Revista Desenvolvimento Socioeconômico *em Debate* - RDSD

website: http://periódicos.unesc.net/index.php/RDSD

ISSN 2446-5496

Tecnologia, criptografia e matemática: da troca de mensagens ao suporte em transações econômicas

José Eustáquio Ribeiro Vieira Filho[1]
Paula Prestes Azeredo[2]

RESUMO

A criptografia pode ser entendida pela ideia de "mensagem cifrada" e faz parte dos estudos e das técnicas que buscam transformar uma informação inteligível em uma mensagem codificada, mas que pode ser decifrada somente pelo seu receptor ou detentor da chave de decodificação. Mensagens criptografadas são extremamente úteis e importantes. Inicialmente, foram utilizadas para manter segredos diplomáticos e de guerras, com o intuito de preservar informações que não fossem acessíveis aos inimigos. Com a expansão do uso das redes informatizadas, o envio de mensagens criptografadas se generalizou, tornando-se cada vez mais complexas, desde mensagens simples entre dois agentes a transações econômicas e financeiras. O presente artigo busca apresentar um relato teórico e aplicado sobre o tema, notadamente no contexto da análise combinatória, que estuda estruturas e relações discretas, como a contagem de subconjuntos de um conjunto finito.

Palavras-chave: Criptografia, Algoritmo, Informação, Análise Combinatória.

ABSTRACT

Encryption can be understood as the idea of "cipher text" and is part of the studies and techniques that seek to change intelligible information on a coded message, but that can be deciphered only by your receiver or holder of the decryption key. Encrypted messages are extremely useful and important. Initially, they were used to keep diplomatic and war secrets, in order to preserve information that was not accessible to the enemy. With the expansion of the use of computer networks, sending encrypted messages were quickly disseminated, becoming increasingly complex, from simple messages between two agents to economic and financial transactions. This paper seeks to show a theoretical and applied debate to the subject, especially in the context of combinatorial analysis, which studies structures and discrete relationships, as subsets counting in a finite set.

Keywords: Cryptography, Algorithm, Information, Combinatorial Analysis.

[1] Doutor em Teoria Econômica pela Universidade Estadual de Campinas. Mestrado em Economia Aplicada pela Universidade Federal de Viçosa, especialização em Administração Pública pela Universidade Federal de Ouro Preto e bacharelado em Economia pela Universidade Federal de Minas Gerais. Técnico de Planejamento e Pesquisa do Instituto de Pesquisa Econômica Aplicada (Ipea), Secretário executivo da Sociedade Brasileira de Economia, Administração e Sociologia Rural (Sober) e Professor do Programa de Pós-graduação em Agronegócio da Universidade de Brasília (Propaga/UnB). E-mail: jose.vieira@ipea.gov.br

[2] Graduada em Administração pela Universidade de Brasília (UnB) e aluna do curso de Matemática da UnB. Assessora da Diretoria de Finanças do Banco do Brasil.

1. INTRODUÇÃO

A criptografia é uma palavra que deriva da união de dois radicais gregos "*kriptos*" e "*graphia*", sendo que o primeiro significa "secreto" e o segundo diz respeito à "escrita". No passado, o envio de mensagens secretas era realizado de forma simples e quase direta. As informações cifradas eram utilizadas por exércitos e governos, os quais buscavam surpreender seus inimigos com táticas de guerra e através de diplomacia.

No presente, com a rapidez das informações e com o aumento da necessidade da garantia de sigilo, muitas mensagens se tornaram essenciais nas atividades econômicas, tornando-se cada vez mais complexas, o que reforçou o uso intensivo da matemática nesse campo de estudo.

Segundo Santos (2013), o desenvolvimento da criptografia pode ser especificado em três fases: *i)* a artesanal; *ii)* a mecânica; e *iii)* a digital. Na fase artesanal, foram registrados os primeiros indícios de utilização da criptografia, paralelamente ao surgimento da escrita (por volta da idade antiga e média)[3]. A fase mecânica surge no início da idade moderna, impulsionada pela invenção do telégrafo e do rádio. O ápice desta fase se dá com o surgimento de máquinas de cifragem utilizadas durante a segunda guerra mundial[4].

