Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20250402030
Volume 4, Issue2 (May-August 2025), PP: 224-226.
www.indjcst.com
ISSN No: 2583-5300

The Everyday Role of Cryptography: Securing Digital Life through Encryption and Authentication

Dr. Mohammed Iliyas
Faculty, Department of Computer Science, Adikavi Sri Maharshi Valmiki University, Raichur, Karnataka, India.

To Cite this Article: *Dr. Mohammed Iliyas, "The Everyday Role of Cryptography: Securing Digital Life through Encryption and Authentication", Indian Journal of Computer Science and Technology, Volume 04, Issue 02 (May-August 2025), PP: 224-226.*

Abstract: *Cryptography plays a crucial role in ensuring the confidentiality, integrity, and authenticity of information in everyday life. The paper explores the application of cryptographic techniques in common digital interactions, focusing on online banking, secure communications, and e-commerce transactions. By analysing the implementation of encryption protocols such as (Secure Sockets Layer / Transport Layer Security) SSL/TLS, and the use of public-key infrastructure (PKI) in digital signatures and certificates, this study demonstrates how cryptography secures sensitive user data against cyber threats. The study highlights the role of end-to-end encryption in messaging apps and the increasing reliance on cryptographic algorithms in mobile payment systems. Additionally, the study examines the practical use of cryptographic hash functions in password storage and block chain technologies. Through real-world scenarios, the paper illustrates the seamless integration of cryptographic tools into devices and platforms that individuals use daily, often without explicit awareness. The findings underscore the importance of robust cryptographic standards and user education in enhancing digital security through authentications. As cyber risks continue to evolve, the continued advancement and widespread application of cryptography remain essential for protecting privacy and trust in the digital age.*

Key Words: *Cryptography, Encryption, Digital Security, Authentications, Public-Key Infrastructure, Hash Functions.*

I.INTRODUCTION

In the digital age, the security of information is paramount. As individuals increasingly rely on technology for banking, communication, shopping, and social interaction, the risk of data breaches, identity theft, and cyber-attacks has grown significantly. Cryptography, the science of secure communication, serves as the backbone of modern information security systems, offering mechanisms to protect data from unauthorized access, manipulation, and misuse. From protecting passwords and personal data to securing national infrastructures, cryptographic technologies are embedded in nearly every aspect of our digital lives.

The primary objective of this study is to explore the application of cryptography in everyday digital interactions, with a focus on how ordinary users benefit from complex cryptographic mechanisms without necessarily understanding their underlying technical details. Specifically, the paper aims to:

1. Identify and analyse the cryptographic techniques used in online banking, messaging, and e-commerce.
2. Evaluate how cryptography contributes to data security, privacy, and trust in these contexts.
3. Demonstrate the effectiveness of cryptographic implementations in real-world scenarios.
4. Highlight potential challenges and limitations associated with the use of cryptography in everyday applications.

This involves a qualitative examination of cryptographic applications in three widely used domains: online banking, secure messaging applications, and e-commerce platforms. Data has been collected through a combination of document analysis, review of publicly available security protocols, and evaluation of platform-specific cryptographic practices. Additionally, user experiences and threat reports from credible sources have been reviewed to provide context and validate the importance of cryptographic security.

Online banking is one of the most security-sensitive digital services. Financial institutions employ encryption protocols such as SSL/TLS (Secure Sockets Layer / Transport Layer Security) to protect data transmitted between users and banking servers. These protocols use both symmetric and asymmetric encryption to secure Communications and authenticate users (Rescorla, 2001). Moreover, multi-factor authentication (MFA) and digital signatures are increasingly used to enhance trust and verify identity

In secure messaging applications like WhatsApp, Signal, and Telegram, end-to-end encryption (E2EE) ensures that messages are only readable by the intended recipients. These applications implement cryptographic algorithms such as AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) in combination with Diffie–Hellman key exchange to safeguard communication (Marlinspike, 2013). This paper evaluates how these protocols function and the role of Perfect Forward Secrecy (PFS) in preventing retrospective data breaches.

E-commerce platforms rely on cryptography to secure financial transactions and customer information. Digital certificates issued by trusted Certificate Authorities (CAs) verify the legitimacy of websites, ensuring users are not victims of phishing or

spoofing attacks (Gutmann, 2004). Hash functions such as SHA-256 are widely used to store passwords securely and verify data integrity during transactions.

This study draws upon secondary sources, including technical documentation, white papers, and cyber security reports, to analyse the cryptographic mechanisms employed by these platforms. It also reviews best practices and real-world incidents to evaluate how effective these systems are in mitigating cyber threats.

