Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Um Sistema de Criptografia de Chave Pública Chamado ElGamal

Paulo Sérgio Lopes da Silva

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Junho de 2015

Um Sistema de Criptografia de Chave Pública Chamado ElGamal

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Paulo Sérgio Lopes da Silva e aprovada pela comissão julgadora.

Cuiabá, 10 de julho de 2015.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo
Prof. Dr. Moiseis dos Santos Cecconello
Prof. Dr. Lenimar Nunes de Andrade

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

S586s Silva, Paulo Sérgio Lopes da.
Um Sistema de Criptografia de Chave Pública Chamado ElGamal / Paulo Sérgio Lopes da Silva. -- 2015
x, 52 f. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2015.
Inclui bibliografia.

1. Grupos Cíclicos. 2. Logaritmo Discreto. 3. Assinatura Digital. I. Título.

Dissertação de Mestrado defendida em 08 **de Junho de** 2015 **e aprovada pela banca examinadora composta pelos Professores Doutores**

Prof. Dr. Martinho da Costa Araújo-UFMT

Prof. Dr. Lenimar Nunes de Andrade-UFPB

Prof. Dr. Moiseis dos Santos Cecconello-UFMT

À minha doce amada.

Agradecimentos

Ao término deste trabalho, deixo aqui meus sinceros agradecimentos:

– a Deus por tudo;

– à minha esposa e filhos por perdoarem os incontáveis fins de semana de ausência;

– ao Prof. Dr. Martinho da Costa Araújo, por toda dedicação, paciência e estímulo em sua orientação;

– a todos os professores do Departamento de Matemática da UFMT;

– aos professores da banca pelas valiosas sugestões;

– a minha família, pelo incentivo e segurança que me passaram durante todo esse período;

– aos amigos do PROFMAT pelo agradável convívio especialmente Jackson e Adilson;

– à gestão da Escola Estadual 29 de Novembro de Tangará da Serra pela paciência;

– a todos que direta ou indiretamente contribuíram para a realização deste trabalho;

– à Capes pelo auxílio financeiro.

"Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade o que proporciona o máximo prazer não é o conhecimento e sim a aprendizagem, não é a posse mas a aquisição, não é a presença mas o ato de atingir a meta "

Carl F. Gauss

Resumo

Neste trabalho trataremos do sistema de criptografia de chave pública de ElGamal. No primeiro capítulo apresentamos todos os conceitos matemáticos envolvidos neste tema, enfatizando o índice. No segundo capítulo trataremos do conceito desse sistema, fatos relevantes para sua implementação e alguns fatos históricos. O método de codificação e decodificação neste criptosistema é apresentado no terceiro capítulo. Finalizamos apresentando no quarto e quinto capítulos a proposta didática de inserção do tema criptografia no ensino regular de matemática.

Palavras chave: Grupos cíclicos, logaritmo discreto, assinatura digital.

Abstract

In this paper we will address public key cryptosystem ElGamal. In the first chapter we present all the mathematical concepts addressed, especially the index. In the second chapter we will talk about the system concepts studied in this paper, historical and relevant facts that were important for its implementation. The coding and encoding method in this cryptosystem is presented in the third chapter. In the fourth and fifth chapter we finish presenting a didactic proposal to include encryption in the regular teaching mathematics.

Keywords: Cyclic groups, discrete logarithm, digital signature.

Sumário

Introdução

"The magic words are squeamish ossifrage "
(RSA-129)

Suponha que você deseja mandar uma mensagem muito importante para alguém, porém, você não queira que o mensageiro leia o que foi escrito. Este é um problema que a humanidade enfrenta desde os primórdios da escrita, cuja solução é dada pela criptografia, que a grosso modo é "a arte de criar mensagens secretas e enviá-las com segurança".

Atualmente os principais interessados na solução deste problema são os diplomatas, militares e o comércio eletrônico, este último só desenvolveu o interesse após a chegada das mensagens eletrônicas e a internet.

Nós vamos apresentar aqui um dos mais importantes métodos de criptografia, porém menos conhecido que o RSA, o criptosistema de ElGamal. Para tanto será necessário, antes expor conceitos como grupos, teorema de Euler, ordem e o logaritmo discreto.

Existem também a necessidade de saber se uma mensagem criptografada é verdadeira ou não. Para suprir esta necessidade apresentaremos a assinatura digital, que verifica a autenticidade de uma mensagem, sem necessariamente decodificá-la.

Por fim, apresentaremos uma sequência didática para aplicação dos conceitos aqui apresentados no ensino básico.

Capítulo 1

Conceitos Básicos

Neste capítulo apresentaremos todos os conceitos para que possamos introduzir as raízes primitivas, para tanto daremos uma definição para ordem.

1.1 Estrutura

O conjunto dos números naturais $\mathbb{N}$ é caracterizado[1] da seguinte forma:

i) Exite uma função injetiva $s : \mathbb{N} \to \mathbb{N}$. A imagem $s(n)$ de cada número natural $n \in \mathbb{N}$ é chamada sucessor de n.

ii) Existe um número natural $1 \in \mathbb{N}$ tal que $1 \neq s(n)$ para todo $n \in \mathbb{N}$.

iii) Se um conjunto $X \subset \mathbb{N}$ é tal que $1 \in X$ e $S(X) \subset X$ então $X = \mathbb{N}$

Os axiomas acima citados permitem caracterizar a operação de adição que associa cada par de naturais (m, n) a um único natural $m + n$ chamado de soma. Definimos o número *zero*, doravante 0, como sendo o elemento neutro desta operação, ou seja $n + 0 = n, \ \forall \ n \in \mathbb{N}$. Definimos também o oposto do número natural n como sendo o número $-n$ de modo que $n + (-n) = 0$.

Definição 1 *Seja* $-\mathbb{N}$ *o conjunto de todos os opostos dos números naturais. Então* $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$ *será chamado de números inteiros.*

A estrutura algébrica que sustenta todo o conceito aqui empregado é a estrutura de grupo, que definimos a seguir.

[1] Essa caracterização é chamada de Axiomas de Peano, para uma leitura aprofundada recomendo Lima (2007).

Definição 2 *Um sistema composto por um conjunto G não vazio e uma operação binária $*$ é chamado de grupo se $(G, *)$ tem as seguintes propriedades:*

1. *Associatividade: Dados a, b e c elementos de G temos $(a * b) * c = a * (b * c)$*
2. *Elemento neutro: Exite um elemento $e \in G$ de modo que para todo $a \in G$ temos $a * e = e * a = a$*
3. *Inverso: Para todo $a \in G$ existe um $a' \in G$ tal que $a * a' = a' * a = e$*

Se um grupo G possui a propriedade

$$a * b = b * a$$

para todo $a, b \in G$ então G é chamado de grupo abeliano ou grupo comutativo.

Exemplo 1

O conjunto $\mathbb{Z}$ dos inteiros com soma usual é um grupo.

Teorema 1 *Dados dois inteiros a e b, $b > 0$, existem um único par de números inteiros q e r tais que*

$$a = qb + r, \quad com \;\; 0 \leq r < b$$

Prova A prova deste teorema pode ser encontrada em Santos (2009).

No teorema acima se tivermos $r = 0$ então diremos que b divide a e denotaremos por $b|a$.

Definição 3 *Dados inteiros a, b e m com $m > 0$ dizemos que a é congruente b módulo m se $a - b$ é um múltiplo de m. Em símbolos escrevemos*

$$a \equiv b \pmod{m} \Leftrightarrow m|(a - b)$$

Congruências possuem algumas propriedades que nos ajudarão a trabalhar com números inteiros.

Proposição 2 *Dados a, b, c e m inteiros com $m > 0$ e $n \in \mathbb{N}$ então:*

i) $a \equiv b \pmod{m} \Leftrightarrow a + c \equiv b + c \pmod{m}$

ii) se $a \equiv b \pmod{m}$ *então* $a \cdot c \equiv b \cdot c \pmod{m}$

iii) $a \equiv b \pmod{m} \Leftrightarrow a^n \equiv b^n \pmod{m}$

Prova:

i) Notemos que a definição de congruência nos indica que $a \equiv b \pmod{m} \Leftrightarrow m|(a-b)$ então

$m|(a-b) \Leftrightarrow (a-b) = k \cdot m \Leftrightarrow (a+c-c-b) = k \cdot m \Leftrightarrow ([a+c]-[b+c]) = k \cdot m \Leftrightarrow m|([a+c]-[b+c])$. Aplicando a definição de congruência temos $a \equiv b \pmod{m} \Leftrightarrow m|(a-b) \Leftrightarrow m|([a+c]-[b+c]) \Leftrightarrow a+c \equiv b+c \pmod{m}$.

ii) Para provar este item devemos salientar que se $p|q$ então $p|q \cdot r$ para qualquer r sendo p, q, r inteiros. Notemos agora que $m|(a-b) \Rightarrow m|(a-b)\cdot c \Rightarrow m|(a\cdot c - b\cdot c)$ aplicando a definição de congruência temos $a \equiv b \pmod{m} \Leftrightarrow m|(a-b) \Rightarrow m|(a\cdot c - b\cdot c) \Leftrightarrow a\cdot c \equiv b\cdot c \pmod{m}$

iii) Provaremos usando indução sobre n.

Se $n = 1$ teremos a hipótese da proposição, Suponhamos que $a^n \equiv b^n \pmod{m}$ é verdadeiro para algum n natural, então pela hipótese de indução temos

$$a^{n+1} = a \cdot a^n \equiv b \cdot b^n = b^{n+1} \pmod{m}$$

□

Definição 4 *Diremos que um número natural d é um máximo divisor comum de dois inteiros a e b não simultaneamente nulos, se possuir as seguintes propriedades:*
i) d é um divisor comum de a e de b, e
ii) d é divisível por todo divisor comum de a e de b.

A condição *ii*) acima pode ser reescrita como segue:

ii') Se c é um divisor comum de a e de b então c|d

Denotaremos o máximo divisor comum dos inteiros a e b por $(a, b) = mdc(a, b)$.

Definição 5 *Chamamos de coprimos os números a e b tal que* $(a, b) = 1$.

O próximo teorema é um dos mais importante da teoria dos números, o algoritmo de Euclides.

Proposição 3 *Sejam $r_0 = a$ e $r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \quad 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, 3, \cdots, n-1$ e $r_{n+1} = 0$ então $(a, b) = r_n$, o último resto não-nulo.

Prova Uma excelente prova desta proposição pode ser encontrada em Hefez (2013).

Definição 6 *Dado um inteiro não nulo m e um inteiro $0 \leq a < m$ definimos a classe residual módulo m como sendo o conjunto $[a] = \overline{a} = \{a + mk, k \in \mathbb{Z}\}$*

Exemplo 2

Note que $6 \equiv 1 \pmod 5$ pois, $5|6-1$ no entanto $5|11-1$, $5|16-1$ e assim por diante. Em geral podemos afirmar que, para todo inteiro k, $5k+1 \equiv 1 \pmod 5$ já que $5|(5k+1-1)$. Generalizando, temos que $\overline{1}$ é o conjunto de todos os números inteiros que ao ser dividido por 5 deixam resto 1, ou seja, a classe

$$[1] = \overline{1} = \{\cdots, -9, -4, 1, 6, 11, \cdots\} = \{1 + 5k, \ k \in \mathbb{Z}\}.$$

Todos os conceitos apresentados neste capítulo pode ser encontrado com mais riqueza de detalhes em Santos (2009).

Definição 7 *Definimos $\mathbb{Z}_m$ como sendo o conjunto de todas as classes residuais módulo m ou seja,*

$$\mathbb{Z}_m = \{[0], [1], \cdots, [m-1]\}$$

Definição 8 *Sejam $[a]$ e $[b]$ classes residuais módulo m então definiremos a operação soma $\oplus$ de classes residuais como sendo $[a] \oplus [b] = [a + b]$.*

Definição 9 *Sejam $[a]$ e $[b]$ classes residuais módulo m, então definiremos a operação multiplicação $\odot$ de classes residuais como sendo $[a] \odot [b] = [a \cdot b]$*

Notemos que $[a] = [a']$ e $[b] = [b']$ dois representantes de cada classe residual módulo m então $a \equiv a' \pmod m$ e $b \equiv b' \pmod m$ e certamente $a+b \equiv a'+b' \pmod m$ e $a \cdot b \equiv a' \cdot b' \pmod m$ o que equivale a dizer que $[a + b] = [a' + b']$ e $[a \cdot b] = [a' \cdot b']$.

Esta observação nos diz que a soma e o produto de classes residuais estão bem definidas, ou seja, não depende da escolha do representante da classe.

