Criptografia como Ferramenta para o Ensino de Matemática

Fábio Borges,
Laboratório Nacional de Computação Científica – LNCC
25651-075, Petrópolis, RJ
E-mail: borges@lncc.br

Resumo

Este trabalho relata a experiência que o autor obteve ministrando disciplinas de graduação na área de segurança da informação e orientando alunos de matemática.

1 Introdução

No centro dos problemas do ensino-aprendizagem em matemática reside a motivação. O aluno não tem atenção para conteúdos que necessitem de abstração ou generalização, sutilezas são totalmente desconhecidas. Por outro lado, o mesmo aluno tem muita atenção para qualquer aparato de alta tecnologia ou assuntos que instiguem seus sentidos. A maioria das aplicações que são usadas nos cursos de graduação envolve pouco sentimento. Além do mais, as aplicações mais belas requerem muito conteúdo, estão no final de uma disciplina e normalmente não são ensinadas.

Para motivar o aluno, não basta dizer que todo aparato tecnológico foi construído a partir de fundamentos matemáticos, ele não vai se motivar a estudar álgebra booleana porque é a base da computação, muito menos cálculo para saber como uma máquina calcula o seno. Ele busca algo novo e não percebe que é necessário conhecer o que existe para poder construir algo novo. Muitos alunos também se apegam a um conhecimento adquirido a partir de ações, algo que possa ser visualizado. Para eles não basta dizer que a série de Fourier é a base da transmissão de sinais [23], ou dizer que os celulares usam a série de Fourier para comunicação, eles querem ver como isto é feito. Infelizmente é inviável mostrar isto a um aluno no início de sua graduação, no entanto, veremos que isto é fácil quando a motivação surge da aplicação em criptografia.

O objetivo básico da criptografia é transmitir uma mensagem a um destinatário sem que outra pessoa possa compreender seu conteúdo. Com o intuito de atingir este objetivo, usa-se todo o conhecimento disponível.

Diferente de outras aplicações que requerem um grande conteúdo, pode-se iniciar os estudos com criptografia com conceitos elementares como a contagem. Porém o embasamento matemático não fica em conteúdos básicos, partindo desta aplicação, o professor pode atingir os maiores problemas da atualidade, que são estudados nos departamentos de matemática pura.

Foi muito surpreendente a chamada de trabalhos do VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2008):

> *é notável o interesse renovado por áreas que até há algumas décadas eram consideradas aparentemente etéreas como a Teoria dos Números, base na qual reside grande parte da criptografia moderna, ferramenta indispensável no repertório das soluções de segurança.*

Assim como foi surpreendente que um aluno de matemática tivesse o trabalho [14] de iniciação científica premiado no SBSeg 2007.

Fazendo um levantamento bibliográfico, descobri que o professor Koblitz teve uma experiência semelhante para motivar seus alunos [12]. Porém, este trabalho apresenta outras aplicações e estas estão organizadas de uma forma mais gradual que tem despertado interesse de colegas [3], onde se originou este trabalho. No decorrer do texto também vamos apresentar alguns problemas em aberto que são relacionados com a criptografia.

2 Introduzindo o conteúdo

A maioria dos alunos já ouviu falar em criptografia, normalmente através de um filme de ficção ou aventura. Os filmes relacionados à segurança da informação mais lembrados são:

- A Rede (The Net, 1995)
- Enigma (Enigma, 2001)
- Código para o inferno (Mercury Rising, 1998)
- Teoria da conspiração (Conspiracy Theory, 1997)
- Hackers (Hackers, 1995)
- Invasão de privacidade (Sliver, 1993)
- Jogos de guerra (WarGames, 1983)
- Piratas do vale do silício (Pirates of Silicon Valley, 1999)
- Uma mente brilhante (A Beautiful Mind, 2001)
- Prenda-me se for capaz (Catch Me If You Can, 2002)

Temos outros bons filmes fora desta lista, por exemplo, Quebra de Sigilo (Sneakers, 1992) trata muito bem do tema. É interessante observar que o último filme da lista é tirado de um livro que relata a história de um estelionatário, estes fatos ocorreram antes do advento da informática, mas o autor usa técnicas conhecidas hoje em dia com Engenharia Social. Mediante este repertório cinematográfico os alunos ficam estimulados e eufóricos.

