UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
CURSO DE GRADUAÇÃO EM MATEMÁTICA

EUGÊNIO CARLOS ROSA ROCHA

FUNDAMENTOS MATEMÁTICOS APLICADO A ALGUNS MÉTODOS DE CRIPTOGRAFIA

FLORIANÓPOLIS – SC
2008

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Matemática do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina – UFSC como requisito para obtenção da Graduação em Matemática – Habilitação: Licenciatura.

Orientador: Professor Dr. Márcio Rodolfo Fernandes

FLORIANÓPOLIS – SC
2008

Este trabalho foi julgado adequado como **TRABALHO DE CONCLUSÃO DE CURSO** no Curso de Matemática – Habilitação: Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 16/CCM/08.

Professora M.Sc. Carmem Suzane Comitre Gimenez
Professora da Disciplina

Banca Examinadora

Professor Dr. Márcio Rodolfo Fernandes
Orientador

Professor M.Sc. Nereu Estanislau Burin

Professor Dr. Daniel Norberto Kozakevich

Agradecimentos

Quero agradecer a quem teve grande importância para a elaboração deste trabalho.

Primeiramente a Deus, pela minha vida.

A minha família, pela presença e por todo apoio.

Ao Professor Márcio Rodolfo Fernandes, pelos esforços empenhados em me orientar e por sua disposição e paciência durante a realização deste trabalho.

A banca examinadora, professores Nereu Estanislau Burin e Daniel Norberto Kozakevich por aceitarem avaliar este trabalho.

Aos amigos da secretaria, Silvia, Iara e Alcino.

“O melhor que podemos fazer de nossa vida é empregá-la em alguma coisa mais duradoura que a própria vida."

(William James)

SUMÁRIO

1. Introdução

A palavra criptografia tem a seguinte origem: kript´os = escondido, oculto e grápho = grafia. Ou seja, criptografia é a arte ou ciência de escrever em cifras ou em códigos, de tal maneira que somente o destinatário tenha permissão para decifrar ou compreender a mensagem, pois a criptografia converte textos originais em uma informação transformada, que chamamos de texto cifrado. Outros termos utilizados são:

- Criptoanálise (kript´os = escondido, oculto e análysis = decomposição) é o estudo de métodos para decifrar uma mensagem codificada sem ser o destinatário legítimo.
- Criptologia (kriptóss = escondido, oculto e logo = estudo, ciência) – é a junção de Criptografia e da Criptoanálise.

Normalmente usamos as palavras decodificar e decifrar com o mesmo sentido. Não nos damos conta que, ao decodificarmos uma mensagem, estaremos realizando o processo que um usuário legítimo do código faz quando recebe uma mensagem codificada. Por outro lado, ao decifrarmos, estaremos realizando o processo de ler a mensagem mesmo não sendo o usuário do código. Desta forma, o principal propósito da criptografia é permitir que seja feita com segurança a transmissão da mensagem de forma restrita ao usuário.

Diante do acima exposto a matemática tem seu papel fundamental. Citamos a Teoria dos Números, uma ciência muito antiga que visa primordialmente entender as propriedades e relações entre os números. A partir daí percebemos, mais uma vez, sua importância.

Pensando nisto, o conteúdo deste trabalho é mostrar alguns algoritmos de criptografia quanto aos modos de cifrar uma mensagem e os fundamentos matemáticos envolvidos. Começaremos com o Método da Matriz e o Método Permutacional. Ambos utilizados no ensino médio com objetivo de evidenciar uma das várias aplicações da matemática. O primeiro com uso de matrizes e sua inversa e o segundo na Análise Combinatória. O Método da Cifra de Hill um método antigo com ênfase a transformações lineares e congruência. Finalmente, o Método RSA e o Método Elgamal usado na internet como, por exemplo, no comércio eletrônico e as transações financeiras com objetivo de manter a privacidade de certas informações. Utiliza congruência, números primos e teoria de números.

O trabalho que segue está longe de ser um estudo concluído ou terminado. O que se pretende realmente é pôr o assunto em discussão.

2. Alguns algoritmos de Criptografia

Neste capítulo introduziremos alguns algoritmos de criptografia e os fundamentos matemáticos envolvidos.

2.1 Criptografia Método Matriz

O Método Matriz é um processo de criptografia que utiliza as mesmas idéias básicas de substituição e transposição, a ênfase atual é diferente, e tem como objetivo tornar o algoritmo mais complexo, e também de uso didático. Sendo assim vamos codificar uma mensagem utilizando a multiplicação da matriz mensagem por outra matriz chave. Um exemplo dessa codificação pode ser dado pela associação das letras do alfabeto segundo a tabela 1 do capítulo anterior.

Suponha que a mensagem a ser criptografada seja "EU TE AMO". Pode-se formar uma matriz 3 x 3, que usando a correspondência numérica da cifra matriz torna-se:

$$M = \begin{bmatrix} E & U & - \\ T & E & - \\ A & M & O \end{bmatrix} = \begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix}$$

Suponha também que a chave para esta codificação seja a palavra "PACIÊNCIA". Seja *C* uma matriz qualquer 3 x 3 inversível (matriz secreta), que descreve esta chave*:*

$$C = \begin{bmatrix} P & A & C \\ I & E & N \\ C & I & A \end{bmatrix} = \begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix}$$

Multiplica-se a matriz mensagem pela matriz secreta obtendo-se S = *MxC*:

$$S = \begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix} \text{ x } \begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix} = \begin{bmatrix} 269 & 110 & 309 \\ 365 & 45 & 130 \\ 178 & 201 & 200 \end{bmatrix}$$

Transmite-se esta nova matriz codifica Dora S (na prática, envia-se a cadeia de números 269, 110, 309, 365, 45, 130, 178, 201, 200).

Quem recebe a mensagem decodifica-a por meio da multiplicação pela inversa ((*M x C*) x C^{-1} = *M)*, ou seja, M x C = S $\Rightarrow$ M x C x C^{-1} = S x C^{-1} $\Rightarrow$ M = S x C^{-1} e posterior transcrição dos números para letras. Vamos fazer a multiplicação pela inversa: S x C^{-1} = M

$$\begin{bmatrix} 269 & 110 & 309 \\ 365 & 45 & 130 \\ 178 & 201 & 200 \end{bmatrix} \text{ x } \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix}$$

Substituindo temos: $\begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix} = \begin{bmatrix} E & U & - \\ T & E & - \\ A & M & O \end{bmatrix}$

2.2 Método Permutacional

Antes da existência do computador este método era o mais usado. Para gerar uma cifra permutacional bastava aplicar uma das 26! permutações das letras do alfabeto. Sem dúvida nenhuma, com a ajuda do computador este problema tornou-se simples. Vamos ver a seguir a implicação matemática envolvida:

Definição: *Uma permutação de um conjunto X é uma função bijetora* $f: X \rightarrow X$.

