Mantendo Segredos com a ajuda da Matemática*

Hemar Godinho
Departamento de Matemática - UnB

21 de outubro de 2002

Vamos imaginar que dois colegas de uma turma estejam planejando uma festa surpresa. O sucesso desta festa estará baseado na capacidade deles de manter tudo em segredo, ou seja, eles precisam estar seguros de que ninguém mais da turma terá acesso as mensagens por eles trocadas. Esta situação tão simples na verdade pode ser vista em ambientes dos mais diversos, com por exemplo quando utilizamos o cartão de crédito, enviamos correio eletrônico, utilizamos computadores para operações bancárias. Em todos estes casos queremos estar seguros de que ninguém, além do endereçado, tenha acesso ao conteúdo da mensagem. Esta é a área de estudos da Criptografia, que busca criar sistemas que garantam que as mensagens enviadas estejam protegidas contra fontes não autorizadas.

Os elementos básicos em um sistema criptográfico são:

$$\begin{cases} T & : \text{ Mensagem original (texto)} \\ C & : \text{ Mensagem codificada} \\ f & : \text{ Função de codificação} \\ f^{-1} & : \text{ Função de decodificação} \end{cases}$$

e este sistema pode ser representado pelo seguinte esquema:

$$T \xrightarrow{f} C \xrightarrow{f^{-1}} T.$$

*Palestra apresentada na I Bienal da SBM, ocorrida em Belo Horizonte-MG, entre 14 e 18 de outubro de 2002.

Um sistema será considerado bom se a função f for "fácil"de ser aplicada, mas f^{-1} for muito dificil de ser determinada. A seguir ilustraremos estas idéias com alguns exemplos de sistemas criptográficos.

O Criptograma de Julio César

Conta a história que este era o sistema criptográfico utilizado pelos romanos, para o envio de mensagens secretas. Este sistema consiste basicamente na substituição de letras utilizando uma tabela como esta abaixo:

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

Assim se queremos codificar a mensagem BIENAL, utilizando a tabela acima chegaremos na mensagem codificada ELHQDO.

Exemplo 1 *Decifre a mensagem abaixo, sabendo que para codificar esta mensagem foi utilizado o Criptograma de César dado pela tabela acima*

HXDPRPDWHPDWLFD

Uma característica importante deste criptosistema é que após a $26^{a\cdot}$ letra, ou seja Z, retornamos à primeira letra A. Assim determinamos um "ciclo". Todo este processo de codificação pode ser completamente descrito matematicamente, utilizando um novo conceito de operação nos números inteiros, chamada de *operação módulo m*, que passamos a descrever a seguir.

Dados números inteiros $a, b \in \mathbb{Z}$ e um número natural $m \in \mathbb{N}$, diremos que a é *congruente* a b módulo m, e escreveremos

$$a \equiv b \ (mod\ m),$$

se m dividir $(a-b)$, ou seja, se existir um $q \in \mathbb{Z}$ tal que $(a-b) = mq$ (divisão exata). Vejamos alguns exemplos.

Exemplo 2 *(a)* $23 \equiv 3\ (mod\ 5)$

(b) $8 \equiv -12 \ (mod\ 20)$

(c)

$$a \equiv \begin{cases} 0 \ (mod\ 2) & se\ a\ é\ par \\ 1 \ (mod\ 2) & se\ a\ é\ impar \end{cases}$$

Quando dividimos dois números inteiros a, m, o fazemos seguindo um "algoritmo", até obter algo do tipo

$$\begin{array}{cc} \text{a} & \big| \ \text{m} \\ \hline \text{resto} & \text{quociente} \end{array}$$

ou seja, $a = m.q + r$ onde q é o quociente e r é o resto da divisão. Um fato muito importante é que sempre podemos escolher r, com $0 \leq r < m$. Portanto sempre temos que $a \equiv r \ (mod\ m)$. Assim verificamos que todo inteiro a é congruente módulo m a um dos números do conjunto

$$\mathbb{Z}_m := \{0, 1, 2, \ldots, m-1\}.$$

Agora observe que se denotamos por $\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{m}\}$, logo temos que

$$\mathbb{Z} \ = \ \overline{0} \cup \overline{1} \cup \cdots \cup \overline{\text{(m-2)}} \cup \overline{\text{(m-1)}}.$$

