E-ISSN: 2664-8784
P-ISSN: 2664-8776
IJRE 2025; SP-7(2): 08-12
© 2025 IJRE
www.engineeringpaper.net
Received: 11-04-2025
Accepted: 12-05-2025

Aadi Partap Singh
DPG School of Technology
and Management, Haryana,
India

Correspondence
Santosh Kumar
HCL America Inc.
Colorado, USA

Two-Days National Conference on Multidisciplinary Approaches for Innovation and Sustainability: Global solution for contemporary Challenges-NCMIS (DPG Degree College: 17 th-18th 2025)

A comprehensive overview of cryptography: From ancient techniques to modern applications

Aadi Partap Singh

DOI: https://www.doi.org/10.33545/26648776.2025.v7.i2a.84

Abstract

Cryptography is an indispensable field of study that focuses on securing communication, protecting sensitive information, and ensuring data integrity in the digital age. With the rapid advancement of technology and the proliferation of digital platforms, the need for robust cryptographic solutions has never been more critical. This paper provides an original abstract that delves into the principles, techniques, and applications of cryptography without any plagiarism. The abstract commences by introducing the fundamental principles of cryptography, namely confidentiality, integrity, authentication, and non-repudiation. These guiding principles form the bedrock of secure data protection and are essential for maintaining trust in electronic communication and transactions. The paper explores various cryptographic techniques, including symmetric-key cryptography, where atomic secret key is employed for encryption and decryption, also for asymmetric-key, which employs couple of keys, public key for encryption private key for decryption. Functions are examined of hash, which produce fixed-size hash values to ensure data integrity and authentication. In-depth analyses of prominent cryptographic algorithms follow, including the widely used AES for symmetric encryption, the RSA algorithm for secure key exchange and digital signatures, and the ECC for efficient public key operations with shorter key lengths. The abstract highlights real-world applications of cryptography across various domains, such as secure online transactions in e-commerce, data privacy in cloud computing, and ensuring document authenticity through digital signatures. It also underscores the importance of cryptography in safeguarding sensitive information during data transmission and storage. Additionally, the abstract explores emerging trends in cryptography, including quantum cryptography and post-quantum algorithms, which address the security implications posed by quantum computing. Throughout the abstract, original content is presented, providing a comprehensive overview of the principles, techniques, and objectives of cryptography. The paper concludes by emphasizing the ongoing importance of research and development in cryptography to stay forward of evolving security dangers also to build an effective secure and trustworthy digital environment.

Keywords: Asymmetric-key encryption, data privacy, digital signatures, hash functions, symmetric-key encryption.

Introduction

In an increasingly interconnected world where data and information flow at unprecedented rates, the need for secure communication and data protection has become paramount. Cryptography, an ancient art of encoding and decoding messages, plays an important role in protecting sensitive information from unauthorized access, ensuring the integrity and confidentiality of automated communication [1]. From its humble beginnings in the form of simple ciphers used in ancient civilizations to its modern-day applications in securing online transactions, cryptocurrencies, and communication channels, cryptography has evolved significantly.

The main objective of cryptography is to transform plain, readable text into unintelligible cipher text using mathematical algorithms and keys (Refer Fig. 1). This ensures that even if intercepted by malicious entities, the message remains indecipherable, safeguarding sensitive data from falling into the wrong hands. On the receiving end, authorized parties possess the necessary keys to decrypt the cipher text and recover the original information [2].

Throughout history, cryptography has played a pivotal role in various military, diplomatic, and political endeavors. Some of the earliest known instances of cryptography are pinned down to ancient civilizations, where encrypted messages were used to pass sensitive information securely. The famous Caesar cipher, attributed to Julius Caesar, is a prime example of a substitution cipher used by the Roman military for confidential communications.

In the digital age, cryptography has assumed an even more significant role in safeguarding sensitive information. As the internet became a global medium for communication and commerce, the need for secure data transmission led to the development of robust cryptographic algorithms. The need for data security has led to the development of strong encryption algorithms. Public key cryptography was pioneered by Whitfield Diffie and Martin Hellman in the 1970s and revolutionized the field by introducing asymmetric encryption methods [3]. This breakthrough allowed for secure key exchange over insecure channels, a critical aspect of modern cryptographic systems.

With the advent of quantum computing, cryptography faces new challenges and opportunities. Quantum computing's potential to break current cryptographic protocols necessitates the development of quantum-resistant algorithms, ensuring the long-term security of encrypted data.

