3.4: Troca de chaves ilustrada pelo exemplo das tintas
Fonte: http://pt.wikipedia.org/wiki/Diffie-Hellman

3.4 A protocolo das trocas de chaves de Diffie-Hellman

Depois de dois anos de trabalho com funções unidirecionais oferecidas pela aritmética modular, em 1976, Hellman finalmente conseguiu resolver o problema da troca de chaves, mudando dos rumos da criptografia desenvolvendo a criptografia assimétrica. Finalmente, um protocolo para a troca de chaves foi criado para a comunicação em um meio não seguro. Esse método é baseado nas operações com logaritmos discretos. Vamos ver como funciona o protocolo Diffie-Hellman na comunicação entre Alice e Bob. Dado um número primo p e α uma raiz primitiva de p.

Alice escolhe um número $x_a < p$. Esse número é mantido em segredo.
Bob escolhe um número $x_b < p$. Esse número também é mantido em segredo.
Alice calcula $y_a \equiv \alpha^{x_a} \bmod p$
Bob calcula $y_b \equiv \alpha^{x_b} \bmod p$
Alice envia o número y_a para Bob.
Bob envia o número y_b para Alice.
Alice calcula $k \equiv (y_b)^{x_a} \bmod p \Rightarrow k \equiv (\alpha^{x_b})^{x_a} \bmod p \Rightarrow k \equiv \alpha^{x_a x_b} \bmod p$
Bob calcula $k \equiv (y_a)^{x_b} \bmod p \Rightarrow k \equiv (\alpha^{x_a})^{x_b} \bmod p \Rightarrow k \equiv \alpha^{x_a x_b} \bmod p$

Alice e Bob chegaram ao mesmo valor k. Esse número k será a chave de comunicação entre eles. Note que na hora em que Alice e Bob trocam as informações é uma oportunidade para que Eva escutar e descobrir os detalhes da informação transmitida. Mas, ela pode escutar toda a conversa, pois mesmo que Eva saiba dos valores de p e α e os números trocados y_a e y_b ela não terá dados suficientes para obter o número k se o valor de p for considerado computacionalmente grande.
Exemplo: Suponha que $p = 97$ e $\alpha = 5$. Então a troca de chaves entre Alice e Bob será da seguinte forma:

- Alice escolhe um número, por exemplo 36;
- Bob escolhe um número, por exemplo 58;
- Alice calcula $5^{36} \equiv 50$ mod97;
- Bob calcula $5^{58} \equiv 44$ mod97;
- Alice informa a Bob o número 50;
- Bob informa a Alice o número 44;
- Alice calcula $44^{36} \equiv 75$ mod97;

- Bob calcula $50^{58} \equiv 75 \text{ mod} 97$;

Portanto a chave entre Alice e Bob é o número 75.

Agora, vamos nos colocar na situação de Eva. Ela sabe os número $p = 97$, $\alpha = 5$, $y_a = 50$ e $y_b = 44$. Vamos tentar obter os números x_a e x_b.

$$5^{x_a} \equiv 50 \text{ mod } 97$$

Ou seja, Eva tem que calcular,

$$x_a = dlog_{5,97}(50)$$

No site http://www.alpertron.com.ar/DILOG.HTM há uma calculadora de logaritmos discretos. Inserindo os valores que Eva tem, obtemos rapidamente que $x_a = 36$ e com isso ela consegue saber que o valor de k é 75.