Com o aperfeiçoamento dos computadores e a capacidade de realizar milhões de operações matemáticas, tem-se o início da fase digital. Os algoritmos criptográficos se tornam de conhecimento público, enquanto que o segredo da decodificação reside exclusivamente na chave criptográfica.

Na Fig.1, está ilustrado um esquema sintético de envio de uma mensagem criptografada entre dois agentes. Uma informação não cifrada enviada de um ponto inicial a outro final (que pode ser transmitida entre pessoas ou mesmo organizações) pode ser interceptada e compreendida por qualquer outro agente, não sendo exclusiva daquele que a originou.

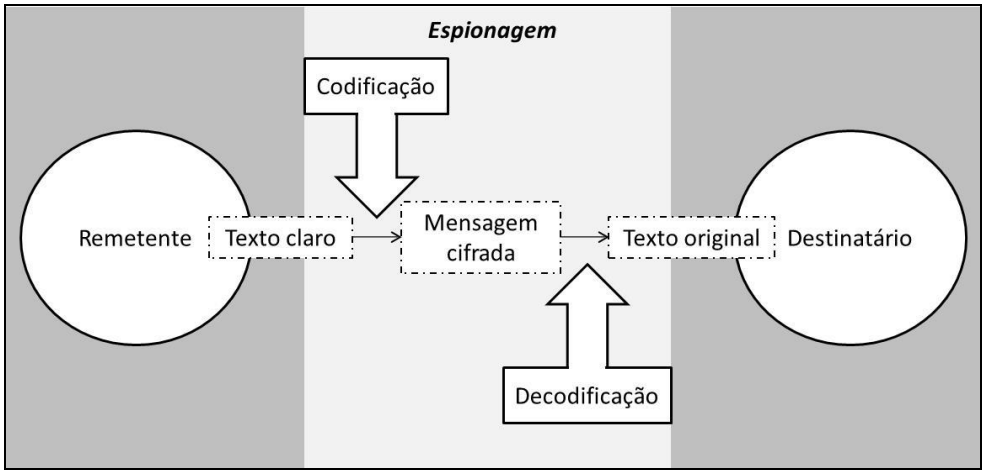
Todavia, uma informação cifrada será decodificada apenas pelo seu destinatário, que terá acesso ao código para decifrar a mensagem enviada. Nesse caso, qualquer agente

[3] Para uma explicação dos sistemas cifrados de numeração, veja Eves (2004).

[4] Destaca-se a máquina alemã *Enigma*, que foi criada em 1918, pelo engenheiro alemão Arthur Scherbius. O governo alemão utilizava esta máquina para se comunicar de maneira eficiente e segura. Acreditava-se à época ser impossível a quebra do código de cifragem. Porém, a resolução desse problema foi um dos principais eventos da criptoanálise de todos os tempos. Poloneses, franceses e ingleses, em um esforço conjunto, sob uma equipe coordenada por Alan Turing, desenvolveram máquinas capazes de decifrar as informações da tecnologia alemã. Este esforço criou uma máquina programável, que foi considerada o vetor precursor dos modernos computadores.

intermediário ou relacionado a um esquema de espionagem, que não possuir a chave de acesso, não será capaz de converter a informação cifrada em um texto inteligível.

Figura 1: Processo de envio de uma mensagem criptografada entre pessoas ou organizações.



Fonte: elaboração dos autores.

No intuito de intercambiar mensagens criptografadas, é necessário que transmissor e receptor conheçam o algoritmo utilizado para codificar a mensagem e a chave utilizada para cifrar. O algoritmo é um conjunto de procedimentos, normalmente matemáticos, em sequência lógica e organizada, para resolver um determinado problema.

Uma mensagem criptografada não seria compreensível por um agente intermediário que não o destinatário final. Assim, cabe somente ao receptor da informação reverter o algoritmo de cifragem, utilizando a chave para reconstituir a mensagem original a partir do texto cifrado. Na prática, a chave pode ser compartilhada entre dois ou mais agentes, no intuito de manter um canal confidencial de informação.