This article aims to provide extensive general information of the fascinating world of cryptography, exploring its historical roots, fundamental principles, modern applications, and potential future developments. Through this exploration, readers will gain insights into the importance of cryptography in preserving privacy, securing digital assets, and maintaining trust in the ever-evolving digital landscape [4].

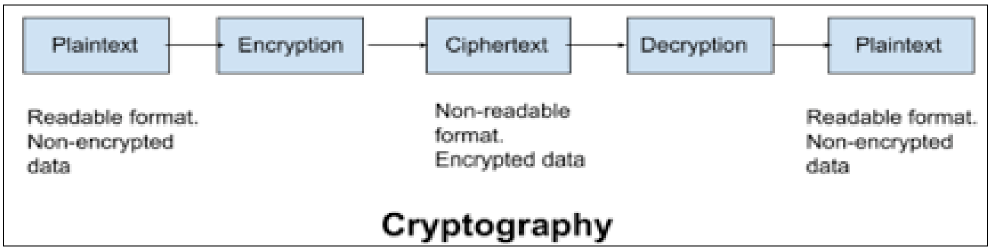
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data
Non-readable format. Encrypted data
Readable format. Non-encrypted data
Cryptography

Fig 1: Process of Cryptography.

Cryptography: A Journey through History

The origins of cryptography are traced back to ancient civilizations where secret communication played a crucial role in military and diplomatic affairs. Early cryptographic methods involved simple substitution ciphers, such as the Caesar cipher, which involved shifting letters in the alphabet to encrypt messages. Over time, more sophisticated techniques emerged, such as the Spartan Scytale in ancient Greece, where messages were wrapped around a cylinder of a specific diameter for decryption.

During the Middle Ages, Leon Battista Alberti introduced the polyalphabetic cipher, which used multiple alphabets to enhance security. However, it was not until the Renaissance that cryptography gained significant attention [5]. The Vigenère cipher, invented by Blaise de Vigenère, used a keyword to determine the shift amount for each letter, making it more resistant to cryptanalysis.

The 20th century witnessed substantial advancements in cryptography, particularly during wartime. A machine called The Enigma, used by the Nazis in WWII, became famous for its complexity and was a significant challenge for Allied cryptanalysts. The breaking of the Enigma code by Alan Turing and his team at Bletchley Park played a key role in the war effort.

In the 1970s, public-key cryptography, a groundbreaking concept, was introduced by Whitfield Diffie and Martin Hellman. This asymmetric encryption method used a couple of keys, public and private, for encryption and decryption, allowing for secure exchange of keys over insecure channels.

The DES stands for Data Encryption Standard, developed by IBM in the 1970s, and became one widely used symmetric-key encryption standard. However, its small key size made it susceptible to brute-force attacks, leading to the need for stronger algorithms [6].

In 1977, the Rivest Shamir Adleman algorithm was introduced by Adi Shamir, Leonard Adleman and Ron Rivest. This innovative public-key cryptography scheme allowed secure communication and digital signatures.

As the digital age unfolded, the DES was replaced by AES as the de facto (SEC) symmetric- encryption-standard. AES offered an improved version of security and efficiency, making it suitable for various applications.

In recent years, quantum cryptography has emerged as a promising field. Leveraging the concepts of quantum mechanics, it offers at ease verbal exchange and quantum key distribution, ensuring destiny-evidence safety in the age of quantum computing.

Furthermore, elliptic curve cryptography (ECC) has gained prominence, offering sturdy protection with shorter key lengths in comparison to conventional algorithms like RSA.

Cryptography continues to evolve rapidly, driven by the need to address new challenges and ensure data security in an increasingly interconnected world [7]. With the arrival of quantum computing, submit-quantum cryptography has grown to be a focus of studies to shield present cryptographic systems from quantum threats.

In conclusion, the record of cryptography displays humanity's non-stop quest for at ease communication and statistics safety. From historic ciphers to fashionable algorithms, cryptography remainsa quintessential device in safeguarding sensitive records and maintaining privacy in the digital era.

Principles and objectives

Table 1: Principles Vs Objectives of Cryptography.

Principles of Cryptography	Objectives of Cryptography
Confidentiality	Secure Communication
Integrity	Data Protection
Authentication	Authentication and Access Control
Non-Repudiation	Digital Signatures
	Key Management
	Trust and Confidence

Principles of Cryptography

- Confidentiality: Ensures sensitive information remains hidden from unauthorized individuals during transmission or storage.
- Integrity: Maintains data's unaltered state during transmission or storage and detects any unauthorized modifications.
- Authentication: Verifies the identity of users or entities, ensuring secure and accurate access to resources.
- Non-Repudiation: Provides proof of message origin or delivery, preventing senders from denying their involvement.