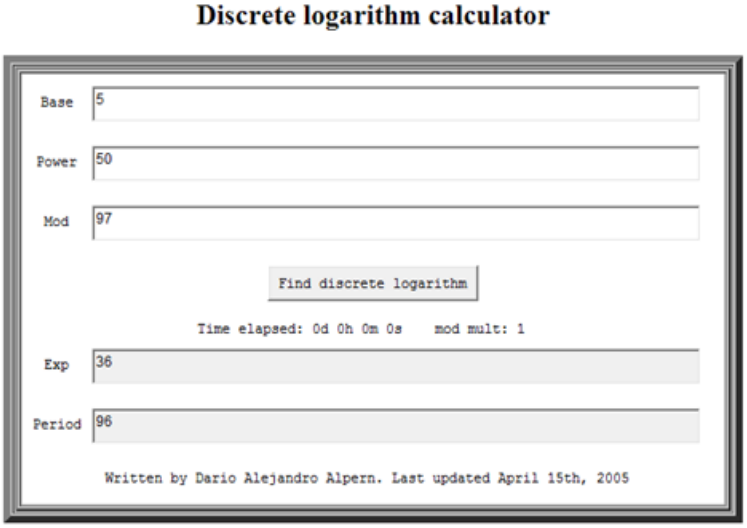


Figura 3.5: Calculadora de logaritmos discretos
Fonte: http://www.alpertron.com.ar/DILOG.HTM

Assim, pode surgir a seguinte pergunta: o problema da troca de chaves não está resolvido? Note que utilizamos números relativamente pequenos. A segurança da criptografia Diffie-Hellman reside no problema de determinar logaritmos discretos muito grandes.

Segundo FIGUEIREDO [9], é importante que a ordem do grupo multiplicativo G seja um primo ou tenha um fator primo muito grande, caso contrário é bem fácil resolver o problema do logaritmo discreto, como fizemos anteriormente. Se utilizarmos $\mathbb{Z}_p^*$, em que p é um número primo, ou seja, a ordem do grupo é $p - 1$,

uma boa escolha são os primos de Sophie German, que são da forma $p = 2q + 1$, onde q também é primo.

Esses primos são famosos, pois a matemática, física e filósofa francesa Marie-Sophie Germain, nascida em Paris, provou que o "Último Teorema de Fermat" é verdadeiro para eles, ou seja, se p é um número primo com estas características, distintos dois a dois, então não existem soluções inteiras não triviais para a equação $x^p + y^p = z^p$. Como curiosidade, há 189 primos de Sophie Germain no intervalo $[1, 10^4]$ e o maior número de Sophie German conhecido até o momento é $18543637900515^{2666667} - 1$ que tem 200701 dígitos e foi descoberto em abril de 2012 por Philipp Bliedung.

```
  2,   3,   5,  11,  23,  29,  41,  53,  83,  89, 113, 131,
173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443,
491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911,
953, 1013, 1019, 1031, 1049, 1103, 1223, 1229, 1289, 1409, 1439, 1451,
1481, 1499, 1511, 1559, 1583, 1601, 1733, 1811, 1889, 1901, 1931, 1973,
2003, 2039, 2063, 2069, 2129, 2141, 2273, 2339, 2351, 2393, 2399, 2459,
2543, 2549, 2693, 2699, 2741, 2753, 2819, 2903, 2939, 2963, 2969, 3023,
3299, 3329, 3359, 3389, 3413, 3449, 3491, 3539, 3593, 3623, 3761, 3779,
3803, 3821, 3851, 3863, 3911, 4019, 4073, 4211, 4271, 4349, 4373, 4391,
4409, 4481, 4733, 4793, 4871, 4919, 4943, 5003, 5039, 5051, 5081, 5171,
5231, 5279, 5303, 5333, 5399, 5441, 5501, 5639, 5711, 5741, 5849, 5903,
6053, 6101, 6113, 6131, 6173, 6263, 6269, 6323, 6329, 6449, 6491, 6521,
6551, 6563, 6581, 6761, 6899, 6983, 7043, 7079, 7103, 7121, 7151, 7193,
7211, 7349, 7433, 7541, 7643, 7649, 7691, 7823, 7841, 7883, 7901, 8069,
8093, 8111, 8243, 8273, 8513, 8663, 8693, 8741, 8951, 8969, 9029, 9059,
9221, 9293, 9371, 9419, 9473, 9479, 9539, 9629, 9689, 9791
```

Figura 3.6: Primos de Sophie German
Fonte: http://es.wikipedia.org/wiki/N%C3%BAmero_primo_de_Sophie_Germain

Trabalhar com logaritmos discretos é totalmente viável no âmbito computacional, pois não existe um algoritmo que calcule em tempo hábil os logaritmos discretos para primos muito grandes. Desta forma, os algoritmos que tentam descobrir o logaritmo discreto fazem testes, ou seja, trabalham utilizando a força bruta. Se o número primo for muito grande o computador irá gastar muito tempo para calcular o logaritmo discreto, pois esse problema é computacionalmente muito difícil.