Nós estamos particularmente interessados nas permutações de conjuntos finitos. Vamos supor que *X* é um conjunto finito, digamos que tenha ***n*** elementos denotados por $a_1, a_2, a_3,..., a_n$. Por exemplo $n = 1$ teremos uma permutação, a função $f(a_1) = a_1$. Se n = 2 teremos duas permutações.

$$f_1: \begin{cases} f_1(a_1) = a_1 \\ f_1(a_2) = a_2 \end{cases} \qquad f_2: \begin{cases} f_2(a_1) = a_2 \\ f_2(a_2) = a_1 \end{cases}$$

Se n = 3 teremos duas permutações.

$$f_1: \begin{cases} f_1(a_1) = a_1 \\ f_1(a_2) = a_2 \\ f_1(a_3) = a_3 \end{cases} \qquad f_2: \begin{cases} f_1(a_1) = a_1 \\ f_1(a_2) = a_3 \\ f_1(a_3) = a_2 \end{cases} \qquad f_3: \begin{cases} f_1(a_1) = a_2 \\ f_1(a_2) = a_1 \\ f_1(a_3) = a_3 \end{cases}$$

$$f_4: \begin{cases} f_1(a_1) = a_2 \\ f_1(a_2) = a_3 \\ f_1(a_3) = a_1 \end{cases} \qquad f_5: \begin{cases} f_1(a_1) = a_3 \\ f_1(a_2) = a_1 \\ f_1(a_3) = a_2 \end{cases} \qquad f_6: \begin{cases} f_1(a_1) = a_3 \\ f_1(a_2) = a_2 \\ f_1(a_3) = a_1 \end{cases}$$

O seguinte teorema mostra a quantia de permutações de um conjunto de *n* elementos.

Teorema 2.1: *O número das permutações de um conjunto de n elementos é n.*

Demonstração:

O exemplo anterior mostrou que um conjunto de um elemento tem uma permutação e que um conjunto de dois elementos têm duas permutações. Esses números confirmam o teorema. Agora suponhamos que um conjunto $X_1 = \{ a_1, a_2, a_3, ..., a_{n-1}\}$ de n – 1 elementos tenha (n – 1)! permutações. Denotaremos essas permutações por f_1, f_2,..., $f_{(n-1)}$. Consideremos um conjunto $X = X_1 \cup \{a_n\}$ de *n* elementos. Em primeiro lugar, podemos estender as permutações f_1 do conjunto X_1 ao conjunto *X*, supondo que as funções f_i mantenham fixo o elemento a_n. Em segundo lugar, a cada permutação f_i do conjunto *X*, associaremos *n* permutações F_1, F_2,..., F_n do conjunto *X* da seguinte maneira.

$$f_i(a_j) = \begin{cases} f_i(a_i) & se \quad j \neq n \\ a_n & se \quad j = n \end{cases}$$

Portanto, no total existem (n – 1)! . *n = n!* permutações no conjunto *X*. ■

Por exemplo: Seja um conjunto *X* do alfabeto existem 26 letras. Existem

26! = 4.032.914.611.266.056.355.840.000.000 permutações

Esse número tem 27 algarismos. Sem dúvida nenhuma antes da era do computador a determinação de todas as permutações estava fora de cogitação. Porém a ajuda do computador tornou esse problema muito simples. Para gerar uma cifra[1] permutacional basta aplicar uma das 26! permutações do alfabeto e então trocar a posição das letras (ou algumas) e obter uma cifra. A tabela abaixo mostra uma cifra permutacional começando pela letra “D” e não por “A” e trocando a posição da letra “N” e “H”.

[1] Na Linguagem da criptografia os códigos são denominadas cifras)

D	E	F	G	N	I	J	K	L	M	H	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

2.3 Método Cifra de Hill

A seguir descreveremos o sistema de criptografia polialfabética chamado cifra de Hill. Essa cifra foi inventada em 1929 por Lester S. Hill. A idéia deste sistema de criptografia é fazer ***m*** combinações lineares dos ***n*** caracteres do texto plano, produzindo os ***m*** caracteres do texto criptografado.

Vamos começar com as cifras[2] mais simples chamadas cifras de substituição:

Comum 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
Cifra 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

Aqui, a letra A é substituída pela letra D, E substituída pela B e assim sucessivamente. Vamos utilizar a seguinte palavra abaixo e sua cifra correspondente:

EUGENIO
HXJHQLR

Ao invés de utilizar as cifras de substituição vamos utilizar as cifras de Hill porque devido à freqüência das letras é fácil quebrar o código por algum método estatístico.

Vamos utilizar o sistema poligráfico[3] chamado cifras de Hill. A cada letra do texto comum e do texto cifrado vamos atribuir um valor numérico que especifica no alfabeto padrão. (Obs.: vamos atribuir o zero à letra z mais tarde ficará mais clara esta opção). Para ficar mais acessível vamos utilizar em nossa mensagem somente letras.

Tabela 1:

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

N	O	P	Q	R	S	T	U	V	X	Y	Z	W	-
14	15	16	17	18	19	20	21	22	23	24	25	26	0

[2] Na Linguagem da criptografia os códigos são denominadas cifras)
[3] É um sistema de criptografia no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas.

Passo1:

Escolha uma matriz 2x2

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{22} & a_{23} \end{bmatrix}$$

Neste exemplo utilizamos uma matriz quadrada 2x2 com entradas inteiras, pois vamos reunir grupo de duas letras. Caso fosse o agrupamento de três a três usaríamos uma matriz 3x3 e assim por diante.

Passo2:

Agrupe letras sucessivas do texto comum em pares, adicionando uma letra fictícia caso não esteja completo o último par. Substituir cada letra do texto comum por seu valor numérico.

Passo3:

Converta cada par sucessivo p_1, p_2, ..., p_n de letras de texto comum em um vetor-coluna

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$ e forme o produto Ax p.

Neste caso, chamaremos p de vetor comum e Ap de vetor cifrado correspondente.

Passo4:

Converta cada vetor cifrado em seu equivalente alfabético.Por exemplo, vamos usar a matriz:

$$A = \begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix}$$ para obter a cifra de Hill da mensagem do seguinte texto comum:

EUGENIO

Como a mensagem possui um número ímpar de letras devemos acrescentar mais uma letra fictícia “G”, pois estamos utilizando uma matriz quadrada 2x2 e com isso agrupamos o texto comum em pares de letras. Temos

EU GE NI OG

Usamos a equivalência conforme tabela 1 :

E = 5 U = 21 G = 7 E = 5 N = 14 I = 9 O = 15 G = 7

Para codificar o par EU (5 - 21) nós efetuamos o produto matricial.

$$\begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix} \text{ x } \begin{bmatrix} 5 \\ 21 \end{bmatrix} = \begin{bmatrix} 88 \\ 47 \end{bmatrix}$$

Para codificar o par GE (7 - 5) nós efetuamos o produto matricial

$$\begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix} \text{ x } \begin{bmatrix} 7 \\ 5 \end{bmatrix} = \begin{bmatrix} 50 \\ 17 \end{bmatrix}$$