Como mostrado por Oliveira (2012), existem dois modelos de criptografia: i) o simétrico (ou chave privada), e ii) o assimétrico. O primeiro é aquele que utiliza a mesma chave (ou elemento que dá acesso à mensagem oculta) entre remetente e destinatário. Os algoritmos de chave simétrica estão relacionados às operações de codificação e decodificação[5].

[5] O *Data Encryption Standard* (DES) foi criado pela IBM em 1977 e é o algoritmo simétrico mais difundido no mundo. Apesar de permitir cerca de 72 quatrilhões de combinações, seu tamanho de chave (56 bits) é considerado pequeno. Depois deste, surgiram outros algoritmos, tal como o 3DES, que foi uma variação simples do primeiro, permitindo o emprego de duas ou três chaves distintas. Embora seguro, mostrou-se lento para realização dos cálculos. O *International Data Encryption Algorithm* (IDEA) foi criado em 1991, sendo estruturado com base no DES. Este se tornou mais rápido nos cálculos, sendo largamente utilizado pelo mercado financeiro e pela criptografia de mensagens pessoais.

Ao contrário, o modelo assimétrico é aquele que dispõe de duas chaves distintas e complementares, uma privada e outra pública. Neste caso específico, as chaves não são apenas senhas, mas arquivos digitais complexos, que podem estar eventualmente associados a uma senha. A chave pública é aberta a qualquer indivíduo; porém, a chave privada é restrita apenas aos interessados na comunicação[6].

O presente artigo pretende, portanto, apresentar um relato teórico e aplicado sobre o tema, notadamente no contexto da análise combinatória, bem como perspectivas de sua aplicação. Para tanto, quatro seções são apresentadas, incluindo esta breve introdução. A seção 2 descreve a metodologia de cálculo das permutações, incluindo combinações e permutações caóticas. A seção 3 elabora a análise dos resultados, mostrando exemplos aplicados de criptografia associados à análise combinatória de dados. Por fim, na seção 4, têm-se as considerações finais.

2. MÉTODO DE ANÁLISE

A criptografia também pode ser entendida dentro de um processo de inovação tecnológica. O agente que inova cria descontinuidades tecnológicas que impactam toda a cadeia produtiva. O avanço da análise criptográfica depende das habilidades gerenciais, que são construídas para explorar e captar novos conhecimentos, enquanto a adoção tecnológica condiciona os parâmetros da difusão da técnica. Num ambiente competitivo, a competição entre os agentes segue uma lógica *schumpeteriana* de análise, na qual os agentes inovadores tendem a conquistar o mercado em detrimento do comportamento dos imitadores (Nelson & Winter, 1982; Vieira Filho, 2015a; 2015b).

Esta seção do trabalho busca apresentar o método de análise para compreensão de alguns casos de criptografia que são utilizados por meio de permutações e combinações. Não se pretende aqui exaurir com toda discussão dos diferentes métodos, que englobam variados referenciais matemáticos, mas essencialmente introduzir os mais ajustados à análise combinatória.

[6] O algoritmo criado por Ron Rivest, Adi Shamir e Len Adleman (denominado pelas iniciais de seus nomes – RSA) é o modelo assimétrico mais utilizado no mundo, sendo criado também em 1977 no *Massachusetts Institute of Technology* (MIT). Além do RSA, outros foram desenvolvidos seguindo a mesma linha. Para alguns exemplos, têm-se o ElGamal (chave pública utilizada para o gerenciamento de chaves que utiliza uma matemática diferente do RSA), o Diffie-Hellman (criptosistema de chave pública mais antigo ainda em uso) e o Curvas Elípticas (algoritmo criptográfico com a utilização de curvas elípticas sobre corpos finitos).

Para um estudo mais aprofundado das várias aplicações da matemática na criptografia, recomenda-se a leitura de Fiarresga (2010) e Santos (2013). Se o interesse for o de desenvolver atividades no ensino médio e fundamental, confira Malagutti (2009). Em relação ao referencial metodológico, consultou-se Santos, Mello e Murari (2007).