Vamos observar na prática como funciona o protocolo da troca de chaves Diffie-Hellman para a encriptação de uma mensagem, para isso vamos utilizar os números p e α pequenos para uma melhor explicação. Suponha que Alice e Bob combinem que irão utilizar os números $p = 97$ e $\alpha = 5$. No exemplo anterior, vimos que a chave secreta entre eles será o número 75 e essa chave será utilizada tanto no algoritmo de criptografia quanto no algoritmo de decriptografia. Por exemplo, vamos supor

que nos computadores de Alice e Bob esteja instalado um algoritmo que utilize a cifra de Vigenère. Esse algoritmo cifra as mensagens utilizando a posição dos alfabetos de acordo com os algarismos da chave obtida. Nesse caso ele irá utilizar, alternadamente, os alfabetos da posição 7 e da posição 5 nessa ordem.

1	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
5	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
7	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Se Bob desejar enviar a mensagem **AMOR** para Alice, então o algoritmo de encriptação irá cifrar a mensagem como **uiin** e o algoritmo de decriptação irá decifrar **uiin** transformando na mensagem inicial **AMOR**.

O grande problema deste modelo é o fato das chaves de Alice e Bob serem as mesmas, apesar da função logaritmo discreto ser unidirecional, o computador de ambos está sujeito a vírus. Suponha que um usuário deseja realizar uma transação bancária via internet, sabemos que o sistema que protege os computadores dos bancos são altamente seguros, mas o computador do usuário não, pois ele está sujeito a ser invadido por um vírus. Como a chave é a mesma é um risco para o banco utilizar esse método. Então, ela é considerada segura se o meio onde as chaves forem guardadas for seguro. Dessa forma, este modelo não é considerado o mais eficiente, pelo contrário, ele está obsoleto em relação a criptografia RSA, por exemplo.

A criptografia RSA se baseia na fatoração de números primos grandes no âmbito computacional e a chave de criptografia é diferente da chave de decriptografia. Assim, se Bob desejar enviar uma mensagem para Alice, ele utilizará a chave pública de Alice para cifrar a mensagem, mas somente Alice será capaz de decifrar a mensagem, pois ela utilizará a sua chave privada, tornado a comunicação entre eles mais segura. Portanto, a segurança da informação na troca de chaves de Diffie-Hellman se torna inferior se comparada a segurança RSA, por isso a sua pouca utilização atualmente.

Capítulo 4

Atividades com criptografia em sala de aula

A abordagem de conteúdos que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos é um ponto de referência no processo de ensino e aprendizagem da Matemática. Dessa forma, a intenção de elaborar as atividades aqui propostas foi de aplicar o conhecimento obtido sobre criptografia neste trabalho no ambiente escolar. Acredita-se que o tema Criptografia pode ser utilizado como gerador de atividades didáticas que permitam revisar, exercitar, fixar e aprofundar os conteúdos matemáticos desenvolvidos no Ensino Fundamental e Médio. Partindo desse princípio, podemos introduzir a criptografia ao começar um novo assunto ou no desenvolvimento dele.

4.1 Atividade 1 - A utilização das funções na Criptografia

Neste trabalho, estudamos a evolução da criptografia ao longo da história e aprendemos vários métodos de cifragem de mensagens. Nesta atividade vamos associar a Cifra de César com uma função definida por várias sentenças, assunto que geralmente é visto após as funções polinomiais do 1º e 2º graus.

Atividade

A função $f : \mathbb{N}^* \to \mathbb{N}^*$, definida por $f(x) = \begin{cases} 2x + 1, \text{ se } x \leq 12 \\ x, \text{ se } x > 12 \end{cases}$, será responsável pela codificação de mensagens cujas letras estarão associadas com os números da tabela a seguir:

Por exemplo, ao codificar a palavra **casa**, temos:

a	b	C	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

$$f(3) = 2.3 + 1 \Rightarrow f(3) = 6 + 1 \Rightarrow f(3) = 7$$
$$f(1) = 2.1 + 1 \Rightarrow f(1) = 2 + 1 \Rightarrow f(1) = 3$$
$$f(19) = 19$$

Note que a imagem do número 3 (que representa a letra **c**) pela função f é o número 7 que representa a letra **g**. Continuando o procedimento a mensagem codificada será **gcsc**.

