Trabalho apresentado no ERMAC, Volta Redonda – RJ, 2023.

SHAMIR SECRET SHARING COMO ELEMENTO MOTIVADOR NO ENSINO DA MATEMÁTICA

Thays Rocha
Laboratório Nacional de Computação Científica (LNCC-MCTI)
tferreira@posgrad.lncc.br

Renato Borseti
Laboratório Nacional de Computação Científica (LNCC-MCTI)
renatojp@posgrad.lncc.br

Fábio Borges
Laboratório Nacional de Computação Científica (LNCC-MCTI)
borges@lncc.br

Resumo: O objetivo deste estudo é empregar a criptografia, mais especificamente o método de *Shamir Secret Sharing*, como uma ferramenta educacional para enriquecer o engajamento nas aulas de matemática. A intenção é utilizar essa abordagem para introduzir, revisitar, consolidar e aprofundar conceitos matemáticos, concentrando-se especialmente no ensino do polinômio interpolador de Lagrange e Corpo Finito, base do método criptográfico em questão. Isso proporcionará uma compreensão mais profunda e significativa destes tópicos, ao mesmo tempo em que demonstra uma aplicação prática no cotidiano dos alunos. Além disso, essa abordagem estimula o desenvolvimento do raciocínio lógico, a resolução de problemas e a colaboração em trabalho em equipe.

Palavras-chave: Educação Matemática. Shamir Secret Sharing. Criptografia. Polinômio Interpolador de Lagrange. Corpo Finito.

Introdução

Um dos grandes desafios do ensino da matemática é a motivação dos alunos, principalmente quando se é utilizado as abordagens tradicionais de ensino, como defende D'ambrosio (2007). E como algumas temáticas dentro da matemática são, por si só, abstratas, tal dificuldade fica mais evidente. Pouco se é mostrado da aplicação do que é estudado em aula. E quando isso ocorre, é de maneira superficial.

Conforme a perspectiva de Borges (2008), o educando não irá aprender álgebra booleana ou cálculo, por exemplo, apenas com a justificativa que é a base da computação e a base de uma máquina que calcula seno, respectivamente. Ele precisa ver acontecer, ver uma aplicação daquilo que estuda em sala de aula.

Com isso, muito é debatido acerca do tratamento de temáticas transversais de forma integradora ao currículo, que contribuem para plena formação do educando, explorando a conexão entre os conceitos discutidos em sala de aula e como eles se aplicam na sociedade. Isso ocorre porque esses componentes já estão integrados em vários documentos curriculares da educação básica no Brasil, onde podemos citar a Base Nacional Comum Curricular (BNCC), os Parâmetros Curriculares Nacionais (PCN) e a Lei de Diretrizes e Bases da Educação (LDB), conforme Brasil (2018); Brasil (2008) e Brasil (1996), respectivamente.

Neste cenário, a criptografia entra como uma ferramenta para auxiliar a motivar os alunos no estudo da matemática. Com ela conseguimos abordar temáticas importantes de álgebra, teoria dos números e matemática discreta. Além de contribuir para o aprimoramento de competências essenciais, como raciocínio lógico, resolução de problemas e colaboração no trabalho em equipe.

Portanto, o propósito deste estudo é empregar a criptografia como meio para introduzir, rever, consolidar e até mesmo aprofundar tópicos matemáticos, com foco particular no ensino do polinômio interpolador de Lagrange e Corpo Finito, conferindo-lhe maior relevância e significado.

Sendo assim, as seções subsequentes estão organizadas da seguinte forma: Primeiramente é apresentado um resumo da criptografia e como ela pode ser utilizada como elemento motivador para o ensino. A

Seção seguinte apresenta a relação dos conteúdos matemáticos que se baseia o método criptográfico utilizado, a saber, o polinômio interpolador de Lagrange e Corpo Finito. Para na seção posterior apresentar o método criptográfico de Múltiplas Partes *Shamir Secret Sharing*. E por fim, apresentar as considerações finais e as perspectivas para possíveis trabalhos futuros.

Criptografia

A origem do termo "Criptografia" vem das palavras gregas "kryptós", que significa "escondido", e "gráphein", que significa "escrita", como visto em Yan (2013). Consiste na habilidade de reescrever mensagens, números e até mesmo efetuar operações matemáticas de maneira incompreensível, tornando-as legíveis somente para o destinatário autorizado a decifrá-las e compreendê-las. E segundo Singh (2014), diferente da esteganografia que tem objetivo de esconder uma informação, a criptografia tem como objetivo ocultar seu significado, ou seja, a mensagem que for transmitida estará toda misturada e sem sentido para quem não conhece o protocolo de decriptação.