Doravante todo grupo cuja operação é uma adição se chamará *grupo aditivo* e cuja operação é uma multiplicação será chamado de *grupo multiplicativo.*

Definição 10 *Dado um grupo $(G, *)$, tal que G é finito então $(G, *)$ será chamado de grupo finito. O número de elemento de G será chamado de ordem do grupo.*

Proposição 4 *O conjunto $\mathbb{Z}_m$ com a operação de adição de classes residuais módulo m formam um grupo, ou seja, $(\mathbb{Z}_m, \oplus)$ é um grupo.*

Prova: *i*)

$$\begin{aligned}
[a] \oplus ([b] \oplus [c]) &= [a] \oplus [b + c] \\
&= [a + (b + c)] \\
&= [(a + b) + c] \\
&= [a + b] \oplus [c] \\
&= ([a] \oplus [b]) \oplus [c]
\end{aligned}$$

ii) Afirmamos que a classe [0] é o elemento neutro da adição e de fato;

$[a] \oplus [0] = [a + 0] = [a]$ e $[0] \oplus [a] = [0 + a] = [a]$

iii) Afirmamos também que a classe $[m - a]$ é o elemento inverso da classe $[a]$, pois, $[m - a] \oplus [a] = [m - a + a] = [m] = [0]$ e $[a] \oplus [m - a] = [a + m - a] = [m] = [0]$

□

Quando nos referimos ao fechamento de um conjunto A em relação a determinada operação $*$, queremos dizer que ao tomarmos dois elementos a e b do conjunto A e realizarmos a operação $a * b$ obtemos um elemento também pertencente a A.

Proposição 5 *O conjunto $\mathbb{Z}_m^* = \mathbb{Z}_m - [0]$ é fechado para a operação de multiplicação se, e somente se, m é primo.*

Prova: Suponhamos que m não seja primo, então exitem a e b com $a, b < m$ tais que $a \cdot b = m$. Como na multiplicação de classes residuais não importa o representante da classe residual, podemos afirmar que $[a] \odot [b] = [m] = [0]$ no entanto, [0] não faz parte do conjunto G, contradição.

Reciprocamente, devemos ver que a única possibilidade de $\mathbb{Z}_m$ não ser fechado para a multiplicação módulo m é se existirem classes $[a]$ e $[b]$, tais que $[a] \cdot [b] = [0]$ o que resultaria em $a \cdot b \equiv 0 \pmod{m}$, ou seja $m|a \cdot b$ mas por hipótese m é primo logo, $m|a$ ou $m|b$. Se $m|a$ então $a = mk$ portanto,

$$[a] = [m \cdot k] = [m] \odot [k] = [0] \cdot [k] = [0]$$

que é absurdo, pois $[a] \in \mathbb{Z}_m^*$. De modo semelhante se $m|b$ obtemos $[b] = [0]$ que também é absurdo.

□

Exemplo 3

Um conjunto que não é fechado com a operação de multiplicação é o conjunto $(\mathbb{Z}_6^*, \odot)$. Basta observarmos que $[2] \cdot [3] = [6] = [0]$. Logo não é um grupo multiplicativo.

Proposição 6 *Se p um número primo então $(\mathbb{Z}_p, \odot)$ é um grupo multiplicativo.*

Prova: É fácil mostrar que a multiplicação de classes residuais é associativa e que $[1]$ é o elemento neutro. Portanto, só resta mostrar que para todo $[a] \in \mathbb{Z}_m^*$ existe um $[b] \in \mathbb{Z}_m^*$ tal que $[a] \cdot [b] = [1]$ e de fato existe, pois,

$$[a][b] = [1] \Rightarrow a \cdot b \equiv 1 \pmod{m} \Rightarrow a \cdot b - km = 1$$

e a equação diofantina tem solução b e k pois $(a, m) = 1$.

□

Definição 11 *Seja G um grupo multiplicativo. Se $a \in G$ e n é um número inteiro, a n-ésima potência de a é o elemento a^n definido por recorrência do seguinte modo:*

- *se $n = 0$ então $a^n = e_G$Elemento neutro de G*
- *se $n > 0$ então $a^n = a^{n-1} * a$*
- *se $n < 0$ então $a^{-n} = (a^{-1})^{-n}$*

Exemplo 4

Tomemos como exemplo o grupo $(\mathbb{Z}_7^*, \odot)$ e a classe residual [3]

$$\begin{aligned}
[3]^0 &= [1] \\
[3]^1 &= [3]^{1-1} \odot [3] = [1] \odot [3] = [1 \cdot 3] = [3] \\
[3]^2 &= [3]^{2-1} \odot [3] = [3] \odot [3] = [1 \cdot 3] = [9] = [2] \\
[3]^3 &= [3]^{3-1} \odot [3] = [2] \odot [3] = [2 \cdot 3] = [6] \\
[3]^4 &= [3]^{4-1} \odot [3] = [6] \odot [3] = [6 \cdot 3] = [18] = [4] \\
[3]^5 &= [3]^{5-1} \odot [3] = [4] \odot [3] = [4 \cdot 3] = [12] = [5] \\
[3]^6 &= [3]^{6-1} \odot [3] = [5] \odot [3] = [5 \cdot 3] = [15] = [1] \\
[3]^7 &= [3]^{7-1} \odot [3] = [1] \odot [3] = [1 \cdot 3] = [3]
\end{aligned}$$

Definição 12 *Um grupo multiplicativo G é chamado de cíclico se existir um $a \in G$ de modo que $G = \{a^n; n \in \mathbb{Z}\}$. Nestas condições a é o gerador de G e escrevemos $< a >= G$.*

Exemplo 5

Podemos notar pelo exemplo 4 que o grupo $G = (\mathbb{Z}_7^*, \odot)$ é cíclico pois, $(\mathbb{Z}_7^*, \odot) = \{[3]^n;\ n \in \mathbb{Z}\}$. Notemos também que [3] é um gerador de $(\mathbb{Z}_7^*, \odot)$, ou seja, $(\mathbb{Z}_7^*, \odot) =< [3] >$.

1.2 Ordem

Antes de darmos a definição de ordem apresentaremos alguns conceitos que serão necessários para demonstrarmos proposições e teoremas importantes.

Definição 13 *Uma função aritmética é uma função definida em todos os inteiros positivos.*

Definição 14 *Seja n um inteiro positivo. A função ϕ de Euler é definida como sendo a função que associa cada n a quantidade de números inteiros positivos k menores que n e coprimos com n.*

Por exemplo:

As vezes escrevemos $\phi(n) = \#\{k,\ 1 \leq k \leq n$ tais que $(k, n) = 1\}$ onde $\#$ significa o número de elementos de um conjunto.

n	2	3	4	5	7	10
$\phi(n)$	1	2	2	4	6	4

Tabela 1.1:

Teorema 7 *Para p primo e a um inteiro positivo temos:*
$i)\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$
$ii)\phi(p) = p - 1$

Prova $i)$ Pela definição da função ϕ sabemos que $\phi(p^a)$ é o número de inteiros positivos não-negativos menores que e igual a p^a coprimos com p^a. Mas os únicos números não primos com p^a menores do que ou iguais a p^a são aqueles que são divisíveis por p, ou seja $M = \{1p, 2p, 3p, \cdots p^{a-1} \cdot p\}$, percebemos que o números de elementos M é p^{a-1} portanto, $\phi(p^a) = p^a - p^{a-1}$, o resultado segue.

$ii)$ Este item é um caso particular de $i)$.

□

Teorema 8 *A função $\phi(n)$ é multiplicativa, isto é $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ para $(n, m) = 1$*

Prova A prova pode ser encontrada em Santos (2009).

□

Teorema 9 *Para $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, temos*

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_n^{a_n-1}(p_1 - 1)(p_2 - 1) \cdots (p_n - 1)$$

Prova A prova deste teorema decorre da aplicação do teorema 8.

□

Exemplo 6

Desejamos calcular $\phi(31)$, $\phi(625)$, $\phi(15)$:

(i) Como 31 é primo temos $\phi(31) = 31 - 1 = 30$;
$(ii)\phi(625) = \phi(5^4) = 5^{4-1}(5-1) = 500$;
$(iii)\phi(15) = \phi(3 \cdot 5) = \phi(3)\phi(5) = (3-1)(5-1) = 8$;

Definição 15 *Um sistema reduzido de resíduos módulo m, doravante SRR_m, é o conjunto de $\phi(m)$ inteiros, de modo que todos sejam coprimos com m e tomados quaisquer dois elementos deste conjunto, estes não são incongruentes módulo m.*

Exemplo 7

Calcularemos SRR_{10} e SRR_5.

Note que $SRR_{10} = \{1, 3, 7, 9\}$ e $SRR_5 = \{1, 2, 3, 4\}$.

Observação 1 *Pela definição SRR_m dado um $SRR_m = \{r_1, r_2, \cdots, r_{\phi(m)}\}$ temos que todos os elementos $r_i; 1 \leq i \leq \phi(n)$ são coprimos com m então concluímos que $(r_1 \cdot r_2 \cdots r_{\phi(m)}, m) = 1$.*

Proposição 10 *Seja $SRR_m = \{r_1, \cdots r_{\phi(m)}\}$ e um inteiro a coprimo com m. Então o conjunto $\{a \cdot r_1, \cdots, a \cdot r_{\phi(m)}\}$ também é SRR_m.*

Prova: Percebemos claramente que $(a \cdot r_i, m) = 1$. Suponhamos agora que existam i e j com $i \neq j$ e $1 \leq i, j \leq \phi(m)$, tal que $a \cdot r_i \equiv a \cdot r_j \pmod{m}$. Pela definição de congruência temos $m|(a \cdot r_i - a \cdot r_j) \Rightarrow m|a(r_i - r_j)$ porém, por hipótese, temos que $(a, m) = 1$, ou seja, $m \not| a$ e deste modo somos levados a concluir que $m|(r_i - r_j)$, ou seja, $r_i \equiv r_j \pmod{m}$ que é um absurdo pois r_i e r_j são elementos do SRR_m.

□

Observe que na proposição anterior $a \cdot r_i$ é congruente à algum r_j.

Teorema 11 *(Euler) Seja a e m inteiros coprimos e $m > 0$, então*

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

Prova Pela observação feita na proposição 10 concluímos que

$$a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}$$
$$a^{\phi(m)}(r_1 \cdot r_2 \cdots r_{\phi(m)}) \equiv (r_1 \cdot r_2 \cdots r_{\phi(m)}) \pmod{m}$$
$$a^{\phi(m)} \equiv 1 \pmod{m}$$

□

Definição 16 *Sejam a e n inteiros coprimos. Então, o menor inteiro positivo x tal que $a^x \equiv 1 \pmod{n}$ é chamado de ordem de a módulo n*

Vamos representar a ordem de a módulo n por $ord_n a$,logo pelo teorema de Euler podemos garantir a existência da ordem de a módulo n, pois sabemos que x pode assumir o valor de $\phi(n)$.

Exemplo 8

Podemos encontrar de $ord_7 2$ calculando. $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$, como vimos acima, a primeira potencia de 2 que é congruente a 1 módulo 7 é 2^3, assim $ord_7 2 = 3$

Exemplo 9

Agora tentaremos calcular $ord_{121} 2$

$$
\begin{array}{rcll}
2^1 & \equiv & 2 & \pmod{121} \\
2^2 & \equiv & 4 & \pmod{121} \\
2^3 & \equiv & 8 & \pmod{121} \\
2^4 & \equiv & 16 & \pmod{121} \\
2^5 & \equiv & 32 & \pmod{121} \\
2^6 & \equiv & 64 & \pmod{121} \\
2^7 & \equiv & 7 & \pmod{121} \\
2^8 & \equiv & 14 & \pmod{121} \\
2^9 & \equiv & 28 & \pmod{121} \\
2^{10} & \equiv & 56 & \pmod{121}
\end{array}
\qquad
\begin{array}{rcll}
2^{11} & \equiv & 112 & \pmod{121} \\
2^{12} & \equiv & 103 & \pmod{121} \\
2^{13} & \equiv & 85 & \pmod{121} \\
2^{14} & \equiv & 49 & \pmod{121} \\
2^{15} & \equiv & 98 & \pmod{121} \\
2^{16} & \equiv & 75 & \pmod{121} \\
2^{17} & \equiv & 29 & \pmod{121} \\
2^{18} & \equiv & 58 & \pmod{121} \\
2^{19} & \equiv & 116 & \pmod{121} \\
2^{20} & \equiv & 111 & \pmod{121}
\end{array}
$$

Podemos ver no exemplo 9 que nem sempre é simples obter a ordem de a módulo n. A proposição abaixo será destinada a facilitar esta procura. Neste caso veremos que a $ord_{121} 2 = 110$.

Proposição 12 *Se a e n são inteiros coprimos e $n > 0$, então o inteiro positivo x será solução da congruência $a^x \equiv 1 \pmod n$ se, e somente se, $ord_n a | x$*

Prova: *i*) Temos que o inteiro x é a solução da congruência $a^x \equiv 1 \pmod n$ pela divisão euclidiana temos que $x = k \cdot ord_n a + r$ com $0 \leq r < ord_n a$ então $a^x = a^{k \cdot ord_n a + r} \equiv a^r \pmod n$ como por hipótese $a^x \equiv 1 \pmod n$ então $a^r \equiv 1 \pmod n$ pela definição de ordem concluímos que $r = 0$, ou seja, $ord_n a | x$

ii) Se $ord_n a | x$ então $x = ord_n a \cdot k$, assim

$$a^x = a^{ord_n a \cdot k} = (a^{ord_n a})^n \equiv 1^n = 1 \mod n$$

concluindo a prova.

