https://repository.uaeh.edu.mx/revistas/index.php/prepa3/issue/archive

Con-Ciencia Boletín Científico de la Escuela Preparatoria No. 3

Publicación semestral, Vol. 12, No. 24 (2025) 73-78

CON - CIENCIA

ISSN: 2007-7653

La criptografía y el poder de los números primos en la seguridad digital

Cryptography and the power of prime numbers in digital security

Olivia Vázquez-Bautista [a]

Abstract:

In the digital age, information security is essential to ensure the confidentiality, integrity, and authentication of data in online communications and transactions. This article explores the fundamental role of cryptography, focusing on the use of prime numbers in encryption. Through a review of basic concepts, the history and development of algorithms such as RSA, it demonstrates how the mathematical properties of prime numbers underpin the security infrastructure of the Internet. Emerging challenges, such as quantum computing, are also analyzed, and future directions for the evolution of cryptography are proposed. Finally, this article also addresses the importance of education and society in general being informed about Internet security.

Keywords:

Cryptography, security, internet, numbers, primes, RSA

Resumen:

En la era digital, la seguridad de la información es esencial para garantizar la confidencialidad, integridad y autenticación de datos en comunicaciones y transacciones en línea. Este artículo explora el papel fundamental de la criptografía, enfocándose en el uso de números primos en la encriptación. A través de un recorrido por conceptos básicos, la historia y el desarrollo de algoritmos como RSA, se demuestra cómo las propiedades matemáticas de los números primos sostienen la infraestructura de seguridad en internet. Además, se analizan los desafíos emergentes, como la computación cuántica, y se proponen líneas futuras en la evolución de la criptografía. Y por último, este artículo también hace referencia a la importancia de que en la educación y en la sociedad en general esté informada sobre la seguridad en internet.

***Palabras Clave**:*

Criptografía, seguridad, internet, números, primos, RSA

Introducción

Vivimos en un mundo hiperconectado donde la información viaja constantemente a través de redes digitales; desde enviar mensajes instantáneos en WhatsApp hasta efectuar compras y transferencias bancarias en línea.

Esta interconexión global ha transformado la manera en que se comparte la información, haciendo imperativo proteger los datos personales y financieros de posibles intrusiones. Actualmente la seguridad de nuestros datos depende de una rama de las matemáticas conocida como **criptografía**.

La criptografía, es el arte y la ciencia de cifrar y descifrar información de manera segura; mediante técnicas matemáticas, se basa en principios matemáticos. Entre los conceptos fundamentales que sustentan muchos de los sistemas criptográficos modernos, está el uso de los **números primos**, que son la base de los sistemas de encriptación como RSA (Rivest-Shamir-Adleman). De esta forma, la criptografía se ha convertido en la piedra angular de la seguridad en internet.

En este artículo profundizaremos en los fundamentos históricos y matemáticos que han permitido la evolución de la criptografía, también analizaremos en detalle el funcionamiento del algoritmo RSA y examinaremos las aplicaciones prácticas de estos sistemas en la vida cotidiana. Además, analizaremos los desafíos

[a] Olivia Vázquez-Bautista, Universidad Autónoma del Estado de Hidalgo | Escuela Preparatoria Numero 3 | Pachuca | Pachuca de Soto, Hidalgo | México, https://orcid.org/0000-0002-5978-7608. Email: olivia_vazquez@uaeh.edu.mx

Fecha de recepción: 21/03/2025, Fecha de aceptación: 28/04/2025, Fecha de publicación: 05/07/2025

DOI: https://doi.org/10.29057/prepa3.v12i24.14779

emergentes, especialmente en el contexto de la computación cuántica, y se exploran las perspectivas futuras en la búsqueda de nuevos métodos criptográficos que garanticen la seguridad digital en un mundo en constante cambio.de manera comprensible y detallada, cómo las matemáticas, especialmente a través del uso de números primos, han permitido desarrollar sistemas de encriptación robustos que resguardan la información en las redes digitales. Y por último, abordaremos la importancia de informar sobre la seguridad digital en la educación y a la sociedad en general.

