

Aplicaciones Básicas de la Criptografía en la Vida Cotidiana

Juan Ezequiel Peña Alvarez
Estudiante Master con énfasis en Ciberseguridad
Universidad San Isidro Labrador
San José, Costa Rica
ezequielpa2004@gmail.com

Resumen — En la actualidad, la criptografía ha dejado de ser una herramienta exclusiva de especialistas en seguridad para convertirse en un componente esencial de las actividades cotidianas. Este artículo explora cómo las aplicaciones criptográficas protegen diversas interacciones diarias, desde la comunicación a través de correos electrónicos hasta la realización de transacciones bancarias en línea. Se examinan las principales técnicas criptográficas utilizadas, como el cifrado de clave simétrica y asimétrica, y cómo estas garantizan la seguridad y privacidad de la información personal en un mundo digitalizado. Además, se analizan casos específicos donde la criptografía ha jugado un papel crucial en la prevención de ataques y en la protección de datos sensibles. El objetivo de este artículo es resaltar la importancia de la criptografía en la vida diaria y proponer recomendaciones para su adopción y mejora continua. Se abordan los retos actuales que enfrenta la criptografía, incluyendo la necesidad de un equilibrio entre seguridad y usabilidad. Concluimos que, en un entorno cada vez más interconectado, la criptografía no solo es una herramienta técnica, sino un elemento clave para la confianza y la seguridad de los usuarios en sus interacciones digitales diarias.

Palabras Claves — *Protección de información, Criptografía en la vida cotidiana, Ciberseguridad, Privacidad en línea.*

Abstract — Nowadays, cryptography has evolved from being an exclusive tool for security specialists to becoming an essential component of everyday activities. This article explores how cryptographic applications protect various daily interactions, from email communication to online banking transactions. The main cryptographic techniques used, such as symmetric and asymmetric key encryption, are

examined, and how they ensure the security and privacy of personal information in a digitized world. Additionally, specific cases are analyzed where cryptography has played a crucial role in preventing attacks and protecting sensitive data. The aim of this article is to highlight the importance of cryptography in daily life and propose recommendations for its continuous adoption and improvement. The current challenges facing cryptography are addressed, including the need to balance security and usability. We conclude that in an increasingly interconnected environment, cryptography is not just a technical tool but a key element for user trust and security in their daily digital interactions.

Keywords — *Information protection, Cryptography in everyday life, Cybersecurity, Online privacy.*

I. INTRODUCCIÓN

La criptografía, una vez considerada un campo especializado de la seguridad informática, ha pasado a formar parte integral de nuestra vida diaria. Hoy en día, dependemos de técnicas criptográficas para proteger una variedad de actividades cotidianas, desde enviar un correo electrónico hasta realizar una compra en línea. A medida que nuestras vidas se digitalizan más, la criptografía garantiza la privacidad y la integridad de la información personal. Este artículo tiene como objetivo analizar las principales aplicaciones criptográficas que encontramos en nuestras actividades diarias, incluyendo el cifrado de datos en transacciones bancarias y la protección de la información en redes sociales. También se abordarán los desafíos actuales y las posibles mejoras en la implementación de la criptografía. En última instancia, este estudio subraya la importancia de la criptografía no solo como una

herramienta técnica, sino como un componente esencial para la confianza y seguridad en la vida digital moderna.

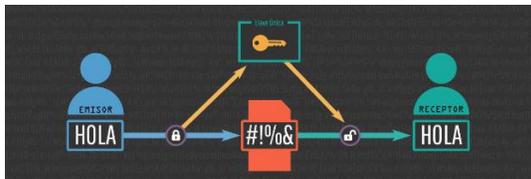
II. ANTECEDENTES

La criptografía, cuya historia se remonta a tiempos antiguos, ha sido un componente vital en la protección de información sensible. Uno de los primeros ejemplos es el cifrado César, utilizado por Julio César para enviar mensajes militares cifrados. Durante la Segunda Guerra Mundial, la criptografía alcanzó un punto culminante con la máquina Enigma, que fue utilizada por las fuerzas alemanas para proteger sus comunicaciones. Sin embargo, el verdadero avance de la criptografía se produjo en la era moderna con la invención del cifrado asimétrico, como el algoritmo RSA en 1977, que revolucionó la forma en que se protege la información digital.

Hoy en día, la criptografía se divide en dos categorías principales: cifrado simétrico y cifrado asimétrico. El cifrado simétrico utiliza la misma clave para cifrar y descifrar datos, con ejemplos notables como DES y AES, este último ampliamente utilizado en la protección de datos sensibles. Por otro lado, el cifrado asimétrico utiliza un par de claves (pública y privada), y es fundamental para la seguridad en internet, permitiendo la protección de las transacciones en línea mediante protocolos como SSL/TLS.

La integración de la criptografía en la vida cotidiana es evidente en aplicaciones como el correo electrónico cifrado, las transacciones bancarias seguras, y la protección de la información en redes sociales. Estos avances no solo han garantizado la seguridad de la información, sino que también han permitido la expansión de las interacciones digitales de manera segura y confiable.

Figura 1: Utilizada como apoyo, descripción visual.