Para codificar o par NI (14 - 9) nós efetuamos o produto matricial

$$\begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix} \text{ x } \begin{bmatrix} 14 \\ 9 \end{bmatrix} = \begin{bmatrix} 97 \\ 32 \end{bmatrix}$$

Para codificar o par OG (15 - 17) nós efetuamos o produto matricial

$$\begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix} \text{ x } \begin{bmatrix} 15 \\ 7 \end{bmatrix} = \begin{bmatrix} 96 \\ 29 \end{bmatrix}$$

Como obtivemos os números maiores que 25 e não encontramos na tabela 1 ele é substituído pelo resto da divisão dele por 26. Usando a congruência mod 26 temos o vetor correspondente. Assim:

$\begin{bmatrix} 88 \\ 47 \end{bmatrix}$ é equivalente a $\begin{bmatrix} 10 \\ 21 \end{bmatrix}$

$\begin{bmatrix} 50 \\ 17 \end{bmatrix}$ é equivalente a $\begin{bmatrix} 24 \\ 17 \end{bmatrix}$

$\begin{bmatrix} 97 \\ 32 \end{bmatrix}$ é equivalente $\begin{bmatrix} 19 \\ 6 \end{bmatrix}$

$\begin{bmatrix} 96 \\ 29 \end{bmatrix}$ é equivalente $\begin{bmatrix} 18 \\ 3 \end{bmatrix}$

Texto cifrado: JU YQ SF RC

Vamos dar uma pausa neste processo e relembrar alguns resultados básicos de aritmética modular.

2.4 Aritmética Modular

Definição: *Dado um numero inteiro positivo m e dois inteiros a e b quaisquer, dizemos que a é congruente a b módulo m, e escrevemos* $a \equiv b \pmod{m}$*, se a – b é múltiplo inteiro de m.*

Exemplo:

$14 \equiv 2 \pmod 6$

$9 \equiv 0 \pmod 3$

$17 \equiv 1 \pmod 4$

$48 \equiv 3 \pmod{15}$

$150 \equiv 67 \pmod{83}$

Dado um inteiro positivo m, pode ser provado que qualquer inteiro a é equivalente módulo m, a exatamente um dos inteiro (1, 2 , 3, ..., m – 1). Temos o seguinte:

Teorema 2.2: *Sejam a e r inteiros, com $0 \leq r < n$. Então $a \equiv r \pmod n$ se, e somente se, r = resto (a,n).*

Demonstração

$\Rightarrow$ Seja $a \equiv r \pmod n$. Então n | (a – r) e existe q tal que (a – r) = nq. Assim, $a = nq + r$, e, como $0 \leq r < n$, tem-se que r = res (a, n).

$\Leftarrow$ Suponha que r = res (a, n). Então existe um q tal que a = nq + r e, com isso, $a - r = nq$, o que implica n | (a − r). Logo, $a \equiv r \pmod n$.■

Para definir a operação módulo m, precisaremos definir o conjunto dos inteiros módulo m. Dizemos que a cada inteiro positivo b, podemos associar um subconjunto infinito dos inteiros a ser chamados classes de b módulo m ou números b (mod m).

2.4.1 Resíduos modulo m:

Chamamos os inteiros (0, 1, 2, ..., m – 1) = Z_m Resíduo de a módulo m. Usaremos o seguinte teorema:

Dado um inteiro a e um módulo m quaisquer, seja R o resto de $\frac{|a|}{m}$. Então o resíduo r de a módulo m é dado por:

$$r = \begin{cases} R & se \quad a \geq 0 \\ m - R & se \quad a < 0 \quad e \quad R \neq 0 \\ 0 & se \quad a < 0 \quad e \quad R = 0 \end{cases}$$

exemplo: Resíduo módulo 26:

a) $\frac{|73|}{26}$ r= 21 $\quad 73 \equiv 21 \pmod{26}$

b) $\frac{|-39|}{26}$ r= 13 $\quad$ R = 26 – 13 = 13 $\quad -39 \equiv 13 \pmod{26}$

2.4.2 Inverso Multiplicativo

Na aritmética usual cada número não nulo a tem um recíproco ou inverso multiplicativo denotado por a^{-1} tal que $a.a^{-1} = a^{-1}.a = 1$. Também temos na aritmética modular o conceito correspondente:

Dado um número a em Zm dizemos que um número a^{-1} em Z_m é um recíproco, ou inverso multiplicativo de a módulo m se $a.a^{-1} = a^{-1}.a = 1 \pmod{m}$.

Ex: O inverso multiplicativo de 3 módulo 26, ou seja, qual o número que satisfaz a equação $3x \equiv 1 \pmod{26}$. Para resolver temos o seguinte Teorema:

Algoritmo de Euclides

Teorema 2.3: *Sejam $a, b \in Z_+$, $b \neq 0$. Então existem números inteiros q e r tais que $a = bq + r$ e $0 \leq r < b$. Além disso, os valores de q e r são únicos.*

Demonstração: (Unicidade)

Sejam a e b inteiros positivos e q, q_1 e r, r_1 números inteiros tais que $a = bq + r$ e $a = bq_1 + r_1$ de tal forma que $0 \leq r < b$ e $0 \leq r_1 < b$. Suponha $r_1 \geq r$. Então, se $r = a - bq$ e $r_1 = a - bq_1$, $r - r_1 = (a - bq) - (a - bq_1)$ ou $r - r_1 = b(q - q_1)$.

Por outro lado, tanto r quanto r_1 são menores que b. Como supomos $r_1 \geq r$ obtemos $0 \leq r - r_1 < b$. Mas $r - r_1 = b(q - q_1)$, ou seja, $0 \leq b(q - q_1) < 1$. Como q e q_1 são inteiros, $q - q_1 = 0 \Rightarrow q = q_1$. Portanto $r = r_1$.

A partir do teorema resolveremos a equação modular e usaremos o Algoritmo de Euclides Estendido:

Teorema 2.4: *Dados inteiros positivos não–nulos a e b, tais que mdc (a, b) = d, com* $d > 0$*, então existem m, n* $\in$ *Z tais que am + bn = d.*

Demonstração:

Seja M = {at + bs | t, s $\in$ Z}. Então existe algum inteiro não–nulo pertencente a M. Isto é, M $\neq \varphi$. Se x $\in$ M então (−x) pertence a M, pois x = at + bs para t, s $\in$ Z, então (−x) = − (at + bs) = a (−t) + b(−s) e (−t), (−s) $\in$ Z. Seja agora A = M $\cap$ Z^+. Pelo Princípio da Boa Ordem, A tem um mínimo, digamos c = am + bn. Quero mostrar que c = d, em que d = mdc (a, b). Pois bem, d | a e d | b. Então d | am e d | bn e, logo, d | c. Observe que c | a e c | b, pois se x $\in$ A então x$\geq$ c e x = at + bs. Por Euclides, $x = kc + r$, 0 $\leq$ r < c, ou seja, (ta + bs) = k(am + bn) + r..

