REDICI
Revista de Difusión Innovadora de la Ciencia e Investigación Mexicana

REVISTA DE DIFUSIÓN INNOVADORA DE LA CIENCIA E INVESTIGACIÓN MEXICANA

Las matemáticas detrás de la criptografía y buenas prácticas asimétricas

The mathematics behind cryptography and asymmetric best practices

Garza-Aguilar, Pedro Alejandro
0009-0001-1977-3682
TECNM-Instituto Tecnológico de la Laguna
México

Resumen

La criptografía es un elemento esencial para proteger la información en la era digital, ya que resguarda transacciones, comunicaciones y datos sensibles. El artículo analiza la evolución y fundamentos matemáticos de la criptografía asimétrica, explicando cómo su aparición resolvió el histórico problema del intercambio seguro de claves que afectaba a los sistemas simétricos. Conceptos como RSA, (Diffie & Hellman, 1976) y la Criptografía de Curva Elíptica (ECC) se describen como pilares tecnológicos que permiten cifrado, autenticación y firma digital mediante el uso de pares de claves vinculadas matemáticamente. Asimismo, se presenta la eficiencia de ECC frente a RSA, así como el uso de esquemas híbridos que combinan cifrado simétrico y asimétrico para optimizar seguridad y rendimiento. El texto también identifica vulnerabilidades derivadas de implementaciones deficientes, como el uso inapropiado de padding en RSA o la mala gestión del valor aleatorio en algoritmos de firma, destacando que la seguridad depende tanto de las matemáticas como de las buenas prácticas. Finalmente, se aborda la amenaza que representa la computación cuántica, capaz de romper los sistemas actuales mediante el algoritmo de Shor (1997) lo que impulsa el desarrollo de la criptografía post-cuántica. Este panorama exige nuevas soluciones, estandarización internacional y la formación de profesionales capaces de enfrentar los retos de seguridad emergentes.

Palabras clave: Criptografía, Computación Cuántica, Algoritmos Matemáticos, Cifrado Asimétrico, Algoritmos De Cifrado.

Abstract

Cryptography is an essential element for protecting information in the digital age, as it safeguards transactions, communications, and sensitive data. The article analyzes the evolution and mathematical foundations of asymmetric cryptography, explaining how its emergence solved the historic problem of secure key exchange that affected symmetric systems.

Concepts such as RSA, (Diffie & Hellman, 1976), and Elliptic Curve Cryptography (ECC) are described as technological pillars that enable encryption, authentication, and digital signatures through the use of mathematically linked key pairs. Likewise, the efficiency of ECC compared to RSA is presented, as well as the use of hybrid schemes that combine symmetric and asymmetric encryption to optimize security and performance.

The text also identifies vulnerabilities derived from poor implementations, such as the improper use of padding in RSA or the poor management of the random value in signature algorithms, emphasizing that security depends not only on mathematics but also on good practices. Finally, the threat posed by quantum computing is addressed, as it is capable of breaking current systems through Shor's algorithm (1997), which is driving the development of post-quantum cryptography. This landscape demands new solutions, international standardization, and the training of professionals capable of facing emerging security challenges.

Keywords: Cryptography, Quantum Computing, Mathematical Algorithms, Asymmetric Encryption, Encryption Algorithms

Introducción

En la era digital, la información se ha convertido en uno de los recursos más valiosos de la sociedad contemporánea. Desde transacciones financieras e historiales médicos hasta comunicaciones privadas y secretos de Estado, la protección de los datos es esencial para garantizar la confianza y la estabilidad digital. La criptografía constituye la disciplina que resguarda esta información, y las matemáticas son su fundamento principal. Algoritmos como RSA y Diffie-Hellman, basados en principios matemáticos avanzados, resultan indispensables para la seguridad de las comunicaciones actuales y futuras (Rashmi, 2024; Torres et al., 2021, p. 1). En particular, la factorización de números primos desempeña un papel crucial en sistemas criptográficos como RSA, asegurando la confidencialidad y autenticidad de la información digital (Souza et al., 2025, p. 1).

Durante siglos, un problema clave limitó la efectividad de los sistemas de cifrado: el intercambio seguro de la clave secreta. Se asemeja a enviar un candado junto con un mensaje cifrado, pero necesitar transmitir también la llave por un canal inseguro para que el destinatario pueda abrirlo. Esta vulnerabilidad inherente a la distribución de claves simétricas reveló la necesidad urgente de mecanismos que permitieran comunicarse de forma segura sin compartir previamente un secreto común, desafío que condujo al surgimiento de la criptografía asimétrica (Mavroeidis et al., 2018, p. 1).