The methodology combines theoretical analysis with practical case studies to provide a holistic view of how cryptography underpins daily digital activities. As cyber threats continue to evolve, understanding these applications not only helps enhance user awareness but also underscores the critical need for robust cryptographic standards and user-centric security policies.

II. THE APPLICATIONS OF CRYPTOGRAPHY IN EVERYDAY LIFE

2.1. Identification and Analysis of Cryptographic Techniques in Online Banking, Messaging, and E-commerce

Online Banking:

Online banking systems rely heavily on cryptographic mechanisms to ensure the confidentiality, authenticity, and integrity of financial data. Key cryptographic techniques include:

- **SSL/TLS Protocols**: Provide secure communication between the user's browser and the banking server using a combination of asymmetric encryption (e.g., RSA, ECC) for key exchange and **symmetric** encryption (e.g., AES) for session data (Rescorla, 2001).
- **Digital Signatures**: Authenticate transactions and verify sender identities using public-key cryptography.
- **Hash Functions**: Used to securely store passwords and to ensure data integrity.
- **Multi-Factor Authentication (MFA)**: Combines cryptographic tokens (e.g., OTPs, biometrics) to enhance login security.

Secure Messaging:

Messaging applications like What Sapp, Signal, and Telegram use end-to-end encryption (E2EE) to ensure that only the sender and recipient can read messages. Techniques include:

- **Signal Protocol**: Implements a combination of the Double Ratchet algorithm, Diffie–Hellman key exchange, and AES-256 encryption to provide forward secrecy and message confidentiality (Marlinspike, 2013).
- **Perfect Forward Secrecy (PFS)**: Ensures that compromise of long-term keys does not compromise past communications.

E-commerce Platforms: E-commerce websites use cryptographic methods to secure transactions and user data:

- **HTTPS (TLS + HTTP)**: Encrypts all data exchanged between the user and the server.
- **Digital Certificates (X.509)**: Issued by Certificate Authorities (CAs) to authenticate legitimate websites.
- **Secure Payment Gateways**: Employ encryption and digital signature mechanisms to protect credit card information.
- **Hash Functions**: Protect stored customer credentials and validate transaction data.

2.2. Evaluation of Cryptography's Contribution to Data Security, Privacy, and Trust.

Cryptography plays a foundational role in establishing a secure digital ecosystem:

- **Data Security**: Encryption algorithms prevent unauthorized access to sensitive data, ensuring confidentiality during transmission and storage.
- **Privacy**: By using protocols like E2EE, users are assured that third parties—including service providers—cannot read their messages.
- **Trust**: Digital certificates and signatures verify the authenticity of websites and transaction participants, fostering user trust in online platforms.

For instance, the success of platforms like PayPal or mobile banking apps is strongly tied to user confidence in the cryptographic measures used to protect transactions and personal data.

2.3. Effectiveness of Cryptographic Implementations in Real-World Scenarios:

Case 1: Online Banking:

Banks worldwide have implemented TLS 1.2 and 1.3, resulting in significant reductions in man-in-the-middle (MITM) attacks and phishing effectiveness. Token-based MFA systems have been shown to reduce fraud by over 90% in sensitive banking transactions (Verizon, 2023).Cryptographic protocols significantly reduce fraud and cyber-attacks in banking.

Example 1: The adoption of TLS 1.2 and 1.3 by banking institutions has improved security through features like forward secrecy, helping prevent man-in-the-middle (MITM) attacks (Rescorla, 2018).

Example 2: According to the Verizon 2023 Data Breach Investigations Report, financial institutions that use token-based Multi-Factor Authentication (MFA) reported over a 90% reduction in fraudulent transactions**,** proving the critical role of cryptographic identity verification (Verizon, 2023).

Example 3: The Heartbleed vulnerability **i**n Open SSL underscored how improperly maintained cryptographic tools can be exploited. The financial industry responded with rapid upgrades to TLS 1.2+, reflecting the importance of current cryptographic implementations (Durumeric et al., 2014).

Case 2: Messaging:

Signal and WhatsApp's use of the Signal Protocol has become a gold standard for secure communication. In 2016,

WhatsApp enabled E2EE for over a billion users, with no reported breaches of the protocol itself. End-to-end encryption ensures message confidentiality even from service providers.

Example1: When WhatsApp implemented end-to-end encryption (E2EE) using the Signal Protocol in 2016, it secured over a billion users' communications. To date, there has been no known breach of the protocol itself, highlighting its effectiveness (Marlinspike & Perrin, 2016).