O que acabamos que fazer era comumente utilizado pelo imperador romano Júlio César para transmitir mensagens confidenciais aos seus aliados. Esse método é chamado de *cifra de César*. O nome dado a técnica de codificar uma mensagem para que apenas o seu destinatário saiba traduzi-la é chamada de *criptografia*. Um ramo muito importante da informática, cuja aplicação está diretamente ligada a segurança das informações transmitidas entre duas pessoas, ou empresas, ou países, etc.

Com base no exemplo, faça o que se pede:

a) cifre a mensagem **eu amo criptografia**;

b) Represente a função f por meio de diagramas utilizando o esquema de flechas;

c) Existem letras que não terão representação no texto cifrado. Quais são elas?

Objetivo geral

Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a funções definidas por várias sentenças.

Objetivos específicos

- Reconhecer uma função definida por várias sentenças;
- Calcular o valor numérico de uma função definida por várias sentenças;
- Retomar a ideia de diagramas por meio do esquema de flechas;
- Relacionar a função definida por várias sentenças a codificação e decodificação de mensagens.

Público Alvo

Estudantes da 1ª série do ensino médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-requisitos

Os alunos deverão saber a definição de função constante e função polinomial do 1º grau; representação de funções por meio do esquema de flechas e cálculo do valor numérico para funções definidas por várias sentenças.

Materiais

Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula ao final do conteúdo de funções definidas por várias sentenças. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente responderá a atividade ou poderá propor aos alunos responderem na lousa.

Dificuldades previstas

Esta atividade requer conhecimentos prévios, ou seja, se por algum motivo o aluno não absorveu esses conhecimentos a atividade será encarada com dificuldades. Dessa forma, ao perceber essas dificuldades o docente deverá dar uma atenção "especial" a esse aluno.

Possíveis continuações ou desdobramentos

O docente poderá associar este conteúdo com outras funções estudadas na 1ª série do ensino médio, basta ter cuidado na escolha da lei de formação destas., para isso poderá mudar os valores associados as letras desta atividade.

4.2 Atividade 2 - O uso das matrizes na Criptografia

Um outro conteúdo visto na educação básica que pode ser relacionar com a Criptografia é o estudo das Matrizes. Geralmente a contextualização desse conteúdo utilizada nos livros de ensino médio diz respeito a multiplicação de matrizes. Nessa atividade vamos relacionar a criptografia com multiplicação de matrizes, mas o diferencial é que vamos envolver matriz inversa nesses cálculos, o que permite fazer uma avaliação sobre o aprendizado dos alunos com relação a esse conteúdo de modo instigante, pois obter a real mensagem será motivante para os discentes. Para isso propomos uma questão que foi explorada no vestibular 2011 da Universidade Federal de Goiás (UFG).

Atividade

Uma técnica para criptografar mensagens utiliza a multiplicação de matrizes. Um codificador transforma sua mensagem numa matriz M, com duas linhas, substituindo cada letra pelo número correspondente à sua ordem no alfabeto, conforme modelo apresentado a seguir.

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

Por exemplo, a palavra **SENHAS** ficaria assim:

$$M = \begin{bmatrix} S & E & N \\ H & A & S \end{bmatrix} = \begin{bmatrix} 19 & 5 & 14 \\ 8 & 1 & 19 \end{bmatrix}$$

Para codificar, uma matriz 2×2, A, é multiplicada pela matriz M, resultando na matriz $E = A \times M$, que é a mensagem codificada a ser enviada.

Ao receber a mensagem, o decodificador precisa reobter M para descobrir a mensagem original. Para isso, utiliza uma matriz 2×2, B, tal que $B \times A = I$, onde I é a matriz identidade (2×2). Assim, multiplicando B por E, obtém-se $B \times E = B \times A \times M = M$.