Além disso temos que $b \in \overline{a}$ se, e somente se, m divide (b-a). Ou seja, se $b - a = mq$, o que nos dá que $b = mq + a$. Portanto temos que

$$\begin{array}{rcl} \overline{0} & = & \{b \in \mathbb{Z} \mid b = mq + 0, \ \text{ para qualquer } \ q \in \mathbb{Z}\} \\ \overline{1} & = & \{b \in \mathbb{Z} \mid b = mq + 1, \ \text{ para qualquer } \ q \in \mathbb{Z}\} \\ \overline{2} & = & \{b \in \mathbb{Z} \mid b = mq + 2, \ \text{ para qualquer } \ q \in \mathbb{Z}\} \\ & \vdots & \\ \overline{\text{m-1}} & = & \{b \in \mathbb{Z} \mid b = mq + \text{(m-1)}, \ \text{ para qualquer } \ q \in \mathbb{Z}\} \end{array}$$

Voltando ao exemplo do Criptosistema de César, vamos identificar letras com números conforme abaixo

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Observe que nosso "alfabeto"agora é o conjunto $\{0, 1, 2, \ldots, 24, 25\}$, que são os possíveis restos da divisão por m=26. E agora podemos facilmente descrever o criptograma de Cesar como

$$\begin{array}{lcll} C = f(T) & \equiv & T + 3 & (\text{mod } 26) \quad (*) \\ T = f^{-1}(C) & \equiv & C - 3 & (\text{mod } 26) \end{array}$$

O Criptograma de Blaise de Vigenère

Em 1586, o diplomata francês da corte de Henrique III de França, Blaise de Vigenère (1523-1596), publicou um livro chamado de "Um tratado sobre a Escrita Secreta", onde apresentou seu sistema criptográfico. Este sistema utiliza uma palavra-chave para a codificação e decodificação, o que torna o sistema bem mais dificil de ser quebrado.

Vamos codificar a frase *ENCONTRAR DOMINGO*, utilizando a palavra chave *SBM*, fazendo uso da tabela de correspondência entre letras e números apresentadas anteriormente.

4	13	2	14	13	19	17	0	17	3	14	12	8	13	6	14
E	N	C	O	N	T	R	A	R	D	O	M	I	N	G	O
S	B	M	S	B	M	S	B	M	S	B	M	S	B	M	S
18	1	12	18	1	12	18	1	12	18	1	12	18	1	12	18
22	14	14	6	14	5	9	1	3	21	15	24	0	14	18	6
W	O	O	G	O	F	J	B	D	V	P	Y	A	O	S	G

Assim a mensagem código enviada será: WOOGOFJBDVPYAOSG

O Criptograma de Chave Pública RSA

Um criptosistema de Chave pública tem por princípio fundamental que o conhecimento da função codificadora (que pode ser um processo, um algoritmo, etc) não permite, computacionalmente falando, a determinação da função decodificadora. O nome Chave Pública se deve ao fato de que a chave codificadora necessária para o envio da mensagem pode ser de conhecimento geral, e mesmo assim continua impossível para qualquer agente não autorizado ter acesso à mensagem original. Cada usuário do sistema torna pública sua chave codificadora, permitindo assim que qualquer outro usuário possa

lhe enviar uma mensagem. Mas como somente ele tem a chave decodificadora, a privacidade da comunicação estará mantida.

