

BREVE HISTÓRIA DA CRIPTOGRAFIA: DO EGITO ANTIGO ATÉ O SÉC. XXI

Clístenes Lopes Da Cunha¹
Divane Aparecida de Moraes Dantas²
Nícolas Francisco Martins Chagas³

RESUMO

Este artigo tem como objetivo apresentar a evolução histórica da criptografia, desde suas manifestações na antiguidade até os desafios contemporâneos associados à computação quântica. A pesquisa caracteriza-se como bibliográfica e documental, fundamentada em obras clássicas da história da criptografia e da segurança da informação. O estudo discute as principais técnicas criptográficas desenvolvidas ao longo do tempo, incluindo cifras de substituição e transposição, a cifra de Vigenère, a máquina Enigma, a cifra Lorenz e sistemas modernos de criptografia assimétrica, com destaque para o RSA e a criptografia de curvas elípticas. Também são abordadas as diferenças entre criptografia e esteganografia, bem como o papel da criptoanálise no aprimoramento dos métodos de proteção da informação. Os resultados evidenciam que a criptografia evoluiu em estreita relação com demandas militares, políticas, científicas e tecnológicas, consolidando-se como elemento fundamental para a segurança das comunicações digitais. Conclui-se que sua trajetória histórica revela um processo contínuo de adaptação frente aos avanços tecnológicos, mantendo sua relevância diante dos desafios impostos pela computação quântica.

Palavras-chave: Criptografia. Cifras. História da Matemática.

INTRODUÇÃO

A comunicação sempre desempenhou papel fundamental na organização das sociedades humanas, intensificando-se com o surgimento da escrita nas primeiras civilizações, quando passou a estruturar práticas administrativas, comerciais, diplomáticas e militares. À medida que o registro escrito se consolidou como instrumento de poder e controle, tornou-se igualmente necessária a proteção de determinadas informações, sobretudo aquelas relacionadas a disputas territoriais, estratégias militares e acordos políticos e econômicos. É nesse contexto histórico que se desenvolve a criptografia, entendida como o conjunto de técnicas destinadas a tornar mensagens legíveis, inacessíveis a indivíduos não autorizados, com a finalidade de assegurar o sigilo e a integridade da comunicação (Musacchio, 2024).

¹Professor e doutorando na Universidade Federal de Ciência e Inovação de Minas Gerais, Belo Horizonte, MG. Mestre pela PUC-Minas. E-mail: clistenes@cefetmg.br, <https://orcid.org/0000-0002-3146-2043>, <http://lattes.cnpq.br/2803469302351136>.

²Professora na Universidade Federal de Minas Gerais, Belo Horizonte, MG. Doutora em Matemática pela UFMG. E-mail: vanedantas@yahoo.com.br, <https://orcid.org/0009-0008-5224-4652>, <http://lattes.cnpq.br/4844317717801610>.

³Estudante da Universidade Federal de Ciência e Inovação de Minas Gerais, Belo Horizonte, MG. Técnico em Informática pelo CEFET-MG. E-mail: nicolaschagas5588@gmail.com, <https://orcid.org/0009-0002-7518-8493>, <http://lattes.cnpq.br/0939442929916629>.

Desde a Antiguidade, diferentes culturas recorreram a formas variadas de codificação, como hieróglifos no Egito Antigo, a Escítala na Grécia e a cifra de César em Roma, evidenciando a associação entre criptografia, poder e estratégia (Kahn, 1996; Singh, 1999). No século XX, a criptografia consolidou-se como elemento estratégico global, especialmente durante as Grandes Guerras Mundiais, e passou a assumir papel central com o desenvolvimento da computação e dos algoritmos de chave pública, como o RSA e a criptografia de curvas elípticas (Costa; Figueiredo, 2010; Stallings, 2020).

No século XXI, em um cenário marcado pela digitalização das relações sociais e econômicas, a criptografia tornou-se indispensável para a segurança das comunicações eletrônicas, das transações financeiras e da proteção de dados. Diante desse panorama, o presente artigo tem como objetivo discutir as principais técnicas criptográficas desenvolvidas ao longo do tempo, incluindo cifras de substituição e de transposição tais como; a cifra de Vigenère, a máquina Enigma, a cifra Lorenz e sistemas modernos de criptografia assimétrica, em especial o RSA e a criptografia de curvas elípticas e os desafios que os computadores quânticos impõem com a partir da quebra desses métodos.