Uma palavra codificada, segundo esse processo, por uma matriz $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ resultou na matriz $E = \begin{bmatrix} 47 & 30 & 29 \\ 28 & 21 & 22 \end{bmatrix}$.

Calcule a matriz B, decodifique a mensagem e identifique a palavra original.

Objetivo geral

Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a multiplicação de matrizes e matriz inversa.

Objetivos específicos

- Identificar quando o produto de matrizes é possível;
- Calcular o produto entre matrizes;
- Obter a matriz identidade de ordem n;
- Calcular a matriz inversa de uma matriz;
- Resolver problemas envolvendo matrizes utilizando sistemas lineares;
- Relacionar matrizes com a codificação e decodificação de mensagens.

Público Alvo

Estudantes da 2ª série do ensino médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-requisitos

Os alunos deverão saber a definição de matrizes bem como identificar quando o produto entre matrizes é possível, multiplicação entre matrizes, obtenção da matriz inversa e matriz identidade.

Materiais

Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula ao final do conteúdo de matrizes para a verificação da aprendizagem dos alunos com relação a esse conteúdo. Os alunos responderão a atividade e, ao término da discussão, o docente responderá a atividade ou poderá propor aos alunos responderem na lousa.

Dificuldades previstas

As dificuldades, que poderão surgir ao longo desta atividade, são aquelas referentes a multiplicação de matrizes e, em especial, ao cálculo de matrizes inversas, pois

o discente irá se deparar com o assunto sistema de equações lineares que foi visto no 8º ano do ensino fundamental, segundo os PCNs. Ao notar essas dificuldades, o docente deverá resgatar esse conteúdo para os alunos por meio de uma rápida revisão.

Possíveis continuações ou desdobramentos

O docente poderá criar outras atividades relacionando outras matrizes e outras mensagens originais para serem codificadas e decodificadas.

4.3 Atividade 3 - A criptografia Diffie-Hellman em sala de aula

No capítulo 3 deste trabalho aprendemos como funciona o algoritmo utilizado no protocolo da troca de chaves de Diffie-Hellman e ao final exemplificamos, no final do capítulo, como ele funciona. A atividade aqui proposta irá fazer os alunos trabalharem com o conteúdo divisão de números inteiros e potenciação de números inteiros ambos vistos no 6º ano do ensino fundamental.

Atividade

A *criptografia* (do grego *kryptos*, "escondido", e *graphein*,"escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas pelo remetente e destinatário da mensagem por meio de uma chave. Dois estudiosos americanos chamados *Whitfield Diffie* e *Martin Hellman* publicaram em 1976 um novo método de duas pessoas trocarem mensagens de modo seguro utilizando o protocolo da troca de chaves de *Diffie-Hellman*, baseado, de maneira simplificada, no resto da divisão entre números naturais.

Vamos supor que Alice e Bob são duas pessoas que desejam se comunicar utilizando uma mensagem secreta, mas para isso eles deverão compartilhar uma chave secreta. O protocolo Diffie-Hellman funciona da seguinte maneira:

i) Alice e Bob trocarão informações utilizando os restos das potências de base 4 com relação ao número primo 7.

ii) Alice deverá escolher um valor natural entre 1 e 7, que vamos chamar de x, e calcular o resto da divisão de 4^x por 7 que denotaremos por a.

iii) Bob deverá escolher um valor natural entre 1 e 7, que vamos chamar de y, e calcular o resto da divisão de 4^y por 7 que denotaremos por b;

iv) Agora, Alice irá calcular o resto da divisão de b^x por 7 e chamar de k_1;

v) Bob irá calcular o resto da divisão de a^y por 7 e chamar de k_2;

vi) Note que $k_1 = k_2$ e essa será a chave da comunicação secreta entre eles, que denotaremos por k.