A criptografia foi primordialmente empregada para fins militares, sendo um exemplo o uso da Máquina Enigma durante o contexto da Segunda Guerra Mundial para a comunicação das forças alemãs, conforme afirma Tavares (2017). Entretanto, atualmente, está presente nas mais diversas atividades do cotidiano, como por exemplo transações bancárias, votações, comunicação, assinatura digital, entre outros.

A criptografia se torna um excelente elemento motivador para o ensino de matemática, porque, conforme afirma Borges (2008), ela consegue abordar desde temáticas mais simples, como o conceito elementar da contagem, como temáticas bem mais complexas, como curvas elípticas e computação quântica, tudo dependendo do método criptográfico utilizado.

Em Tavares (2017) e Olgin e Groenwald (2011), temos a utilização da criptografia direcionado a matemática abordada na educação básica, mais especificamente as temáticas operações matriciais e funções, respectivamente. Assim como em Carvalho (2020), com ênfase em cursos técnicos, temos a utilização da criptografia direcionado a análise combinatória, porcentagem e números binários. Já em Lunkes (2022) e Fusco (2005), os autores abordam a criptografia como motivador no estudo do homomorfismo e das estruturas algébricas, respectivamente, no contexto do ensino superior.

Assim, destacamos a atualidade e a relevância desta temática no dia a dia dos estudantes, abrindo caminho para atividades pedagógicas em matemática que abordem a codificação e decodificação de mensagens. Isso capacita os alunos a desenvolverem tanto a independência para comunicar de maneira cifrada, quanto a habilidade de criar estratégias para resolver desafios.

Relacionando o Conteúdo

Dentre as várias temáticas da matemática em que a criptografia se fundamenta, concentraremos nossa discussão naquela que serve de base para o método criptográfico empregado neste trabalho, a interpolação de Lagrange e Corpo Finito.

A interpolação é um método muito utilizado na matemática para se encontrar uma função $g(x)$ que se aproxima da função $f(x)$, quando a função $f(x)$ possui operações de integração ou diferenciação extremamente difícil, ou até mesmo impossível, ou quando são conhecidos apenas um conjunto de valores numéricos da função dada um conjunto de pontos específicos, como explica Ruggiero e Lopes (1997). Dentre tantos métodos de interpolações disponíveis na literatura, podemos citar o Polinômio Interpolador de Lagrange.

Conforme apresentado em Burden (2016), temos o seguinte teorema para tal método:

Teorema 1: Se $x_0, x_1, \ldots, x_n$, são $n+1$ pontos distintos, e f uma função cujo valores são dados para esses números, então existe um único polinômio $P(x)$ de grau n máximo com

$$f(x_k) = P(x_k) \qquad \text{para } k = 0, 1, \ldots, n.$$

Este polinômio é dado por

$$P_n(x) = f(x_0)L_{n,0}(x) + \cdots + f(x_n)L_{n,n}(x) = \sum_{k=0}^{n} f(x_k)L_{n,k}(x), \tag{1}$$

e $L_{n,k}(x)$ é definido por

$$L_{n,k}(x) = \frac{(x-x_0)(x-x_1)\ldots(x-x_{k-1})(x-x_{k+1})\ldots(x-x_n)}{(x_k-x_0)(x_k-x_1)\ldots(x_k-x_{k-1})(x_k-x_{k+1})\ldots(x_k-x_n)} \tag{2}$$

$$L_{n,k}(x) = \prod_{i=0, j\neq i}^{n} \frac{(x-x_i)}{(x_j-x_i)}. \tag{3}$$

Entretanto, assim como aplicado por Burden (2016), iremos utilizar daqui por diante $L_{n,k}(x)$ como $L_k(x)$ com o objetivo de evitar possíveis confusões quanto ao seu grau. Bem como, ao longo deste texto, não faremos distinção entre polinômios e funções polinomiais.