Então (t − km)a + (s − kn)b = r. E, desta forma, r = 0, pois c é mínimo de A. Ou seja, para qualquer x$\in$ A, c | x. Em particular, c | a e $c \mid b$, isto é, c | d. Portanto tem–se que c = d. ■

Utilizando o algoritmo de Euclides para descobrir o mdc:

26 = 3.8 + 2 com resto 2 - divide-se o valor pelo módulo

3 = 2.1 + 1 com resto 1 - divide-se o divisor pelo resto anterior

2 = 2.1 + 0 com resto 0

Como no último divisor com resto zero divisor exato é 1, sabemos que o MDC (26,3) = 1. Este algoritmo também serve para determinar se os números são primos entre si.

Agora vamos utilizar os restos das divisões para solução da equação ax + by = d e encontar o inverso de 3.

2 = 26 – 3.8

1 = 3 – 1.2 = 3 – 1 (26 – 3.8)

1 = 1.3 – 26 + 3.8

1 = 9.3 – 26.1 Logo o inverso de 3 (mod 26) é = 9

DECIFRANDO

Porque funciona? E porque achar a inversa?

Um resultado básico em Álgebra Linear nos afirma que uma Transformação Linear fica completamente determinada pela imagem de sua base. Além disso, uma matriz A ***nxn*** é invertível se, e somente se, os vetores colunas de A formam uma base para $R^{n.}$.

Para decifrar a mensagem devemos encontrar a inversa (mod 26) da matriz codificadora.

Se A é invertível e, $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ é um vetor comum então c = A.p e o correspondente vetor cifrado A^{-1}. c = A^{-1}. A p $\Rightarrow$ p = A^{-1}.c. Desta maneira o vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação à esquerda por A^{-1} (mod 26). Na aritmética usual uma matriz quadrada A é invertível se, e somente se, det (A) ≠0 ou equivalente, det (A) tem inverso.

Teorema 2.5 *Uma matriz quadrada A com entrada em Z_m é invertível módulo m se, e somente se, o inverso de Det (A) módulo m tem um inverso módulo m.*

Como o inverso de *Det* A módulo m terá um inverso módulo m se, e somente se, este inverso e m não tiverem fator primo em comum.

No caso módulo 26 m = 26 temos dois fatores primos comuns que é o 2 e 13. Neste caso a matriz A com entradas em Z_{26} é invertível módulo 26, se e somente se, o inverso multiplicativo do det (A), modulo 26 não é divisível por 2 ou 13.

Para decifrar a mensagem precisamos achar a inversa. Ela é calculada da seguinte forma:

$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ (mod 26) onde $(ad - bc)^{-1}$ é o inverso multiplicativo do resíduo ad – bc (mod 26). Achando a inversa:

$A = \begin{bmatrix} 5 & 3 \\ 1 & 2 \end{bmatrix}$ *Det* (A) = *(ad – bc) = 10 – 3 = 7*

MDC (26,7) = 1

5 = 26 – 7.3 → 2 = 7 – 5.1 → 1= 5 – 2.2

1 = 5 – 2 (7-5.1) → 1 = 15 – 2.7 + 5.2 → 1 = 3.5 – 2.7

$1 = 3\,(26 - 7.3) - 2.7 \rightarrow \quad 1 = 3.26 - 9.7 - 2.7 \quad \rightarrow \quad 1 = 3.26 - 11.7$

Encontramos (– 11) e de acordo com o item 2.1.4.1 temos:

$$R = \frac{|a|}{m} = \frac{|-11|}{26} = \frac{11}{26} \rightarrow m - R = 15$$

2.5 Método RSA

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais.

Para utilização do método deve-se proceder com as seguintes etapas:

1 . São escolhidos dois números primos extensos *p* e *q* (geralmente maiores que 10^{100}).

Calcula-se:

$$n = pxq \tag{5}$$
$$\varphi\,(n) = (p - 1)\,.(q - 1) \tag{6}$$

2. Escolhe-se um número ***d*** que seja co-primo a $\varphi\,(n)$, isto é, MDC (d, $\varphi(n)$) = 1.

3. Encontra-se ***e*** de forma que:

$$e\,.\,d \equiv 1 \pmod{\varphi\,(n)} \tag{7}$$

4. O texto simples é dividido em blocos, de modo que cada mensagem, *M*, fique no intervalo $0 \leq M < n$..

Para criptografar a mensagem, *M*, é calculado:

$$C \equiv M^{\boldsymbol{e}} \,(mod\ n) \tag{8}$$

5. Para decriptografar *C*, é calculado:

$$C \equiv M^{d} (mod\ n) \tag{9}$$

É possível provar que, para todo *M* na faixa especificada, as funções de criptografia e decriptografia são inversas entre si. Para realizar a criptografia, é

necessário conhecer o valor do "***e***" e do "***n***", ao passo que para decriptografar, são necessários "***d***" e "***n***". Portanto, a chave pública consiste no par (*e*, *n*) e a chave privada consiste em (*d*, *n*).

Exemplo: Utilizando o algoritmo RSA para encriptar a palavra ANDRÉ.

Escolhe-se $\boldsymbol{p} = 3$ e $\boldsymbol{q} = 11$.

Calcula-se : $n = p.q = 3.11 = 33$

$\varphi(n) = (p - 1)(q - 1) = (3 - 1)(11 - 1) = 20$

O valor escolhido como número ***d*** que seja co-primo a $\varphi(n)$, devendo satisfazer a equação MDC (20, d) = 1. Desse modo, pelo algoritmo de Euclides, d = 7.

$6 = 20 - 2.7$

$1 = 7 - 1.6 = 7 - 1\ (20 - 2.7)$

$1 = 1.7 - 1.20 + 2.7$

$1 = 3.7 - 20.1$ Logo o inverso de 7 (mod 20) é 3

Portanto, a chave privada consiste em (*d*, *n*) = (7, 33).

Para que a equação $e \,.\, d \equiv 1 \pmod{\varphi(n)}$ seja verdadeira o "*e*" deverá ser um número que multiplicado por 7 (mod 20) seja igual a 1. Usando o método de Euclides acima chegamos ao número 3, pois 3.7 (mod 20) = 1, portanto, a chave pública consiste em $(e, n) = (3, 33)$.

Representando cada letra do alfabeto por um número, conforme a Tabela1. E após chega-se a seguinte tabela abaixo:

Simbólico	Numérico	M^3	$C = M^3 \pmod{33}$
A	1	1	1
N	14	2744	5
D	4	64	31
R	18	5832	24
E	5	125	26

A Tabela (Decriptografia) a seguir apresenta o processo de decriptar a mensagem.

$C = M^3 \pmod{33}$	C^7	$M = C^7 \pmod{33}$	Simbólico
1	1	1	A
5	78125	14	N
31	31^7	4	D
24	24^7	18	R
26	26^7	5	E

2.6 Algoritmo de ElGamal

Taher Elgamal em 1984 introduziu o algoritmo que recebeu seu nome. Assim como o RSA é baseado no problema do logaritmo discreto. E este é baseado na raiz primitiva.