Esta pesquisa caracteriza-se como qualitativa, de natureza bibliográfica e documental, com abordagem histórico-descritiva. Foram analisados livros, artigos, dissertações, documentos e registros históricos sobre a evolução da criptografia. A investigação foi organizada em perspectiva cronológica, buscando compreender as transformações dos métodos criptográficos, suas aplicações em diferentes contextos e sua contribuição para o desenvolvimento da segurança da informação.

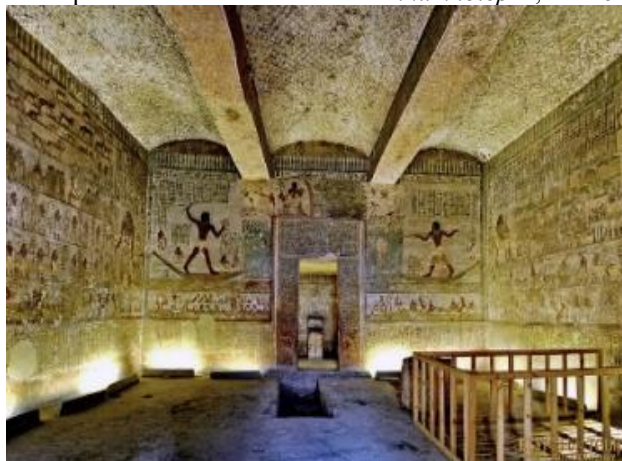
CRIPTOGRAFIA NO EGITO ANTIGO

Há registros históricos que, no Egito Antigo, empregaram-se formas de escrita não convencionais, vistas como codificação inicial. Tais informações surgem principalmente em inscrições hieroglíficas de caráter religioso e funerário, nas quais símbolos eram modificados, substituídos ou organizados de maneira incomum, tornando a leitura acessível apenas a grupos específicos, como sacerdotes e escribas. Diferentemente do uso voltado à comunicação secreta no sentido moderno, essas técnicas tinham forte dimensão simbólica e ritual, funcionando como um marcador de saber especializado. Um dos exemplos mais citados pela literatura é o conjunto de inscrições do Médio Império, como as encontradas no túmulo de *Khnumhotep II* (aproximadamente entre 1870 AEC e 1810 AEC), nas quais observa-se o uso de hieróglifos criptografados. Esses vestígios encontram-se preservados em sítios arqueológicos egípcios e documentados em coleções museológicas internacionais, sendo analisados por historiadores da criptografia como

manifestações embrionárias de estratégias de ocultação e restrição do conhecimento escrito (Kahn, 1996; Singh, 1999).

O texto registrava os monumentos que *Khnumhotep II*, que governou o pequeno território de *El Oryx*, ergueu a serviço do faraó *Amenemhet II* (1929-1892 AEC), da XII dinastia. A figura 1, representa a tumba de *Khnumhotep II* que se situa no sítio arqueológico de Beni Hassan, localizado próximo à cidade de *El Minya*. A necrópole abriga 39 tumbas de sacerdotes, nobres e oficiais do Reino Médio (2040-1640 AEC).

Figura 1 – Capela funerária no túmulo de *Khnumhotep II*, em Beni Hasan.



Fonte: Egypt fun tours (2026, n.p.)

Esse registro é considerado o mais antigo exemplo de criptografia de substituição, segundo Kahn (1996). O escriba substituíam símbolos comuns por variantes mais raras e de difícil compreensão para leitores não especializados. O objetivo dessa estratégia não era de proteção de segredos militares, finalidade que a criptografia viria a assumir séculos depois, mas estava associada a práticas ritualísticas e à preservação de conhecimentos restritos às elites, ou de seus tesouros. Embora rudimentar, esse tipo de escrita evidencia duas características centrais da criptografia: a ideia de ocultar informações do público geral e a de restringir a leitura a um grupo específico de destinatários (Singh, 1999). No contexto egípcio, a criptografia era um recurso de poder simbólico e social, antes mesmo de se tornar uma ferramenta política e militar.

ESTEGANOGRAFIA X CRIPTOGRAFIA

Com o desenvolvimento da linguagem escrita como meio de comunicação, surgiu o interesse em criar medidas que adicionassem confidencialidade a uma troca de informações. Para tanto, surgiram duas áreas: a esteganografia e a criptografia. Em comum possuem a intenção de proteger informações, mas de modos distintos. Nada impede que sejam utilizadas ao mesmo tempo, para aumentar ainda mais a segurança.