Um exercício simples é a transmissão de mensagens cifradas pelo celular. Basta que o emissor da mensagem aperte uma vez a mais a tecla de cada letra e o receptor olhe no teclado qual é a tecla anterior, certamente se ambos tiverem o mesmo teclado. Tal método pode impedir que um bisbilhoteiro leigo leia a mensagem, mas na criptografia devemos ter em mente que o bisbilhoteiro é muito esperto.

A primeira coisa que deve ser definida para os alunos é um alfabeto, o conjunto de elementos usados na comunicação. A maioria da literatura usa 26 letras, algumas vezes eu prefiro inserir o espaço e usar 27 símbolos. Apesar de dizemos que o alfabeto no Brasil tem 23 letras, usamos três estrangeiras, além dos mais, em um conjunto de símbolos **a** e **á** são diferentes. Na Tabela 1 temos um conjunto ordenado de letras que formam o alfabeto resumido que pode ser usado em exemplos. Poderíamos usar qualquer outro alfabeto, na computação é comum usar a tabela ASCII.

A	$\leftrightarrow$	0	N	$\leftrightarrow$	13
B	$\leftrightarrow$	1	O	$\leftrightarrow$	14
C	$\leftrightarrow$	2	P	$\leftrightarrow$	15
D	$\leftrightarrow$	3	Q	$\leftrightarrow$	16
E	$\leftrightarrow$	4	R	$\leftrightarrow$	17
F	$\leftrightarrow$	5	S	$\leftrightarrow$	18
G	$\leftrightarrow$	6	T	$\leftrightarrow$	29
H	$\leftrightarrow$	7	U	$\leftrightarrow$	20
I	$\leftrightarrow$	8	V	$\leftrightarrow$	21
J	$\leftrightarrow$	9	W	$\leftrightarrow$	22
K	$\leftrightarrow$	10	X	$\leftrightarrow$	23
L	$\leftrightarrow$	11	Y	$\leftrightarrow$	24
M	$\leftrightarrow$	12	Z	$\leftrightarrow$	25

Tabela 1: Símbolos do Alfabeto Resumido.

Se substituirmos cada letra de uma mensagem M por outra letra, poderemos deixar o método de criptografia mais seguro que no caso do celular. Como cada letra está relacionada a um número é possível somarmos um número a cada letra para deslocarmos mais que no exemplo do celular, este número é a chave K criptográfica. Se subtrairmos o mesmo número K das letras da mensagem cifrada, obtemos a mensagem original. No entanto, temos um problema na primeira e última letra que pode ser resolvido calculando o resto da divisão por 26, isto é

$$M + K \mod 26.$$

Este é o famoso Código de César. Daqui já começa a surgir uma questão mais complicada, se tentarmos multiplicar

$$M \times K \mod 26$$

nem sempre vamos encontrar a inversa de K. Um aluno perspicaz poderia notar que K não pode ser par, nem 13; e se nosso alfabeto tivesse 27 símbolos então K não poderia ser múltiplo de 3. Neste ponto começa a surgir a teoria de grupos, o algoritmo euclidiano estendido e a função aritmética Phi de Euler.

Os alunos começam a observar que é simples descobrir uma mensagem com o Código de César, basta tentar 25 possibilidades. Mas mesmo se gerássemos uma permutação do alfabeto poderíamos descobrir a mensagem sem tentar as $26! - 1 \approx 4,03 \times 10^{26}$ possibilidades. Além de elementos de álgebra e teoria dos números, podemos inserir alguns elementos de estatística para fazermos uma análise de

freqüência das letras. A partir desta análise mostramos que todos os métodos por substituição são fáceis de serem quebrados, inclusive os códigos usados em diários de adolescentes, isto ocorre porque a entropia [20] da mensagem não se altera. A probabilidade nos fornece um resultado surpreendente, existe um tipo de método de criptografia inquebrável [21]. Por exemplo, se somarmos em cada letra um valor K_i escolhido aleatoriamente, não será possível descobrir a mensagem, nem mesmo tentando todos os valores possíveis de K_i. Isto ocorre porque todas as mensagens são equiprováveis.

3 Relacionando o conteúdo

Nesta seção, diversos conteúdos de matemática são relacionados com a segurança, iniciamos com os mais simples e vamos avançando por problemas que estão em aberto e constam entre os mais difíceis da atualidade.

