# CONHECENDO E PRATICANDO: A CRIPTOGRAFIA DENTRO DA SALA DE AULA

*Arlete de Jesus Brito*
*Universidade Estadual Paulista*
*arlete@rc.unesp.br*

*Beatriz Fernanda Litoldo*
*Universidade Estadual Paulista*
*Beatrizfernanda_rc@hotmail.com*

**Resumo:** Sendo possível relacionar o tema Criptografia com alguns conceitos matemáticos, o presente minicurso objetiva proporcionar aos participantes uma experiência de investigação na resolução das atividades propostas. Sendo convidados a tomarem posturas de cifradores e decifradores, será solicitado que os participantes trabalhem com atividades envolvendo problemas criptográficos com o proposito de explorar as ideias associadas à função afim. Em um ambiente investigativo, espera-se promover um momento de debate e reflexão sobre as atividades propostas e instigar outras possibilidades de conceitos matemáticos para atividades desse caráter, além de discussões sobre esse tema como agente motivador em sala de aula e de possíveis alternativas de apresentação desse assunto na formação inicial e continuada dos professores.

**Palavras-chave:** Educação Matemática, Ensino Médio; Cifras; Função Afim; Resolução de Problemas.

## 1. Introdução

O objetivo do minicurso é propor problemas para a sala de aula que envolva o tema Criptografia e o conceito de função afim. Essa tarefa pretende oportunizar os participantes de vivenciarem uma atividade envolvendo mensagens cifradas com o intuito de explorar as ideias associadas à função afim. Também é almejado desenvolver debates sobre de que maneiras a Criptografia pode se compor como um tema motivador para promover o ensino e a aprendizagem dos conteúdos do Ensino Médio por meio da resolução de problemas e quais outros conceitos poderiam ser abordados no sentido de suas explorações e investigações.

Considerada tão antiga quando a própria escrita, a arte ou ciência de se esconder ou ocultar uma mensagem é chamada de Criptografia (TAMAROZZI, 2001). Originada das palavras gregas *kriptós* e *gráphein* a Criptografia consiste em cobrir uma mensagem de modo que apenas a pessoa autorizada consiga descobrir seu conteúdo. Sabendo que as cifras são os métodos utilizados para ocultar uma mensagem e a cifração é o método de aplicação dessa

cifra,

podemos pensar em situações nas quais, as mesmas, sejam constituídas por meio de transformações matemáticas. É exatamente nesse ponto que os conteúdos do Ensino Médio podem se atrelar a esse tema e constituir atividades interessantes e desafiadoras.

Embora as pessoas possam não entender muito bem sobre a Criptografia e de como ela faz parte da sociedade, ele está presente em muitas ações do nosso cotidiano. Nessa mesma direção Groenwald e Olgin (2011) argumentam sobre a importância desse tema nos dias de hoje. De acordo com essas autoras a Criptografia é aplicada nos

> Recursos humanos (auditoria eletrônica e lacre de arquivos de pessoal e pagamentos), em compras e vendas (autenticação de ordens eletrônicas de pagamentos), nos processos jurídicos (transmissão digital e custodias de contratos), na automação de escritórios (autenticação e privacidade de informações), nos navegadores de Internet, entre outras situações da vida moderna (GROENWALD; OLGIN, 2011, p. 70).

Em relação à apresentação desse tema em sala de aula Litoldo e Lazari (2014) encontraram, em alguns livros didáticos aprovados pelo PNLD 2012, algumas propostas de atividades baseadas no ato de cifrar e decifrar mensagens. Ao analisa-los acerca da aparição desse tema em seus conteúdos esses autores apontam que "embora o tema Criptografia esteja presente nos sistemas eletrônicos digitais da vida moderna e que a segurança destes depende exclusivamente da capacidade de proteção da cifra usada para se Criptografar, este assunto encontra-se pouco presente nos Livros Didáticos" (LITOLDO; LAZARI, 2014, p. 151), no entanto, segundo eles, como esse tema tem cada vez mais estado presente nas notícias da atualidade, proporcionando uma maior aproximação dos alunos, e da população em geral a respeito desse tema, é possível que ele se dissemine entre os autores de livros didáticos e estes se sintam estimulados a utilizar a Criptografia em suas coleções realizando conexões desse tema com alguns conceitos matemáticos (LITOLDO; LAZARI, 2014).