Si un espía interceptaba la llave secreta, todos los mensajes pasados y futuros quedaban comprometidos. Este era el talón de Aquiles de la criptografía simétrica, donde la misma clave se emplea para cifrar y descifrar la información. Esta vulnerabilidad evidenció la necesidad crítica de desarrollar métodos criptográficos capaces de permitir una comunicación segura sin depender de secretos previamente compartidos, lo que abrió el camino hacia la criptografía asimétrica (Morić et al., 2024, p. 60).

Este desafío logístico, conocido como el problema de la distribución de claves, limitaba la seguridad a pequeñas redes y hacía inviable la comunicación protegida entre personas u organizaciones que no hubieran establecido previamente una relación de confianza. La verdadera revolución ocurrió en la década de 1970 con el surgimiento de la criptografía asimétrica o de clave pública, un paradigma que rompió con milenios de tradición criptográfica.

La propuesta innovadora de Diffie & Hellman (1976) introdujo el uso de dos claves distintas: una clave pública para cifrar y una clave privada para descifrar, eliminando así la necesidad de compartir un secreto con anterioridad y transformando por completo la comunicación segura (Clarisse, 2021, p. 8; Housni, 2018, p. 3). Dos años después, Rivest et al. (1978) desarrollaron el primer criptosistema práctico de clave pública, consolidando los cimientos de la seguridad digital moderna (Georgieva, 2013, p. 59).

Su relevancia es absoluta: constituye la tecnología invisible que posibilita el comercio electrónico, protege la privacidad en internet, autentica identidades en línea y sostiene la infraestructura crítica de naciones enteras. Sin ella, servicios como la banca en línea, las videollamadas seguras o el almacenamiento en la nube serían simplemente impensables. El cambio fundamental introducido por la criptografía asimétrica donde cada usuario posee un par de claves matemáticamente vinculadas, una pública para cifrar y otra privada para descifrar revolucionó la comunicación segura al hacer computacionalmente inviable deducir la clave privada a partir de la pública (Chávez & Henríquez, 2021; Simmons, 1979).

Comprender su funcionamiento, sus fortalezas y, especialmente, sus vulnerabilidades no es solo un ejercicio académico, sino una condición necesaria para sostener la confianza en el ecosistema digital interconectado del siglo XXI. El origen de esta tecnología, conocida también como criptografía de clave pública, suele atribuirse a Whitfield Diffie y Martin Hellman, quienes en 1976 sentaron las bases de su desarrollo conceptual (Banerjee, 2024, p. 610; Marrez, 2019, p. 9; Neppolian & Kumar, 2025, p. 90).

Este conocimiento adquiere aún mayor urgencia ante la inminente llegada de la computación cuántica, una tecnología que promete redefinir los límites de lo computable y que amenaza con quebrar los fundamentos matemáticos sobre los cuales se sostiene la seguridad digital contemporánea. El trabajo pionero de (Diffie & Hellman, 1976) introdujo el concepto de la criptografía de clave pública, transformando radicalmente el panorama de la comunicación segura al permitir intercambios confiables sin la necesidad de un secreto previo compartido (Razeghi et al., 2024, p. 6).

La criptografía asimétrica resuelve el problema de la distribución de claves mediante una idea ingeniosa: emplear un par de claves matemáticamente vinculadas, pero de tal forma que una no pueda derivarse de la otra mediante métodos computacionales prácticos. Este sistema permite que cualquier persona cifre un mensaje utilizando una clave pública disponible, mientras que solo el poseedor de la clave privada correspondiente puede descifrarlo, garantizando la confidencialidad (Diffie, 1988).

Cada usuario genera un conjunto compuesto por una clave pública, que puede compartirse libremente como si fuera un número de teléfono publicado en un directorio, y una clave privada, que debe mantenerse en secreto, semejante a la combinación de una caja fuerte. Esta dualidad permite establecer canales de comunicación seguros incluso cuando no existe un medio confidencial previo, resolviendo de manera efectiva los desafíos de gestión de claves inherentes a la criptografía simétrica (Nitulescu, 2019, p. 20; Winn, 2022, p. 270).
La esencia de la criptografía asimétrica radica en que lo cifrado con la clave pública solo puede ser descifrado por la clave privada correspondiente. A la inversa, los datos firmados con la clave privada pueden autenticarse mediante la clave pública, lo que garantiza la integridad del mensaje y evita el repudio de su autoría (Stanišić et al., 2024, p. 365). Los fundamentos matemáticos de estos sistemas se apoyan en funciones unidireccionales con trampa (trapdoor one-way functions), operaciones que son computacionalmente sencillas en una dirección, pero extraordinariamente complejas de revertir sin disponer de la información secreta conocida como trapdoor (Yoon et al., 2023, p. 1).