□

Corolário 13 *Se a e n são coprimos então $ord_n a | \phi(n)$*

Prova: Pelo teorema Euler temos que $a^{\phi(n)} \equiv 1 \pmod{n}$; o teorema anterior nos garante que $ord_n a | \phi(n)$

□

Exemplo 10

Agora podemos retornar ao exemplo 9 e obter $ord_{121}2$. Como $\phi(121) = 110$ os candidatos ao valor de $ord_{121}2$ são os divisores de 110 que são os elementos do conjunto $\{1, 2, 5, 10, 11, 22, 55, 110\}$. Já sabemos que $\{1, 2, 5, 10, 11\}$ não são, então tentaremos os demais.

$$2^{22} \equiv 81 \pmod{121}$$
$$2^{55} \equiv 120 \pmod{121}$$
$$2^{110} \equiv 1 \pmod{121}$$

Observemos que $ord_{121}2 = 110 = \phi(121)$, neste caso, o número 2 recebe o nome de raíz primitiva módulo 121, que definimos agora.

1.3 Obtendo uma Raiz Primitiva

Definição 17 *Se $ord_m a = \phi(m)$ dizemos que a é uma raiz primitiva módulo m*

Exemplo 11

Afirmamos que 3 é raiz primitiva módulo 5, e de fato é pois $3^1 \equiv 3 \pmod{5}$, $3^2 \equiv 4 \pmod{5}$ e $3^4 \equiv 1 \pmod{5}$.

Dado um natural n estamos interessados em obter todas as raízes primitivas incongruentes módulo n, caso existam. Construiremos este resultado.

Proposição 14 *Se a e n são inteiros coprimos com $n > 0$ e i, j inteiros não negativos, então $a^i \equiv a^j \pmod{n}$ se, e somente se $i \equiv j \pmod{ord_n a}$*

Prova: Por hipótese temos que $(a, n) = 1 \Rightarrow (a^j, n) = 1$. Notemos agora que se dividirmos os temos equivalentes na congruência $a^i \equiv a^j \pmod{n}$ por a^j obtemos $a^{i-j} \equiv 1$

(mod n), pela proposição 12 concluímos que $ord_n a|(i-j)$ e pela definição de congruência temos $i \equiv j \pmod{ord_n a}$.

Reciprocamente se $i \equiv j \pmod{ord_n a}$ então $i = k \cdot ord_n a + j$ assim $a^i = a^{k \cdot ord_n a + j} = \left(a^{ord_n a}\right)^k \cdot a^j \equiv a^j \pmod{n}$, uma vez que $a^{ord_n a} \equiv 1 \pmod{m}$

□

Proposição 15 *Se $ord_n a = t$ e u é um inteiro positivo, então*

$$ord_n a^u = \frac{t}{(u,t)}$$

Prova: Vamos definir $ord_n a = t$, $ord_n a^u = s$, $(t,u) = d$. Pela divisão euclidiana temos $u = d \cdot u_1$ e $t = d \cdot t_1$.

Notemos agora que

$$(a^u)^{t_1} = \left(a^{d \cdot u_1}\right)^{\frac{t}{d}} = \left(a^t\right)^{u_1} \equiv 1 \pmod{n}$$

de onde concluímos que $ord_n a^u = s$ divide t_1.

Por outro lado temos que $(a^u)^s = a^{us} \equiv 1 \pmod{n}$. Sabemos agora que $t|us$, pois $t = ord_n a$ então $d \cdot t_1 | d \cdot u_1 \cdot s$ que resulta em $t_1 | u_1 \cdot s$. É fácil ver que $(u_1, t_1) = 1$, concluímos que $t_1|s$. Como $s|t_1$ e $t_1|s$ provamos que $s = t_1$. Ou seja, $ord_n a^u = \frac{t}{(u,t)}$

□

Proposição 16 *Dados r e n inteiros positivos coprimos com $n > 0$, se r é uma raiz primitiva módulo n, então os inteiros*

$$r,\ r^2,\ ,\cdots,\ r^{\phi(n)}$$

formam um sistema reduzido de resíduos módulo n.

Prova: Para provar que as primeiras $\phi(n)$ potência de uma raiz primitiva forma um sistema reduzido de resíduos módulo n, precisamos apenas mostrar que elas são coprimas com n e não são congruentes duas a duas.

Pela hipótese de r ser raiz primitiva módulo n concluímos que $(n,r) = 1$. Consequentemente $(n, r^k) = 1$ para todo $k \in \mathbb{N}$, assim todas as potências de r são coprimas com n.

Assumindo que $r^i \equiv r^j \pmod{n}$, pela proposição 14 isso só ocorre se $i \equiv j \mod ord_n r$, o que implica em $i \equiv j \mod \phi(n)$ com $1 \leq i \leq \phi(n)$ e $1 \leq j \leq \phi(n)$. Pela definição de congruência temos $\phi(n)|i-j$ que só ocorre se $i-j=0$, pois $i-j < \phi(n)$. Concluímos que $r^i \equiv r^j \pmod{n}$ se, e só se, $i=j$.

□

Exemplo 12

Pelo exemplo 11, já sabemos que 3 é uma raiz primitiva módulo 5 então temos $SRR_5 = \{3, 3^2, 3^3, 3^4\}$que podem ser $SRR_5 = \{1, 2, 3, 4\}$

Proposição 17 *Seja r uma raiz primitiva módulo n onde n é um inteiro maior que 1, então r^u é também raiz primitiva módulo n se, e só se, $(u, \phi(n)) = 1$.*

Prova: Pela proposição 15 temos que $ord_n a^u = \dfrac{ord_n a}{(u, ord_n a)}$ então $ord_n r^u = \dfrac{ord_n r}{(u, ord_r n)} = \dfrac{\phi(n)}{(u, \phi(n))}$, consequentemente, $ord_n r^u = \phi(n)$, ou seja, r^u será uma raiz primitiva módulo n se e só se $(u, \phi(n)) = 1$.

□

Exemplo 13

Como $\phi(5) = 4$ e $(4,1) = (4,3) = 1$ concluímos que $3^1 \equiv 3 \pmod{5}$ e $3^3 \equiv 2 \pmod{5}$ são raizes primitivas módulo 5.

Proposição 18 *Se um inteiro n tem uma raiz primitiva, então n tem exatamente $\phi(\phi(n))$ raízes primitivas incongruentes.*

Prova: A proposição 16 nos garante que $r,\ r^2, \cdots, r^{\phi(n)}$ forma um sistema reduzido de resíduos módulo n e conforme a proposição 17 concluímos que apenas as i-potencias, $1 \leq i \leq \phi(n)$, com $(i, \phi(n)) = 1$ são raízes primitivas módulo n, então, existe $\phi(\phi(n))$ raízes primitivas módulo n.

□

Exemplo 14

Vamos obter as raízes primitivas módulo 11. Afirmamos que 2 é raiz primitiva módulo 11, e de fato é pois $\phi(11) = 11 - 1 = 10$ e $2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^5 \equiv 10 \pmod{11}$ e $2^{10} \equiv 1 \pmod{11}$. Agora podemos obter as demais raízes primitivas, e são elas: $2^1 \equiv 2 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$ e $2^9 \equiv 6 \pmod{11}$

As raízes primitivas é um parte da teoria dos números importantíssima, poderíamos escrever muitas páginas sobre este tópico, entretanto escaparíamos e muito do nosso objetivo neste trabalho. Para um estudo profundo deste tema recomendamos Rosen (2005).

Todavia nosso objetivo é apresentar que todo primo tem raiz primitiva. Pra alcançar esta meta lançamos mão de alguns teoremas cujas as demonstrações podem ser encontradas em Rosen (2005).

Definição 18 *Seja $f(x)$ um polinômio de coeficientes inteiros. Dizemos que c é uma raiz de $f(x)$ módulo m se $f(c) \equiv 0 \pmod{m}$.*

É fácil ver que se c é uma raiz de $f(x)$ módulo m então todo inteiro x congruente a c módulo m também será raiz.

Exemplo 15

Afirmamos que $f(x) = x^2 + x + 1$ tem exatamente duas raízes módulo 7, $x \equiv 2 \pmod{7}$ e $x \equiv 4 \pmod{m}$ e de fato, substituindo $x = 0, 1, 2, 3, 4, 5, 6$ em $f(x)$, temos:

$0^2 + 0 + 1 \not\equiv 0 \pmod{7}$, $1^2 + 1 + 1 \not\equiv 0 \pmod{7}$, $2^2 + 2 + 1 = 7 \equiv 0 \pmod{7}$ $3^2+3+1 \not\equiv 0 \pmod{7}$, $4^2+4+1 = 21 \equiv 0 \pmod{7}$, $5^2+5+1 \not\equiv 0 \pmod{7}$, $6^2+6+1 \not\equiv 0 \pmod{7}$

Exemplo 16

O polinômio $g(x) = x^2 + 2$ não tem raízes módulo 5, pois,

$0^2+2 \not\equiv 0 \pmod{5}$, $1^2+2 \not\equiv 0 \pmod{5}$, $2^2+2 \not\equiv 0 \pmod{5}$, $3^2+2 \not\equiv 0 \pmod{5}$, $4^2 + 2 \not\equiv 0 \pmod{5}$.

Exemplo 17

O pequeno teorema de Fermat nos diz que caso p seja primo, então o polinômio $h(x) = x^{p-1} - 1$ tem exatamente $p - 1$ raízes módulo p.

Teorema 19 *Seja p um primo e seja d um divisor de $p - 1$. Então o polinômio $x^d - 1$ tem exatamente d raízes incongruentes módulo p.*

Prova A prova deste teorema pode ser encontrada em Rosen (2005).

□

Teorema 20 *Seja p um primo e tomemos d um divisor de $p - 1$. Então o número de inteiros incongruentes de ordem d módulo p é igual a $\phi(p)$.*

Prova A prova deste teorema pode ser encontrada em Rosen (2005).

□

Teorema 21 *Todo primo tem um raiz primitiva.*

Prova: Seja p um primo. Pelo teorema 20, sabemos que existem $\phi(p-1)$ inteiros incongruentes de ordem $p - 1$ módulo p. Devido a este fato e pela definição de raiz primitiva, p tem $\phi(p-1)$ raízes primitiva.

□

A existência de raízes primitivas não está restrita aos números primos. Sabemos que todos os números da forma $1,\ 2,\ 4,\ p^t$ e $2p^t$ com p primo e t inteiro positivo possuem raiz primitiva. Para um justificativa ver Rosen (2005).

1.4 A Aritmética dos Índices

Com base na proposição 16 sabemos que os inteiros $r,\ r^2,\ r^3, \cdots, r^{\phi(m)}$ forma um sistema reduzido de resíduos módulo m. A partir deste fato percebemos que se a é um inteiro coprimo com m estão existe um único x com $1 \leq x \leq \phi(m)$ de modo que

$$a \equiv r^x \pmod{m}$$

Definição 19 *Seja m um inteiro positivo com uma raiz primitiva r e a é um inteiro positivo com $(a, m) = 1$ então o inteiro x com $1 \leq x \leq \phi(m)$ tal que $r^x \equiv a \pmod{m}$ é chamado de índice de a na base r módulo m.*

Neste caso escrevemos $\text{ind}_r a$ para indicar o indice de a na base r módulo m.

Exemplo 18

5 é uma raiz primitiva módulo 18.

É fácil ver que

$$5^1 \equiv 5 \pmod{18} \qquad 5^2 \equiv 7 \pmod{18} \qquad 5^3 \equiv 17 \pmod{18}$$
$$5^4 \equiv 13 \pmod{18} \qquad 5^5 \equiv 11 \pmod{18} \qquad 5^6 \equiv 1 \pmod{18}$$

assim:

$$\text{ind}_5 5 = 1 \qquad \text{ind}_5 7 = 2 \qquad \text{ind}_5 17 = 3$$
$$\text{ind}_5 3 = 4 \qquad \text{ind}_5 11 = 5 \qquad \text{ind}_5 1 = 6$$

Observando a definição de $\text{ind}_r a$, vemos que este número é um expoente positivo e que $r^{\text{ind}_r a} \equiv a \pmod{n}$ e ainda, $\text{ind}_r a$ é o menor expoente positivo onde $1 \leq \text{ind}_r a \leq \phi(n)$.

Suponha que $a \equiv b \pmod{m}$ e que r é um raiz primitiva módulo m. Então $r^{\text{ind}_r a} \equiv a \pmod{m}$ e $r^{\text{ind}_r b} \equiv b \pmod{m}$, logo $r^{\text{ind}_r a} \equiv r^{\text{ind}_r b} \pmod{m}$. Pela proposição 14 temos $\text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(n)}$, portanto

$$a \equiv b \pmod{m} \Leftrightarrow \text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)} \tag{1.1}$$

Desta forma a propriedade $r^{\text{ind}_r a} \equiv a \pmod{m}$ nos faz lembrar o número real w definido como logaritmo de u na base v com um u e v números reais positivos e $v \neq 1$, ou seja, $w = \log_v u$. Equivalentemente $v^w = u$ e também sua propriedade de que $v^{\log_v u} = u$ de modo semelhante 1.1 nos faz lembra que $\log_v u = \log_v x \Leftrightarrow u = x$. Veremos algumas propriedades dos índices aritméticos.