Se a é uma raiz primitiva de p, então $a^1 \pmod p$, $a^2 \pmod p$, ..., $a^{p-1} \pmod p$ são distintos e consistem em inteiros de 1 a p-1.

Exemplo: $5^1 \equiv 5$, $5^2 \equiv 4$, $5^3 \equiv 6$, $5^4 \equiv 2$, $5^5 \equiv 3$, $5^6 \equiv 1 \pmod 7$, então diz-se que 5 é raiz primitiva mod 7. Já as potências de 4 geram $4^1 \equiv 4$, $4^2 \equiv 2$, $4^3 \equiv 1$, $4^4 \equiv 4$, $4^5 \equiv 2$, $4^6 \equiv 1 \pmod 7$ e não geram as classes de congruência 3, 5 e 6, daí 4 não é raiz primitiva (mod 7).

Então: Para um inteiro b uma raiz primitiva a de um número primo p é possível encontrar um expoente i tal que: $b = a^i \pmod p$ onde $0 \leq i \leq (p-1)$. O expoente i é chamado de logaritmo discreto de b na base a mod p.

Na sua forma mais simples, o sistema do logaritmo discreto tenta descobrir o expoente x na fórmula $y = g^x \pmod p$. Vamos ao método:

a) Primeiramente é gerado um número primo p, e dois outros valores quaisquer a e α.

b) De posse desses valores geramos β segundo a fórmula:

$$\beta \equiv \alpha^a \ (mod\ p)$$

Os valores α,β e p são públicos e a é secreto.

Cifrando um bloco:

a) Antes de começar a cifragem propriamente dita, devemos gerar uma chave de sessão, para tanto devemos escolher um valor randômico k < p. Neste caso, "k" um número aleatório com três algarismos.

b) De posse do valor de k, geramos a chave de sessão y_1 segundo a fórmula:

$$y_1 = \alpha^k \ (mod\ p)$$

c) A partir daí podemos gerar o bloco criptografado da seguinte forma:

$$y_2 = \times \beta^k \ (mod\ p)$$

Onde $\times$ representa o bloco em texto plano.

d) O bloco de texto plano deve ser escolhido de forma que **x** < **p**

e) A chave de sessão (valor "k") deve ser gerada para cada bloco separadamente.

f) Por exemplo para a mensagem: Criptografando

g) Transformamos em código AISII:

06711410511211611110311409710209711010011 1

h) Utilizando as chaves:

p = 7457 ; α = 4 ; a = 93 e β = 725

i) Separamos o texto plano em blocos (consideramos o número de algarismos de $\times$ menor do que o de p, como p tem 4 algarismos, utilizaremos blocos de 3 algarismos):

067 114 105 112 116 111 103 114 097 102 097 110 100 111

j) Criptografando temos $e_1(x,k) = (y_1, y_2)$:

e_1 (067, 271) = (0526, 2208)

e_2 (114, 252) = (4341, 1600)

e_3 (105, 876) = (1852, 4800)

e_4 (112, 737) = (3711, 2769)

e_5 (116, 137) = (4738, 2400)

e_6 (111, 012) = (4096, 1181)

e_7 (103, 894) = (3963, 0318)

e_8 (114, 199) = (2987, 5578)

e_9 (097, 299) = (4034, 5564)

e_{10} (102, 661) = (2686, 1576)

e_{11} (097, 284) = (2656, 4753)

e_{12}(110, 469) = (1547, 3305)

e_{13} (100, 065) = (1277, 0897)

e_{14} (111, 988) = (0824, 2753)

Ou seja, a mensagem criptografada é:

(0526, 2208) (4341, 1600) (1852, 4800) (3711, 2769) (4738, 2400)

(4096, 1181) (3963, 0318) (2987, 5578) (4034, 5564) (2686, 1576)

(2656, 4753) (1547, 3305) (1277, 0897) (0824, 2753)

A segurança dos sistemas depende da dificuldade de determinar o valor de x. Modificações desse problema utilizam a exponencial discreta, que parece ser mais segura que o problema original.

Decifrando um bloco

De posse do par (y_1, y_2) que consiste no bloco criptografado, aplicamos a fórmula : $d(y_1,y_2) = y_2 . (y_1^a)^{-1} \pmod p$

Obtendo desta maneira o bloco decriptografado. Para o exemplo acima foi utilizado a chave secreta a = 93. chegamos novamente no texto:

067 144 105 112 116 111 103 114 097 102 097 110 100 111 = Criptografando

3. Considerações Finais

Procurei através deste trabalho mostrar algumas das muitas aplicações da Matemática. O desenvolvimento e o estudo destas aplicações exigem o conhecimento de assuntos como teoria dos números, matrizes e congruências.

Além disso, este trabalho foi uma boa oportunidade de correlacionar conteúdos estudados nas primeiras disciplinas do curso.

Também foi importante porque nas disciplinas de Fundamentos da Matemática, muitas vezes por indisponibilidade de tempo, não foram vistas e trabalhadas.

Assim, consideramos que o objetivo principal deste trabalho foi alcançado plenamente.

4. Referências Bibliográficas

1. ANTON, H. **Álgebra Linear**. Rio de Janeiro: Campus, 2001.

2. BAYER, F. M. **Matrizes - Codificação e Decodificação de Mensagens**. Disponível em: <http://coralx.ufsm.br/depmat/matriz.html> Acesso em 05 mai 2008.

3. SLIPSCHUTZ, S. **Álgebra Linear.** São Paulo: Makron Books, 1994**.**

4. SHOKRANIAN, S. **Criptografia para Iniciantes**. Editora: Universidade de Brasília, 2005.

5. Criptografia. Disponível em: <http://www.numaboa.com.br/criptologia/> Acesso em 10 out 2007.

6. História e Aplicações da Criptografia. Disponível em: <http://www.numaboa.com.br/criptologia/> Acesso em 10 out 2007.

Apêndice

A.1 PRIMALIDADE

Um dos problemas práticos e muito importante na criptografia é o problema de achar números primos grandes. Na criptografia atual são as escolhas dos números primos grandes. Uma vez que sabemos os fatores "x" são 5 e 7, é fácil obter computacionalmente esse número multiplicando os fatores. Entretanto, para descobrir os fatores uma vez dado o número 35 se torna mais difícil. O problema cresce mais ainda quando este número x é o produto de dois números primos na casa de 10^{100}. Os algoritmos atuais o número de 200 dígitos requereria 4 bilhões e anos de tempo de computação.

Vamos conhecer primeiramente a propriedade fundamental dos números primos.

Teorema A.1: *Sejam a, b, c* $\in Z_+$ *mdc (a, b) = 1. Então:*

1. $b \mid a.c \Rightarrow b \mid c.$

2. $a \mid c$ *e* $b \mid c \Rightarrow a.b \mid c.$

Teorema A.2: *Seja p um número primo e a, b* $\in$ *Z+. Se* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b.$

A seguir vamos conhecer o Crivo de Erastóstenes. É o algoritmo mais antigo, e talvez o mais simples e rápido de implementar. Ele foi criado por Erastóstenes, um matemático grego do mundo antigo.