El algoritmo RSA, uno de los más antiguos y ampliamente utilizados, se basa en la dificultad de factorizar números enteros grandes. Multiplicar dos números primos enormes es una tarea trivial para cualquier computadora, pero realizar la operación inversa, es decir, encontrar los factores primos originales a partir del producto resulta impracticable para los sistemas clásicos actuales. Esta asimetría computacional constituye la base de la seguridad de RSA, donde la clave pública se obtiene del producto de dichos primos, mientras que la clave privada depende del conocimiento exclusivo de esos factores (Tolba, 2024, p. 22).

Otro pilar criptográfico es el problema del logaritmo discreto, que sustenta tanto el protocolo de intercambio de claves de (Diffie & Hellman, 1976) como su evolución moderna: la Criptografía de Curva Elíptica (ECC). Esta última aprovecha las propiedades de las curvas elípticas sobre campos finitos para ofrecer niveles de seguridad equivalentes a RSA, pero con claves más pequeñas y tiempos de procesamiento significativamente más rápidos (Dorin & Montenegro, 2024, p. 88).

ECC ofrece el mismo nivel de seguridad que RSA, pero con claves considerablemente más cortas; por ejemplo, una clave ECC de 256 bits proporciona una seguridad comparable a una clave RSA de 3072 bits, lo que la convierte en una opción ideal para dispositivos con recursos limitados, como tarjetas inteligentes y sensores IoT. Esta eficiencia hace que ECC sea especialmente adecuada para aplicaciones que requieren alta seguridad en entornos con restricciones computacionales (Sahu & Mazumdar, 2024, p. 4).

En la práctica, la criptografía asimétrica rara vez se emplea para cifrar grandes volúmenes de información debido a su elevado costo computacional. Por ello, se recurre a esquemas híbridos. Cuando se inicia una comunicación segura como sucede al acceder a un sitio web mediante HTTPS el navegador y el servidor utilizan criptografía asimétrica (como RSA o ECDH) para autenticarse mutuamente y acordar una clave de sesión simétrica de forma segura. Una vez establecida dicha clave, el sistema cambia a un algoritmo simétrico como AES, mucho más eficiente, para cifrar el resto del tráfico. Este enfoque híbrido combina las fortalezas de ambos mundos: la seguridad del intercambio inicial mediante criptografía asimétrica y la velocidad de la criptografía simétrica para la protección masiva de datos.

La seguridad esencial de ECC radica en la dificultad matemática del Elliptic Curve Discrete Logarithm Problem (ECDLP), un problema significativamente más complejo que el logaritmo discreto en campos finitos o la factorización de enteros, especialmente cuando se comparan claves de tamaños equivalentes (Alkhudhayr et al., 2021). Esta intratabilidad computacional permite que ECC ofrezca una seguridad robusta con longitudes de clave mucho menores que otros criptosistemas de clave pública como RSA, lo que la convierte en una herramienta altamente eficiente para una amplia variedad de aplicaciones (Sabbry & Левина, 2025; Tanksale, 2024).

El análisis de la criptografía asimétrica revela hallazgos críticos que trascienden su solidez teórica y se adentran en los desafíos reales de su implementación práctica. En primer lugar, se confirma que la principal fuente de vulnerabilidades no proviene de los algoritmos en sí como RSA o ECDSA, sino de la brecha entre su diseño matemático y su aplicación correcta. Cuando son implementados de manera inapropiada, incluso algoritmos robustos pueden volverse inseguros.

Un ejemplo emblemático es el RSA de libro de texto: al omitir esquemas de relleno estandarizados, como los definidos en PKCS #1, queda expuesto a múltiples ataques criptoanalíticos. De forma similar, en algoritmos de firma como DSA y ECDSA, la reutilización o la generación predecible del valor aleatorio interno (k) permite a un atacante calcular la clave privada en segundos. Esto demuestra que la seguridad no reside únicamente en la teoría matemática, sino también en la correcta implementación de estándares y en la calidad de las fuentes de aleatoriedad, como las definidas en el NIST SP 800-90A.

En segundo lugar, la revisión confirma la tendencia consolidada hacia la Criptografía de Curva Elíptica (ECC), impulsada por su mayor eficiencia. Las comparaciones de longitud de clave para niveles equivalentes de seguridad muestran una ventaja contundente a favor de ECC, lo que se traduce en certificados digitales más compactos, menor consumo de ancho de banda y operaciones significativamente más rápidas, especialmente para dispositivos con hardware limitado.