Teorema 22 *Seja m um inteiro positivo com raiz primitiva r e seja a e b inteiros coprimos com m. Então:*

i) $ind_r 1 \equiv 0 \mod \phi(m)$

ii) $ind_r(a \cdot b) \equiv (ind_r a + ind_r b) \pmod{\phi(m)}$

iii) $ind_r a^k \equiv k \cdot ind_r a \pmod{\phi(m)}$ *para* k *natural*

Prova *i)* Pelo teorema de Euler temos que $r^{\phi(m)} \equiv 1 \pmod{m}$ como r é uma raiz primitiva de m então $\phi(m)$ é a menor potência de r congruente a 1 então $\text{ind}_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$.

ii) Notemos que $r^{\text{ind}_r(a\cdot b)} \equiv a \cdot b \pmod{m}$ e $r^{\text{ind}_r a + \text{ind}_r b} = r^{\text{ind}_r a} \cdot r^{\text{ind}_r b} \equiv a \cdot b \pmod{m}$ então $r^{\text{ind}_r(a\cdot b)} \equiv r^{\text{ind}_r a + \text{ind}_r b} \pmod{m}$, consequentemente $\text{ind}_r(a \cdot b) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$

iii) Inicialmente notemos que $r^{\text{ind}_r a^k} \equiv a^k \pmod{m}$ e de fato $\text{ind}_r a^k = x \Rightarrow r^x \equiv a^k \pmod{m} \Rightarrow r^{\text{ind}_r a^k} \equiv a^k \pmod{m}$ e $r^{k\cdot \text{ind}_r a} \equiv \left(r^{\text{ind}_r a}\right)^k \equiv a^k \pmod{m}$ então $r^{\text{ind}_r a^k} \equiv r^{k\cdot ind_r a} \pmod{m}$ e consequentemente $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$.

□

Por isso na definição 19 também dizemos que x é o logaritmo discreto de a na base r, ou seja, $r^{\log_r a} \equiv a \pmod{m}$. Logo o teorema 22 pode ser reescrito da seguinte forma:

Teorema 23 *Seja m um inteiro positivo com raiz primitiva r e seja a e b inteiros coprimos com m. Então:*

i) $\log_r 1 \equiv 0 \pmod{\phi(m)}$

ii) $\log_r(a \cdot b) \equiv (\log_r a + \log_r b) \pmod{\phi(m)}$

iii) $\log_r a^k \equiv k \cdot \log_r a \pmod{\phi(m)}$ *para* k *natural*

Exemplo 19

Seja $m = 7$ temos que $r = 3$ é uma raiz primitiva módulo 7.

É fácil ver que

$$3^1 \equiv 3 \pmod 7 \qquad 3^2 \equiv 2 \pmod 7 \qquad 3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4 \pmod 7 \qquad 3^5 \equiv 5 \pmod 7 \qquad 3^6 \equiv 1 \pmod 7$$

assim:

$$\log_3 1 = 6 \qquad \log_3 3 = 1 \qquad \log_3 5 = 5$$
$$\log_3 2 = 2 \qquad \log_3 4 = 4 \qquad \log_3 6 = 3$$

Exemplo 20

Considerando ainda $m = 7$ e $r = 5$ temos

$$5^1 \equiv 5 \pmod 7 \qquad 5^2 \equiv 4 \pmod 7 \qquad 5^3 \equiv 6 \pmod 7$$
$$5^4 \equiv 2 \pmod 7 \qquad 5^5 \equiv 3 \pmod 7 \qquad 5^6 \equiv 1 \pmod 7$$

$$\log_5 1 = 6 \qquad \log_5 3 = 5 \qquad \log_5 5 = 1$$
$$\log_5 2 = 4 \qquad \log_5 4 = 2 \qquad \log_5 6 = 3$$

Pelo exemplo 20 podemos notar que:

$$\log_5 1 = 6 \equiv 0 \pmod{\phi(7)}$$

e

$$\log_5 2 + \log_5 3 = 4 + 5 \equiv 3 = \log_5 6 \pmod{\phi(7)}.$$

Capítulo 2

Noções de Criptografia

Criptografia é a junção de duas palavras oriundas do grego, e são elas *kryptós* que significa "escondido", "oculto", "obscuro" e *gráphein* de significado "descrever", "escrever"; "escrita", portanto, a grosso modo, podemos entender que criptografar um mensagem é escreve-la de modo difícil compreensão por uma pessoa que não saiba com descriptografá-la.

Acredita-se que a primeira mensagem criptografada foi usada pelo escriba do faraó egípcio Khnumhotep II, por volta de 1900 antes de Cristo, que documentou em tabletes de argila os segredos do tesouro de uma pirâmide e teve a ideia de substituir algumas palavras ou alguns trechos do texto por códigos. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro e morreria de fome, perdido nas catacumbas da pirâmide.

Antes do avanço da criptografia usava-se a técnica de esconder a mensagem de forma a não ser lida pelo inimigo, um exemplo cruel de esteganografia antiga é escolher um escravo, rapava a cabeça e tatuava a mensagem no couro cabeludo. Após o cabelo ter crescido novamente o enviava ao destinatário da mensagem.

Além do Egito, também existe registro dos primórdios da criptografia na China, na Mesopotâmia e até na bíblia, porém os gregos tiveram mais destaque principalmente em dois métodos.

O primeiro deles é o sistema monoalfabético de Cesar que baseia em trocar cada letra do alfabeto por uma outra, de tal forma que esta relação se mantenha fixa. Por exemplo se usarmos a chave 5 a letra l será substituída pela letra $l' \equiv (l+5)\ mod\ 26$ logo a primeira letra do alfabeto será substituída pela letra $l' \equiv (1+5)\ mod\ 26 \Rightarrow l' = 6$, assim

a letra F corresponderá a letra A. Repetindo os cálculos teremos que G corresponde a B, H corresponde a C e assim por diante.

Este sistema parece eficiente, no entanto, um texto de uma determinada língua as letras aparecem com determinada frequência e algumas regras de concordância tornam este sistema frágil.

O segundo é conhecido atualmente como "quadrado de Polybius", neste método as letras do alfabeto eram distribuídas em uma matriz quadrada de ordem 5 e seu valor correspondente seria o número $i \cdot 10 + j$, onde i é a linha e j é a coluna.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

Tabela 2.1: O quadrado de Polybius

Por exemplo se desejo escrever $Isaac$ terei 2444111113.

A criptografia teve muita importância no decorrer da história humana.

Em 8 de fevereiro de 1587 era executada a rainha Maria Stuart da Escócia por tramar a morte da rainha Elizabeth I da Inglaterra. A principal prova contra Maria era um conjunto de cartas criptografadas interceptadas cujo conteúdo consistia num plano para substituir Elizabeth por Maria. Nestas cartas continham a prova de que Maria estava tramado a morte de Elizabeth, deste modo, Maria subiria ao trono já que era prima de Elizabeth.

Durante a segunda guerra mundial a criptografia foi um dos principais fatores para o desfecho. Quando a Inglaterra conseguiu decifrar os códigos produzidos pela máquina *Enigma* dos Nazistas.

Podemos notar que a criptografia é tão antiga quanto a própria escrita. Entretanto, só recentemente se tornou alvo de extenso estudo científico. Uma das grandes motivações é a segurança de dados, como compras eletrônicas, assinatura digital de documentos, controle de acesso, transações de dinheiro eletrônico.

Um criptosistema moderno é uma coleção de cinco elementos $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ com as seguintes propriedades:

- $\mathcal{P}$ é um conjunto chamado de *Espaço de texto comum.* onde estão as informações que podem ser lidas por todos, muitas vezes chamado de texto puro.

- $\mathcal{C}$ é um conjunto chamado de *Espaço de texto cifrado*, onde estão todos os textos criptografados.

- $\mathcal{K}$ é um conjunto onde se encontram todas as chaves para codificar uma mensagem.

  Devemos entender que "chave"neste texto é o nome dado ao objeto de codificação e decodificação de um texto, nos métodos criptográficos recentes este objeto é um número.

- $\mathcal{E}$= $\{E_k : k \in \mathcal{K}\}$ é uma família de funções $E_k : \mathcal{P} \to \mathcal{C}$, cujos elementos são chamados de funções de codificação criptográfica.

- $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ é uma família de funções $D_k : \mathcal{C} \to \mathcal{P}$. Seus elementos são funções de decodificação criptográfica.

Devemos perceber que as funções das famílias E_k e D_k são sobrejetivas, pois todo texto $\mathcal{P}$ e $\mathcal{C}$ devem ser levados a algum elemento, para garantir a funcionalidade do sistema. E certamente estas funções devem ser injetivas para evitar ambiguidade na mensagem tornando o sistema criptográfico falho.

Observemos que a bijetividade das funções E_k e D_k nos garante que estas admitem uma função inversa, no entanto estas inversas estão em conjuntos diferentes, ou seja, temos que $E_e \in \mathcal{E}$ enquanto que a sua inversa $D_d \in \mathcal{D}$. Em símbolos $\forall e \in \mathcal{K}$, $\exists d \in \mathcal{K}$ tal que $D_d(E_e(p)) = p$ para todo $p \in \mathcal{P}$.

Notemos que os elementos dos conjuntos $\mathcal{P}$ e $\mathcal{C}$ são letras, então a primeira coisa a fazer se desejarmos usar algum criptosistema numérico devemos converter a mensagem em uma sequência de números. Suporemos, para simplificar, que a mensagem original é um texto onde não haja números (caso tenha, basta escrevê-los usando o alfabeto e não os algarismos), apenas palavras.

Na pré-codificação convertemos as letras em números usando a seguinte tabela de conversão.

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

Tabela 2.2: Pré Codificação de Textos

E o espaço entre duas palavras será substituído pelo número 99

Adotaremos aqui que cada letra corresponde a um número de dois algarismos, afim de evitar ambiguidades. Podemos, agora, "escrever" numericamente uma mensagem usando a tabela 2.2, por exemplo, pré-codificamos a mensagem " teoria dos números" e obtemos

29142427181099132428992302214272428

Se em um criptosistema a chave de codificação criptográfica e é sempre igual à chave de decodificação criptográfica, então o criptosistema é chamado *simétrico*.

A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entenda que se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.

Usuários de um sistema simétrico precisam trocar a chave secreta e antes de começarem sua comunicação. A chave e precisa ser mantida secreta dado que qualquer um que conheça e pode determinar a correspondente chave d de decodificação criptográfica.

Uma solução para problema de trocar a chave no sistema simétrico é o seguinte:

Seja R o remetente e D destinatário de uma mensagem secreta TP que será enviada por um meio não seguro. O remetente R escolhe uma chave e_1 e criptografa a mensagem TP resultando em $e_1(TP)$ e envia para D, ao receber a mensagem $e_1(TP)$, D escolhe uma outra chave e_2 e criptografa a mensagem novamente resultando agora em $e_2(e_1(TP))$ e retorna a mensagem para R. Desta vez R descriptografa a mensagem usando a chave d_1 do seguinte modo $d_1(e_2(e_1(TP))) = d_1(e_1(e_2(TP))) = e_2(TP)$ e retorna a mensagem para D faltando agora apenas aplicar d_2 e $d_2(e_2(tp)) = tp$.

Mas esta solução ainda contém dois problemas; o primeiro é que temos que enviar

a mensagem três vezes pelo canal de comunicação, que é um risco; e segundo, precisamos que nosso criptosistema seja comutativo, ou seja, não importará a ordem que a mensagem será criptografada e descriptografada. Estes dois problemas devem expor o sistema a sérios riscos de se conhecer a chave secreta.

Os principais algoritmos criptográficos simétricos são:

- AES

  O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo National Institute of Standards and Technology (NIST) em 2003.

- 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.

- 3DES

  O 3DES é uma simples variação do DES, utilizando-o em três ciframentos sucessivos.

- IDEA

  O International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec.

- Blowfish

  Algoritmo desenvolvido por Bruce Schneier, que oferece a escolha, entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou o no Twofish.

- RC2

  Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo.

- CAST

  É um algoritmo de cifra de bloco, sendo criado em 1996 por Carlisle Adams e Stafford Tavares.

Nos *criptosistemas assimétricos*, as chaves d e e são distintas e o cálculo de d a partir de e é inviável. Em tais sistemas, a chave de codificação pode ser tornada pública. Assim se eu desejar receber mensagens criptografadas, eu publico uma chave de

codificação criptográfica e e mantenho secreta a correspondente chave d de decodificação criptográfica.

Este modelo de criptografia foi criado na década de 1970 - pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ - Government Communications Headquarters- na qual cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública.

A segurança deste modelo de criptografia é a dificuldade de obter e a partir de d. Vejamos agora os exemplos mais conhecidos de criptosistemas assimétricos e no que se baseia sua segurança.

- RSA

  O 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 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. A segurança 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.

- Diffie-Hellman

  Baseado no problema do logaritmo discreto, é o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste criptosistema em 1976.

- Curvas Elipticas

  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, que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos.

- ElGamal

  Que é o principal objetivo. Cuja segurança também está baseada na dificuldade de

obter solução do problema do logaritmo discreto em grupo ciclíco finito.

Capítulo 3

O Criptosistema de ElGamal

O ElGamal é um 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 na dificuldade de calcular logaritmos discretos em um grupo cíclico finito, o que lembra bastante o problema de escrever números inteiros em um produto de fatores primos.

3.1 O Problema do Logaritmo Discreto

A segurança de várias técnicas criptográficas dependem da dificuldade de se obter uma solução para o logaritmos discreto que definiremos agora.