Atentando-se para o leque de possibilidades da Criptografia dentro do nosso cotidiano e levando em consideração a importância de divulgar esse assunto para as pessoas é que se criou atividades que entrelaçasse esse tema a um conceito matemático, a saber, função afim. O intuito é utilizar as ideias de cifração e decifração em sala de aula a fim de explorar as ideias associadas e esse conceito e debater sobre as possibilidades de outros conceitos matemáticos a serem explorados.


ISSN 2178-034X

Mediado

pela metodologia de resolução de problemas, a qual permite que os alunos investiguem as situações problemáticas e explorem hipóteses de resolução para tal, é que as atividades propostas nesse minicurso foram aperfeiçoadas. Como destacado por Groenwald e Olgin (2011) a "metodologia resolução de problemas é indicada para o desenvolvimento de atividade didáticas com o tema Criptografia", já que problemas criptografados não apresentam em seus enunciados algoritmos para a sua resolução.

## 2. Público alvo

Professores do Ensino Fundamental, Ensino Médio, Ensino Superior e Alunos do curso de Licenciatura em Matemática.

## 3. Criptografia: da *Cifra de César* a *Criptografia RSA*

Considerado como o primeiro documento a registrar o uso da Criptografia, em *Guerras da Gália*, Júlio César descreve com detalhes com foi o processo de envio de mensagens cifradas. O imperador romano utilizava muito um tipo de cifra chamada de substituição. Essa Criptografia tinha como característica o deslocamento do alfabeto três casas à frente, como mostra a Figura 1. De tanto utilizar esse método para cifrar suas mensagens, ela ficou sendo conhecida como sendo a *Cifra de César*.

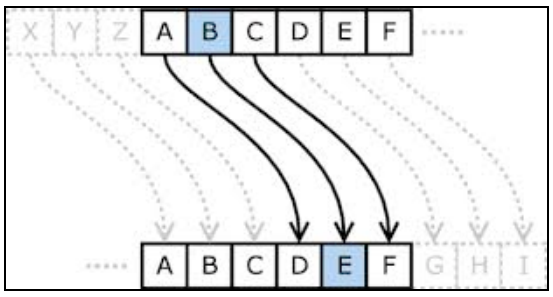


**Figura 1** - Exemplo do deslocamento da Cifra de César.
Fonte: Google imagens (2015) [1].

Pelo fato da *Cifra de César* possuir apenas um alfabeto em sua cifração ela é caracterizada como sendo um cifra monoalfabética, no entanto, em 1440, Leon Alberti sugeriu o uso de dois ou mais alfabetos cifrados para a cifração de uma mensagem. Essa ideia foi desenvolvida em sua forma final por Vigenère, em 1562, e ficou conhecida como sendo a *Cifra de Vigenère*. Sendo esta uma cifra polialfabética por ser composta por 26 alfabetos

[1] Disponível em: <http://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar>. Acessado em: 11/06/2015.

cifrados

distintamente (Figura 2) ela era utilizada na cifração de mensagens e por muito tempo foi uma cifra segura e poderosa.

| Alfabeto correto | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 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 | A |
| 2 | C | 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 |
| 3 | 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 |
| 4 | 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 | D |
| 5 | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| 6 | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| 7 | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| 8 | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| 9 | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| 10 | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| 11 | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| 12 | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| 13 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 14 | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 15 | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 16 | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| 17 | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| 18 | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| 19 | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| 20 | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| 21 | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| 22 | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| 23 | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| 24 | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| 25 | Z | 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 |
| 26 | 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 |

**Figura 2** - Exemplo da Cifra de Vigenère.

Fonte: Singh (2008, p. 66).