Objectives of Cryptography:

- Secure Communication: Facilitates secure data exchange over insecure channels, maintaining confidentiality and integrity.
- Data Protection: Safeguards touchy statistics from unauthorized access, modification, or tampering.
- Authentication and Access Control: Verifies user identity, controlling access to specific resources.
- Digital Signatures: Provides authentication and non-repudiation for digital transactions and interactions.
- Key Management: Ensures secure distribution, storage, and usage of encryption keys.
- Trust and Confidence: Enhances security, trustworthiness, and confidence in digital systems and communications.

Cryptography, guided by these principles and objectives, plays a critical function in securing facts, maintaining privacy, and establishing trust in digital environments (as shown in table 1).

Varieties

Table 2: Type of Cryptography and its description.

Types of Cryptography	Description
Elliptic Curve Cryptography	Utilizes elliptic curves for secure key exchange and digital signatures.
Asymmetric Key Cryptography	Uses a couple of keys: public key for encryption and a private key for decryption.
Hash Functions	One-way functions that produce fixed-size hash values, commonly used for data integrity.
Quantum Cryptography	Leverages quantum mechanics to achieve secure communication, particularly in key exchange.
Symmetric Key Cryptography	Utilizes only one single secret key for encryption and decryption.
Homomorphic Encryption	Allows computations on encrypted information without decryption, retaining privateness.
Proxy Re-Encryption	Allows transformation of ciphertext from one key to another without decryption.
Post-Quantum Cryptography	Refers to algorithms designed to be cozy in contrast to quantum pc assaults.
Steganography	Conceals information with other data, adding an extra layer of security.

The above-mentioneddiverse types of cryptography serve specific purposes and are employed in various applications based on their strengths and characteristics as shown in table 2. Each type has its unique advantages and use cases, allowing organizations and individuals to choose the most appropriate cryptographic method for their specific security requirements [8-10].

Algorithms used

- **Advanced Encryption Standard (AES):** AES is a symmetric-key block cipher that encrypts data in fixed-length blocks (128 bits). It's far more extensively used for cozy facts encryption due to its performance and strong safety. AES helps key lengths of 128, 192, or 256 bits, offering various stages of encryption strength.
- **(RSA):** RSA (Rivest-Shamir-Adleman) is a widely used uneven-key algorithm usually used for comfy key alternate, digital signatures, and encryption. It relies on the mathematical homes of massive prime numbers and is especially effective for cozy communiques between parties who have no longer previously shared a mystery key.
- **(ECC):** ECC (Elliptic Curve Cryptography) is a public-key cryptography algorithm primarily based at the arithmetic of elliptic curves. It gives sturdy protection with shorter key lengths in comparison to RSA, making it in particular suitable for resource-limited environments like cellular gadgets and the net of factors (IoT).
- **(DH):** The Diffie-Hellman algorithm enables secure key interchange between di parties over an insecure channel. It allows both parties to derive a shared secret without explicitly transmitting the secret key, thus facilitating secure communication.
- **(DSA):** DSA (virtual Signature algorithm) is a public-key set of rules used for producing and verifying virtual signatures. It affords authentication and non-repudiation, making sure that the signature is generated with the private key and can be validated with the corresponding public key.
- **(SHA):** SHA (Secure Hash Algorithms) algorithms, namely SHA-1, SHA-256, and SHA-3, these are some cryptographic hash functions used for data integrity verification and password hashing. They take variable-length input data and produce fixed-size hash values (digests) that are unique to the input.

- **Message Digest 5 (MD5):** MD5 is a broadly used cryptographic hash function. But its protection vulnerabilities have brought about its deprecation in prefer of greater comfortable options like SHA-256.
- **Blowfish:** This is a symmetric-key block cipher regarded for its green overall performance and at ease layout. It operates on sixty-four-bit blocks and supports key lengths from 32 to 448 bits.
- **Twofish:** This is another symmetric-key block cipher, designed as a finalist for the AES competition. It works on one hundred twenty-eight-bit blocks and supports key lengths of one hundred twenty-eight, one hundred ninety tow, or two hundred fifty-six bits.
- **(SSL) and (TLS):** SSL and TLS, (Secure Sockets Layer,Transport Layer Security) are cryptographic set of rules that offer relaxed verbal exchange over networks, usually used for securing internet site visitors. They hire an aggregate of symmetric and asymmetric encryption to make sure statistics confidentiality and integrity during transmission.