Utilizando o conjunto de pontos $(1,2)$, $(3,4)$, $(5,1)$, $(7,3)$ e $(8,9)$, é possível realizar uma representação geométrica do método em questão, por meio da Figura 1 com base na Equação 1. Em outras palavras, ao calcular cada valor de n, obteremos um correspondente $P_n(x_n)$ e, posteriormente, o valor de $P(x) = \frac{5x^3}{24} - \frac{5x^2}{2} + \frac{199x}{24} - 4$, indicado no gráfico pela cor preta.

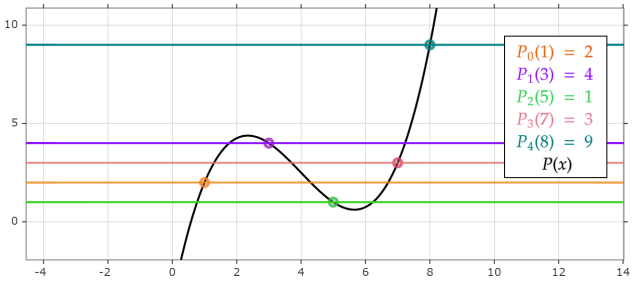

Figura 1: Representação Geométrica do Exemplo do Polinômio Interpolador de Lagrange.
Fonte: autores.

Dizemos que um determinado conjunto não-vazio é um corpo quando se verifica a satisfação das propriedades algébricas das operações de adição e multiplicação, as quais consistem na associatividade, comutatividade, existência de elemento neutro e inversos aditivos para a adição, bem como a associatividade, comutatividade, existência de elemento neutro e inversos multiplicativos, juntamente com a propriedade distributiva em relação à operação de adição, de acordo com Garcia e Lequain (2006). Sendo assim, Corpo Finito consiste em um corpo que possui um conjunto finito de elementos, diferente do conjunto dos números reais $\mathbb{R}$, por exemplo, que possui um número infinito de elementos. Dentre as definições e teoremas referentes a temática, baseada em Howie (2005), podemos destacar:

Teorema 2.1: Seja K um corpo finito, se $|K| = p^m$ para algum primo p e inteiro $m \geq 1$, então todo elemento de K é raiz do polinômio $X^{p^m} - X$ sobre subcorpo primo $\mathbb{Z}_p$.

Teorema 2.2: Seja p um primo e $m \geq 1$ um inteiro, então existe, a menos de isomorfismos, exatamente um corpo de ordem p^m.

Definição 1: Dado p primo e um inteiro $m \geq 1$, o corpo de ordem p^m é chamado de **Corpo de Galois** de ordem p^m, e é denotado por $GF(p^m)$.

Definição 2: Seja $\alpha \in K^*$, onde $K^* = K - \{0\}$ é um corpo finito, define-se a ordem do elemento α como sendo o menor inteiro m tal que $\alpha^m = 1$.

Teorema 3: Seja α um elemento não-nulo do corpo finito $GF(q)$, então $\alpha^{q-1} = 1$.

Com o objetivo de ilustrar as operações de adição e multiplicação definias, bem como a ordem e elemento primitivo do corpo finito, consideraremos o $GF(5)$ com as operações definidas na Tabela 1 abaixo.

Tabela 1: Operações mod 5

(a) Adição mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(b) Multiplicação mod 5

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tomando o elemento 3, utilizando a Tabela 1b, temos as Equações (4) a (9), nos oferece a informação de que 4 é a ordem do elemento 3, como afirmam os teoremas e definições citadas anteriormente.

$$3^1 = 3 \tag{4}$$
$$3^2 = 3 \cdot 3 = 4 \mod 5 \tag{5}$$
$$3^3 = 3 \cdot 3^2 = 2 \mod 5 \tag{6}$$
$$3^4 = 3 \cdot 3^3 = 1 \mod 5 \tag{7}$$
$$3^5 = 3 \cdot 3^4 = 3 \mod 5 \tag{8}$$
$$3^6 = 3 \cdot 3^5 = 4 \mod 5 \tag{9}$$

Shamir Secret Sharing

Na criptografia, temos a área de Computação Segura de Múltiplas Partes, que permite que várias partes colaborem na computação sem revelar suas entradas individuais, mantendo a privacidade das informações enquanto obtêm resultados precisos. Um ótimo exemplo são os métodos de *Secret Sharing*, que particionam um dado sigiloso em partes e distribuem para diferentes entidades. Só é possível reconstruir o dado sigiloso combinando um número suficiente destas partes.