Teorema A.3: *Se* $n \in Z$, $n > 1$, *não é divisível por nenhum primo positivo p tal que* $p^2 \leq n$ *, então n é primo.*

Demonstração:

Suponhamos que n não seja primo e p é o menor primo positivo que divide n. Desta forma: n = p.m com $p \leq m$ assim, $p^2 \leq p.m = n$. Desta forma, n é divisível por p primo tal que $p^2 \leq n$. Absurdo. ■

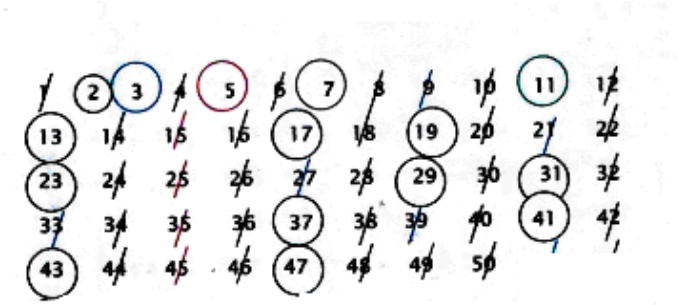
A.1.1 Crivo de Erastóstenes

Vejamos abaixo como seria o Crivo de Erastóstenes até 50.

O funcionamento do algoritmo é o seguinte:

Escrevemos os números inteiros de 2 até o ***n*** que se queira incluir na tabela. Risque todos os números maiores que 2 que são divisíveis por 2 (a cada segundo número). Encontre o menor remanescente maior que 3. Risque os números maiores que 3 que são divisíveis por 3 (a cada terceiro número). Encontre o menor número remanescente maior que 3 (5). Risque todos os números maiores que 5 que são divisíveis por 5 (a cada quinto número). Continuar até que se tenha marcado todos os números que são divisíveis por $\sqrt{n}$. Os números restantes (não marcados) são primos. A figura abaixo são determinados os primos até 50. Observe que são marcados os números até $\sqrt{50}$ = 7.

Crivo de Eratóstenes



O seguir veremos o Teorema de Fermat. Através dele verificamos a probabilidade de ser primo ou não. Pois a condição do teorema é uma condição necessária, mas não suficiente.

Teorema A.4: (Pequeno Teorema de Fermat): *Para qualquer* $a \in Z$, *se* $p > 0$ *é primo, então* $p \mid (a^p - a)$, *ou seja,* $a^p \equiv a \bmod p$.

Estatisticamente a distribuição de números primos pode ser decidida por meio do famoso teorema do número primo, provado no fim do século XIX. Para compreender o que é esse teorema devemos definir a função $\varphi(n)$.

Seja a Função φ de Euler: $\varphi(n)$ é o número de inteiros a no intervalo $1 \leq a \leq n$, tais que mdc (a,n) = 1. Por exemplo: $\varphi(2) = 1$, $\varphi(5) = 3$, $\varphi(10) = 4$

Quando o número ***n*** é pequeno o cálculo de $\varphi(n)$ é fácil. Porém, quando o número é maior não sabemos calcular o valor exato de $\varphi(n)$. O teorema do número primo mostra-nos qual é o comportamento de $\varphi(n)$ no infinito. Ele foi demonstrado *em* 1896.

Teorema A.5: (Teorema do número primo): A seguinte igualdade é verdadeira:

$$\lim_{n\to\infty} \{\varphi(n) / (\frac{n}{\ln n})\} = 1$$

A.1.2 A Pseudoprimalidade

Pelo pequeno teorema de Fermat se *mdc (a,n)* = 1 e *n* é um número primo, então $a^{n-1} \equiv 1 \pmod n$. *Agora seja* $(Z/nZ)^+ := \{1, 2, ..., n-1\}$

Com essa notação o Pequeno Teorema de Fermat pode ser escrito na seguinte de forma:

Teorema A.6: (Pequeno Teorema de Fermat): *Se n é um número primo, então para todo* $a \in (Z/nZ)^+$ *temos:* $a^{n-1} \equiv 1 \pmod n$.

O teorema acima é uma recíproca do teorema de Fermat:

Teorema A.7: *Seja p um número primo. Se a é um número inteiro tal que* $mdc(p,a)=1$, *então:* $a^{p-1} \equiv 1 \pmod p$

A partir deste teorema temos o seguinte Corolário:

Corolário A.1: *Se existir um número* $\boldsymbol{a} \in (Z/nZ)^+$ *tal que* $a^{n-1} \not\equiv 1 \pmod n$, *então n não* é primo é composto.

Entretanto, na prática podemos considerar $a = 2$ e usar o corolário acima. Se para um dado número inteiro positivo *n* teremos $2^{n-1} \not\equiv 1 \pmod n$, então *n* é primo, pois o teorema 6 não implica que se a identidade (corolário) é verdadeira, então *n* é primo (é necessário que *n* seja primo). A partir daí, temos a seguinte definição para números pseudoprimos:

Teorema A.8: *Dizemos que um inteiro positivo n é a-pseudoprimo ou pseudoprimo na base a* $(Z/nZ)^+$, *se* $a^{n-1} \equiv 1 \pmod n$

Quando $a = 2$ simplesmente dizemos que *n* é pseudoprimo. Nesse caso *n* satisfaz $2^{n-1} \equiv 1 \pmod n$.

Observação: Os números primos $p \neq 2$ são a-pseudoprimos para todo $a \in (Z/nZ)^+$. E isso não deve causar confusão na interpretação da palavra "pseudo" que nos dicionários de língua portuguesa é interpreetado como "falso". Do ponto de vista da língua, não é certo que um número primo também seja falso primo. Então, é melhor interpretar pseudoprimo como "semelhante" a um primo, pois os números pseudoprimos, que não são primos têm uma semelhança com os primos, eles

satisfazem a congruência $a^{n-1} \equiv 1 \ (mod\ n)$. Eles são falsamente primos. Um caso muito interessante acontece quando um número é a-pseudoprimo para toda base *a*.

Teorema A.9: *Se um número n é pseudoprimo para toda base* $a \in (Z/nZ)^+$ *dizemos que esse número é um* ***número de Carmichael***

Exemplo1: Os seguintes números são os primeiros quatro números pseudoprimos que não são primos 341, 561, 645, 1105. Eles são respectivamente fatorados da seguinte forma:

341 = 11x 31

561=3x11x17

645 = 3x5x43

1105 = 5x13x17

Exemplo2: Os primeiros cinco números de Carmichael são 561, 1105, 1725, 2465, 2821. Eles são fatorados da seguinte forma:

561 = 3x11x17

1105 = 5x13x17

1729 = 7x13x19

2465 = 5x17x29

2821 = 7x13x31

Como podemos observar todos esses números de Carmichael têm três fatores primos. Porém isso não ocorre sempre. O primeiro número de Carmichael com quatro fatores primos é: 41041 = 7x11x13x41, e o primeiro com cinco fatores primos é: 825265 = 5x7x17x19x73. A existência de infinitos números de Carmichael foi provada em 1994. A razão para que os números de Carmichael sejam raros está baseado no fato de que tais números satisfazem várias condições. Os seguintes resultados abaixo mostram este resultado e outras propriedades deste número.