Em 1854 Charles Babbage desenvolveu a quebra da *Cifra de Vigenère*, no entanto, somente em 1863 a técnica para decifrar essa cifra ficou conhecida por meio de uma publicação de Friedrich Wilhen Kassiski, o qual desenvolveu isoladamente os métodos de decifração dessa cifra.

Após essa descoberta, no final do século XIX, a Criptografia sofria uma crise. Os criptógrafos não conseguiram desenvolver nenhum cifra segura que substituísse a *Cifra de Vigenère*. Além disso, o século seguinte marcou o surgimento do rádio, uma poderosa ferramenta de telecomunicação inventada por Guglielmo Marconi. Essa ferramenta de interlocução, embora tivesse ótimas vantagens para comunicações rápidas ele se mostrava como sendo um instrumento de frágil segurança. A interceptação de mensagens transmitidas

por esse meio poderia ser realizado com facilidade, o que gerava, neste meio de comunicação, uma fraqueza em relação ao sigilo das mensagens.

Da mesma maneira que a tecnologia se fez presente na criação do rádio ela surgiu nos meios de cifração. Sendo criada pelo inventor Artur Scherbius, a máquina *Enigma* surgiu na historia da Criptografia, em 1918, como uma máquina complexa proveniente do mais terrível sistema de cifragem da história da Criptografia (SINGH, 2008). Sendo muito utilizada pelos alemães durante a Segunda Guerra Mundial, a *Enigma* se tornou protagonista de muitas conversas militares entre os comandantes alemães e seus soldados nos terrenos de batalhas. Foi somente em 1940 que Alan Turing, utilizando estudos anteriores a *Enigma* realizados por Marian Rejewski, criou e desenvolveu uma máquina chamada *bomba*[2] que conseguia decifrar as mensagens da *Enigma*.

Após o episódio da descoberta de Turing, as máquinas *Enigma* já não se constituíam em um meio de cifragem segura. No entanto, tais máquinas marcaram a historia da Criptografia, pois atreladas a elas é que houveram os primeiros passos para o surgimento dos computadores modernos[3]. Com o surgimento da tecnologia programável, e com sua difusão entre as empresas é que houve a necessidade de se padronizar um tipo de cifragem para que as ações entre as empresas (transferência de dinheiro e negociações comerciais) ocorressem de forma eficiente e totalmente segura.

É dentro desse novo contexto que o problema da distribuição de chaves se agrava. Com a comercialização dos computadores e da difusão das cifras entre as empresas civis, surgiu a necessidade de se desenvolver um meio de distribuição de chaves seguro, o qual não dependesse de terceiros e nem que envolvesse altos custos. Como solucionadores esse entrave, Whitfield Diffe e Martin Hellmam realizaram pesquisas sobre as funções matemáticas e encontraram na aritmética modular um campo matemático cheio de funções de mão única[4]. Foi no ano de 1976 que a função modular $Y^x$ *(mod P)* foi apresentado como a solução para o problema de distribuição de chaves. O esquema para a troca de chaves de Diffie-Hellman-Markle, como ficou conhecido, (Figura 3) permitia a troca de informações seguras sem a necessidade da troca de chaves.

[2] Para mais informações a respeito da máquina *bomba* e sua criação ver Singh (2008, p. 143 – 211).
[3] A recriação do computador ocorreu por outros cientistas em 1945, quando J. Presper Eckert e John W. Mauchyl criaram o ENIAC (Electronic Numerical Integrator and Calculator). Durante muito tempo, o ENIAC foi considerado a mãe de todos os computadores, no entanto já em 1943 se tem informações do primeiro computador moderno desenvolvido.
[4] Funções de mão única são entendidas como sendo funções de fácil aplicabilidade, mas extremamente difíceis de desfazer.