La importancia de este tema radica en la necesidad de comprender las bases matemáticas que hacen posible que, nuestros datos se mantengan protegidos, al enviar un mensaje o realizar una transacción,. Conocer estos fundamentos no sólo es relevante para ciertos sectores, sino también para ciudadanos que quieren estar informados en una sociedad digitalizada.

Fundamentos de la Criptografía

La criptografía tiene raíces que se extienden a la antigüedad. Civilizaciones como la egipcia y la romana ya empleaban técnicas sencillas para ocultar mensajes importantes. Por ejemplo, el cifrado César, atribuido a Julio César, consistía en desplazar cada letra del mensaje a un número fijo de posiciones en el alfabeto. Aunque primitivo, este método sentó las bases para la idea de transformar la información de modo que solo quienes conocieran la clave pudieran comprenderla.

Otros ejemplos históricos incluyen el uso de jeroglíficos y códigos secretos en las culturas asiáticas y europeas, donde la necesidad de resguardar información militar y política impulsó el desarrollo de métodos criptográficos más sofisticados.

Así que podemos decir que desde los antiguos jeroglíficos y códigos como el cifrado César, hasta los modernos algoritmos basados en teoría de números, la criptografía ha evolucionado en paralelo con el desarrollo matemático y tecnológico. El surgimiento de la criptografía asimétrica en el siglo XX, en el que destacan el algoritmo RSA, revolucionó la seguridad digital al permitir la comunicación segura sin necesidad de compartir previamente una clave secreta.

¿Qué es la criptografía?

La criptografía es una disciplina que combina técnicas matemáticas, algoritmos y protocolos de seguridad para transformar la información en formatos ilegibles para terceros no autorizados. Su función principal es asegurar [1]:

- **Confidencialidad**: Solo usuarios autorizados pueden leer la información.
- **Integridad**: La información no se altera sin detección.
- **Autenticación**: Verificar la identidad de los comunicantes.
- **No repudio**: Garantizar que el emisor no pueda negar la autoría de un mensaje.

Transición a la criptografía moderna

Con el advenimiento de la era digital, la criptografía experimentó una transformación radical. El desarrollo de la criptografía simétrica en el siglo XX, donde el mismo secreto se utiliza tanto para cifrar como para descifrar mensajes, permitió la comunicación segura en entornos donde la clave se compartía previamente. Sin embargo, la limitación de esta técnica se hizo evidente en situaciones que requerían el intercambio seguro de claves a través de canales inseguros.

La verdadera revolución llegó con la criptografía asimétrica, que permite la generación de un par de claves: una pública y una privada. Este avance, ejemplificado por el algoritmo RSA, eliminó la necesidad de compartir una clave secreta de antemano y abrió el camino para una amplia adopción de la seguridad digital en aplicaciones comerciales y gubernamentales.

Números Primos

Desde Euclides, quien demostró la infinitud de los números primos, hasta matemáticos modernos que han desarrollado algoritmos para la detección de primos (como el test de Miller-Rabin), el estudio de los números primos ha sido fundamental en el avance del conocimiento matemático. La aplicación de estos conceptos en la criptografía se convirtió en una solución natural para resolver el problema de la transmisión segura de información [9].

¿Qué es un número primo?

Un número primo es un entero mayor que 1 que únicamente puede dividirse por 1 y por sí mismo. Algunos ejemplos son 2, 3, 5, 7, 11 y 13. La simplicidad de esta definición esconde propiedades matemáticas profundas que han fascinado a los matemáticos durante siglos.

Propiedades relevantes de los números primos para la criptografía

- **Multiplicación fácil y factorización difícil:** Multiplicar dos números primos es una operación sencilla computacionalmente, mientras que factorizar el producto de dos números primos grandes resulta extremadamente difícil. Esta asimetría es la base del algoritmo RSA.
- **Distribución irregular:** La distribución de números primos entre los enteros es aparentemente aleatoria, lo que contribuye a la complejidad de predecir su aparición.
- **Teorema fundamental de la aritmética:** Todo número entero mayor que 1 se puede expresar de manera única como producto de números primos (salvo el orden de los factores), lo que subraya la importancia de estos números en la estructura de la aritmética.