Na Figura 2 temos uma ilustração de um esquema de *Secret Sharing* baseado em um limiar, onde podemos notar que o segredo é particionado em quatro chaves, um para cada participante, onde para recuperação do segredo é necessário a união de pelo menos dois destes. É válido reforçar que, por ser baseado em um limiar, qualquer subconjunto de dois participantes, ou mais, é suficiente para recuperar o segredo.

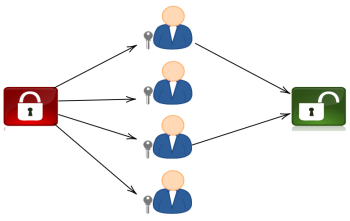

Figura 2: Exemplo de *Secret Sharing*, baseado em um limiar.
Fonte: autores.

Dentre os métodos de *Secret Sharing*, podemos citar o *Shamir Secret Sharing*, formulado por Shamir (1979). Nele, a informação privada é chamada de segredo, e ao ser cifrado ele é reescrito em forma de polinômio, com a parte constante sendo o segredo. Ele é definido como (k,n) *Shamir Secret Sharing*, onde k é o quórum, valor mínimo de participantes necessários para recuperar o segredo; e n é o número de

participantes do grupo. Cada participante irá receberá suas respectivas chaves, $Sk_i = (x_i, f(x_i) \mod p)$ para todo $i \in [1,n]$, ou seja, o valor do seu ponto, necessariamente diferente de zero, e o valor da função no ponto em questão, onde p é primo. Desta forma, asseguramos que qualquer união de $k-1$, ou menos, não consegue obter qualquer informação referente ao segredo.

A reconstrução do segredo é baseada na interpolação de *Lagrange* sobre o Corpo Finito GF_p, que utilizando, pelo menos, k chaves recupera o polinômio de grau $k-1$, e ao analisar o polinômio no ponto $x = 0$ iremos recuperar o segredo desejado.

Logo, seja n o número máximo de participantes e GF um corpo finito que contém o domínio dos possíveis segredos, onde a cardinalidade de GF é maior do que n. Sejam $x_1, x_2, \ldots, x_n \in GF$ elementos não-nulos, distintos entre si e fixos. Temos:

Compartilhamentos: Dado um segredo $s \in GF$, quem inicia o esquema escolhe os coeficientes $a_1, a_2, \ldots, a_{k-1} \in GF$ e define o polinômio $\mathcal{P}(X) = s + \sum_{i=1}^{k-1} a_i X^i$. O compartilhamento, ou *share*, do usuário P_i é $s_i := \mathcal{P}(x_i) \in GF$.

Reconstrução: Quando k usuários reúnem seus segredos $s_{i_1}, s_{i_2}, \ldots, s_{i_k}$ eles reconstroem o segredo usando a interpolação polinomial calculando um polinômio único de grau $(k-1)$ definido por $\mathcal{P}'$ onde o segredo é $\mathcal{P}'(0)$. A reconstrução funciona a partir do momento que $\mathcal{P}' = \mathcal{P}$ e $\mathcal{P}(0) = s$. Nenhum usuário consegue inferir nenhuma informação sobre o segredo a partir de sua *share*.

Exemplo Contextualizado e Proposta de Atividade

A seguir, apresentaremos uma situação hipotética que servirá como ponto de partida para introduzir a atividade proposta à turma, com o objetivo de explorar as temáticas mencionadas anteriormente de forma contextualizada. Além disso, com a atividade proposta, estimular o desenvolvimento do raciocínio lógico e promover o trabalho em equipe como parte fundamental para a resolução do desafio proposto.

Há uma empresa composta por cinco sócios formadores que, em comum acordo, decidiram que para assinar digitalmente qualquer documento referente à empresa seria necessário a aprovação de pelo menos três dos cinco sócios. A senha da empresa para sua assinatura digital é 1947. Aplicando o *Shamir Secret Sharing*, utilizando o primo $p = 20231$, cada sócio receberá uma das seguintes chaves:

$$Sk_1 = (20, 2767) \quad Sk_2 = (51, 7200) \quad Sk_3 = (83, 15808) \quad Sk_4 = (73, 12678) \quad Sk_5 = (31, 3900)$$