Definição 20 (O problema do logaritmo discreto, PLD) *Tome um primo p, um gerador α de $\mathbb{Z}_p^*$, e um elemento β de $\mathbb{Z}_p^*$, encontrar um inteiro x tal que $0 \leq x \leq p-2$, de modo que $\alpha^x \equiv \beta \pmod{p}$*

A definição anterior por ser generalizada para um grupo cíclico finito qualquer G

Definição 21 *Tomemos um grupo cíclico e finito G de ordem n, um gerador α de G e um elementos de $\beta \in G$, encontrar um inteiro x, $0 \leq x \leq n-1$, de modo que $\alpha^x = \beta$*

Apesar de ser intratável computacionalmente, o PLD tem algumas soluções que apresentaremos no próximo capítulo.

Sem uma boa calculadora é muito difícil calcular a ordem de um número inteiro módulo p, as raízes primitivas e mais ainda o logaritmos discreto, para auxiliar nesta empreitada, uma poderosa ferramenta na resolução de alguns problemas é o software Maple© um dos mais conhecidos no meio acadêmico.

3.2 Usando o MAPLE

Todos os cálculos apresentado para obter a ordem, a raiz primitiva, e até mesmo o logaritmo discreto são simples porém, se desejarmos operar com valores muito altos não será fácil.

Apresentamos uma ferramenta computacional para facilitar este processo.

O Maple é um software algébrico pago, desenvolvido inicialmente em 1981 na universidade de Waterloo no Canadá. Todas os conceitos empregados aqui são obtidos no manual fornecido em MapleSoft (2008). Existem inúmeros tutoriais disponíveis na internet.

Para efetuarmos as operações citadas anteriormente, primeiro devemos carregar o pacote teoria dos números clicando em ferramentas $\rightarrow$ carregar pacotes $\rightarrow$ teoria dos números.

Após carregado o pacote, podemos obter a ordem de um número usando o comando: order(n,m) onde n é um inteiro qualquer e m é um inteiro positivo, de modo que $n^i = 1 \pmod{m}$ caso queira saber a ordem de 30 módulo 999983 obteremos 999932. Caso $(m, n) \neq 1$ o programa responderá a mensagem $FAIL$

Para calcularmos uma raiz primitiva de um número devemos, ainda com o pacote carregado, inserir o comando primroot(n) e terá como resposta a menor raiz primitiva do número n ou primroot(g,n) e terá como resposta a menor raiz primitiva módulo n maior que g

E para obtermos o logaritmo discreto y da equação $a^y \equiv x \pmod{m}$ fornecemos os dados no comando mlog(x,a,m), por exemplo se inserirmos mlog(963878,1002,999983) teremos como resposta $y = 452$.

3.3 O processo de Codificação e Decodificação

Em cada etapa a seguir usaremos um exemplo para ilustrá-las. Posteriormente este, apresentaremos um segundo exemplo mais amplo.

3.4 Criando uma chave

Deve-se, em primeiro lugar, escolher um número primo aleatório p em seguida cálcula-se uma raiz primitiva g de p e depois deve-se escolher um número x aleatório com $x < p$. Calcula-se

$$y \equiv g^x \pmod{p}$$

A chave pública será $[y, g, p]$, e a chave particular será o número x. Para garantir a segurança do algoritmo, todos os números apresentados devem ter no mínimo 100 casas decimais pois, a segurança do sistema esta relaciona à quantidade de algarismos dos números.

Exemplo 21

Tomemos o número 10007 vamos verificar se este número é primo. Existem inúmeros teste de primalidade de um inteiro, usaremos o método chamado de Crivo de Erastótenes, por ser o mais simples e mais acessível a iniciantes em teoria dos números.

Sabemos que $\sqrt{10007} \cong 100$ e o conjunto dos primos p menores que 100 é $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$ vamos começar os testes:

$$\begin{array}{lcl}
10007 = 5003 \cdot 2 + 1 & \Rightarrow & 2 \not| 10007 \\
10007 = 3335 \cdot 3 + 2 & \Rightarrow & 3 \not| 10007 \\
10007 = 2001 \cdot 5 + 2 & \Rightarrow & 5 \not| 10007 \\
10007 = 1429 \cdot 7 + 4 & \Rightarrow & 7 \not| 10007 \\
10007 = 909 \cdot 11 + 8 & \Rightarrow & 11 \not| 10007 \\
10007 = 769 \cdot 13 + 10 & \Rightarrow & 13 \not| 10007 \\
10007 = 588 \cdot 17 + 11 & \Rightarrow & 17 \not| 10007 \\
10007 = 526 \cdot 19 + 13 & \Rightarrow & 19 \not| 10007 \\
10007 = 435 \cdot 23 + 2 & \Rightarrow & 23 \not| 10007 \\
10007 = 345 \cdot 29 + 2 & \Rightarrow & 29 \not| 10007 \\
10007 = 322 \cdot 31 + 25 & \Rightarrow & 31 \not| 10007 \\
10007 = 270 \cdot 37 + 17 & \Rightarrow & 37 \not| 10007
\end{array}$$

$$\begin{array}{lcl}
10007 = 244 \cdot 41 + 3 & \Rightarrow & 41 \not| 10007 \\
10007 = 232 \cdot 43 + 31 & \Rightarrow & 43 \not| 10007 \\
10007 = 212 \cdot 47 + 43 & \Rightarrow & 47 \not| 10007 \\
10007 = 188 \cdot 53 + 43 & \Rightarrow & 53 \not| 10007 \\
10007 = 169 \cdot 59 + 36 & \Rightarrow & 59 \not| 10007 \\
10007 = 164 \cdot 61 + 3 & \Rightarrow & 61 \not| 10007 \\
10007 = 149 \cdot 67 + 24 & \Rightarrow & 67 \not| 10007 \\
10007 = 140 \cdot 71 + 67 & \Rightarrow & 71 \not| 10007 \\
10007 = 137 \cdot 73 + 6 & \Rightarrow & 73 \not| 10007 \\
10007 = 126 \cdot 79 + 53 & \Rightarrow & 79 \not| 10007 \\
10007 = 120 \cdot 83 + 47 & \Rightarrow & 83 \not| 10007 \\
10007 = 112 \cdot 89 + 39 & \Rightarrow & 89 \not| 10007 \\
10007 = 103 \cdot 97 + 16 & \Rightarrow & 97 \not| 10007
\end{array}$$

Concluímos que 10007 é primo. Devemos agora obter uma raiz primitiva de $p = 10007$, o faremos por tentativa e erros, no entanto é necessário ter em mente o corolário 13.

Tentaremos inicialmente 2, calculamos $\phi(10007) = 10006$ pelo corolário 13 sabemos que os candidatos a $ord_{10007}2$ são os divisores de $\phi(10007)$ que são $\{1, 2, 5003, 10006\}$. Calculando temos $2^1 \equiv 2 \not\equiv 1 \pmod{10007}$, $2^2 \equiv 4 \not\equiv 1 \pmod{10007}$, $2^{5003} \equiv 1 \pmod{10007}$ como $ord_{10007}2 = 5003 \neq 10006 = \phi(10007)$ concluímos que 2 não é uma raiz primitiva módulo 10007

Tentaremos agora 5, $5^1 \equiv 5 \not\equiv 1 \pmod{10007}$, $5^2 \equiv 25 \not\equiv 1 \pmod{10007}$, $5^{5003} \equiv -1 \pmod{10007}$ e $5^{10006} \equiv 1 \pmod{10007}$ como $ord_{10007}5 = 10006 = \phi(10007)$ concluímos que 5 é uma raiz primitiva módulo 10007.

Basta agora escolher um número inteiro, digamos $x = 1000$, e calcularmos
$y \equiv 5^{1000} \pmod{10007}$ ou seja $y \equiv ((5^{10})^{10})^{10} \equiv ((8800)^{10})^{10} \equiv 8230^{10} \equiv 5801 \pmod{10007}$

Logo temos a chave pública $[5801, 5, 10007]$ e a chave privada $x = 1000$

3.5 Codificando uma Mensagem

Queremos criptografar a mensagem tp. Primeiro escolhe-se um número k com $0 \leq k \leq p-2$, tal que $(k, p-1) = 1$. Então calculamos,

$$\begin{aligned} a &\equiv g^k \pmod{p} \\ b &\equiv (tp \cdot y^k) \pmod{p} \end{aligned}$$

Então o texto criptografado será $[a, b]$.

Exemplo 22

Vamos criptografar $tp = 1516$ com a chave pública $[5801, 5, 10007]$. Escolhemos um número $k = 30$ então:

$$\begin{aligned} a &\equiv 5^{30} \equiv 3290 \pmod{10007} \\ b &\equiv (1516 \cdot 5801^{30}) \equiv 4528 \pmod{10007} \end{aligned}$$

Assim o texto criptografado será $[3290, 4528]$

3.6 Decodificando a Mensagem

Agora para o receptor decodificar a mensagem ele toma o valor a e calcula

$$\xi \equiv \left(a^{-1}\right)^{x} \pmod{p}$$

e usará o resultado para calcular

$$tp \equiv (b \cdot \xi) \pmod{p}.$$

Exemplo 23

Tomemos a chave privada $x = 1000$ e calcularmos $\xi \equiv \left(3290^{-1}\right)^{1000} \pmod{10007}$, que faremos por partes. Um processo simples para obtermos o inverso 3290^{-1} módulo 10007 é resolver a congruência $3290 \cdot a^{-1} \equiv 1 \pmod{10007}$ que é o mesmo que resolver a equação diofantina $3267 \cdot a^{-1} - 10007 \cdot z = 1$, pelo algoritmo de Euclides estendido teremos $1 = 3290 \cdot 5040 - 10007 \cdot 1657$, ou seja, $a^{-1} = 5040$. Agora $\xi \equiv 5040^{1000} \equiv 5437 \pmod{10007}$

Teremos o texto puro será $tp \equiv (4528 \cdot 5437) \pmod{10007}$ que será $tp \equiv 1516 \pmod{10007}$ retomando o texto original.

3.7 Exemplo Completo

Para ilustrar este fato, criaremos uma situação onde Jhon e Isaac desejam intercambiar uma mensagem secreta por um meio inseguro. Vamos supor que a mensagem seja $tp = 251018$.

Jhon escolhe os números $p = 999983$ $g = 48732$ e $x = 532$ e calcula

$$y \equiv 48732^{532} \pmod{999983}$$

obtendo $y = 532760$ e divulga $[532760, 48732, 999983]$

Quando Isaac recebe a chave pública e escolhe $k = 997$, pois $(997, \phi(999983)) = 1$ calcula

$$a \equiv 48732^{997} \pmod{999983} \text{ e } b \equiv 251018 \cdot 532760^{997} \pmod{999983}$$

obtendo a mensagem cifrada $[831610, 658822]$, agora basta envia-la para Jhon.

Jhon recebe a mensagem enviada por Isaac e deseja decifrá-la, para tanto calcula

$$\xi \equiv \left(831610^{532}\right)^{-1} \pmod{999983}$$

obtendo $\xi = 933484$ e posteriormente calcula

$$tp \equiv 658822 \cdot 933484 \pmod{999983}$$

Chegando a $tp = 251018$ que realmente é a mensagem enviada por Isaac.

Em 1977 os criadores do RSA lançaram o desafio intitulado RSA-129, que consistia em decifrar uma mensagem criptografada pelo método RSA com uma chave de 129 bits. Esse problema foi resolvido em 1993 por uma rede de 600 computadores coordenados por Derek Atkins, Michael Graff, Arjen Lenstra e Paul Leyland cuja solução é "The Magic Words are Squeamish Ossifrage".

Em homenagem a este problema codificaremos "The Magic Words are Squeamish Ossifrage"pelo sistema criptográfico de ElGamal usando a chave pública $[y, g, p] = [15, 5, 227]$.

$[5, 208]$	$[125, 171]$	$[174, 159]$	$[35, 86]$	$[125, 154]$	$[174, 52]$
$[17, 7]$	$[37, 149]$	$[125, 175]$	$[174, 78]$	$[37, 165]$	$[17, 169]$
$[128, 68]$	$[17, 130]$	$[37, 165]$	$[17, 182]$	$[174, 91]$	$[37, 58]$
$[17, 182]$	$[125, 154]$	$[174, 185]$	$[37, 110]$	$[17, 137]$	$[174, 112]$
$[198, 57]$	$[37, 45]$	$[198, 180]$	$[125, 141]$	$[5, 225]$	$[198, 206]$
$[174, 156]$	$[17, 208]$	$[125, 134]$			

Tabela 3.1: Texto Criptografado

3.8 Resolvendo o PLD

Uma pergunta razoável é "Por que o criptosistema funciona?". A resposta para essa pergunta se dá em duas partes: A primeira diz respeito ao protocolo. Notemos que

$$
\begin{aligned}
b \cdot \xi &\Rightarrow (tp \cdot y^k) \cdot a^{-x} \pmod{p} \\
&\Rightarrow tp \cdot y^k \cdot (g^k)^{-x} \pmod{p} \\
&\Rightarrow tp \cdot y^k \cdot y^{-k} \pmod{p} \\
&\Rightarrow tp \pmod{p} \\
&\Rightarrow tp
\end{aligned}
$$

o que garante que o protocolo funciona.

A segunda diz respeito à segurança. Ainda não existe um algoritmo eficiente para resolver o problema do logaritmo discreto, apesar disto, apresentaremos alguns esquema para obter o logaritmo discreto.