3.1 Hill e Álgebra

Uma forma interessante de dificultar a análise estatística alterando a entropia é usar álgebra linear através do método de Hill [9, 10].

Seja uma matriz $K_{n\times n}$ invertível sobre um anel R, isto é,

$$\mathrm{MDC}(\det K, |R|) = 1.$$

O método consiste em agrupar a mensagem em vetores M_i de comprimento n e aplicar uma função definida como

$$\begin{aligned} f : R^n &\to R^n \\ M_i &\mapsto M_i K. \end{aligned}$$

Como este método foi desenvolvido antes da criação do primeiro computador, foi interessante facilitar as contas. Desta forma, desenvolveu-se um método para cifrar e decifrar a mensagem com a mesma matriz K, sem a necessidade de se calcular a matriz inversa. Tais matrizes ficaram conhecidas como Involutórias [15] e satisfazem a condição $K^2 = I$.

Para gerarmos uma matriz Involutória, basta escolhermos duas matizes retangulares $A_{r\times s}$ e $B_{s\times r}$ ambos sobre R e calcularmos

$$K = \begin{bmatrix} BA - I & B \\ 2A - ABA & I - AB \end{bmatrix}.$$

Observe que as matrizes Involutórias formam um grupo abeliano. Sejam K e K' Involutórias, assim

$$(KK')^2 = I = K^2 K'^2$$

Logo,

$$KK'KK' = KKK'K'.$$

Portanto,

$$K'K = KK'.$$

Apesar do método de Hill garantir uma segurança a ataques estatísticos, podemos descobrir a chave K se deduzirmos ou acertarmos o conteúdo de um dos vetores. Além disto, caso uma mensagem seja retransmitida a outro destinatário com as cifras usando matrizes Involutórias, podemos mostrar que é possível reduzir consideravelmente o espaço de busca pelas chaves usadas deixando o método inseguro.

3.2 Assimetria e Teoria dos Números

Alguns algoritmos de criptografia têm duas chaves criptográficas, uma para cifrar a mensagem e outra para decifrar, chamamos estes métodos de assimétricos, sendo que dado somente uma chave é inviável calcular a outra. Diferente dos métodos simétricos, que tem apenas uma chave, os assimétricos possibilitam estabelecer uma comunicação segura em um canal inseguro como a internet [2], ou seja, podemos estabelecer uma comunicação segura onde qualquer pessoa possa interceptar a mensagem, sem termos combinado uma chave previamente. Antes de explicar como é feito, costumo solicitar aos alunos de computação que pensem em um algoritmo que permita transmitir uma mensagem em um canal inseguro a um estranho e manter a mensagem em segredo. Pode-se ter uma visão geral destes métodos através do artigo [13].

O método de Diffie-Hellman [4] foi o precursor da criptografia assimétrica. Ele se baseia na dificuldade de se encontrar o logaritmo discreto, também conhecido como índice [22]. O Problema do Logaritmo Discreto (PLD) consiste em encontrar um inteiro K em

$$x^K \equiv y \mod z$$

onde x, y e z são inteiros conhecidos.

Para combinarmos uma chave K usando o PLD, o remetente da mensagem escolhe dois

inteiros x e z, então envia x e z para o destinatário da mensagem.

O remetente escolhe r, calcula $y_1 = x^r \mod z$ e envia o resultado, mantendo r em segredo. O destinatário escolhe s, calcula $y_2 = x^s \mod z$ e envia o resultado, mantendo s em segredo.

Tanto o remetente como o destinatário têm $K \equiv y_1^s \equiv y_2^r \equiv x^{r\,s} \mod z$. Neste caso tendo x, y_1, y_2 e z é inviável encontrar K, com aproximadamente 309 dígitos decimais, isto é, 1024 *bits*.

Outro método assimétrico amplamente usado na internet é o RSA [19], cuja segurança está baseada no problema da fatoração de inteiros, desta forma este método também trabalha com número de aproximadamente 309 dígitos decimais.