2.1. Permutação

Sejam *n* e *k* inteiros quaisquer, tal que *k* seja menor ou igual a *n*. Uma permutação de *n* objetos distintos dispostos *k* a *k* – denominado por $P_{(n,k)}$ – pode ser calculada através de:

$$P_{(n,k)} = \frac{n!}{(n-k)!} \qquad (1)$$

Para $k = n$, é definido que $0! = 1$. Nesse sentido, a permutação simples de *n* objetos dispostos *n* a *n* – P_n – é derivada da Eq.1 acima:

$$P_{(n)} = n! = n(n-1)(n-2)\dots 1$$

A permutação nada mais é do que o embaralhamento dos objetos, de modo que a ordem dessa reordenação e o lugar ocupado pelo objeto sejam relevantes.

2.2. Combinação

Não obstante, quando se considera combinações de *n* objetos tomados *k* a *k*, os agrupamentos de *k* elementos, selecionados dentro dos *n* objetos disponíveis, diferem entre si apenas pela natureza dos elementos, não importando a ordem que os mesmos ocupam. Assim, a combinação simples de *n* objetos dispostos *k* a *k* – denotada por $C_{(n,k)}$ – é descrita pela Eq.2:

$$C_{(n,k)} = \frac{n!}{k!\,(n-k)!} \qquad (2)$$

Cabe ressaltar que este conjunto é mais restrito ao se comparar com as permutações, já que um mesmo conjunto de elementos específicos não se altera pela ordenação dos elementos.

2.3. Permutação caótica

Uma permutação dos termos de uma sequência $a_1, a_2, a_3, \dots, a_n$ é chamada de caótica quando nenhum dos elementos ocupa a sua posição original, ou seja, se cada termo a_i da sequência não ocupa a localização dada pelo número *i*, com $i = 1,2,3, \dots, n$.

Dado um conjunto de *n* elementos $A = \{a_1, a_2, a_3, \dots, a_n\}$ e supondo A_i como sendo o conjunto das permutações em que o elemento a_i está na posição de número *i*, para se calcular o número de permutações caóticas, denotadas por D_n (que advém da palavra desarranjo), deve-se calcular o número de elementos permutados que não pertencem à posição inicial, isto é, o número de elementos complementar da união dos A_i. Logo,

$$D_n = n! - \sum_{i=1}^{n} n(A_i) + \sum_{1 \le i < j} n(A_i \cap A_j) - \sum_{1 \le i < j < k} n(A_i \cap A_j \cap A_k) + \dots + (-1)^n n(A_1 \cap A_2 \cap \dots \cap A_n)$$

Como,

$$\begin{aligned} n(A_i) &= (n-1)!; \\ n(A_i \cap A_j) &= (n-2)!; \\ n(A_i \cap A_j \cap A_k) &= (n-3)!; \\ &\vdots \\ n(A_1 \cap A_2 \cap \dots \cap A_n) &= 1; \end{aligned}$$

tem-se que,

$$D_n = n! - n(n-1)! + C_{(n,2)}(n-2)! - C_{(n,3)}(n-3)! + \dots + (-1)^n . 1$$

Logo, a permutação caótica é dada pela Eq.3:

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n . \frac{1}{n!}\right) \qquad (3)$$

3. DEMONSTRAÇÕES E ANÁLISE DOS RESULTADOS

Esta seção busca demonstrar a aplicação dos conceitos apresentados de análise combinatória na criptografia, trazendo métodos utilizados ao longo dos anos. Serão discutidos o código de César, a máquina *Enigma* (tanto no caso da permutação simples quanto da caótica), bem como o algoritmo de assinatura digital RSA. Este último é o algoritmo assimétrico mais utilizado de chave pública, além de ser uma das maneiras mais poderosas de criptografia.

3.1. Código de César

O Código de César é um dos métodos de criptografia mais antigos que se tem notícia. O seu desenvolvimento baseava-se no deslocamento das letras do alfabeto, a letra A era representada pela letra D, a letra B era representada pela letra E, e assim sucessivamente. Esse código permitia apenas 26 variações possíveis, dado que o alfabeto tem 26 letras e cada letra era sempre substituída por uma mesma letra ou símbolo, tal como observado abaixo.