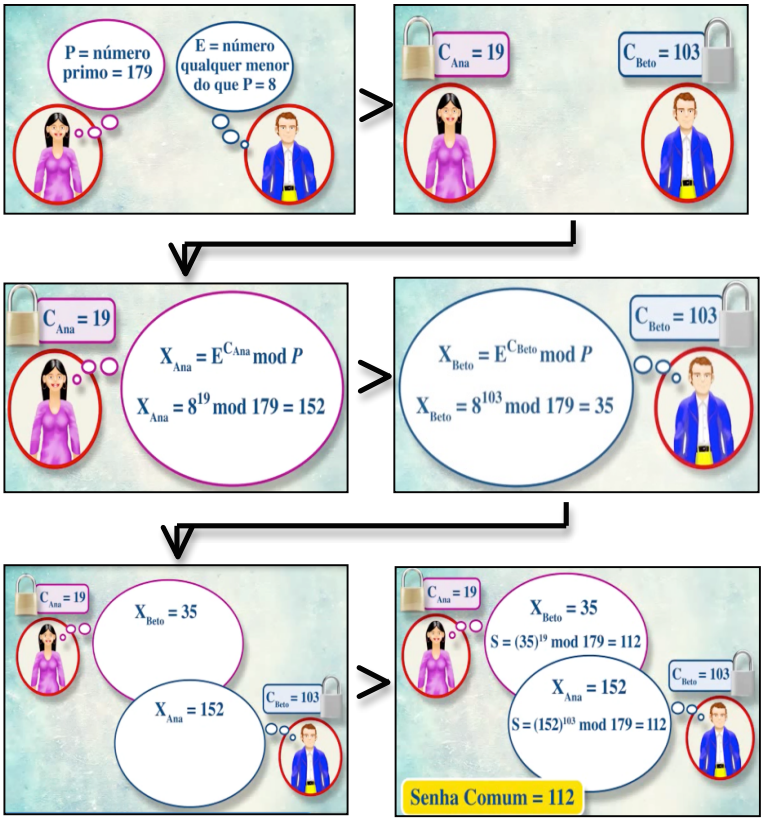


**Figura 3 -** Esquema da troca de chave de Diffie-Hellman-Merkle.
Fonte: Recortes do vídeo "Criptografia, Chave privada e Chave pública" (2012) [5].

Apensar do esquema apresentado acima apontar uma solução para o problema de distribuição de chaves[6], ele não era perfeito, ainda precisava-se aperfeiçoa-lo em termos de sua agilidade. Buscando melhorar o esquema para que ele funcionasse de forma rápida, é que Diffie projetou uma nova forma de se Criptografar. A chamada *chave assimétrica* foi arquitetada por ele, mas, no entanto, foi somente Ron Rivest, Adi Shamir e Leonard Adleman que desenvolveram a Criptografia RSA, um sistema assimétrico, que também é conhecido como *Criptografia de chave pública*.

A RSA é baseada em uma função modular da forma $C = M^e \ (mod\ N)$[7], na qual tem como principal segurança a dificuldade de se fatorar o número $N$, que é o resultado do produto de dois números primos. A Criptografia RSA resolveu os problemas associados às cifras tradicionais e eliminou o problema da distribuição de chaves, além de oferecer, até os dias de hoje, a segurança da troca de mensagens cifradas. Sendo ela muito utilizada em meios

[5] Vídeo disponível em: <https://www.youtube.com/watch?v=pEfEgCEKcJ0>. Data de acesso: 19/02/16.
[6] Chave é um componente que transforma o algoritmo de cifragem geral num método especifico de cifragem.
[7] As letras da fórmula $C = M^e \ (mod\ N)$ representam: $C$ = texto cifrado; $M$ = mensagem convertida, por exemplo, em ASCII ou em DES; $e$ = um número qualquer público; $N$ = o produto de dois números primos. Os valores de $e$ e $N$ formam, juntos, a chave pública. Para mais informações sobre a Criptografia RSA, ver em Sousa (2013).