O primeiro e mais obvio método para solucionar o PLD é através da procura exaustiva na sequência $\alpha^{x_1} \equiv \beta_1 \pmod{p}$, $\alpha^{x_2} \equiv \beta_2 \pmod{p}$, $\alpha^{x_3} \equiv \beta_3 \pmod{p}$, até encontrar um $\beta_j = \beta$ obtendo a chave secreta. É notório que este esquema não é eficiente, principalmente se tratando de criptografia onde a ordem de $\mathbb{Z}_p$ é gigantesca.

O segundo método é conhecido como Baby-Step Giant-Step Menezes et al. (1996), que funciona assim:

Estamos interessados em obter

$$
\log_r a \pmod{p} \text{ ou } r^x \equiv a \pmod{p} \tag{3.1}
$$

Tomemos m como sendo o maior inteiro mais próximo de $\sqrt{\text{ord}_p r} = \sqrt{p-1}$.

Em seguida devemos observar que pelo algoritmo de Euclides temos $x = im + j$ com $i, j \in \mathbb{N}$ e $0 \leq j < m$ e substituindo em 3.1 teremos

$$
\begin{aligned}
r^{im+j} &\equiv a \pmod{m} &&\Leftrightarrow \\
r^{im} \cdot r^j &\equiv a \pmod{m} &&\Leftrightarrow \\
r^j &\equiv a \cdot (r^{im})^{-1} \pmod{m} &&\Leftrightarrow
\end{aligned}
$$

que, implica em

$$a \cdot \left(\left(r^{-1}\right)^m\right)^i \equiv r^j \pmod{m} \tag{3.2}$$

Agora basta variar o valor de i até encontrar o valor de $0 \leq j < m$, recomenda-se construir uma tabela com os valores de j e $r^j \pmod{p}$.

Por exemplo. Estamos interessado em calcular $15^x \equiv 54 \pmod{157}$

Notemos que $p = 157$ é primo e 15 é uma raiz primitiva de 157 então $\text{ord}_{157}15 = \phi(157) = 156$ logo $m = \left\lceil \sqrt{156} \right\rceil = 13$ então

$$x = 13i + j \tag{3.3}$$

e substituindo em 3.2 obtemos

$$15^j = 54 \left(\left(15^{-1}\right)^{13}\right)^i \tag{3.4}$$

realizando alguns cálculos temos que $15^{-1} \equiv 21 \pmod{157}$ e $21^{13} \equiv 22 \pmod{157}$, trocando estas informações em 3.4 encontramos

$$15^j = 54 \cdot 22^i \pmod{157} \tag{3.5}$$

Como nossa solução será alguma potência de 15 módulo 157 é interessante construir uma tabela com os possíveis valores para estas potências. Como em 3.3 usamos o algoritmo de Euclides então $0 \leq j < 13$

j	0	1	2	3	4	5	6	7	8	9	10	11	12
15^j	1	15	68	78	71	123	118	43	17	98	57	70	108

Tabela 3.2:

Agora que tenho as possíveis respostas basta variar o valor de $0 \leq i < \infty$ até encontrar algum valor na tabela 3.2.

Iniciamos nossa busca, construindo uma nova tabela.

Para $i = 0$ temos

i	0
$54 \cdot 22^i \pmod{157}$	54

Como 54 não consta na tabela 3.2 faremos o mesmo cálculo para $i = 1$

i	0	1
$54 \cdot 22^i \pmod{157}$	54	89

Como 89 não consta na tabela 3.2 faremos o mesmo cálculo para $i = 2$, e assim por diante, até encontrarmos algum número que conste na tabela 3.2

i	0	1	2	3	4	5	6	7
$54 \cdot 22^i \pmod{157}$	54	89	74	58	20	126	103	68

Por fim encontramos um número, neste caso, $i = 7$ que consta na tabela 3.2 que ocorre quando $j = 2$ pela equação 3.3 temos que $x = 13 \cdot 7 + 2 = 93$ portanto

$$15^{93} \equiv 54 \pmod{157}$$

Apesar do método baby-step Giant-step ser simples ele não é eficiente,pois a procura para o valor de i para chave pública muito grande será exaustiva. Caso i seja pequeno podemos obter a chave privada com facilidade que afetará a segurança do sistema.

Caso o leitor esteja interessado existem mais métodos para encontrar o logaritmo discreto e podem ser encontrados em Menezes et al. (1996) e em ElGamal (1984).

3.9 Assinaturas Digitais

Assinatura digital é um par de números naturais (γ, s) que devem ser adicionados ao texto cifrado de modo que apenas o emissor da mensagem pode obtê-la. Esse par de número deve ser verificável sem a necessidade de saber o teor da mensagem, visto que em caso de desacordo entre as partes com relação ao texto da mensagem, uma terceira pessoa possa verificar a autoria da mensagem.

Assinaturas digitais têm muitas aplicações em segurança da informação, incluindo autenticação e integridade de dados. Uma das aplicações mais importantes de assinatura digital é a certificação de chaves públicas em grandes redes.

O conceito e utilidade de uma assinatura digital foram reconhecidos vários anos antes que qualquer aplicação prática deste conceito estivesse disponível. O primeiro método descoberto foi o esquema de assinatura RSA, que permanece até hoje como uma das técnicas mais práticas e versáteis disponíveis.

3.9.1 Assinando uma Mensagem com ElGamal

Trataremos agora sobre assinaturas digitais pelo criptosistema de ElGamal. Suponha que uma pessoa deseja assinar uma mensagem usando o criptosistema de ElGamal e que também que essa pessoa tenha a chave pública $[y, g, p]$ e a chave privada x de modo que $y \equiv g^x \pmod{p}$.

Para assinar a mensagem tp, essa pessoa com a chave privada x fará o seguinte:
(i) Primeiro selecionará um inteiro k coprimo com $p-1$, ou seja $(k, p-1) = 1$, o que garante a existência do inverso de k módulo $p-1$;
(ii) em seguida calcula γ tal que $\gamma \equiv g^k \pmod{p}$ com $0 \leq \gamma \leq p-1$;
(iii) $s \equiv (tp - x \cdot \gamma)k^{-1} \pmod{p-1}$, com $0 \leq s \leq p-2$;
(iv) A assinatura na mensagem será o par (γ, s) que será anexado ao texto tp.

3.9.2 Verificando a Assinatura

O sistema de criação de assinatura digital só terá efeito se a assinatura for verificável. Para verificar se a assinatura na mensagem tp é autêntica, devemos tomar a chave pública $[y, g, p]$ e a assinatura (γ, s) e calcular os verificadores V_1 e V_2 os quais não dependem da chave privada:

$$V_1 \equiv \gamma^s y^\gamma \pmod{p}, \quad 0 \leq V_1 \leq p-1$$

e

$$V_2 \equiv g^{tp} \pmod{p}, \quad 0 \leq V_2 \leq p-1.$$

Para que a assinatura seja verdadeira devemos obter $V_1 \equiv V_2 \pmod{p}$, ou seja:

$$\begin{aligned}
V_1 &\equiv \gamma^s y^\gamma \pmod{p} \\
&\equiv \gamma^{(tp - x\cdot\gamma)k^{-1}} y^\gamma \pmod{p} \\
&\equiv \left(\gamma^{k^{-1}}\right)^{tp - x\cdot\gamma} y^\gamma \pmod{p} \\
&\equiv g^{tp - x\cdot\gamma} y^\gamma \pmod{p} \\
&\equiv g^{tp} \left(g^{x\cdot\gamma}\right)^{-1} y^\gamma \pmod{p} \\
&\equiv g^{tp} \left(y^\gamma\right)^{-1} y^\gamma \pmod{p} \\
&\equiv g^{tp} \pmod{p} \\
&\equiv V_2 \pmod{p}
\end{aligned}$$

3.9.3 Segurança da Assinatura

Jamais podemos escolher o mesmo k para duas assinaturas diferentes. Se tomarmos o mesmo valor de k para duas assinaturas (γ_1, s_1) e (γ_2, s_2), este valor pode ser encontrado. De fato,para o mesmo k teríamos duas assinaturas

$$s_1 \equiv k^{-1}(tp_1 - x\gamma) \pmod{p-1}$$

e

$$s_2 \equiv k^{-1}(tp_2 - x\gamma) \pmod{p-1},$$

multiplicando as duas congruências por k teremos

$$s_1 k \equiv (tp_1 - x\gamma) \pmod{p-1}$$

e

$$s_2 k \equiv (tp_2 - x\gamma) \pmod{p-1},$$

subtraindo as duas congruências teremos

$$k(s_1 - s_2) \equiv tp_1 - tp_2 \pmod{p-1}$$

e finalizando, podemos calcular

$$k \equiv (tp_1 - tp_2)(s_1 - s_2)^{-1} \pmod{p-1}.$$

Uma vez conhecendo o valor de k em mãos temos

$$s_1 \equiv k^{-1}(tp_1 - x\gamma) \pmod{p-1}$$

$$s_1 k \equiv tp_1 - x\gamma \pmod{p-1}$$

$$x\gamma \equiv tp_1 - s_1 k \pmod{p-1}$$

$$x \equiv \gamma^{-1}(tp_1 - s_1 k) \pmod{p-1}$$

obtenmos a chave privada, colocando todo o processo em risco.

Caso alguém tente forjar uma assinatura na mensagem tp escolhendo um k e usando a chave pública para calcular $\gamma \equiv g^k \pmod{p}$. Mas para calcular

$$s = (P - x\gamma)k^{-1} \pmod{p-1}$$

seria necessário conhecer a chave privada x.

3.9.4 Exemplos

Exemplo 24 *Queremos assinar o texto $tp = 10$ usando o criptosistema de ElGamal, com as chaves pública $[y, g, p] = [11, 2, 13]$ e a chave privada $x = 7$.*

Para assinar este texto primeiro devemos escolher aleatoriamente um $k = 5$, mas este k não pode ser qualquer número, este k deve ser maior que zero e menor que $\phi(13)$ e coprimo com $\phi(13)$. Notemos que $5^{-1} \equiv 8 \pmod{13}$

Agora para obtermos a assinatura calculamos

$$\gamma \equiv 2^5 \pmod{13}$$

facilmente chegamos a $\gamma = 6$ e

$$s \equiv (10 - 7 \cdot 6) \cdot 8 \mod 12$$

obtendo $s = 8$ assim a nossa assinatura será o par $(6, 8)$ e o texto será $P = 10$

Podemos verificar a validade da assinatura calculando

$$V_1 \equiv 11^6 \cdot 6^8 \pmod{13}$$

o que implica que $V_1 = 10$ e

$$V_2 \equiv 2^{10} \pmod{13}$$

e resultando em $V_2 = 10$ a assinatura é verdadeira devido o fato de $V_1 = V_2$.

Exemplo 25

Assinaremos agora o texto cifrado no exemplo 21.

Temos como texto criptografado $tc = [3290, 4528]$ então assinaremos cada um individualmente com a chave pública $[y, g, p] = [5801, 5, 10007]$ e a chave privada $x = 1000$.

Para assinarmos 3290 usaremos $k = 197$, calculemos

$$\gamma \equiv 5^{197} \pmod{10007}$$

que resulta em

$$\gamma \equiv 5488 \pmod{10007}$$

e calculando s:

$$s \equiv (3290 - 1000 \cdot 5488) \cdot 197^{-1} \pmod{1006}.$$

$$s \equiv 2380 \pmod{10006};$$

portanto para o texto 3290 temos a assinatura $[5488, 2380]$.

Agora assinando o texto 4528 escolhemos $k = 167$ então

$$\gamma \equiv 5^{167} \equiv 172 \pmod{10007}$$

e

$$s \equiv (4528 - 1000 \cdot 172) \cdot 167^{-1} \equiv 9842 \pmod{10006}$$

assim a assinatura para o texto 4528 é o par $[172, 9842]$.

Quando enviarmos os texto criptografado $tc = [3290, 4528]$ devemos enviar junto as respectivas assinaturas digitais $[5488, 2380]$ e $[172, 9842]$

Para verificarmos a confiabilidade da origem da mensagem que recebemos devemos verificar a assinatura antes de decodificar a mensagem. Verificando

$$V_1 \equiv 5488^{2380} \cdot 5801^{5488} \equiv 6809 \pmod{10007}$$

e

$$V_2 \equiv 5^{3290} \equiv 6809 \pmod{10007}$$

$$V_1 \equiv 172^{9842} \cdot 5801^{172} \equiv 4420 \pmod{10007}$$

e

$$V_2 \equiv 5^{3290} \equiv 4420 \pmod{10007}$$

concluímos que a origem da mensagem é confiável.

Exemplo 26

Assinar a mensagem $tp = 3517$ usando a chave pública $[y, g, p] = [18, 5, 37]$ e a chave particular $x = 7$

Como o texto tp é maior que o primo $p = 37$ devemos inicialmente "quebrar"o texto em textos menores que p. Agindo deste forma teremos $tp_1 = 35$ e $tp_2 = 17$. Inicialmente estaremos assinando o texto tp_1 escolhendo $k = 5$, calculando o valor de γ temos

$$\gamma \equiv 5^5 \equiv 17 \pmod{37}$$

e calculando

$$s \equiv (35 - 7 \cdot 17)29 \pmod{36}$$

ou seja

$$s \equiv 12 \pmod{36}.$$

Portanto a assinatura do texto $tp_1 = 35$ é o par

$$(\gamma, s) = (17, 2).$$

Agora faremos o mesmo processo para assinar $tp_2 = 17$ escolhemos $k = 11$, calculando o γ chegamos em

$$\gamma \equiv 5^{11} \equiv 2 \pmod{37}$$

e calculando o s temos

$$s \equiv (35 - 7 \cdot 2)23 \pmod{36}$$

ou seja

$$s \equiv 15 \pmod{36}.$$

Então a assinatura do texto $tp_2 = 17$ será $(\gamma, s) = (2, 15)$.