Escolhendo de forma aleatória, por exemplo, as chaves Sk_2, Sk_3 e Sk_5 e aplicando no polinômio interpolador de Lagrange, calcularemos:

$$L_{Sk_2} = \frac{(x-x_3)\cdot(x-x_5)}{(x_2-x_3)\cdot(x_2-x_5)} = \frac{(x-83)\cdot(x-31)}{(51-83)\cdot(51-31)} = \frac{-x^2+114x-2573}{640} \tag{10}$$

onde, L_{Sk_3} e L_{Sk_5} são calculadas de forma análoga. Aplicando na Equação (1), teremos então:

$$\begin{aligned} P(x_i) &= 7200 \cdot \left(\frac{-x^2+114x-2573}{640}\right) + 15808 \cdot \left(\frac{x^2-82x+1581}{1664}\right) \\ &\quad + 3900 \cdot \left(\frac{x^2-134x+4233}{1040}\right) \qquad (11) \\ P(x) &= 2x^2 + x + 1947 \qquad (12) \end{aligned}$$

Ao analisarmos o polinômio resultante no ponto $x = 0$, iremos obter o valor 1947, senha desejada. De forma análoga, se utilizássemos quatro ou cinco chaves, o procedimento seria o mesmo e chegaríamos no mesmo resultado. Entretanto, se utilizássemos apenas duas chaves, realizando o mesmo procedimento, o resultado que iriamos obter ser o polinômio $143x - 93$ e ao analisarmos no ponto $x = 0$, iremos obter o valor $(-93) \mod 20231 = 20138$. Valor distinto da senha desejada. Vale ressaltar que cada sócio receberá somente seu conjunto de dados da chave, sem ter acesso às chaves dos outros sócios. Além

disso, mesmo que dois dos cinco sócios se unam para assinar em nome da empresa, a assinatura não será bem-sucedida, pois o método foi configurado para requerer a participação de pelo menos três deles.

Baseado no que foi exposto, e com o objetivo de abordar temáticas de forma colaborativa entre os alunos, podemos sugerir a atividade denominada "Cofre da Turma". Nesse contexto, o conteúdo armazenado dentro do cofre somente pode ser compartilhado com aqueles que obtiverem acesso ao mesmo. Nesse cenário, o papel do professor assemelha-se ao de um "computador central" encarregado de receber as senhas necessárias para a abertura do cofre. Ele será responsável para analisar as estratégias e os cálculos feitos pelos alunos, que poderão ser auxiliados por softwares, dependendo da turma a ser aplicada. Também ficará a critério do professor, o nível de dificuldade da atividade, sendo um exemplo a não informação do quórum necessário para maior dificuldade na resolução. A turma é dividida em cinco grupos distintos, sendo que cada grupo recebe seu próprio conjunto Sk_i de chaves. A tarefa desses grupos consiste em colaborar entre si, a fim de encontrar a melhor estratégia para combinar suas chaves de modo a abrir o cofre com sucesso.

Os participantes têm a liberdade de explorar diferentes abordagens, incluindo a tentativa de inserção de senhas incorretas, bem como a possibilidade de tentar subjugar um membro de outro grupo, entre outras estratégias, sempre visando identificar a abordagem mais vantajosa. Cada uma dessas situações deve ser analisada a posterior, uma vez que elas podem gerar discussões significativas em sala de aula. O uso de senhas incorretas, mesmo que o número mínimo necessário de k chaves seja atingido, não revela informação sobre a senha correta, por exemplo. Assim como a vulnerabilidade a diversos tipos de ataques, inclusive de suborno, que ficamos quando confiamos nossas senhas a terceiros. Com isso, pode-se pensar em atividades em que grupos distintos tentam desvendar a senha de outro grupo, por exemplo.

Considerações Finais

O objetivo central deste estudo é complementar a prática pedagógica de ensino da Matemática no processo de ensino-aprendizagem, buscando na interdisciplinaridade uma abordagem que enriqueça a compreensão dos conceitos matemáticos e promova uma aprendizagem mais significativa. Além disso, busca trazer ao debate a importância de trabalhar a matemática de forma mais articulada com a realidade. Desse modo, há a possibilidade de motivar o aluno à aprendizagem, mostrando a importância de aprender matemática. Isso resulta em um enriquecimento da educação matemática, promovendo uma abordagem mais abrangente e relevante para o desenvolvimento dos estudantes.