A esteganografia visa tornar uma mensagem indetectável para um possível leitor indesejado; ela a “esconde”. Ao longo da história, diversas técnicas esteganográficas foram desenvolvidas, tais como a prática de escrever com tinta invisível até métodos mais elaborados, como o microponto. Heródoto (484-425 AEC), historiador e geógrafo grego, descreveu mensagens secretas escondidas sob a cera em tábuas de madeira ou como marcações sobre a pele (tatuagem), especificamente na cabeça de um escravo, que se ocultava quando o cabelo crescia, o que representa um tipo de esteganografia. O microponto, tática usada pelos alemães na Segunda Guerra Mundial (1939-1945), consistia em reduzir uma foto de um texto até transformá-la em um ponto, para que pudesse se passar por um sinal de pontuação. Segundo Baird (1945), Colepaugh foi o primeiro americano a ver o equipamento alemão de micropontos. Diferentemente da esteganografia, cujo objetivo é “ocultar” a mensagem, a criptografia tem como finalidade, tornar o conteúdo da informação “ininteligível”, para indivíduos não autorizados. Isso confere à criptografia uma vantagem importante, pois mesmo que a mensagem seja interceptada, seu significado permanece protegido.

No contexto atual, de intensa informatização e circulação de dados digitais, segundo Stallings (2020), a criptografia estrutura-se a partir de quatro princípios fundamentais: confidencialidade, integridade, autenticação e não repúdio. Esses princípios asseguram que as informações circulem de forma segura, confiável e restrita aos usuários legitimamente autorizados. A confidencialidade impede o acesso indevido ao conteúdo por meio do uso de algoritmos criptográficos e chaves, a integridade garante que os dados não sejam alterados durante a transmissão ou o armazenamento, a autenticação possibilita a verificação da identidade das partes envolvidas na comunicação e o não repúdio é o princípio que garante que uma entidade não possa negar posteriormente a autoria de uma ação realizada. Conforme destacado pela Federação Brasileira de Bancos (Febraban, 2023), tais fundamentos sustentam grande parte das transações realizadas no ambiente digital contemporâneo, especialmente nas comunicações entre usuários e aplicações via *web*.

A consolidação desses princípios também impulsiona o desenvolvimento de novas abordagens, como a criptografia quântica, que busca elevar os níveis de segurança ao apoiar-se em fenômenos físicos fundamentais, ampliando as perspectivas de proteção da informação em cenários futuros cada vez mais complexos.

CRIPTOANÁLISE E TÉCNICAS CRIPTOGRÁFICAS SIMPLES

A criptoanálise tem como finalidade identificar fragilidades em sistemas criptográficos e desenvolver métodos capazes de quebrar cifras, acompanhando a evolução da criptografia. Esse campo cresce à medida que novos mecanismos de proteção surgem, exigindo técnica de ataque e defesa (Loureiro, 2014). Um dos métodos mais elementares de criptoanálise é o ataque por força bruta, que testa sistematicamente todas as chaves possíveis até que a mensagem seja recuperada.

Entre as técnicas criptográficas mais simples destacam-se as cifras de transposição, reorganizando os caracteres do texto simples sem alterá-los, formando um texto cifrado anagramático. O primeiro dispositivo criptográfico conhecido é a *Scytale* (ou Escítala), utilizada pelos espartanos, que aplicava esse princípio pelo enrolamento de uma fita em um bastão de madeira, permitindo a leitura apenas com outro bastão de mesmo diâmetro (Loureiro, 2014). Esse método associa a criptografia e esteganografia, pois a mensagem não chamava atenção durante o transporte. As cifras de substituição, modificam os símbolos do texto original, podendo ser monoalfabéticas, quando cada símbolo corresponde sempre ao mesmo substituto, ou polialfabéticas, quando um símbolo pode ter múltiplas representações. A Cifra de César é um exemplo monoalfabético baseado no deslocamento fixo das letras. Esse método tornou-se obsoleto por ser quebrável por força bruta em computadores modernos (Costa e Figueiredo, 2010).

Cifras monoalfabéticas complexas, que exploram permutações completas do alfabeto, apresentam vulnerabilidades à análise de frequência. A recorrência estatística de letras em um idioma permite inferir substituições prováveis, conforme demonstrado por tabelas de frequência, tornando esse tipo de cifra inseguro (Loureiro, 2014). A Figura 2, representa a frequência das letras no alfabeto português brasileiro.

Figura 2 – Frequência de Letras no alfabeto português brasileiro.