O método consiste em elevar uma mensagem M a uma potência a para criptografar, gerando uma mensagem cifrada C. Para descriptografar basta elevar C a uma potência b. Toda a engenhosidade do método consiste em encontrar expoentes a e b inversos. Para isto, escolha dois primos p e q grandes e calcule

$$\varphi = \varphi(pq) = (p-1)(q-1).$$

Escolha a inversível em φ, isto é,

$$\mathrm{MDC}(a, \varphi) = 1.$$

Com o algoritmo Euclidiano Estendido encontre b, tal que

$$ab \equiv 1 \mod \varphi$$

Finalmente, temos que

$$M^{ab} \equiv M \mod pq \quad \forall M \in \mathbb{Z}.$$

Isto significa que a e b são inversas.

Observe que conhecendo apenas uma chave e o produto dos primos, fica inviável calcular a outra chave. No entanto, se conhecermos φ ou um dos primos, fica fácil encontrar a outra chave.

A fatoração de inteiros é a base da segurança do RSA, conseqüentemente de grande parte da internet. Dado o número 15, é trivial encontrar seus fatores, em geral uma pessoa tem dificuldades de dizer os fatores de 1313, para garantir que uma máquina não vai encontrar os fatores com os algoritmos conhecidos atualmente precisamos de um número de 309 dígitos.

Podemos facilmente fazer um algoritmo que encontre $n = p \times q$, mas como encontrar os primos p e q em tempo polinomial? O produto nos números naturais é ensinado junto com o processo de alfabetização, no entanto, os alunos de graduação se espantam quando são questionados pela operação inversa, isto é, dado n encontre um fator primo.

É fácil de entender os objetivos de uma fatoração e muito difícil de encontrar um algoritmo em tempo polinomial.

3.3 Complexidade Computacional

Até 2002 não se conhecia um algoritmo determinístico que decidisse em tempo polinomial se um dado número é ou não é primo, foi quando surgiu o algoritmo AKS [1].

Atualmente, os algoritmos probabilísticos ainda são muito mais rápidos. Por exemplo, no teste de Miller existe apenas um número composto, 3215031751, menor que 2.5×10^{13}, cujos quatro primeiros primos não servem como testemunha. Além disto, o número composto n tem uma testemunha t menor que $2(\log n)^2$, caso a hipótese de Riemann seja verdadeira [16, 18]. Desta forma, o algoritmo de Miller-Rabin pode ser considerado determinístico se testarmos t para todo o intervalo $1 < t \leqslant 2(\log n)^2$.

A Hipótese de Riemann afirma que as raízes interessantes de

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

estão em $\mathcal{R}(s) = 1/2$. Esta conjectura tem forte relação com a distribuição dos números primos e conseqüentemente grande impacto nos métodos de criptografia. Atualmente existe um premio de um milhão de dólares para quem demonstrá-la, sendo um dos sete Problemas do Milênio.

A função ζ envolve conceitos muito sofisticados para quem está aprendendo variáveis complexas. Com certeza é mais fácil e atraente usar como aplicação a curva de Joukowski que descreve o perfil da asa do avião em um fluido irrotacional e incompressível. A Hipótese de Riemann é um problema que motiva aqueles que já terminaram suas disciplinas.

Outro Problema do Milênio fortemente vinculado à criptografia é uma questão de complexidade computacional, o famoso P versus NP, ou seja, determinar se todos os algoritmos não determinísticos podem ser resolvidos deterministicamente em tempo polinomial. Determinar se um grafo possui um círculo Hamiltoniano em tempo polinomial é equivalente a resolver a questão P $\times$ NP, pois é um problema NP-completo. O problema consiste em fechar um circuito passando por todos os vértices somente uma vez. Na Figura 1 vemos um grafo orientado, que obviamente não é um círculo Hamiltoniano, pois não tem como chegar ao vértice 3 e não tem como sair do 4. Por outro lado, retirando estes dois vértices temos um círculo Hamiltoniano. Fácil de entender, difícil de solucionar para qualquer quantidade de vértices.

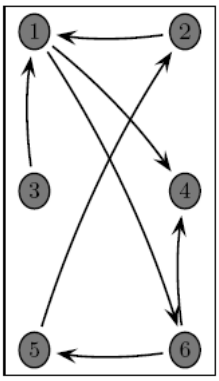

Figura 1: Grafo Orientado.