Herramientas matemáticas para el estudio de los primos

Con el auge de la criptografía, se han desarrollado numerosos algoritmos para la detección y verificación de números primos. Entre ellos se encuentran:

- **El Test de Primalidad de Miller-Rabin:** Un algoritmo probabilístico que, aunque no garantiza una verificación al 100%, es altamente eficiente para determinar si un número es primo con un grado de certeza configurable.
- **El Algoritmo de AKS:** Un test determinista que, pese a ser menos práctico para números extremadamente grandes, ofrece una demostración teórica de la primalidad en tiempo polinomial.
- **Métodos de Criba:** Como la Criba de Eratóstenes, que permite identificar de forma sistemática todos los números primos menores a un cierto límite, siendo útil en aplicaciones donde se requiere la generación de listas de primos para cálculos criptográficos.

Estos métodos no solo potencian la capacidad de construir sistemas seguros, sino que también enriquecen el campo de la teoría de números, ofreciendo caminos para investigaciones futuras en matemáticas y criptografía.

El Algoritmo RSA: Principios y Funcionamiento

El algoritmo RSA, desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, se fundamenta en la asimetría matemática entre la multiplicación y la factorización de números primos. La seguridad de RSA reside en la dificultad computacional que implica factorizar el producto de dos grandes números primos, denominados p y q. Este proceso asimétrico permite la generación de claves públicas y privadas, esenciales para la encriptación y el descifrado de mensajes.[7]

Pasos para la generación de claves [7]

1. **Selección de Dos Números Primos Grandes:** Se eligen dos números primos, p y q, de forma aleatoria y suficientemente grandes para garantizar la seguridad.

2. **Cálculo del Módulo n:** Se multiplica p y q para obtener:
$$n = p\ x\ q$$
Este número n será parte de la clave pública y es utilizado en los procesos de encriptación y desencriptación.

3. **Cálculo del Totiente:** Se determina el totiente de n mediante la fórmula:
$$\varphi(n) = (p - 1)x(q - 1)$$
Este valor es fundamental para el siguiente paso en la generación de claves.

4. **Elección de la Clave Pública e:** Se selecciona un número ee que cumpla con la condición de ser coprimo con $\varphi(n)$; es decir, e y $\varphi(n)$ no comparten factores primos.

5. **Determinación de la Clave Privada d:** Se calcula d como el inverso multiplicativo de e módulo $\varphi(n)$, cumpliendo la ecuación:
$$d\ \times\ e\ \equiv\ 1\ (mod\ \varphi(n))$$

Proceso de Cifrado y Descifrado con RSA

El proceso de encriptación y desencriptación utilizando RSA se lleva a cabo de la siguiente manera:

Cifrado:

Si un usuario desea enviar un mensaje, este se representa como un número M (usualmente mediante un proceso de codificación). El mensaje se cifra aplicando la siguiente operación:

$$C = M^e mod\ n$$

Donde C es el mensaje cifrado.

Descifrado:

El receptor, que posee la clave privada dd, puede recuperar el mensaje original mediante:

$$M = C^d mod\ n$$

Este proceso garantiza que solo la persona con la clave privada (d) pueda descifrar el mensaje, manteniendo la confidencialidad.

Seguridad del RSA y el papel de los números primos

La seguridad del RSA se fundamenta en la dificultad computacional de factorizar n en sus factores primos p y q. Aunque la multiplicación de números primos es computacionalmente eficiente, el proceso inverso, es decir, la factorización de números grandes, se vuelve inabordable con las tecnologías actuales si los primos elegidos son lo suficientemente grandes. Esta “asimetría” matemática es lo que otorga robustez al sistema. Actualmente, los ordenadores más potentes tardarían millones de años en factorizar un número de 300 dígitos en sus factores primos, lo que hace que RSA sea una barrera fuerte contra ataques.