Texto original	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
Texto cifrado	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

Esse método, por apresentar poucas variações entre os elementos, era mais fácil de ser quebrado, bastando poucas interações para desvendá-lo.

3.2. Máquina *Enigma*

De forma a criar novas formas de codificação, dificultando a quebra de um código e, consequentemente, aumentando a segurança entre o mensageiro e o receptor, foi desenvolvida a codificação baseada na permutação simples dos elementos do alfabeto, e não apenas um deslocamento fixado, tal como visto em 3.1. Ao permutar o alfabeto, $P_{(26)}$, tem-se $P_{(26)} = 26! - 1 = 4.03 \times 10^{26}$ maneiras possíveis de reescrevê-lo e criar novas chaves de encriptação, excluindo apenas o elemento referente a própria mensagem.

Essa forma de criptografar foi desenvolvida em 1918 e passou a ser possível sua utilização com a elaboração de uma maquina codificadora, chamada na época de *Enigma*. Composta de três elementos, essa maquina possuía um teclado onde era introduzida a

mensagem, um misturador que permutava o alfabeto e um mostrador para visualizar a mensagem cifrada (SANTOS, 2012).

Esta tecnologia ficou conhecida após ser utilizada pelo exército Alemão durante a Segunda Guerra Mundial para tornar sua rede de transmissão mais segura, e concedendo ao país uma vantagem competitiva sobre os inimigos por muitos anos[7].

3.3. Maquina do *Enigma* – Permutação caótica

Considerando o exemplo 3.2 e imaginando que o emissor deseja preservar a ordem original, ou seja, não se deseja apresentar nenhuma das letras na mesma posição de origem, a máquina pode ser programada de forma a realizar uma permutação caótica.

Como neste caso não se pode repetir os elementos da posição inicial, utiliza-se a permutação caótica ou desordenamento. Assim, ao invés de se ter $P_{(26)} = 26!$ elementos permutáveis, encontram-se apenas: $D_{(26)} = 26!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{1}{26!}\right) = 1{,}48 \times 10^{23}$.

Embora haja uma diminuição na quantidade de permutações possíveis, ainda é um número expressivo, impossibilitando a descoberta do segredo de forma manual. No entanto, algumas técnicas de análise permitem a descoberta da mensagem, seja por "força bruta", através de tentativa e erro, ou mesmo por cálculos computacionais dedicados a fazer interações e as possíveis combinações; ou também por análise linguística e frequência de letras.

3.4. Algoritmo de assinatura digital – RSA

Este algoritmo foi desenvolvido por Ron Rivest, Adi Shamir e Len Adleman em 1977 no *Massachusetts Institute of Technology* (MIT), principal universidade americana de engenharia e tecnologia. O mesmo foi denominado pelas iniciais dos inventores. Assim, o RSA é um modelo que utiliza o conceito de chave pública, o qual permite que qualquer usuário codifique mensagens. Porém, a chave de decodificação é secreta e só o destinatário final poderá decodificá-la.

[7] O filme "*The imitation game*" (de tradução para o português - O Jogo da Imitação) é baseado na história real do lendário criptoanalista inglês Alan Turing, considerado o pai da computação moderna, e narra a tensa corrida contra o tempo da equipe de Turing para decifrar os códigos de guerra nazistas e contribuir para a finalização do conflito.

A chave de codificação do RSA é constituída essencialmente por $n = pq$, onde p e q são primos grandes e distintos. Definindo-se os elementos, é possível calcular o $\varphi(x)$ de Euler, ou seja, a quantidade de números que são primos entre si do número escolhido. O próximo passo é escolher um número e em que $1 < e < \varphi(n)$, de forma que e seja co-primo de $\varphi(n)$. Em outras palavras, busca-se um e onde o $MDC(\varphi(n), e) = 1$, sendo $e > 1$.

Por exemplo, sejam dois números primos p e q, com $p = 17$ e $q = 41$, e $n = 697$.