El hallazgo más trascendental, sin embargo, es la vulnerabilidad fundamental que comparten todos estos sistemas frente a la computación cuántica. Con el algoritmo de Shor (1977) formulado en 1994, se demostró que una computadora cuántica suficientemente potente podría resolver la factorización de enteros y el logaritmo discreto en tiempo polinomial, comprometiendo así RSA, (Diffie & Hellman, 1976) y ECC. Aunque hoy no existe una máquina cuántica capaz de ejecutar estas operaciones a la escala necesaria, la amenaza es real y ha impulsado una carrera global por desarrollar y estandarizar la Criptografía Post-Cuántica (PQC).

Este esfuerzo, liderado por el NIST, busca algoritmos resistentes tanto a ataques clásicos como cuánticos. Sin embargo, la fragilidad de este campo emergente quedó patente con el colapso abrupto del candidato SIKE en 2023, un esquema inicialmente prometedor cuya ruptura rápida subraya la necesidad de un escrutinio riguroso antes de su adopción generalizada.

Conclusión

El impacto de la criptografía asimétrica es ubicuo y constituye la columna vertebral de la confianza digital contemporánea. Sus aplicaciones más relevantes incluyen el protocolo TLS/SSL, que protege las conexiones HTTPS y posibilita el comercio electrónico seguro; la Infraestructura de Clave Pública (PKI), responsable de gestionar los certificados digitales X.509 que autentican sitios web y entidades; y las firmas digitales, esenciales para otorgar validez legal a contratos, historiales clínicos y diversos documentos electrónicos. Asimismo, resulta indispensable para el acceso seguro a redes privadas (VPN), la mensajería cifrada y tecnologías emergentes como blockchain. Sin estos mecanismos, la economía digital global simplemente no podría sostenerse.

No obstante, este ecosistema de confianza enfrenta un desafío sin precedentes: la transición hacia la criptografía post-cuántica. La migración no se limitará a sustituir algoritmos; implicará un proceso de actualización masiva que afectará a miles de millones de dispositivos, protocolos y sistemas heredados que conforman la infraestructura crítica del mundo digital.

El desafío no radica únicamente en adoptar nuevos estándares PQC como los basados en retículos (LWE) o los esquemas de firma hash como SPHINCS+, sino en formar profesionales capaces de comprender y aplicar estos enfoques matemáticos radicalmente distintos.

La reflexión final es contundente: la seguridad no es un producto estático, sino un proceso dinámico. La criptografía asimétrica clásica ha ofrecido décadas de estabilidad, pero su ciclo de vida se acerca a su límite. El futuro exige una cultura de resiliencia y adaptación constante, sustentada en educación especializada, auditorías rigurosas y una anticipación sistemática a las amenazas emergentes. La próxima era de la seguridad digital no dependerá únicamente de algoritmos más complejos, sino de una comprensión profunda y una aplicación cuidadosa de los principios criptográficos, asegurando que la confianza el recurso más frágil en el entorno digital pueda perdurar en la era cuántica y más allá.

Referencias

Alkhudhayr, F., Moulahi, T., & Alabdulatif, A. (2021). Evaluation Study of Elliptic Curve Cryptography Scalar Multiplication on Raspberry Pi4. International Journal of Advanced Computer Science and Applications, 12(9). https://doi.org/10.14569/ijacsa.2021.0120954

Banerjee, S. (2024). Exploring Cryptographic Algorithms: Techniques, Applications, and Innovations. International Journal of Advanced Research in Science Communication and Technology, 607. https://doi.org/10.48175/ijarsct-18097

Chávez, M. A., & Henríquez, F. R. (2021). Post-Quantum Digital Signature for the Mexican Digital Invoices by Internet. Computación y Sistemas, 25(4). https://doi.org/10.13053/cys-25-4-4048

Clarisse, R. (2021). Elliptic curve design and applications. HAL (Le Centre Pour La Communication Scientifique Directe). https://hal.science/tel-03506116

Diffie, W. (1988). The first ten years of public-key cryptography. Proceedings of the IEEE, 76(5), 560. https://doi.org/10.1109/5.4442

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dorin, M., & Montenegro, S. (2024). Pruebas de cifrado asimétrico en un Laboratorio de Hacking Sostenible. Interfases, 19, 77. https://doi.org/10.26439/interfases2024.n19.7058

Georgieva, M. (2013). Probabilistic analysis of reduced cryptographic Euclidean networks. HAL (Le Centre Pour La Communication Scientifique Directe). https://hal.science/tel-01081679