A: 13.90%	B: 1.00%	C: 4.40%	D: 5.40%	E: 12.20%	F: 1.00%	G: 1.20%	H: 0.80%
I: 6.90%	J: 0.40%	K: 0.10%	L: 2.80%	M: 4.20%	N: 5.30%	O: 10.80%	P: 2.90%
Q: 0.90%	R: 6.90%	S: 7.90%	T: 4.90%	U: 4.00%	V: 1.30%	W: 0.00%	X: 0.30%
Y: 0.00%	Z: 0.40%						

Fonte: Rocha (2020, n.p., adaptada).

Como resposta a essas fragilidades, surgiu a cifra polialfabética de Vigenère, que utiliza uma chave composta por letras e uma tabela que varia as substituições ao longo do texto (Kahn, 1996). Esse mecanismo reduz a eficácia da análise de frequência e foi seguro por séculos, até que, no século XIX, Friedrich Kasiski demonstrou que padrões repetidos no texto cifrado poderiam revelar o tamanho da chave, possibilitando sua quebra (Kasiski, 1863). O exame de Kasiski marcou o declínio da cifra de Vigenère e impulsionou o desenvolvimento de técnicas criptográficas mais robustas (Singh, 1999).

ENIGMA, CIFRA LORENZ E O PRECURSOR DOS COMPUTADORES

Durante a Segunda Guerra Mundial (1939-1945), os nazistas desenvolveram a *Enigma*, um aparelho semelhante a uma máquina de escrever que representou um grande salto na aparelhagem criptográfica. Ela foi um dos mecanismos mais utilizados pelos alemães para a troca de informações táticas e mensagens estratégicas durante a guerra. O equipamento possuía um conjunto de misturadores que podiam ser dispostos em diferentes posições, representando chaves distintas. O método criptográfico determinava pares de letras com base na chave. Quando uma tecla era pressionada, uma luz acendia indicando qual o par correspondente. Dessa forma, quando duas máquinas estavam configuradas do mesmo modo, era simples cifrar e decodificar as mensagens.

Com o objetivo de quebrar a segurança da *Enigma*, o cientista e matemático britânico Alan Mathison Turing (1912-1954) desenvolveu uma máquina chamada *Bombe* ou Máquina de Turing. Ela permitia testar combinações possíveis e encontrar rapidamente a configuração correta. Esse processo buscava por palavras comuns ou esperadas nas combinações para encontrar a correta. Os nazistas empregavam dois mecanismos de criptografia: a *Enigma* e a Cifra de Lorenz, sendo esta última utilizada pelo alto comando alemão. A Cifra de Lorenz, por ser mais complexa que a *Enigma*, exigiu o desenvolvimento de uma máquina mais sofisticada para sua decodificação. Foi nesse ponto que Thomas H. Flowers (1905-1998) projetou e construiu a máquina *Colossus*, com a colaboração de Turing. Era uma máquina programável e consideravelmente mais rápida do que a *Bombe*. Muitos a veem como o primeiro computador digital (Copeland, 2006). A maior rapidez no processamento de dados deve-se ao fato de que o novo dispositivo utilizava válvulas eletrônicas em vez das engrenagens mecânicas da *Bombe*. Foi um grande passo para a tecnologia mundial.

CRIPTOGRAFIA ASSIMÉTRICA NA COMPUTAÇÃO

Apesar dos progressos alcançados, os sistemas criptográficos clássicos ainda apresentavam fragilidades. As cifras de César, de Vigenère e o método empregado pela *Enigma* enquadravam-se como cifras simétricas, pois utilizam a mesma chave para cifrar e decifrar (Singh, 1999; Kahn, 1996). Essa característica impõe a necessidade de compartilhamento prévio da chave entre os interlocutores, o que representa um ponto crítico de vulnerabilidade, uma vez que sua interceptação comprometeria integralmente a segurança da informação (Stallings, 2020). Além disso, com a ampliação das comunicações digitais e bancárias, a distribuição segura de chaves passou a configurar um problema logístico relevante (Diffie; Hellman, 1976). Soma-se a isso o aumento expressivo do poder computacional, que tornou ataques de força bruta cada vez mais viáveis contra métodos criptográficos menos complexos (Stallings, 2020).

Nesse contexto, em 1976, Bailey e Hellman propuseram o conceito de criptografia assimétrica, oferecendo uma solução para essas limitações. Diferentemente das cifras simétricas, esse modelo baseia-se no uso de um par de chaves distintas, uma pública e outra privada. A chave pública pode ser divulgada e utilizada para cifrar a mensagem, enquanto a chave privada, mantida em sigilo pelo destinatário, é a única capaz de realizar a decifração (Stallings, 2020). Assim, elimina-se a necessidade de compartilhamento prévio de uma chave comum, reduzindo expressivamente os riscos de comprometimento da segurança e simplificando a gestão das comunicações em ambientes amplos e distribuídos.