Sin embargo, con la llegada de la computación cuántica, los métodos actuales de encriptación podrían volverse vulnerables. Algoritmos como el de Shor, diseñados para computadoras cuánticas, podrían factorizar números grandes rápidamente, lo que obligaría a desarrollar nuevas técnicas criptográficas.

Aplicaciones prácticas de la criptografía en la vida cotidiana

La criptografía no sólo se usa en el ámbito militar o gubernamental, sino que está presente en nuestra vida cotidiana en [5]:

1. **Comunicación segura**

El cifrado end-to-end utilizado en aplicaciones de mensajería (por ejemplo, WhatsApp y Telegram) se basa en protocolos que emplean algoritmos como RSA y otros métodos de criptografía asimétrica. Esto asegura que solo el emisor y el receptor puedan leer los mensajes intercambiados.

2. **Transacciones bancarias y comercio electrónico**

Cuando realizamos una compra en línea o accedemos a nuestra banca digital, la transmisión de información personal y financiera se realiza mediante protocolos seguros (como SSL/TLS). Estos protocolos dependen en gran medida de técnicas de encriptación para evitar fraudes y garantizar la privacidad de los datos.

3. **Protección de datos y firmas digitales**

Las firmas digitales son otro uso crucial de la criptografía. Permiten verificar la autenticidad de documentos electrónicos y garantizar que no han sido alterados. Al combinar técnicas de hash con algoritmos basados en números primos, se genera un sello digital que es único para cada documento, ofreciendo un alto grado de seguridad.

4. **Redes y comunicaciones gubernamentales**

Los gobiernos y grandes corporaciones utilizan sistemas de encriptación avanzados para proteger comunicaciones sensibles y estratégicas. La robustez de estos sistemas, que se fundamenta en los principios matemáticos expuestos en el RSA, es vital para la seguridad nacional y la protección de la información crítica.

En sí, cada vez que ingresamos a un sitio web con "https://", estamos utilizando criptografía basada en números primos para proteger nuestra información.

Desafíos y el futuro de la seguridad digital

- **La amenaza de la computación cuántica**

La llegada de la computación cuántica plantea un desafío considerable para los algoritmos criptográficos actuales. Algoritmos cuánticos, como el algoritmo de Shor, prometen factorizar números grandes en tiempos mucho menores que los métodos tradicionales. Esto significa que, en un futuro no muy lejano, sistemas como RSA podrían volverse vulnerables.

- **Criptografía post-cuántica**

Ante la amenaza de la computación cuántica, la comunidad científica y tecnológica está desarrollando una nueva generación de algoritmos criptográficos denominados "post-cuánticos". Estos algoritmos buscan ser resistentes a los ataques de ordenadores cuánticos, utilizando estructuras matemáticas alternativas, como:

- ➔ Redes de retículas (lattices), que ofrecen propiedades de complejidad y seguridad difíciles de vulnerar incluso con métodos cuánticos.
- ➔ Códigos de error, que se basan en la teoría de códigos y ofrecen una resistencia robusta ante ataques sofisticados.

La transición hacia la criptografía post-cuántica representa un campo de investigación activo y multidisciplinario, en el que convergen matemáticas, informática y criptografía.

- **Retos en la implementación y normativas**

El avance tecnológico en criptografía plantea no sólo desafíos técnicos, sino también normativos y éticos, que permitan estandarizar y regular los nuevos métodos criptográficos. La adopción global de protocolos post-cuánticos requerirá no sólo innovaciones en el diseño de algoritmos, sino también acuerdos internacionales y actualizaciones en normativas de seguridad digital, como:

- ➔ Cooperación internacional: Para establecer estándares y normativas que aseguren la interoperabilidad de sistemas a nivel mundial.
- ➔ Actualización de políticas: Que aborden las implicaciones de seguridad y privacidad en un entorno digital en constante evolución.
- ➔ Capacitación y educación de profesionales y ciudadanos para comprender y adaptarse a las nuevas tecnologías criptográficas.