Uma das questões mais importantes em criptografia é a autenticação de uma mensagem. Como ter certeza que a mensagem recebida realmente vem da pessoa que a assinou? Se um banco recebe uma mensagem de um cliente pedindo para transferir todos os seus recursos para uma outra conta, como ter certeza de que realmente a ordem veio deste cliente e não de um impostor? No sistema de chave pública existe uma maneira fácil de fazer a autenticação de uma mensagem. Vamos dizer que A e B sejam usuários de um sistema. Vamos denotar por f_A e f_B as funções de codificação de A e B respectivamente. Vamos supor que a assinatura eletrônica de A seja P. Observe que não é suficiente que A envie para B sua assinatura na forma $f_B(P)$, tendo em vista que todos conhecem a chave pública f_B de B, assim qualquer um poderia enviar para B a mensagem $f_B(P)$. Assim a solução seria para A enviar a mensagem $f_B f_A^{-1}(P)$. Assim quando B aplicar a função f_B^{-1} (que somente ele conhece) ao texto recebido, tudo será decodificado, exceto o pequeno texto $f_A^{-1}(P)$. Como B sabe que a mensagem é supostamente de A, ele poderá aplicar a chave pública de A, ou seja f_A a este texto, reconhecendo a assinatura P de A. Como somente A possui f_A^{-1}, isto deixa B com a certeza que somente A poderia ter enviado esta mensagem.

O criptosistema de chave pública mais famoso foi proposto por Rivest, Shamir e Adleman (RSA) em 1978. E é baseado na dificuldade de se fatorar um número natural.

Descrição do método RSA:

1. Escolha dois primos p e q grandes (com mais de 100 dígitos) e calcule $n = pq$. O número a seguir é um primo com 300 dígitos

   $p =$ 203956878356401977405765866929034577280193993314348263094772646453283062722701277632936616063144088173312372882677123879538709400158306567338328279154499698366071906766440037074217117805690872792848149112022286332144876183376326512083574821647933992961249917319836219304274280243803104015000563790123

2. Determine $\theta = (p-1)(q-1) = n + 1 - p - q$.

3. Escolha $r \in \mathbb{N}$ tal que $r \leq \theta$ e $mdc(r, \theta) = 1$.

4. Determine $w \in \mathbb{N}$ tal que $rw \equiv 1 \pmod{\theta}$

Então chave pública será o par : (n, r) e a chave secreta será o par (n, w). Agora se queremos codificar uma mensagem faremos $C = F(T) \equiv T^r \pmod{n}$ e para decodificar $T = f^{-1}(C) \equiv C^w \pmod{n}$

Exemplo 3 *Vamos tomar os primos* $p = 11$ *e* $q = 7$. *Logo* $n = pq = 77$ *e* $\theta = (p-1)(q-1) = 60$. *Como* $60 = 2^2 \times 3 \times 5$, *vamos escolher* $r = 17$, *que podemos facilmente verificar ser co-primo com* 60. *De fato, vamos explicitamente calcular o mdc(17,60), utilizando o algoritmo de divisões sucessivas:*

	3	*1*	*1*	*8*
60	*17*	*9*	*8*	*1*
9	*8*	*1*	*0*	

Reescrevendo estes cálculos teremos:

60=	*3× 17 + 9*	$\Longrightarrow$	*9=*	*60-(3× 17)* *(1)*
17=	*9+8*	$\Longrightarrow$	*8=*	*17-9* *(2)*
9=	*8+1*	$\Longrightarrow$	*1=*	*9-8* *(3)*

Substituindo (1) em (2), teremos

$$8 = 17 - (60 - (3 \times 17)) = 4 \times 17 - 60. \quad (4)$$

Substituindo agora (1) e (4) em (3), poderemos escrever

$$1 = 2 \times 60 + (-7) \times 17.$$

Portanto temos que $1 - (-7) \times 17 = 2 \times 60$, *ou seja, 60 divide* $1 - (-7) \times 17$, *logo* $17 \times (-7) \equiv 1 \pmod{60}$. *Assim determinamos que* $w = -7$ *é uma solução para*

$$17w \equiv 1 \pmod{60}.$$

Mas como o w que devemos escolher deve pertencer a $\mathbb{N}$, *somente precisamos observar que se* -7 *é solução, então* $53 = 60 - 7$ *também é solução, pois*

$$1 - (60-7) \times 17 = 1 - (-7) \times 17 - 60 \times 17 = 2 \times 60 - 17 \times 60 = (-15) \times 60.$$