Esse princípio foi concretizado em 1977, com o desenvolvimento do algoritmo RSA por Ronald Linn Rivest, Adi Shamir e Leonard Max Adleman, pesquisadores do *Massachusetts Institute of Technology*, cujas iniciais originaram a denominação do método (Rivest; Shamir; Adleman, 1978). O RSA baseia-se na dificuldade computacional de fatorar números inteiros grandes, processo que, mesmo com os recursos tecnológicos atuais, permanece impraticável em tempo hábil. Tal característica confere elevada robustez ao algoritmo, tornando-o amplamente utilizado na proteção de informações digitais, embora seu alto custo computacional represente uma limitação em determinados contextos. Em busca de maior eficiência, especialmente em ambientes com restrições de processamento, em 1985, surgiu a Criptografia de Curvas Elípticas, desenvolvida de forma independente por Victor Saul Miller e Neal Izadore Koblitz. Assim como o RSA se apoia na dificuldade da fatoração de grandes números, a *Elliptic Curve Cryptography* (ECC), baseia-se na complexidade do Problema do Logaritmo Discreto em Curvas Elípticas, o que possibilita alcançar níveis equivalentes de segurança com chaves muito menores, conforme mostra o comparativo da tabela 1

Tabela 1: Comparativo de tamanho de chaves por nível de segurança (em bits).

Esquema Simétrico(bits)	Esquema Baseado em ECC(bits)	RSA/DSA(bits)
80	160	1024
112	224	2048
128	256	3072
256	512	15360

Fonte: Adaptado de Stallings (2020).

Essa característica torna a ECC particularmente adequada a aplicações que demandam economia de recursos computacionais, energéticos e de memória, como dispositivos móveis, sistemas embarcados, sensores da internet das coisas, cartões inteligentes e protocolos de segurança da informação amplamente utilizados, como o *Transport Layer Security* e o *Hypertext Transfer Protocol Secure*, além de mecanismos de assinatura digital (Menezes; Vanstone; Okamoto, 1993).

Outra abordagem relevante para otimizar o desempenho dos sistemas criptográficos é a criptografia híbrida. O *Pretty Good Privacy*, desenvolvido por Philip Rogaway Zimmermann Jr., que combina técnicas simétricas e assimétricas com o objetivo de equilibrar segurança e eficiência computacional (Costa; Figueiredo, 2010). Nesse modelo, a mensagem é cifrada inicialmente por um algoritmo simétrico, enquanto a chave utilizada nesse processo é protegida por meio da criptografia assimétrica, reduzindo o custo computacional do envio e mantendo elevados níveis de segurança.

No cenário contemporâneo, marcado pela consolidação da era digital, novos desafios se apresentam com o avanço da computação quântica. Em 1981, Richard Phillips Feynman propôs a ideia de um simulador quântico, inaugurando um campo de pesquisa que promete revolucionar o processamento de dados ao explorar princípios da mecânica quântica. A perspectiva de computadores quânticos plenamente funcionais impõe riscos aos métodos criptográficos atuais, tornando necessária a investigação e o desenvolvimento de técnicas de criptografia pós quântica. Conforme aponta a Febraban (2023), esse avanço tecnológico possui potencial para transformar profundamente a segurança da informação. Ainda assim, a trajetória histórica da criptografia demonstra sua capacidade contínua de adaptação, indicando que, diante de novos desafios computacionais e analíticos, soluções inovadoras tendem a emergir, assegurando sua permanência como elemento essencial das sociedades modernas.

CONSIDERAÇÕES FINAIS

A pesquisa realizada evidencia que a criptografia não surgiu como fenômeno

isolado ou meramente matemático, mas como resposta direta a problemas concretos de comunicação, sigilo e poder, que se transformaram ao longo do tempo conforme as necessidades das sociedades. Desde os registros simbólicos do Egito Antigo até os algoritmos modernos empregados em sistemas digitais, observa-se uma continuidade histórica marcada pela busca por controle da informação e proteção do conhecimento.