Teorema A.10 (Korset): *Um inteiro positivo* $n = p_1p_2 \ldots p_k$ *representado pelo produto de seus divisores* p_i *é número de Carmichael se e somente se, os divisores* p_i *para todo* $i = 1, 2, \ldots\ldots, k$ *são distintos e o mínimo múltiplo comum mmc* $(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$ *divide* $n - 1$.

Demonstração:

Se *n* é um número de Carmichael então $a^{n-1} \equiv 1 \ (mod\ n)$ para todo $a \in (Z/nZ)^+$. Logo *n* satisfaz o sistema $a^{n-1} \equiv 1 \ (mod\ p_i)$ i = 1, 2, 3, ..., *k*

Pelo Teorema de Resto Chinês, o sistema tem solução se e somente se o mínimo múltiplo comum $(p_1 - 1, p_2 - 1, ..., p_k - 1)$ divide $n - 1$. A demonstração está completa. ■

Corolário A.2*: n é um número Carmichael se e somente se ele é livre de quadrados e (p – 1)| (n – 1) para todo divisor primo p de n.*

Corolário A.3: *Números de Carmichael são ímpares e têm pelo menos três divisores primos.*

A.1.3 Teorema de Lucas e Pocklington

Estes teoremas, o primeiro do ano de 1876 e, o segundo de 1914, são práticos pra verificação se um número é primo. Eles são usados para implementação de testes de primalidade.

Teorema A.11 (Lucas) : *Seja* $n \geq 3$ *um inteiro e* $a \in Z$ *tal que* $a^{n-1} \equiv 1 \pmod n$ *e* $a^x \not\equiv 1 \pmod n$ *para todo x com* $1 \leq x < -1$, *então n é primo.*

Demonstração:

A congruência $n^{a-1} \equiv 1 \pmod n$ implica que o $mdc(a,n) = 1$. Por outro lado, os inteiros a^i e a^j para todo número *i* e *j* tal que $1 \leq i < j \leq n - 1$ são incongruentes módulo *n*, pois caso contrário teremos $a^i \equiv a^j \pmod n$. Isso implica que $a^i(a^{j-i} - 1) \equiv 0 \pmod n$. Mas o mdc $(a,n) = 1$, e então $a^{j-i} \equiv 1 \pmod n$. Isso é impossível pela segunda condição do teorema. Logo os números $a, a^2, ..., na^{-1}$ são congruentes a $1, 2, ..., n - 1$. Isso implica que se *p* é o menor número primo que divide *n*, então existe um inteiro positivo *r* tal que $a^r \equiv p \pmod n$. Mas isso é impossível, pois $mdc(a,n) = 1$. Logo, não existem primos que dividem *n*. Portanto *n* é primo. ■

Teorema A.12 (Pocklington): *Seja n > 1 inteiro e s > 0 um divisor de n – 1. Suponha que exista um inteiro a satisfazendo* $a^{n-1} \equiv 1 \pmod n$ *e mdc* $(a^{(n-1)/q} - 1, n) = 1$ *para todo divisor primo q de s. Então, todo divisor primo p de n satisfaz a congruência* $p \equiv 1 \pmod s$, *e se* $s > \sqrt{n} - 1$, *n é primo.*

Demonstração:

Seja *p* um divisor primo de *n*, e *b* o resto da divisão de $a^{(n-1)/s}$ por *n*. Então temos que $a^{(n-1)/s} \equiv b \pmod n$. Portanto, também, $a^{n-1} \equiv b^s \pmod n$. *Por outro lado a congruência* $a^{n-1} \equiv 1 \pmod n$ *implica que* $b^s \equiv 1 \pmod p$. Logo, o expoente de *b (mod p)* (na terminologia de teoria dos números*)* ou a ordem de *b (mod p)* (na terminologia de teoria dos grupos) no grupo *(Z/pZ) divide s*. Do outro lado, se *q* é um divisor primo de *s*,

$b^{s/q} \not\equiv 1 \pmod p$, pois pela hipótese $a^{(n-1)/q} - 1$ não é divisível por p. Portanto, a ordem de b $(mod\ p)$ não é um divisor de s/q, qualquer que seja o divisor primo q de s. Então essa ordem é igual a s. Mas o expoente (ou ordem) divide $p - 1$. Portanto $p \equiv 1 \pmod s$. Isto completa a primeira parte do teorema. Para provar a segunda afirmação, primeiro observe que de $p \equiv 1 \pmod s$ segue-se $p - 1 = ks \geq s$, para certo inteiro positivo k. Logo $p \geq s + 1 > \sqrt{n}$. Mas, $s > \sqrt{n} - 1$, então $p > \sqrt{n}$. E isso só pode ser verdadeiro para todo divisor primo p de n uma vez que n é primo. ■

A.1.4 Números de Fermat e Mersenne

Uma das aplicações do teorema de Pocklington é para verificar se certos números notáveis são primos. Entre os números notáveis devemos considerar pelo menos os números de Fermat e Mersenne.

Definição A.1: *O número $F_n = 2^{2^n} + 1$ é chamado n-ésimo número de Fermat*

Nem todos os números de Fermat são primos. Alguns deles são, mas não sabemos se o conjunto dos números de Fermat primos é infinito. Por exemplo, os seguintes são alguns números de Fermat primos e compostos.

$F_1 = 5$

$F_2 = 17$

$F_3 = 257$

$F_4 = 65537$

$F_5 = 4294967297 = 641 \times 6700417$

Os seguintes teoremas indicam algumas propriedades de números de Fermat que são bem conhecidas.

Teorema A.13: *Quaisquer dois números distintos de Fermat são primos entre si. Em outras palavras, se $F_m \neq F_n$ são números de Fermat, então mdc $(F_n, F_m) = 1$.*

Teorema A.14: *Um número de Fermat ou é primo ou pseudoprimo.*

O outro conjunto de números notáveis usados nos problemas de primalidade é o conjunto dos números de Mersenne.

Definição A.2: *O n-ésimo número de Mersenne é o número $M_n = 2^n - 1$.*

O próximo, e último, teorema mostram que uma condição necessária, mas não suficiente, para que M_n seja primo é que o n seja primo também.

Teorema A.15: *Se n é um número composto (não primo), então M_n é composto.*

6. Glossário

ALGORITMO - Conjunto de operações elementares que devem ser efetuadas para se obter um resultado desejado. Por exemplo, uma receita de bolo é um algoritmo.

ASCII (American Standard Code for Information Interchange) - Código Padrão Americano para o Intercâmbio de Informação que traduz os nomes dos caracteres de um alfabeto para outros. Por exemplo, a letra "A" é traduzida para 65.

ASSIMÉTRICO - Um algoritmo de criptografia que utiliza uma chave pública para encriptar e uma chave privada (diferente) para decifrar as mensagens. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave. Também conhecido como algoritmo de chave pública.