Após isso, calcula-se a função de Euler, $\varphi(n) = (p-1) \times (q-1) = (17-1) \times (41-1)$ $\varphi(697) = 640$. Um número co-primo no qual o $MDC(\varphi(697), e) = 1$ que se pode usar no exemplo é o número 13. Logo, a chave de codificação seria $(n, e) = (697, 13)$. Para cifrar uma mensagem, utiliza-se a fórmula $c = m^e \times mod(n)$, onde e é a chave pública e m é o valor numérico da letra. Adaptando para o exemplo aqui demonstrado, tem-se que: $c = m^{13} \times mod(697)$.

Utilizando-se a letra T como exemplo, tem-se que $m = 19$ e o valor de c, ou o código, seria 15. O leitor para identificar a mensagem teria que realizar o processo inverso ao apresentado, calculando $m \equiv cd\ (modn)$ para realizar a decodificação. Esse é um dos métodos mais seguros atualmente devido à dificuldade existente em quebrar a chave de decodificação. Isso só foi possível devido ao fato de não existir algoritmos eficientes para a fatoração de inteiros em fatores primos com o número de algarismos ultrapassando os 100 elementos ou mais.

4. CONSIDERAÇÕES FINAIS

A criptografia é uma técnica de segurança usada em todos os sistemas computacionais que requerem proteção das informações transmitidas e armazenadas. Esse artigo apresentou um breve histórico, as formas conceituais básicas, a criptografia simétrica e a assimétrica, bem como suas propriedades, vantagens e desvantagens.

Embora a criptografia tenha surgido de forma relativamente simples para gerar confidencialidade das mensagens, é atualmente técnica de segurança essencial usada nos sistemas computacionais, que requerem proteção das informações transmitidas e registradas.

O avanço da criptoanálise está inserido em um processo de inovação tecnológica, em que os agentes inovadores tendem a sobressair frente aos agentes imitadores. Por meio da criptografia, podem-se programar técnicas de garantia de integridade dos dados e de

autenticação das mensagens. A garantia de integridade garante que se um dado for modificado, essa alteração é detectada, informando ao destinatário que a mensagem foi comprometida ou mesmo corrompida. Já a autenticação das mensagens é o que comumente chama-se de assinatura digital.

Esse artigo não visou extinguir todas as aplicações da matemática no desenvolvimento da criptografia, mas se propôs a demonstrar a contribuição da análise combinatória para o desenvolvimento dessa nova tecnologia, apresentando também um histórico e uma contextualização da importância da criptografia no contexto recente.

REFERÊNCIAS

EVES, Howard. **Introdução à história da matemática**. Campinas: UNICAMP, 2004.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e matemática**. Lisboa: Universidade de Lisboa: 2010. (Dissertação de Mestrado).

MALAGUTTI, Pedro Luiz. **Atividades de contagem a partir da criptografia**. Rio de Janeiro: IMPA, 2009.

NELSON, Richard R.; WINTER, Sidney. **An evolutionary theory of economic change**. Massachusetts: Harvard University Press, 1982.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital.** v. 31, p.11-15, 2012.

SANTOS, José Luiz. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes motivadoras para atividades de matemática básica**. Salvador: UFBA, 2013. (Dissertação de Mestrado).

SANTOS, José Plínio de Oliveira; MELLO, Margarida Pinheiro; MURARI, Idani Theresinha Calzolari. **Introdução à análise combinatória**. Rio de Janeiro: Ciência Moderna, 2007.

VIEIRA FILHO, José Eustáquio Ribeiro. **Modelagem evolucionária da dinâmica industrial (parte 1):** concorrência, regimes tecnológicos e difusão de conhecimento. Brasília: Ipea, 2015a. (Texto para Discussão, n.2144).

VIEIRA FILHO, José Eustáquio Ribeiro. **Modelagem evolucionária da dinâmica industrial (parte 2):** trajetórias tecnológicas, capacidade de absorção e aprendizado. Brasília: Ipea, 2015b. (Texto para Discussão, n.2146).