Capítulo 4

Criptografia Na Sala da Aula

O nosso objetivo neste capítulo é dar um proposta de inserção de criptografia no ensino regular de matemática. Primeiro daremos algumas atividades lúdicas e em seguida apresentaremos uma sequência didática para o sistema ElGamal.

4.1 A Esteganografia

Sabemos que esteganografia (do grego "escrita escondida") é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra. Em outras palavras, esteganografia é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido.

Esta técnica é mais aconselhada para os aluno do inicio de ensino médio, cujo conhecimento em matemática não está preparado para cálculos avançados.

Um dos exemplos mais conhecido de esteganografia é a inserção de uma sílaba entre as sílabas da palavra que desejamos transmitir. Por exemplo: fixamos como sílaba PE como a sílaba de codificação, então se desejo transmitir a palavra MATEMÁTICA, devo transmitir o código MAPETEPEMÁPETIPECA

Outro método que podemos usar é transformar o alfabeto em outros símbolos, vejamos um exemplo na figura 4.1

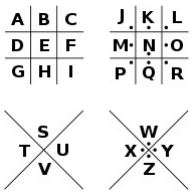
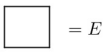
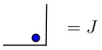


Figura 4.1: Chave Criptográfica

Neste modelo, cada letra será representada pela figura que a circunda com por exemplo:





4.2 Construindo um Disco Criptográfico

O disco criptográfico é uma ferramenta para auxiliar no método criptografia de César dado no primeiro capítulo deste trabalhos.

Os materiais necessários são:

- duas folhas A4 ou papel cartão ou cartolina;
- uma régua;
- um esquadro;
- um compasso;
- uma tesoura e
- um prendedor de saco plástico em pastas tipo ficheiro

Usando compasso construa dois círculos concêntricos, em seguida construa um novo círculo de mesmo raio do menor. Usando construção geométrica[1] divida estes círculos em 27 partes iguais e trace raios ligando essas partes ao centro.

Em cada parte escreva uma letra do alfabeto. Em seguida faça um furo no centro de cada circunferência pequeno o suficiente para passar o prendedor sem folga.

[1]Este tema não é contemplado neste trabalho, na internet existem vários vídeos de como se fazer esta construção, mas preferimos a referência Wagner (2009)

Agora já esta pronto o disco criptográfico, basta usá-lo como indicado no capítulo 1
.

4.3 Construindo um cilindro de Thomas Jefferson

Este é um método criptográfico criado por Tomas Jefferson, que foi o terceiro presidente dos Estados Unidos e também inventor. Para construirmos uma réplica precisaremos de:

- Folhas de papel A4
- No máximo 27 copos descartáveis de mesmo tamanho;
- tesoura;
- cola branca;
- régua;
- caneta;
- caneta para cd.

É incrivelmente simples confeccionar este cilindro. Primeiro use uma folha de A4 e corte um tira de 1 cm de largura e de comprimento total da folha em seguida enrole esta o mais próximo da boca do copo possível e retire o excesso; agora você tem uma tira de papel de comprimento igual ao comprimento do circulo que forma boca deste copo.

Agora você deve desenhar 27 retângulos iguais de modo a não faltar nem sobrar tira de papel neste processo, são nestes retângulos você deve escrever o alfabeto de forma mais aleatória possível, recomendo fazer um sorteio de cada letra. Faça 27 tiras exatamente iguais a primeira, porém o alfabeto deve estar em ordem diferente. Quando as tira de papel estiverem prontas cole uma em cada copo, desta forma teremos 27 copos cada um com um alfabeto aleatório colado.

Use a caneta para cd para numerar os copos de preferência no fundo e também use números aleatórios.

Para criptografar mensagem devemos colocar os copos um dentro do outro de forma que as tiras de papel se encaixem sem nenhuma sobrepor outra.

Se desejarmos criptografar a palavras **Escola**, escolhemos 6 copos, digamos os copos $c_1,\ c_2,\ c_3,\ c_4,\ c_5,\ c_6$ e giramos estes copos de modo a escreve a palavra **Escola** daí escolhemos uma das outras 26 palavras possíveis para se formar com 6 letras do alfabeto nas ordens dos copos escolhidos, suponha que tenha escolhido a palavra composta pelas letras $L_1,\ L_2,\ L_3,\ L_4,\ L_5,\ L_6$, então a palavra **Escola** será o par

$$[L_1L_2L_3L_4L_5L_6,\ c_1 - c_2 - c_3 - c_4 - c_5 - c_6]$$

4.4 Criptografia e Funções Bijetivas

Um poderoso método para apresentação da criptografia como ramo da matemática para os leigos é a função afim. A vantagem da função afim em relação as demais é o fato de ser de fácil manipulação e principalmente por ser bijetiva em todo o seu domínio.

Exemplo 27

Separamos os alunos em duplas e em seguida pedimos para escolherem uma função afim qualquer, digamos $y = 2x + 3$.

Um dos alunos escolhe um mensagem e a pré-codifica usando a tabela 1.1, suponhamos que a mensagem seja 17241914 291422 10302110 ao passar cada número pelo processo criptográfico o aluno terá 34483831 582847 20604223 que é uma mensagem criptografada. O outro aluno da dupla que queira decodificar a mensagem calcula a inversa da função criptográfica, neste caso $x = \dfrac{y-3}{2}$ e efetua o cálculo $\dfrac{34483831-3}{2}\ \dfrac{582847-3}{2}\ \dfrac{20604223-3}{2}$ resultando 17241914 291422 10302110 que é a mensagem "hoje tem aula".

Este é um exemplo de criptografia onde se criptografa toda a palavra, no entanto podemos criptografar letra por letra. Pode ser mais demorado para efetuar os cálculos, porém é muito mais vantajoso quanto a gama de escolhas de funções criptográficas.

Podemos criptografar a mensagem

$$17 - 24 - 19 - 14 - 99 - 29 - 14 - 22 - 99 - 10 - 30 - 21 - 10$$

substituindo os espaços por 99 usando uma função de duas sentenças

$$y = \begin{cases} 2x - 24, \text{ se } x \geq 22 \\ x - 2, \text{ se } x < 22 \end{cases}$$

Resultando na mensagem criptografada $15 - 24 - 17 - 12 - 174 - 34 - 12 - 20 - 174 - 8 - 36 - 19 - 8$.

E para descriptografar esta mensagem basta usar a sua inversa, que é dada por

$$x = \begin{cases} \dfrac{y + 24}{2}, \text{ se } x \leq 20 \\ y + 2, \text{ se } x > 20 \end{cases}$$

Exemplo 28

Outra forma de estabelecer uma função criptográfica é através de funções do segundo grau, como a função $y = x^2 + 5x - 50$, é do conhecimento de todos que esta função não é bijetiva, mas se restringirmos seu domínio ao conjunto $D = \{x \in \mathbb{N}; 10 \leq x \leq 99\}$ esta função passa a ser bijetiva. Portanto devemos tomar muito cuidado ao escolhermos essa função do segundo grau.

Criptografando a mesma mensagem do exemplo anterior temos,

$$324 - 646 - 406 - 216 - 10246 - 936 - 216 - 544 - 10246 - 100 - 1000 - 496 - 100$$

E para decodificar a mensagem acima basta usar a inversa

$$x = \frac{-5 + \sqrt{25 + 4 \cdot (50 + y)}}{2}$$

Capítulo 5

ElGamal Em Sala de Aula

Após a motivação dada pelo capítulo anterior poderemos apresentar um sistema muito mais forte de criptografia porém menos acessível aos alunos do ensino médio.

Faremos um roteiro de como deve ser esta apresentação, tentaremos fornecer o máximo de exemplos e detalhes possível.

5.1 Trabalhando com a função ϕ de Euler

O funcionamento da função ϕ depende do conceito de máximo divisor comum, doravante MDC, que definimos agora.

Definição 22 *: Máximo divisor comum de dois números inteiros a e b é o maior inteiro m que divide esses dois números. Neste caso escrevemos* $m = MDC(a, b) = (a, b)$.

Pela definição 22 podemos dizer que $m = (a, b)$ quando m satisfas as seguintes condições:

i) $m|a$ e $m|b$

ii) se existe um inteiro c de modo que $c|a$ e $c|b$ então $c|m$

Exemplo 29

Qual é o MDC(12,18)=?

Para resolver este problema devemos elencar o conjunto dos divisores de 12 e de 18 e são eles $D(12) = \{1, 2, 3, 4, 6, 12\}$ e $D(18) = \{1, 2, 3, 6, 9, 18\}$ e os divisores comuns são os números $\{1, 2, 3, 6\}$ e o maior deles é 6 consequentemente $MDC(12, 18) = 6$

Sabemos que este processo pode ser exaustivo, então daremos um outro método:

12,	18	2	← Escolhemos um número primo que divida ambos os números
6,	9	3	← repetimos o processo acima
2,	3	1	← paramos quando somente o número 1 os divide

então o $MDC(12, 18) = 2 \cdot 3 \cdot 1 = 6$

Exemplo 30

Obter $MDC(75, 105)$

75,	105	5
15,	21	3
5,	7	1

concluímos que $MDC(75, 105) = 5 \cdot 3 \cdot 1 = 15$

Exemplo 31

Calcular $MDC(462, 1155)$

Repetindo o processo

462,	1155	3
154,	385	7
22,	55	11
2,	5	1

Portanto $MDC(462, 1155) = 3 \cdot 7 \cdot 11 \cdot 1 = 231$

Agora que já estamos com ideia de máximo divisor comum estabelecido podemos passar para a próxima definição.

Definição 23 *Chamamos de coprimos os números a e b tal que* $MDC(a, b) = 1$

Exemplo 32

Podemos afirmar que 10 e 12 são coprimos?

A resposta para essa pergunta é não, pois

10,	12	2
5,	6	1

concluímos que $MDC(10, 12) = 2 \cdot 1 = 2$ e diferente de 1 que fere a definição de números coprimos.

Exemplo 33

Os números 21 e 20 são coprimos?

Notemos que os divisores de 21 são $D(21) = \{1, 3, 7, 21\}$ e de 20 são $D(20) = \{1, 2, 4, 5, 10, 20\}$ e o único elemento em comum neste conjuntos é o número 1 então $MDC(21, 20) = 1$, então a resposta para a pergunta é sim. Os números 21 e 20 são coprimos.

Definição 24 *Dado um número natural n definiremos como $\phi(n)$ como sendo a quantidade de números naturais k menores que n e coprimos com n*

Existem dois métodos para se calcular o valor de $\phi(n)$ dado um natural n qualquer. O primeiro é fazer uma lista com todos os números menores que n e tirar da lista os não coprimos e em seguida contar os que sobraram então $\phi(n)$ será esta quantidade. É obvio que este método não é eficiente quando se trata de números muito grande.

O segundo método é mais eficiente e já conhecemos pelo teorema 9.

Exemplo 34

Calcular $\phi(19)$.

Notemos que 19 é primo, concluímos que $\phi(19) = 19 - 1 = 18$ Para facilitar a verificação dos próximos exemplos ampliaremos a tabela 1.1.

n	1	2	3	4	5	6	7	8	9
$\phi(n)$	1	1	2	2	4	2	6	4	6

n	10	11	12	13	14	15	16	17	18	19
$\phi(n)$	4	10	4	12	6	8	8	16	6	18

n	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$	8	12	10	22	8	20	12	18	12	28	8

5.2 Definindo ordem de um número

Para termos noção de ordem de um número é preciso antes ter noção de congruência, que daremos na próxima definição.

Definição 25 *Dados os números inteiros a, b e m a única restrição para estes números é $m > 1$. Dizemos que a é congruente a b módulo m, em símbolos $a \equiv b \pmod{m}$, se e somente se $b - a$ for divisível por m.*

Apesar de parecer ser de difícil compreensão, congruência é um dos tópicos mais simples da matemática e também um dos mais fecundos. Para avaliarmos que dois números são ou não congruentes módulo determinado número, basta verificar se a diferença destes números é divisível pelo terceiro.

Exemplo 35

Vamos verificar se 35 é congruente a 8 módulo 2

Notemos que $35 - 8 = 27$ com 27 não é divisível por 2 concluímos que 35 não é congruente a 8 módulo 2, em símbolos $35 \not\equiv 8 \pmod{2}$

Exemplo 36

Verificar se 45 é congruente a 6 módulo 3

Temos que $45 - 6 = 39$ e 39 é divisível por 3 então 45 é congruente 6 módulo 3, em símbolos $45 \equiv 6 \pmod{3}$

Nem sempre é possível observar esta congruência apenas com uma subtração, nestes caos, precisamos de algumas propriedades para facilitar este cálculo, estas propriedades já foram mencionadas e provadas neste trabalho, mais especificamente na proposição 2

Segue um exemplo de como trabalhar com estas propriedades

Exemplo 37

2^{100} é congruente a quanto módulo 10?