A criptografia entra como um recurso didático para, além de aguçar a curiosidade, aproximar o educando com problemáticas reais que lhe cercam, como defende Olgin (2011). Então, com métodos criptográficos podemos introduzir, revisar, reforçar e aprofundar alguns conteúdos matemáticos presente em sala de aula, seja na educação básica, técnica ou na educação superior.

O presente trabalho é uma proposta para professores de cursos de graduação que envolvam matemática e computação, tendo em vista que consegue atender muito bem ambos os cursos. A criptografia em si, tem demonstrado seu papel de facilitador na compreensão de temáticas, até então abstratas, em virtude de sua aplicação no cotidiano. No caso do Shamir Secret Sharing, apresentado no presente trabalho, abordamos temáticas da interpolação de Lagrange, bem como o conceito de Corpo Finito com a aritmética modular.

Para trabalhos futuros, temos outros métodos de *Secret Sharing* para aprofundar e utilizar como motivador em sala de aula, tanto para ensino básico como ensino superior. O *Blakley's Scheme*, por exemplo, proposto por Blakley (1979), pode ser utilizado como motivador para o ensino de matrizes para o ensino básico e de para o ensino de hiperplanos e resolução de sistemas lineares para o ensino superior.

Agradecimentos

A CAPES pelo apoio para o desenvolvimento do presente trabalho.

Referências

BLAKLEY, G. R. Safeguarding cryptographic keys. In: IEEE. 1979 **International Workshop on Managing Requirements Knowledge** (MARK). [S.l.], 1979. p. 313–318.

BRASIL. **Lei de Diretrizes e Bases da Educação Nacional.** Lei número 9394, 20 de dezembro de 1996

BRASIL. MINISTÉRIO DA EDUCAÇÃO. SECRETARIA DA EDUCAÇÃO BÁSICA. **Orientações curriculares para o Ensino Médio: Ciências da Natureza.** Ministério da Educação, vol. 2, 2008.

BRASIL. MINISTÉRIO DA EDUCAÇÃO. **Base Nacional Comum Curricular.** Brasília, 2018.

BORGES, F. **Criptografia como Ferramenta para o Ensino de Matemática.** Anais da SBMAC. p. 822, 2008.

BURDEN, R. L. et al. **Análise numérica.** Cengage Learning, 2016.

CARVALHO, J. Z. D. S. **A aplicabilidade da criptografia no ensino de matemática no contexto da educação profissional**. 2020. 108 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) – Universidade Federal de Rondônia, Porto Velho, 2020.

D'AMBROSIO, U. **Educação Matemática: da teoria à prática**. Papirus Editora, 2007.

FUSCO, C. A. S. **Educação superior: estratégia de aula aliando pesquisa e recursos multimídias.** Associação Nacional de Pós-Graduação e Pesquisa em Educação, v. 28, 2005.

GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra.** Instituto de Matemática Pura e Aplicada, 2006.

HOWIE, M. J., **Fields and Galois Theory**, *Springer Undergraduate Mathematics Series*, 2005.

LUNKES, A. L. Z.; BORGES, F. Sobre a aplicação de homomorfismo na criptografia. **Proceeding Series of the Brazilian Society of Computational and Applied Mathematics**, v. 9, n. 1, 2022.

OLGIN, C. A., GROENWALD, C. L. O. Criptografia e conteúdos de Matemática do Ensino Médio. *In: IICNEM-Congresso Nacional de Educação Matemática*, 2011

OLGIN, C. A. **Currículo no Ensino Médio: uma experiência com o tema criptografia.** 2011. 136f. Tese (Doutorado em Ensino de Ciências e Matemática). Universidade Luterana do Brasil, Canoas-RS. 2011.

RUGGIERO, M. A. G.; LOPES, V. L. D. R. **Cálculo numérico: aspectos teóricos e computacionais**. *Makron Books do Brasil*, 1997.

TAVARES, N. P. et al. Criptografia: Uma ferramenta de ensino das operações matriciais. *In: IV CONEDU*, 2017, Joao Pessoa. Anais. Campina Grande: CONEDU, 2017.

SHAMIR, A. How to share a secret. **Communications of the ACM**, v. 22, n. 11, p. 612-613, 1979.

SINGH, S., **O livro dos Códigos: A ciência do sigilo - do antigo Egito à Criptografia Quântica**, Record, 10a Edição, 2014.

YAN, S. Y. **Computational number theory and modern cryptography.** John Wiley & Sons, 2013.