O levantamento desenvolvido ao longo do texto permite sustentar a posição de que a criptografia evolui em permanente diálogo com a criptoanálise, sendo essa relação de oposição um dos principais motores de seu aprimoramento. O estudo dos métodos clássicos, como as cifras de transposição e substituição, evidencia suas limitações diante do avanço das técnicas analíticas, ao passo que episódios históricos como a quebra da *Enigma* e da Cifra Lorenz demonstram que o domínio da criptografia pode produzir impactos decisivos em contextos estratégicos e geopolíticos. Nesse sentido, o trabalho reforça que os avanços criptográficos do século XX não apenas garantiram a segurança da informação, mas impulsionaram o desenvolvimento da computação moderna.

No contexto da segurança da informação no mundo contemporâneo, o estudo aponta que a introdução da criptografia assimétrica representou uma solução estrutural para limitações logísticas e técnicas das cifras simétricas, viabilizando a comunicação segura em larga escala. A análise do RSA e da ECC sustenta a posição de que a eficiência matemática se tornou critério central na adoção de algoritmos modernos, especialmente em ambientes com restrições computacionais. A escolha da ECC confirma que a criptografia atual não se orienta apenas pela robustez teórica, mas também por exigências práticas de desempenho e escalabilidade. A trajetória histórica analisada sustenta a posição de que a obsolescência de alguns métodos não representa o enfraquecimento da área, mas sim o estímulo à criação de novas soluções. Dessa forma, o trabalho defende que a criptografia continuará a ocupar papel central na organização das sociedades digitais, reafirmando sua relevância científica, tecnológica e histórica frente aos desafios presentes e futuros da segurança da informação.

REFERÊNCIAS

BAIRD JÚNIOR, Willard Machle. Secret Inks: information taken from the record of trial of William C. Colepaugh and Erich Gimpel. *In*: ESTADOS UNIDOS. Signal Security Agency. **Record of Trial of German Saboteurs**. Washington, DC: Signal Security Agency, 1945. p. 13-14.

COPELAND, Brian Jack (org.). **Colossus: the secrets of Bletchley Park's codebreaking computers**. Oxford: Oxford University Press, 2006. 480 p.

COSTA, Celso; FIGUEIREDO, Luiz Manoel. **Introdução à criptografia**, v. 1. Rio de Janeiro: UFF/CEP-EB, 2010. 100 p.

DIFFIE, Whitfield; HELLMAN, Martin Edward. **New directions in cryptography**. IEEE Transactions on Information Theory, v. 22, n. 6, p. 644–654, 1976.

EGYPT FUN TOURS. **Beni Hasan Tombs: Middle Kingdom Guide**. [s.d.]. Disponível em: <https://www.egyptfuntours.com/beni-hasan-tombs-middle-kingdom-guide/>. Acesso em: 23 jun. 2026.

FEBRABAN – Federação Brasileira de Bancos. **Criptografia quântica**. Laboratório de Segurança Cibernética. São Paulo: FEBRABAN, 2023. Disponível em: FEBRABAN - Laboratório de Segurança Cibernética. Acesso em: 19 fev. 2026.

KAHN, David. **The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet**. New York: Scribner, 1996.

KASISKI, Friedrich. **Die Geheimschriften und die Dechiffirkunst**. Berlin: E. S. Mittler und Sohn, 1863.

LOUREIRO, Flávio Ornellas. **Tópicos de criptografia para o ensino médio**. 2014. 129 f. Dissertação (Mestrado em Educação Matemática) – Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista (UNESP), Rio Claro, 2014.

MENEZES, Alfred John; VANSTONE, Scott Alexander; OKAMOTO, Tatsuaki. Reducing elliptic curve logarithms to logarithms in a finite field. **IEEE Transactions on Information Theory**, [S. l.], v. 39, n. 5, p. 1639-1646, Sept. 1993.

MUSACCHIO, Fabrizio. **A brief history of writing**. Disponível em: https://www.fabriziomusacchio.com/weekend_stories/told/2024/2024-12-22-brief_history_of_writing/. Acesso em: 19 fev. 2026.

RIVEST, Ronald Linn; SHAMIR, Adi; ADLEMAN, Leonard Max. **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM, v. 21, n. 2, p. 120–126, 1978.

ROCHA, Rogério Reis. **Tabelas de Criptografia**. Porto: Universidade do Porto (DCC/FCUP), 2020. Disponível em: <https://www.dcc.fc.up.pt/~rvr/naulas/tabelasPT/>. Acesso em: 19 fev. 2026.

SINGH, Simon. **The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography**. New York: Doubleday, 1999.

STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. 8th ed. Boston: Pearson, 2020.

Submetido em: 27 de abril de 2026.
Aprovado em: 14 de setembro de 2026.