Fuente:

<https://nic.ar/index.php/es/enterate/novedades/que-es-criptografia>

En la Figura 1, La imagen muestra el proceso de cifrado simétrico: un "Emisor" envía el mensaje "HOLA," que se cifra en caracteres aleatorios usando una "Llave Única." El "Receptor," con la misma llave, descifra el mensaje para recuperarlo. Esto asegura la comunicación segura entre emisor y receptor mediante una clave compartida.

III. APLICACIONES PRINCIPALES

1. Cifrado de Correos Electrónicos

La criptografía protege el contenido de los correos electrónicos, asegurando que solo el destinatario pueda acceder a la información. Herramientas como PGP y S/MIME son ampliamente utilizadas para este propósito, garantizando la privacidad y la autenticidad del mensaje.

2. Transacciones Bancarias en Línea

Las transacciones en línea dependen de la criptografía para proteger los datos financieros. Protocolos como SSL/TLS cifran la información transmitida, asegurando que los datos sensibles, como números de tarjetas de crédito, estén protegidos contra el acceso no autorizado.

3. Protección de Datos en Redes Sociales

Las redes sociales utilizan criptografía para proteger la información personal de los usuarios. El cifrado de extremo a extremo en aplicaciones de mensajería y el cifrado de datos en reposo son fundamentales para garantizar que la información compartida esté segura.

4. Almacenamiento Seguro de Datos Personales

La criptografía asegura el almacenamiento de datos en dispositivos y servicios en la nube. Herramientas como el cifrado de discos y el cifrado de archivos protegen la información personal en caso de pérdida o robo del dispositivo.

IV. PRACTICA

La importancia de la práctica para entender la criptografía, enfatizando cómo la aplicación práctica de los conceptos teóricos ayuda a consolidar el conocimiento y prepararse para desafíos reales.

1. Creación Llave Criptográfica mensaje cifrado

En este apartado vamos a crear un mensaje y una llave criptográfica, y lograr entender lo fácil que

son las Aplicaciones Básicas de la Criptografía en la Vida Cotidiana, mediante algunas figuras se va a reflejar un mensaje, pero solo las persona que obtenga la llave criptográfica tendrá acceso a esta información.

Figura 2: Utilizada como llave criptográfica.

ABC	DEF	GHI
JKL	MNÑ	OPQ
RST	UVW	XYZ

Fuente: Elaboración Propia

En la Figura 2, la imagen muestra la llave criptográfica para lograr resolver los mensajes que envía el Emisor, se utiliza el juego clásico conocido como “gato” en el cual cada cuadrante tiene un valor en letra.

Figura 3: Utilizada como primer mensaje, cifrado.



Fuente: Elaboración Propia

En la Figura 3, la imagen muestra el primer mensaje, como receptor ciframos el mensaje de la siguiente forma, en cuestión buscamos el primero símbolo esto muestra que el valor es la letra “T”, el segundo símbolo es la letra “E”, el tercer símbolo es la letra “A”, el cuarto símbolo es la letra “M”, el quinto símbolo en la letra “O”, la palabra cifrada es “TE AMO”.

Figura 4: Utilizada como ejemplo, sin estar cifrado.

HOLA



Fuente: Elaboración Propia

En la Figura 4, la imagen muestra, otro ejemplo de un mensaje correctamente cifrado.

V. CONCLUSIONES

Crear una llave criptográfica puede parecer una tarea compleja, pero en realidad es un proceso relativamente sencillo con las herramientas adecuadas. La generación de una clave ya sea para cifrado simétrico o asimétrico, se puede lograr en pocos pasos y proporciona una poderosa herramienta para proteger la información. Sin embargo, es crucial recordar que, si un intruso logra descifrar esta llave, toda la información protegida se vuelve vulnerable. Por ello, la seguridad de la clave es tan importante como su creación. Insto a todos a experimentar creando sus propias llaves criptográficas y a comprender cómo funcionan en la práctica, ya que esto no solo fortalece su conocimiento, sino también su capacidad para proteger su información personal. Las llaves criptográficas juegan un papel esencial en la vida cotidiana, desde asegurar nuestras comunicaciones hasta proteger nuestras transacciones financieras, y es vital que todos entendamos su importancia para mantenernos seguros en un mundo digital cada vez más interconectado.

REFERENCIAS

- [1] Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education. ISBN: 9780134444284.
- [2] Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). Wiley. ISBN: 9781119096726.
- [3] National Institute of Standards and Technology (NIST). (2020). *Cryptographic Standards and Guidelines*. Retrieved from <https://www.nist.gov/programs-projects/cryptographic-standards-and-guidelines>
- [4] SpringerLink. (2023). *Cryptography in Everyday Life*. Retrieved from <https://link.springer.com/>

- [5] Krebs, B. (2023). Krebs on Security Blog. Retrieved from <https://krebsonsecurity.com/>
- [6] IEEE. (2023). Cryptography and Network Security [Online]. Available: <https://ieeexplore.ieee.org/>
- [7] Dark Reading. (2023). Cryptography in Business Security. Retrieved from <https://www.darkreading.com/>
- [8] RSA Conference. (2023). Cryptography Trends in Information Security [Conference]. Retrieved from <https://www.rsaconference.com/>