Example 2: The Signal Protocol uses a combination of Curve25519 for key exchange**,** AES-256 for encryption**,** and HMAC-SHA256 for integrity**,** making interception without decryption impossible (Cohn-Gordon et al., 2016).

Example 3: Given their high privacy standards, platforms like Signal are widely used by journalists, human rights activists, and politicians, especially in hostile environments, demonstrating real-world trust in cryptographic implementations (Electronic Frontier Foundation, 2021).

Case 3: E-commerce:

Major platforms like Amazon and eBay use TLS encryption, digital certificates, and secure checkout gateways. The integration of these cryptographic techniques has led to a significant decrease in fraudulent transactions and has made secure online shopping scalable and reliable. Cryptographic tools have made secure online shopping scalable, reliable, and trusted.

Example 1: Amazon and eBay **use** TLS encryption, PKI-based digital certificates**,** and HTTPS protocols to protect sensitive data during checkout and communication processes, making transactions secure (Symantec, 2017).

Example 2: TLS 1.3 has improved both security and performance, leading to quicker transactions without compromising encryption standards (Rescorla, 2018).

Example 3: PCI DSS standards require encryption of cardholder data. Non-compliance has historically led to data breaches and financial penalties, emphasizing the economic necessity of strong cryptographic practices (PCI Security Standards Council, 2022).

Example 4: The use of tokenization and secure checkout systems has significantly reduced chargeback fraud and improved customer trust (Kshetri, 2018).

III. CONCLUSION

Cryptography plays a pivotal role in securing modern digital communications, financial transactions, and online interactions. This paper has examined real-world applications in online banking, messaging, and e-commerce, demonstrating how cryptographic tools like TLS, public key infrastructure, end-to-end encryption, and digital certificates effectively protect sensitive data. The use of robust cryptographic protocols has significantly reduced fraud, prevented data breaches, and reinforced user trust. From the prevention of man-in-the-middle attacks in banking to the secure messaging of over a billion users through apps like WhatsApp and Signal, cryptography has become deeply integrated into our daily digital lives. However, the continued evolution of cyber threats highlights the importance of maintaining up-to-date cryptographic standards and promoting user awareness. As digital systems grow more interconnected, the effectiveness and resilience of cryptographic implementations will remain a cornerstone of information security and privacy protection in the digital age. Further research and innovation are essential to adapt to emerging challenges.

References

1. *Gutmann,P.(2004).*EngineeringSecurity.*https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf*
2. *Marlinspike, M. (2013). The Signal Protocol. Open Whisper Systems.*
3. *Marlinspike, M. (2013).* The Signal Protocol: Secure Messaging for Everyone. *Open Whisper Systems.*
4. *Rescorla, E. (2001). SSL and TLS: Designing and Building Secure Systems. Addison-Wesley.*
5. *Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing.*
6. *Verizon (2023).Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/*
7. *Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2016). A formal security analysis of the Signal messaging protocol.* IEEE European Symposium on Security and Privacy. *https://doi.org/10.1109/EuroSP.2017.11*
8. *Durumeric, Z., Kasten, J., Adrian, D., Halderman, J. A., Bailey, M., Li, F., ... & Paxson, V. (2014). The matter of Heartbleed.* Proceedings of the 2014 Conference on Internet Measurement Conference, *475–488. https://doi.org/10.1145/2663716.2663755*
9. *Electronic Frontier Foundation. (2021).* Surveillance Self-Defense: Secure Messaging Tools. *https://ssd.eff.org*
10. *Kshetri, N. (2018). 1 The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns.* Big Data for Development, *1–12. https://doi.org/10.1007/978-3-319-99549-6_1*
11. *Marlinspike, M., & Perrin, T. (2016).* The Signal Protocol. *Open Whisper Systems. https://signal.org/docs/*
12. *PCI Security Standards Council. (2022).* PCI DSS v4.0 Requirements and Security Assessment Procedures. *https://www.pcisecuritystandards.org*
13. *Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3.* Internet Engineering Task Force (IETF) RFC 8446. *https://doi.org/10.17487/RFC8446*
14. *Symantec. (2017).* Internet Security Threat Report. *https://symantec-enterprise-blogs.security.com*
15. *Verizon. (2023).* Data Breach Investigations Report. *https://www.verizon.com/business/resources/reports/dbir/.*
16. *Introduction to cryptography and network security, Behrouz.A.Forouzan, Published by Mc Graw-Hill, 2008.*