ASSINATURA - Associada a uma mensagem, prova a identidade do remetente.

AUTENTICAÇÃO - Verificação reivindicada de uma identidade. O processo de determinar a identidade de um usuário que esteja tentando alcançar um sistema

B

BIGRAMA - Seqüência de duas letras consecutivas. Exemplos: pa, le,...

C

CHAVE - Num sistema de encriptação, corresponde a um nome, uma palavra, uma frase, etc, que permite, mediante o algoritmo de encriptação, cifrar ou decifrar uma mensagem.

CHAVE DUPLA - Cifra de chave dupla. Outro nome para cifra polialfabética.

CHAVE FRACA - Chave que, por uma razão qualquer (seu comprimento, uma propriedade matemática, etc), permite quebrar rapidamente o código.

CHAVE PRIVADA - Chave que deve ser mantida secreta, (ver Assimétrico).

CHAVE PÚBLICA - Uma chave criptográfica disponível para distribuição sem necessidade de segredo. É o oposto de uma chave privada ou chave secreta. Veja "Assimétrico".

CIFRA - Conjunto de procedimentos e conjunto de símbolos (letras, nomes, sinais, etc.) usados para substituir as letras de uma mensagem para encriptá-la. É geralmente classificada como cifra de transposição e cifra de substituição.

CIFRAGEM - Cifrar ou cifragem. Procedimento pelo qual se torna impossível a compreensão de um documento a qualquer pessoa que não possua a chave da cifra.

CIFRAR - O mesmo que fazer uma cifragem.

CODIFICAR - Modificar a estrutura de um conjunto de documentos aplicando um algoritmo (cifra, método de compressão, etc).

CÓDIGO - Sistema de símbolos (palavras, nomes, símbolos, etc.) que substituem palavras inteiras. Por exemplo, a substituição de "007" por "James Bond".

CONFIDENCIALIDADE - Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. O conceito de garantir a informação sensível confidencial, limitada para um grupo apropriado de pessoas ou organizações. Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação.

CRIPTOANÁLISE - Criptoanálise ou criptanálise. 1. Métodos de analisar mensagens cifradas com o objetivo de decifrá-las. 2. Arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise é chamada ataque.

CRIPTOGRAFIA - 1. Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo, impedir modificações e o uso ilegal dos mesmos. 2. Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem.

A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito a formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem.

CRIPTOGRAMA - Mensagem cifrada ou codificada.

CRIPTOLOGIA - Ciência das mensagens secretas. É composta pelas disciplinas de criptografia e de criptanálise.

D

DECIFRAR - Operação inversa de cifrar, ou seja, obter a versão original de uma mensagem cifrada. Ao contrário da desencriptação, aqui se conhece o método de cifragem.

DECRIPTAR - Restaurar documentos cifrados, restaurando-os ao estado original, sem dispor das chaves teoricamente necessárias.

DICIONÁRIO - Lista de palavras e expressões mais utilizadas que servem de base para se procurar uma senha.

DIGRAMA - O mesmo que bigrama.

DSA - Algoritmo de assinatura digital é um algoritmo assimétrico que permite criar assinaturas digitais.

DSS (Digital Signature Standard) - Padrão do governo dos E.U.A. que combina DSA e SHA-1 para especificar um formato para assinatura digital.

E

ENCRIPTAÇÃO - Um processo de disfarçar a informação de modo que não possa ser compreendida por uma pessoa desautorizada. A transformação de uma seqüência de caracteres em outra por meio de uma cifra, de uma tabela de transposição, ou de um algoritmo a fim fazer com que a informação não seja entendida a qualquer um que não possua o mecanismo da decodificação.

ENIGMA - Máquina Enigma, utilizada durante a Segunda Guerra Mundial.

ESTEGANOGRAFIA - Do grego "escrita escondida". Ramo particular da criptologia que consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença. Ao contrário da criptografia, que procura esconder a informação da mensagem, a esteganografia procura esconder a existência da mensagem.

F

FORÇA BRUTA - É um ataque que consiste em testar todas as chaves possíveis até encontrar a correta. Não é um bom método de acesso porque pode demorar dias, meses, ou até anos.

FREQUÊNCIA - Porcentagem de ocorrência de uma letra ou palavra em uma determinada língua. Calcular a freqüência de ocorrência é uma das primeiras etapas de um processo de desencriptação.

H

.

HOMOFÔNICA - Do grego "o mesmo som". O conceito de ter seqüências diferentes de letras que sejam pronunciadas do mesmo modo. Em criptografia, uma cifra que

traduz um único símbolo do texto plano em qualquer um de múltiplos símbolos do texto cifrado, todos com o mesmo significado. Veja também polifônica, poligâmica e monogrâmica.

I

IDEA - (International Data Encryption Algorithm)

INTEGRIDADE - 1. A condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas. 2. Garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.

M

MENSAGEM CLARA - Mensagem clara ou mensagem original. Também denominado texto plano.

MENSAGEM ORIGINAL - Mensagem com o texto original, sem ter sofrido qualquer alteração de métodos criptográficos.

MONOALFABÉTICA - Substituição usando um único alfabeto. Também chamada de substituição simples.

MONOGRÁFICA - O mesmo que monogrâmica.

MONOGRÂMICA - Monogrâmica ou monográfica, do grego "uma letra". Uma cifra que traduz um a um os símbolos do texto original em texto cifrado. O oposto de poligrâmico; veja também homofônica e polifônica.

P

PASSWORD - Veja "Senha".

POLIALFABÉTICA - Um tipo de substituição na qual múltiplos alfabetos de substituição distintos são usados.

POLIGRÂMICA - Poligrâmica ou poligráfica, do grego "múltiplas letras". Uma cifra que traduz vários símbolos do texto original, em grupo e ao mesmo tempo, em texto cifrado.

Exemplos: a cifra de Playfair e a cifra de Hill. O oposto de monogrâmico; veja também homofônica e polifônica.

R

RECIFRAGEM - Fazer nova cifragem a partir de uma mensagem que já tenha sido cifrada por outro método. Geralmente, a encriptação de nível mais alto (ou mais externo) de uma encriptação múltipla. Classicamente, recifragens são muito fracas, dependendo do efeito randômico do nível de encriptação anterior. Também conhecida como superencriptação ou supercifragem.

RSA - Algoritmo de cifragem por chave pública utilizado principalmente no PGP, usado principalmente na cifragem da assinatura, permitindo a identificação do documento. Permite criptografar dados, criar e verificar assinaturas digitais.

S

SENHA - Uma única palavra ou seqüência de caracteres usada para autenticar uma identidade. A senha é confidencial, opostamente a identificação do usuário.

SIMÉTRICO - Algoritmo de criptografia que usa somente uma chave, tanto para criptografar como para descriptografar. Esta chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta.

SUBSTITUIÇÃO - Uma cifra de substituição troca os caracteres de uma mensagem original por símbolos (caracteres, nomes, sinais, etc.) predefinidos.