3.4 Curvas Elípticas

Curvas elípticas têm sido usadas na demonstração do Último Teorema de Fermat, na fatoração de inteiros, primalidade e em muitas outras áreas da matemática. Em criptografia, tal estudo é denominado ECC (*Elliptic Curve Cryptography*). Entre as motivações de usar um método de criptografia baseado em curvas elípticas, temos a possibilidade de reduzir o tamanho da chave criptográfica e, conseqüentemente, tornar a criptografia assimétrica viável aos dispositivos de pouco poder computacional. Veja a Tabela 2 que resume os trabalhos [7] e [6].

É interessante observar que este método foi apresentado independentemente por Miller [11] e Koblitz [17] em 1985. Uma descrição mais completa pode ser encontrada em [8] e [24].

Simétrico	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Tabela 2: Número de bits recomendado por chave.

Definimos a característica de um corpo $\mathbb{F}$, com identidade multiplicativa 1, como o menor n, tal que, $\underbrace{1+1+\cdots+1}_{n\times} = 0$ e se não existir n que satisfaça esta condição, dizemos que $\mathbb{F}$ tem característica zero.

Seja $\mathbb{F}$ um corpo de característica diferente de 2 e 3, e sejam $c, d \in \mathbb{F}$ tal que $x^3 + cx + d$ seja livre de raiz, isto é,

$$\Delta = -16(4c^3 + 27d^2) \neq 0 \qquad (1)$$

então, o conjunto dos pontos $(x, y) \in \mathbb{F} \times \mathbb{F}$ que são soluções de

$$y^2 = x^3 + cx + d$$

junto com um elemento neutro chamado ponto no infinito $\overline{O}$ é uma curva elíptica E.

Com a operação definida abaixo, $(E, +)$ forma um grupo abeliano. Definimos:

- $P + \overline{O} = P \qquad \forall P \in E$
- Se $P = (x, y)$ então definimos $-P = (x, -y)$
- Se $P, Q \in E$ e $P \neq \pm Q$ e a reta $\overline{PQ}$ não é tangente a P ou Q então a reta vai interceptar um ponto R. Definimos $P + Q = -R$
- Se $P \neq \pm Q$ e $\overline{PQ}$ é tangente a P definimos $P + Q = -P$
- Se P não é ponto de inflexão, definimos $P + P = -R$
- Se P é ponto de inflexão $P + P = -P$

Tratamos agora de definir a operação no caso de E ser discreto, na verdade em criptografia trabalhamos com corpos finitos.

Se $P = Q$ definimos:

$$x_3 = \left(\frac{3x_1^2+c}{2y_1}\right)^2 - 2x_1 \mod p$$

$$y_3 = \left(\frac{3x_1^2+c}{2y_1}\right)(x_1 - x_3) - y_1 \mod p$$

Se $P \neq \pm Q$ definimos:

$$x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 \mod p$$

$$y_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3) - y_1 \mod p$$

Como exemplo, vamos considerar uma curva elíptica em $\mathbb{Z}_{23}$. Se $c = 1$ e $d = 0$, temos $y^2 = x^3 + x$. Primeiramente, verificamos se a expressão (1) é satisfeita,

$$\Delta = -16(4) \mod 23 \equiv 18 \neq 0,$$

depois escolhemos um ponto, por exemplo (9,5), que satisfaz a equação: Existem 23 pontos que satisfazem esta equação, veja Figura 2.

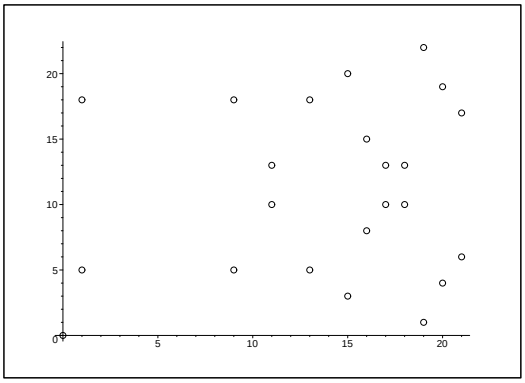

Figura 2: Gráfico $y^2 = x^3 + x$.

Poderíamos pensar que $|E| = |\mathbb{F}|+1$, mas isto raramente acontece, estas curvas são chamadas de supersingular. Logo uma preocupação importante é garantir que o grupo cresça na ordem do corpo. Isto é garantido pelo teorema de Hasse cuja demonstração pode ser encontrada em [24].