ISSN 2178-034X

comerciais, essa cifra ainda é considerada muito forte, visto que, a tarefa de se fatorar o número *N* quando este é extremamente grande é muito difícil, se não, uma tarefa quase impossível.

## 4. Etapas do minicurso

- ✓ *Introdução ao tema*: Os participantes serão convidados a trabalhar em grupos para resolver uma atividade inicial proposta pela ministrante.

- ✓ *Discussão e apresentação do tema*: Os participantes serão convidados a discorrer sobre o processo de resolução utilizado pelo grupo para resolver a primeira atividade. Após a discussão, haverá uma breve apresentação acerca do tema Criptografia.

- ✓ *Iniciando a exploração do conceito de função afim*: Os participantes serão convidados a resolver uma segunda atividade agora já envolvendo o conceito de função afim. Após a sua resolução haverá um compartilhamento de resolução e sua discussão.

- ✓ *Explorando mais um pouco:* Os participantes serão convidados a resolveram uma atividade mais complexa que abordara diferentes mensagens cifradas. Posteriormente a essa terceira atividade, haverá uma apresentação das estratégias de resolução bem como uma discussão sobre as explorações observadas nas cifrações das mensagens a respeito das particularidades da função afim.

- ✓ *Pensando mais além:* nesta Será proposto para cada grupo que eles pensem e esquematizem uma atividade com outros conceitos matemáticos do Ensino Básico que poderiam ser aliados ao tema Criptografia dentro da metodologia da resolução de problemas a fim de promover suas explorações conceituais.

- ✓ *Discussão sobre as ideias:* Discussões sobre as ideias que os grupos tiveram acerca de outros conteúdos matemáticos pensados por eles dentro da perspectiva da resolução de problemas serão realizadas.

- ✓ *Discussão sobre como conhecer esse tema:* Discussões sobre quais maneiras esse tema pode ser abordado com os alunos de uma graduação em Licenciatura em Matemática e de que forma esse tema poderia aparecer na formação continuada dos professores serão promovidos.

- ✓ *Discu*

  *ssão sobre o tema*: Será realizada uma discussão de natureza didática com os participantes. Neste momento, eles analisarão a aplicabilidade dessas tarefas em sala de aula.

- ✓ *Apresentação:* Apresentados aos participantes sobre alguns trabalhos relacionando o tema Criptografia com os conteúdos do Ensino Médio.

- ✓ *Conclusão*: Os participantes serão convidados a responder uma avaliação sobre o desenvolvimento do minicurso.

## 5. Resultados esperados

Espera-se proporcionar aos participantes do minicurso um momento em que eles vivenciem atividades propostas com o tema Criptografia, não somente para apresentar esse assunto a eles, mas também, para oportunizar uma situação de debates a respeito das atividades propostas e sobre as possibilidades desse tema ser aliado a alguns conteúdos matemáticos com a intenção de abordá-los por meio da resolução de problemas tendo em consideração o objetivo de investigação e exploração de seus conceitos.

## 6. Referências

GROENWALD, C. L. O.; OLGIN, C. DE A. Criptografia e o Currículo de Matemática no Ensino Médio. *Revista de Educação Matemática*, v. 13, p. 71–78, 2011.

LITOLDO, B. F.; LAZARI, H. Uma análise do uso da criptografia nos livros didáticos de Matemática do Ensino Médio. *REMATEC - Revista de Matemática, Ensino e Cultura*, n. 17, p. 133–152, 2014.

SINGH, S. *O livro dos códigos: A ciência do sigilo - do antigo Egito à criptografia quântica*. 7. ed. Rio de Janeiro: Record, 2008.

TAMAROZZI, A. C. Codificando e Decifrando mensagens. *Revista do Professor de Matemática*, v. 45, p. 41–43, 2001.