Após esse procedimento ser feito, Bob deseja enviar uma palavra secreta para Alice, por exemplo, **amor**. Por exemplo, se o valor de k obtido for o número 5,

LINHA	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	L	M	N	T	U	V	P	Q	R	A	B	C	X	Y	Z	F	G	H	D	E	O	I	J	K	W	S
2	S	T	U	L	M	N	A	B	C	X	Y	Z	D	E	F	P	Q	R	O	V	W	G	H	I	J	K
3	C	D	E	J	K	L	V	W	X	P	Q	R	A	B	F	M	N	O	S	T	U	Y	Z	G	H	I
4	B	C	D	F	G	H	J	K	L	N	O	P	R	S	T	V	W	X	Z	A	E	I	M	Q	U	Y
5	N	O	R	S	B	C	K	L	V	W	E	F	H	I	A	D	Y	Z	P	Q	G	J	T	U	M	X
6	T	U	V	H	I	J	C	D	E	N	O	P	X	Y	Z	K	L	M	A	B	W	F	G	Q	R	S

então Bob irá codificar a palavra **amor** substituindo cada letra dessa palavra pela representante dela na 5 linha da tabela abaixo.

Então, ele substituirá a letra A por N, M por H, O por A e R por Z, obtendo a palavra **nhaz**. Alice receberá essa mensagem decodificará utilizando a 5ª linha com relação a linha do alfabeto da Língua Portuguesa. Dessa forma, ela substituirá a letra N por A, H por M, A por O e Z por R, obtendo a mensagem original **amor**.

Reúnam-se em duplas e troquem palavras utilizando o protocolo Diffie-Hellman.

Objetivo geral

Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a divisão e potenciação de números inteiros.

Objetivos específicos

- Identificar o dividendo, divisor, quociente e resto de uma divisão;
- Saber a definição de números primos;
- Calcular potências de números naturais;
- Relacionar o resto de uma divisão com a codificação e decodificação de mensagens.

Público Alvo

Estudantes do 6º ano do ensino fundamental, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-requisitos

Os alunos deverão conhecer o algoritmo da divisão de Euclides, a definição e propriedades das potências de números naturais e a definição e obtenção de números primos.

Materiais

Os materiais utilizados nesta atividade são lápis, borracha, calculadora e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula ao final do conteúdo de potenciação para a verificação da aprendizagem dos alunos com relação a esse conteúdo. Os alunos deverão formar duplas para verificar, utilizando a calculadora para o cálculo de potências, se conseguiram chegar a mesma chave e codificar e decodificar as mensagens transmitidas. Ao final desta atividade o professor deverá discutir os resultados obtidos com os discentes, verificando se as mensagens foram trocadas com êxito.

Dificuldades previstas

As dificuldades, que poderão surgir ao longo desta atividade, são aquelas referentes ao assunto divisão, pois estudos comprovam a dificuldades dos alunos em todo o país com relação a esse conteúdo. O professor ao andar pela sala e ver o andamento das atividades poderá ajudar os alunos percebendo essa dificuldade.

Possíveis continuações ou desdobramentos

O docente poderá utilizar outros valores para o número primo e a base da potência, bem como mudar o alfabeto utilizado no final desta atividade para a codificação e decodificação das mensagens.

Referências Bibliográficas

[1] ALMEIDA, Paulo J., *Criptografia e segurança.* Departamento de Matemática de Aveiro. Portugal, (2012). Disponível em: `http://arquivoescolar.org/bitstream/arquivo-e/195/1/CS11_12.pdf>`. Acesso em 05 fevereiro 2013.

[2] ARAÚJO, Maria Julieta Ventura Carvalho, *Fundamentos de Matemática Elementar.* Notas de aula, (2010). Disponível em: `http://www.ufjf.br/andre_hallack/files/2012/07/fund-09.pdf`. Acesso em 20 janeiro 2013.

[3] BRASIL, *Orientações curriculares para o ensino médio.* Ciências da natureza, matemática e suas tecnologias. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2006. Disponível em: `http://portal.mec.gov.br/seb/arquivos/pdf/book_volume_02_internet.pdf`. Acesso em 28 fevereiro 2013.

[4] _____, *Parâmetros Curriculares Nacionais: matemática.* Secretaria de Educação Fundamental. Brasília: MEC, SEF, 1997. Disponível em: `http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf`. Acesso em 25 fevereiro 2013.

[5] COUTINHO, S. C., *Números inteiros e Criptografia RSA.* Série de Computação e Matemática n. 2. 2 ed. Rio de Janeiro, IMPA e SBM, (2000).