Educación, conciencia y el rol de la sociedad en la seguridad digital

Importancia de la formación en criptografía

El conocimiento de los fundamentos matemáticos y tecnológicos que subyacen a la criptografía es esencial no sólo para especialistas, sino también para la ciudadanía en general. La integración de estos temas en programas educativos a nivel secundaria y universitario puede:

- **Fomentar el pensamiento crítico**: Ayudando a los estudiantes a comprender la importancia de la seguridad digital.
- **Promover la innovación:** Al formar a la próxima generación de expertos capaces de desarrollar soluciones de encriptación avanzadas.
- **Concienciar sobre la privacidad**: En un mundo donde la información personal es un activo cada vez más vulnerable.

Iniciativas y talleres de divulgación

Diversos organismos y universidades están impulsando iniciativas, talleres y cursos en línea para difundir el conocimiento sobre criptografía. Estas iniciativas incluyen:

- Seminarios y conferencias internacionales donde expertos en seguridad digital comparten los avances y retos actuales.
- Cursos masivos abiertos en línea (MOOC), que permiten a cualquier interesado profundizar en temas de criptografía y seguridad informática.
- Publicaciones y boletines científicos, que difunden investigaciones y desarrollos tecnológicos en este campo.

La comprensión de los fundamentos matemáticos de la criptografía es crucial para formar profesionales capaces de innovar y mejorar la seguridad en internet. Por ello, la integración de estos temas en la educación a nivel bachillerato y superior es esencial, para crear una nueva generación de expertos en seguridad digital.

El objetivo es construir una sociedad digital más informada y resiliente, en la que los ciudadanos comprendan y valoren la importancia de proteger sus datos.

Conclusión

La criptografía basada en números primos ha demostrado ser un pilar fundamental para la seguridad en internet. Desde la implementación del algoritmo RSA hasta el desarrollo de técnicas emergentes en criptografía post-cuántica, los principios matemáticos que rigen la multiplicación y factorización de números primos han permitido construir barreras efectivas contra el acceso no autorizado a la información en la era digital.

A medida que la tecnología avanza, también lo hacen los métodos de encriptación. La llegada de la computación cuántica podría cambiar las reglas del juego, pero mientras tanto, la criptografía basada en números primos sigue siendo nuestra mejor defensa en el mundo digital.

Referencias

[1] López, M. J. L., Sánchez, J. I. P., Solana, A. M. S., García, J. E. G., & del Moral, P. G. (1996). Criptografía y seguridad en computadores. Universidad de Jaén, Servicio de Publicaciones e Intercambio Científico.

[2] Maiorano, A. (2009). Criptografía: técnicas de desarrollo para profesionales. Alpha Editorial.

[3] Lema Andrango, A. R. (2022). Estudio Introductoria a la Criptografía Cuántica (Bachelor's thesis, Quito: EPN, 2022). Recuperado de: https://bibdigital.epn.edu.ec/handle/15000/23301

[4] Carlos, B. (2007). Bases matemáticas de la criptografía de clave asimétrica: la aritmética modular y la clave RSA. Vector, 59-70.

[5] Delgado, V., & Palacios Hielscher, R. (2006). Aplicaciones prácticas de la criptografía. Recuperado de: https://repositorio.comillas.edu/xmlui/handle/11531/7751

[6] Ramirez, J. C., Huerta, H. V., Rodriguez, C. R., & Bailón, F. E. (2020). Firma digital basada en criptografía asimétrica para generación de historial clínico. 3c Tecnología: glosas de innovación aplicadas a la pyme, 9(4), 65-85.

[7] Joven Sanagustín, M., & Ciria Cosculluela, J. C. Criptografía RSA: Fundamentos y Desarrollo . Recuperado de: https://zaguan.unizar.es/record/47889

[8] Cipriano, M. (2008). Factorización de N: recuperación de factores primos a partir de las claves pública y privada. In XIV Congreso Argentino de Ciencias de la Computación. Recuperado de: https://sedici.unlp.edu.ar/handle/10915/21677

[9] Merayo, F. G. (2005). Secretos de los números primos. Manual formativo de ACTA, (37), 87-97.