Assim 60 também divide $1-(60-7)\times 17$*, ou seja, 60 divide* $1-53\times 17$*, o que nos dá*

$$17\times 53\equiv 1 \pmod{60},$$

Portanto podemos tomar $w=53$*.*

Então se desejamos codificar uma mensagem devemos utilizar a função

$$C=f(T)\equiv T^{17} \pmod{77},$$

e para decodificar essa mensagem utilizamos

$$T=f^{-1}(C)\equiv C^{53} \pmod{77}.$$

Quebra de Código

Nós utilizamos a critpografia pois queremos evitar que outros leiam nossas mensagens. Mas existem casos quando a quebra de um código pode ter um bom objetivo. Imagine que a polícia esta seguindo um grupo de sequestradores, e estes se comuniquem utilizando um sistema criptográfico, então seria do maior interesse que o serviço de inteligência da polícia conseguisse quebrar este código. Se desejamos quebrar um código precisamos ter uma idéia de qual sistema criptográfico foi utilizado e paralelamente a isto fazer uma análise de frequência das letras que ocorrem na mensagem codificada que foi interceptada. vamos supor que a mensagem apresentada no exemplo acima tenha sido interceptada, ou seja, captamos a mensagem HXDPRPDWHPDWLFD. Esta mensagem apresenta quatro ocorrências da letra D. Supondo que esta mensagem esteja em português, sabemos que as letras que mais aparecem em qualquer palavra em português são as vogais, e dentre as vogais a letra A aparece em geral com maior frequência. Assim uma boa tentativa seria imaginar que a letra D na mensagem codificada corresponderia a um A na mensagem original. Como D corresponde ao número 3 e A corresponde ao 0, nossa tentativa nos levaria a função decodificadora $T\equiv C-3 \pmod{26}$, que corresponde exatamente a função decodificadora do Criptograma de Júlio César (ver (*)). Poderíamos com um pouco mais de esforço repetir esta análise para quebrar um criptosistema do tipo de Vigenère. Mas para isto teríamos que estudar a mensagem recebida para tentar conseguir alguma indicação do comprimento da palavra chave utilizada (número de letras). Vamos supor que nosso "palpite"seja que a palavra chave tenha 5 letras. Então dividiríamos a mensagem em grupos de 5 letras e então

repetiríamos a análise de frequência em todas as primeiras letras, depois em todas as segundas letras e assim por diante.

A dificuldade em se quebrar um sistema do tipo RSA consiste na impossibilidade computacional que temos hoje de fatorar grandes números naturais. Mesmo conhecendo o número n, se este for grande o suficiente, poderia levar "anos"para os computadores atuais fatorarem n, ou seja, escrever $n = pq$. Pois precisamos determinar p e q para poder encontrar θ e só então encontrar a chave decodificadora (n, w).

A seguir apresentamos ums lista dos primeiros números primos para que os leitores possam fazer suas experiências com o método RSA. Bom divertimento!

Lista dos primeiros números primos

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	101	103	107	109	113	127	131	137
139	149	151	157	163	167	173	179	181	191	193
197	199	211	223	227	229	233	239	241	251	257
263	269	271	277	281	283	293	307	311	313	317
331	337	347	349	353	359	367	373	379	383	389
397	401	409	419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503	509	521	523
541	547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659	661
673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823
827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977
983	991	997	1009	1013	1019	1021	1031	1033	1039	1049
1051	1061	1063	1069	1087	1091	1093	1097	1103	1109	1117
1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213

ALGUMAS REFERÊNCIAS

1. Kahn, David. "The Codebreakers". The Macmillan Company. New York, 1967

2. Koblitz, N. "A Course in Number Theory and Criptography". Springer-Verlag, 1987.

3. Shokranian, S., Soares, M., Godinho, H. "Teoria dos Números". Editora UnB, (1994).

4. PET/UnB(1/98). "Corpos Finitos: Teoria e Aplicações". Trabalhos de Graduação em Matemática no.1/98.