[6] DIÁZ, José Raúl Durán, *Números primos especiales y sus aplicaciones criptográficas.* Tese (Departamento de Física Aplicada a las Tecnologias de la Información). Escuela Técnica Superior de Engenieros de Telecomunicación. Madrid, (2003). Disponível em: `http://oa.upm.es/193/1/09200317.pdf`. Acesso em 12 fevereiro 2013.

[7] DOMINGUES, H. H.; IEZZI, G., *Álgebra moderna.* 4 ed. São Paulo: Atual, (2003).

[8] FIARRESGA, Victor Manuel Calhabrês, *Criptografia e Matemática.* Dissertação (Mestrado em Matemática para Professores) - Universidade de Lisboa, Lisboa, (2010). Disponível em: `http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf`. Acesso em: 05 janeiro 2013.

[9] FIGUEIREDO, Luiz Manoel Silva, *Números primos e Criptografia de chave pública.* Rio de Janeiro: Universidade Federal Fluminense, (2006). Disponível em: `http://pt.scribd.com/doc/52956969/48189108-Criptografia-Numeros-Primos`. Acesso em: 20 dezembro 2012.

[10] FILHO, Edgard de Alencar, *Teoria das congruências.* São Paulo: Nobel, (1986).

[11] HEFEZ, Abramo, *Elementos de aritmética.* 2 ed. Rio de Janeiro: SBM, (2011).

[12] KAKUTA, Neuza, *Álgebra I.* Universidade Estadual Paulista, São José do Rio Preto, (2005).

[13] MALAGUTTI, Pedro Luiz, *Atividades de Contagem a Partir da Criptografia.* OBMEP, Rio de Janeiro, (2009). Disponível em: `http://server22.obmep.org.br:8080/media/servicos/recursos/296660.o`. Acesso em: 14 janeiro 2013.

[14] ODLYZKO, Andrew. *Discrete logarithms over finite fields.* University of Minnesota, (2009). Disponível em: `http://www.dtc.umn.edu/~odlyzko/doc/discrete.logs.hff.pdf`. Acesso em: 14 de fevereiro 2013.

[15] OLIVEIRA, Ronielton Rezende, *Criptografia tradicional simétrica de chave privada e Criptografia assimétrica de chave pública: análise das vantagens e desvantagens.* Trabalho da pós-graduação Criptografia e Segurança em Redes da UFF, Niteroi, (2006).

[16] ORE, Oystein, *Invitation to number theory.* New York: Random House, (1967).

[17] RAYMOND, J. F.; STIGLIC, A., *Security Issues in the Diffie-Hellman Key Agreement Protocol.* (2003). Disponível em: `http://crypto.cs.mcgill.ca/~stiglic/Papers/dhfull.pdf`. Acesso em: 12 fevereiro 2013.

[18] SANTOS, José Plínio de Oliveira, *Introdução à teoria dos números.* 3 ed. Rio de Janeiro: IMPA, (2010).

[19] SHOKRANIAN, Salahoddin, *Uma introdução à teoria dos números.* Rio de Janeiro: Editora Ciência Moderna Ltda., (2008).

[20] SINGH, Simon; tradução de Jorge Calife, *O livro dos códigos.* 6 ed. Rio de Janeiro: Record, (2007).

[21] STALLINGS, Willian; traduzido por Daniel Vieira, *Criptografia e segurança de redes.* 4 ed. São Paulo: Pearson Prentice Hall, (2008).

[22] TÁBARA, José Luis, *Breve história de la Criptografia clássica.* Madrid, (2011). Disponível em: `http://pt.scribd.com/doc/123095010/Breve-Historia-de-La-Criptografia-Clasica`. Acesso em: 05 Janeiro 2013.

[23] VERISSIMO, Fernando, *Segurança em redes sem fio.* Monografia. Universidade Federal do Rio de Janeiro, Rio de Janeiro, (2012). Disponível em: `http://www.lockabit.coppe.ufrj.br/sites/lockabit.coppe.ufrj.br/files/publicacoes/lockabit/wnsmono.pdf`. Acesso em: 02 Janeiro 2013.