Com o teorema de Hasse sabemos que a ordem do grupo formado por uma curva elíptica E sobre $\mathbb{Z}_p$ está no intervalo

$$p + 1 - 2\sqrt{p} \leqslant |E| \leqslant p + 1 + 2\sqrt{p}.$$

De posse destas informações, já podemos apresentar o algoritmo de ElGamal [5] que serve para qualquer grupo G.

O destinatário da mensagem escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$, então calcula $b = a^n$ e envia a, b e G, escondendo n. O remetente escolhe $M \in G$ e $k \in \mathbb{N}^*$, calcula $y = a^k$ e $z = Mb^k \in G$, depois envia y e z. Somente o destinatário pode calcular $zy^{-n} = Mb^k(a^k)^{-n} = M(ba^{-n})^k = M(1)^k = M$.

Observe que este algoritmo combina uma chave criptográfica e envia a mensagem cifrada.

4 Conclusão

Além de ter amplo potencial para enriquecer o ensino de matemática, a criptografia desperta grande interesse por estar lindando com segurança, seja de um e-mail pessoal ou das transações financeiras de uma grande instituição. Isto desperta a curiosidade e aguça a imaginação dos estudantes.

A experiência com alunos, do curso de graduação em computação e em matemática, tem sido muito satisfatória, tendo-se conseguido inserir até noções de álgebra abstrata, para respondermos as questões dos alunos. Além da criptografia ser uma ótima ferramenta para o ensino-aprendizagem de matemática, observa-se que ela prove uma ótima fonte para pesquisa em matemática.

O ensino da criptografia tem demonstrado ser um facilitador da compreensão da matemática em virtude das aplicações em segurança da informação.

Referências

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):781–793, 2004.

[2] F. Borges. Falando um segredo em público a um estranho e mantendo o segredo. In *XXIII Semana da Matemática*, pages 1–7, Londrina - PR, 2007.

[3] F. Borges. Motivando o estudo da matemática através da criptografia. In *Resumos do I Encontro Acadêmico de Modelagem Computacional do Laboratório Nacional de Computação Científica*, page 8, Petrópolis - RJ, 2008.

[4] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31(4):469–472, 1985.

[6] V. Gupta, S. Gupta, S. Chang, and D. Stebila. Performance analysis of elliptic curve cryptography for ssl. In *WiSE '02: Proceedings of the 3rd ACM workshop on Wireless security*, pages 87–94, New York, NY, USA, 2002. ACM Press.

[7] V. Gupta, D. Stebila, S. Fung, S. Chang, N. Gura, and H. Eberle. Speeding up secure web transactions using elliptic curve cryptography. In *11th Ann. Symp. on Network and Distributed System Security – NDSS 2004*. Internet Society, February 2004.

[8] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer Professional Computing. Springer-Verlag, New York, 2004.

[9] L. S. Hill. Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6):306–312, jun 1929.

[10] L. S. Hill. Concerning certain linear transformation apparatus of cryptography. *The American Mathematical Monthly*, 38(3):135–154, mar 1931.

[11] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, jan 1987.

[12] N. Koblitz. Cryptography as a teaching tool. *Cryptologia*, XXI(4):317–326, 1997.

[13] N. Koblitz and A. J. Menezes. A survey of public-key cryptosystems. *SIAM Rev.*, 46(4):599–634 (electronic), 2004.

[14] P. C. S. Lara and F. Borges. Curvas elípticas: Aplicação em criptografia assimétrica. In *Workshop de Trabalhos de Iniciação Científica e de Graduação do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 1–10, Rio de Janeiro, 2007.

[15] Levine, Jack and Nahikian, H. M. On the construction of involutory matrices. *The American Mathematical Monthly*, 69(4):267–272, apr 1962.

[16] G. L. Miller. Riemann's hypothesis and tests for primality. In *Seventh Annual ACM Symposium on Theory of Computing (Albuquerque, N.M., 1975)*, pages 234–239. Assoc. Comput. Mach., New York, 1975.

[17] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer, Berlin, 1986.

[18] C. Pomerance. Review: [untitled]. *Mathematics of Computation*, 48(177):441–443, 1987.

[19] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[20] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[21] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[22] S. Shokranian, M. Soares, and H. Godinho. *Teoria dos números*. Editora Universidade de Brasilia, 1999.

[23] W. Stallings. *Business Data Communications (5th Edition)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2004.

[24] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 2003.