Housni, Y. E. (2018). Introduction to the Mathematical Foundations of Elliptic Curve Cryptography. HAL (Le Centre Pour La Communication Scientifique Directe). https://hal.archives-ouvertes.fr/hal-01914807

Marrez, J. (2019). Representations adapted to modular arithmetic and fuzzy system resolution. HAL (Le Centre Pour La Communication Scientifique Directe). https://tel.archives-

ouvertes.fr/tel-03359401

Mavroeidis, V., Vishi, K., Mateusz, D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/ijacsa.2018.090354

Morić, Z., Milovec, M., & Petrunić, R. (2024). Application of Quantum Cryptography in Securing Network Communications. In Annals of DAAAM for ... & proceedings of the ... International DAAAM Symposium (p. 55). DAAAM International Vienna. https://doi.org/10.2507/35th.daaam.proceedings.008

Neppolian, K., & Kumar, M. (2025). Applying Public Key Cryptography to Enhance Content Protection in Maritime Logistics and E-Commerce. Journal of Internet Services and Information Security, 15(2), 88. https://doi.org/10.58346/jisis.2025.i2.007

Nitulescu, A. (2019). Un recueil de SNARKs : sécurité quantique, extractabilité et confidentialité des données. HAL (Le Centre Pour La Communication Scientifique Directe). https://theses.hal.science/tel-02129544

Rashmi, S. (2024). Advances in Cryptographic Algorithms: The Mathematics behind Secure Communication. International Journal for Research in Applied Science and Engineering Technology, 12(12), 1674. https://doi.org/10.22214/ijraset.2024.66102

Razeghi, B., Rahimi, P., & Marcel, S. (2024). Deep Privacy Funnel Model: From a Discriminative to a Generative Approach with an Application to Face Recognition. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2404.02696

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342

Sabbry, N. H., & Левина, А. (2025). An optimized elliptic curve digital signature strategy for resource-constrained devices. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-05601-0

Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. Frontiers in Physics, 12. https://doi.org/10.3389/fphy.2024.1456491

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Simmons, G. J. (1979). Symmetric and Asymmetric Encryption [Review of Symmetric and Asymmetric Encryption]. ACM Computing Surveys, 11(4), 305. Association for Computing Machinery. https://doi.org/10.1145/356789.356793

Souza, E. R. L. de, Silva, M. M. da S. M., Xavier, N., & Brandão, O. (2025). Teoria dos números e aplicações criptográficas: A fatoração de primos na segurança digital. Research Society and Development, 14(10). https://doi.org/10.33448/rsd-v14i10.49705

Stanišić, S., Stojanović, H., & Đorđević, I. (2024). The utilization of Solidity programming language in blockchain. Vojnotehnicki Glasnik, 72(1), 363. https://doi.org/10.5937/vojtehg72-47942

Tanksale, V. (2024). Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices. Electronics, 13(18), 3631. https://doi.org/10.3390/electronics13183631

Tolba, Z. (2024). Cryptanalysis and improvement of multimodal data encryption by machine-learning-based system. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2402.15779

Torres, N. N., Carlos, J., & Alexis, E. (2021). Systems Security Affectation with the Implementation of Quantum Computing. International Journal of Advanced Computer Science and Applications, 12(4). https://doi.org/10.14569/ijacsa.2021.0120405

Winn, J. K. (2022). Couriers Without Luggage: Negotiable Instruments and Digital Signatures. In Routledge eBooks (p. 245). Informa. https://doi.org/10.4324/9781315193939-9

Yoon, C. S., Hong, C. H., Kang, M. S., Choi, J.-W., & Yang, H. J. (2023). Quantum asymmetric key crypto scheme using Grover iteration. Scientific Reports, 13(1). https://doi.org/10.1038/s41598-023-30860-0

Financiación

El presente artículo no cuenta con financiación específica para su desarrollo y/o publicación.

Conflicto de interés

Los autores del artículo declaran no tener ningún conflicto de intereses en su realización.

Contribución de autoría

Declaración uso de IA

Los autores declaran uso de IA y supervisión humana en cada proceso

SI	*Propósito principal*
X	*Generación de texto o contenido escrito*
X	*Corrección gramatical y ortográfica*
NA	*Creación de gráficos, tablas o visualizaciones*
NA	*Apoyo en estructura o formato de la obra*
NA	*Investigación bibliográfica o recopilación de referencias bibliográficas*
NA	*Diseño o perfeccionamiento metodológico*
NA	*Redacción o construcción del estado del arte*
NA	*Depuración, diagnóstico y análisis de datos*

Recepción 20 dic 2025
Revisión 02 ene 2025
Aceptación 27 ene 2026