Mesmo com uma boa calculadora é quase impossível saber esta resposta usando apenas uma subtração. Portanto devemos usar as propriedades. Sabemos que $2^4 = 16$ e que é fácil ver que $16 \equiv 6 \pmod{10}$, devemos perceber agora que $6^5 = 7776$ ou seja $6^5 \equiv 6 \pmod{10}$ então $(2^4)^5 \equiv 6^5 \equiv 6 \pmod{10}$ e com $(2^4)^5 = 2^{20}$ temos $2^{20} \equiv 6 \pmod{10}$, como nosso objetivo não foi alcançado devemos continuar o processo, $(2^{20})^5 \equiv 6^5 \equiv 6 \pmod{10}$ ou seja $2^{100} \equiv 6 \pmod{10}$.

Definição 26 *Ordem de a módulo n é o menor número x que satisfaça a congruência $a^x \equiv 1 \pmod{m}$ e $MDC(a, m) = 1$.*

Para encontrar a ordem de um número módulo m basta testar todos os divisores de $\phi(m)$.

Exemplo 38

Determinar a ordem de 5 módulo 19

Sabemos pelo exemplo 34 que $\phi(19) = 18$ e os divisores de 18 são $\{1, 2, 3, 6, 9, 18\}$, agora basta testa cada um dos divisores de 18 na congruência $5^x \equiv 1 \pmod{19}$

$5^1 \equiv 5 \pmod{19}$, $5^2 \equiv 6 \pmod{19}$, $5^3 \equiv 11 \pmod{19}$ $5^6 \equiv 7 \pmod{19}$ $5^9 \equiv 1 \pmod{19}$ concluimos que a ordem de 5 módulo 19 é 9. Simbolicamente $ord_{19}5 = 9$

Exemplo 39

Vamos determinar $ord_{11}2$

Antes de iniciarmos devemos calcular o valor de $\phi(11)$ que é dado por $\phi(11) = 11 - 1 = 10$. Agora devemos encontrar os divisores de 10 que são $\{1, 2, 5, 10\}$, falta apenas testar os divisores na congruência $2^x \equiv 1 \pmod{11}$ o primeiro que cumprir será a ordem.

$2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^5 \equiv 10 \pmod{11}$ e $2^{10} \equiv 1 \pmod{11}$ então concluímos que $ord_{11}2 = 10$

Exemplo 40

Obter $ord_{13}6$

Sabemos que $\phi(13) = 13 - 1 = 12$ e os divisores de 12 são $\{1, 2, 3, 4, 6, 12\}$ então

$6^1 \equiv 6 \pmod{13}$, $6^2 \equiv 10 \pmod{13}$, $6^3 \equiv 8 \pmod{13}$, $6^4 \equiv 9 \pmod{13}$, $6^6 \equiv 12 \pmod{13}$ e $6^{12} \equiv 1 \pmod{13}$ Portanto $ord_{13}6 = 12$

5.3 Definindo raiz primitiva

Definição 27 *Dizemos que r é uma raiz primitiva de um número inteiro m com $MDC(r, m) = 1$ quando $ord_m r = \phi(m)$.*

Exemplo 41

Pelos exemplos 39 e 40 concluímos: 6 é uma raiz primitiva de 13 e que 2 é uma raiz primitiva de 11

Exemplo 42

Pelo exemplo 38 podemos concluir que 5 não é uma raiz primitiva de 19.

5.4 Definindo o criptosistema

Como apresentado em todo esse trabalho, o criptosistema de ElGamal é muito eficiente, tentaremos agora transpor esta ideia para o ensino médio.

Para criptografar uma mensagem devemos primeiro criar uma chave pública que será divulgada, para que qualquer pessoa possa me enviar uma mensagem criptografada. Para isso eu devo escolher um número primo p, um número natural x qualquer menor que esse primo e encontra uma raiz primitiva g deste primo, em seguida calculamos $y \equiv g^x \pmod{m}$. A chave pública será o trio $[y, g, p]$ e a chave secreta será o número x

Exemplo 43

Crie uma chave pública e um chave privada no sistema criptográfico de ElGamal usando o primo $p = 37$ e a raiz primitiva $g = 5$

Como já temos o primo $p = 37$ e a raiz primitiva $g = 5$, então agora falta apenas escolher um número para ser a chave privada e calcularmos a chave pública. Escolhemos o números $x = 6$, notemos que apesar de $x = 6$ ser um número pequeno os cálculos se tornam complicados e é neste empecilho que se garante a segurança do criptosistema. Vamos aos cálculos:

$$5^3 \equiv 14 \pmod{37}$$

$$5^6 \equiv (5^3)^2 \equiv 14^2 \equiv 11 \pmod{37}.$$

Assim construímos a chave pública $[11, 5, 37]$ para a chave privada $x = 6$

Este exemplo é muito rico, pois ele nos mostra que mesmo dado um número primo e uma raiz primitiva, a chave pública e a chave privada não são únicas, portanto uma sala pode ter o mesmo número primo e a mesma raiz primitiva e chave diferentes.

5.5 Criptografando uma mensagem

O processo de criptografia de uma mensagem é simples. Mais uma vez devemos escolher um número natural k e resolver o seguinte par de congruências:

$$\begin{aligned} a &\equiv g^k \pmod{p} \\ b &\equiv (tp \cdot y^k) \pmod{p} \end{aligned}$$

Onde tp é a mensagem já pré-codificada.

Exemplo 44

Codifique a mensagem $tp = 10$ usando $k = 3$ e a chave pública do exemplo 43.Dando início aos cálculos

$$a \equiv 5^3 \pmod{37},$$

ou seja,

$$a \equiv 14 \pmod{37}$$

e

$$b \equiv (10 \cdot 11^3) \pmod{37}$$

$$b \equiv 13310 \pmod{37}$$

$$b \equiv 27 \pmod{37}.$$

Portanto a mensagem criptografada será o par $[a, b] = [14, 27]$

Exemplo 45

Codifique a mensagem $tp = 10$ usando $k = 7$ e a chave pública do exemplo 43.

Calculando

$$a \equiv 5^7 \pmod{37}$$

$$a \equiv 18 \pmod{37}$$

$$b \equiv (10 \cdot 11^7) \pmod{37}$$

usando uma calculadora teremos,

$$11^7 \equiv 11 \pmod{37}$$

o que resulta em

$$b \equiv 10 \cdot 11^7 \equiv 10 \cdot 11 \equiv 36 \pmod{37}.$$

A mensagem será $[a, b] = [18, 36]$.

5.6 Decodificando um texto

Para decodificar a mensagem devemos tomar o valor a e calcular

$$\xi \equiv \left(a^{-1}\right)^{x} \pmod{p}$$

e usamos o resultado para calcular

$$tp \equiv (b \cdot \xi) \pmod{p}$$

O grande problema que temos para decodificar uma mensagem é encontrar o inverso a^{-1}, que definiremos agora.

Definição 28 *O inverso módulo m de um inteiro a é o número inteiro a^{-1} de modo que $a \cdot a^{-1} \equiv 1 \pmod{m}$.*

Exemplo 46

Encontre o inverso de $a = 7$ módulo 13.

Basta encontrar a^{-1} de modo que $7 \cdot a^{-1} \equiv 1 \pmod{13}$. Iniciando os cálculos:

$7 \cdot 1 \equiv 7 \pmod{13}$

$7 \cdot 2 \equiv 1 \pmod{13}$

Concluímos que $a^{-1} = 2$, ou seja, que o inverso de 7 módulo 13 é 2.

Exemplo 47

Obtenha o inverso de $a = 9$ módulo 11

$9 \cdot 1 \equiv 9 \pmod{11}$

$9 \cdot 2 \equiv 7 \pmod{11}$

$9 \cdot 3 \equiv 5 \pmod{11}$

$9 \cdot 4 \equiv 3 \pmod{11}$

$9 \cdot 5 \equiv 1 \pmod{11}$

portanto $a^{-1} = 5$

Exemplo 48

Vamos obter o inverso de $a = 14$ módulo 37

$$
\begin{aligned}
14 \cdot 1 &\equiv 14 \pmod{37} \\
14 \cdot 2 &\equiv 28 \pmod{37} \\
14 \cdot 3 &\equiv 05 \pmod{37} \\
14 \cdot 4 &\equiv 19 \pmod{37} \\
14 \cdot 5 &\equiv 33 \pmod{37} \\
14 \cdot 6 &\equiv 10 \pmod{37} \\
14 \cdot 7 &\equiv 24 \pmod{37} \\
14 \cdot 8 &\equiv 01 \pmod{37}
\end{aligned}
$$

Portanto $a^{-1} = 8$

Exemplo 49

Calcular o inverso de $a = 18$ módulo 37

$$
\begin{aligned}
18 \cdot 1 &\equiv 18 \pmod{37} \\
18 \cdot 2 &\equiv 36 \pmod{37} \\
18 \cdot 3 &\equiv 17 \pmod{37} \\
\vdots \quad &\quad \vdots \quad\quad \vdots \\
18 \cdot 34 &\equiv 20 \pmod{37} \\
18 \cdot 35 &\equiv 01 \pmod{37}
\end{aligned}
$$

Exemplo 50

Decodifique a mensagem do exemplo 44.

Observando o exemplo 48 concluímos que

$$a^{-1} = 8.$$

Então, falta calcular

$$\xi \equiv 8^6 \pmod{37}$$

para obtermos

$$\xi \equiv 36 \pmod{37}.$$

Finalizando temos

$$tp \equiv (27 \cdot 36) \pmod{37}$$

$$tp \equiv 972 \pmod{37}$$

$$tp \equiv 10 \pmod{37},$$

resultando que o texto original 10.

Exemplo 51

Decodifique a mensagem do exemplo 45.

Com o exemplo 49 já temos que

$$a^{-1} = 35$$

então, calculamos

$$\xi \equiv 35^6 \pmod{37},$$

logo

$$\xi \equiv 27 \pmod{37}$$

e o texto puro será

$$tp \equiv 36 \cdot 27 \pmod{37},$$

ou seja,

$$tp \equiv 10 \pmod{37}$$

A sequência de exemplos que acabamos de apresentar nos sugere que a escolha do k é indiferente no processo de criptografia do texto.

Conclusão

As denuncias Edward Joseph Snowden mostram que vivemos em um mundo onde as informações trocadas via internet não estão em total segurança. Neste trabalho mostramos que o sistema de criptografia de ElGamal é eficiente no que diz respeito a transmissão de dados por um meio de comunicação, devido a dificuldade de se calcular o logaritmo discreto.

A grande vantagem do sistema de criptografia de ElGamal, está no fato de se codificar facilmente as mensagens e ser extremamente difícil de um intruso obter o logaritmo discreto que é a chave privada do processo criptográfico, somente com o conhecimento da chave pública, . Também tratamos técnicas já existentes de ataque ao logaritmo discreto quando utilizamos números primos com a quantidade de dígitos pequena que servem para a construção da chave pública. Deixamos duas referências que tratam de outras formas de ataque.

Neste trabalho não nos preocupamos em expor técnicas de cálculo de raiz primitiva, consequentemente de logaritmos discretos através de algoritmos já existente, pois preferimos evidenciar a segurança do sistema como também o seu funcionamento.

Apresentamos também a assinatura digital que é um par (γ, s) que deve ser inserido ao texto para certificar a autenticidade da mensagem.

Expomos um passo a passo de como inserir o sistema de criptografia de ElGamal para os alunos do ensino médio. A motivação para esta exposição é que os alunos premiados pela Obmep que são destinados ao PIC, estudam criptografia em dois módulo, porém, é dado enfase ao RSA. Após todo o estudo efetuado percebemos que o sistema criptográfico de ElGamal requer conceitos matemáticos mais profundo e certamente seria mais enriquecedor ao conhecimento destes alunos.

Concluímos que o sistema criptográfico de ElGamal é uma excelente porta de entrada para a matemática avançada e devido a isso não podemos deixar de apresentá-lo

aos alunos do ensino básico na forma de estímulo aos que acreditam que a matemática do ensino básico seja simplória.

Finalizamos afirmando que criptografia deveria fazer parte do currículo de matemática do ensino médio e de maneira mais avançada no currículo das graduações em matemática.

Referências Bibliográficas

ElGamal, T. (1984). A public key cryptosystem and a signature scheme based on discrete logarithms. URL:http://groups.csail.mit.edu/cis/crypto/classes/6.857/papers /elgamal.pdf Acesso em: 18/11/2014.

Hefez, A. (2013). *Aritmética*. Ed. SBM, R. Janeiro.

Lima, E. L. (2007). *Análise Real*. Ed. SBM, R. Janeiro.

MapleSoft (2008). Manual user guide. URL: www.maplesoft.com/view.aspx?sl=5883 Acesso em: 17/11/2014.

Menezes, A. J., van Oorschot, P. C., e Vanstone, S. A. (1996). Handbook of applied cryptography. URL:http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838 &rep=rep1&type=pdf Acesso em: 20/07/2014.

Rosen, K. H. (2005). *Elementary Number Theory and Its Applications*. Pearson Addilson Wesley, New York.

Santos, J. P. O. (2009). *Introdução à Teoria dos Números* . Ed. SBM, R. Janeiro.

Wagner, E. (2009). *Construções Geométricas* . Ed. SBM, R. Janeiro.