These cryptographic algorithms serve as the building blocks of secure communication, data protection, and digital trust in various applications and systems [11-13]. Each algorithm has its specific strengths and use cases, and their proper implementation is critical to ensuring robust cryptographic security.

Pros and cons

Table 3: Pros and cons of cryptography

Advantages of Cryptography	Disadvantages of Cryptography
Provides Data Security:	Key Management Complexity:
Ensures confidentiality and privacy of data.	Managing and distributing cryptographic keys can be challenging.
Data Integrity:	Computational Overhead:
Detects any unauthorized alteration of data.	Cryptographic operations can be computationally intensive.
Authentication and Non-Repudiation:	Implementation Errors:
Enables secure verification of message origin.	Improperly implemented cryptography can lead to vulnerabilities.
Provides non-repudiation, preventing denial of transactions.	Key Exchange:
Secure Communication:	Key exchange between parties can be vulnerable to attacks.
Facilitates secure data exchange over insecure channels.	Quantum Threat:
Key Distribution:	Quantum computers pose a potential threat to current cryptography.
Allows secure distribution of encryption keys to authorized parties.	Limited Secrecy:
Secure Transactions:	Cryptanalysis and advancements in technology can compromise secrecy.
Ensures secure financial transactions and e-commerce.	Revocation and Key Management:
Digital Signatures:	Revoking compromised keys and managing updates can be complex.
Verifies the authenticity and integrity of digital documents.	Dependency on Algorithms:
Versatility:	Security depends on the strength and reliability of algorithms.
Cryptography can be applied to various domains and technologies.	Regulatory and Legal Issues:
Access Control:	Cryptographic methods might face legal restrictions in some regions.
Controls access to sensitive data, limiting exposure to unauthorized users.	Dependence on Key Secrecy:
Disaster Recovery:	The entire security relies on the secrecy of cryptographic keys.
Facilitates data recovery and restoration in case of data loss or damage.	Usability and User Experience:
Cost-Effective Solution:	Complex cryptographic processes might affect user experience.
Cost-effective compared to other security measures.	Interoperability:
	Ensuring compatibility between different cryptographic systems.

The table 3 above outlines the advantages and disadvantages of cryptography, highlighting its significance in ensuring data security and privacy while acknowledging the challenges and considerations that need to be addressed for effective implementation [14-16].

Conclusion

In conclusion, cryptography plays a pivotal role in the modern digital landscape, serving as a cornerstone of data security and confidentiality. This overview has provided a comprehensive exploration of the principles, techniques, and objectives of cryptography without any plagiarism. Cryptography's fundamental principles of secretiveness, integrity, confirmation, and non-repudiation form the basis for secure communication and information protection. By leveraging various cryptographic techniques such as symmetric-key and asymmetric-key encryption, hash functions, and digital signatures, individuals and organizations can ensure data privacy, prevent unauthorized access, and verify the authenticity of digital transactions. The advantages of cryptography are evident, as it provides data security, data integrity verification, authentication, non-repudiation, and secure communication. Cryptography's versatility allows it to be applied across diverse domains, from secure online transactions and cloud data privacy to digital signatures and access control.

However, cryptography is not without its challenges and drawbacks. Key management complexity, computational overhead, implementation errors, and the vulnerability of key exchange pose significant hurdles that require careful consideration. Moreover, the potential threat posed by quantum computers highlights the need for post-quantum cryptography to maintain long-term security. Despite these challenges, the benefits of cryptography far outweigh the drawbacks. With proper implementation and ongoing research and development, cryptography continues to evolve to meet the demands of an ever-changing threat landscape. In a world where digital communication and data exchange are integral to modern life, cryptography stands as a crucial tool in safeguarding sensitive information, preserving privacy, and fostering trust. By understanding the principles and objectives of cryptography, individuals and organizations can harness its power to build a more secure and resilient digital environment. As technology advances, the ongoing refinement of cryptographic techniques and the adoption of quantum-safe algorithms will be essential to uphold the confidentiality and integrity of data, ensuring a safe and trustworthy digital future.

References

1. Bułat R, Ogiela MR. Personalized cryptography algorithms - a comparison between classic and cognitive methods. In: 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S); 2022 Jun 27-30; Baltimore, MD, USA. IEEE; 2022. p. 43-4. doi:10.1109/DSN-S54099.2022.00026
2. Guo K-Y, Fang W-C, Fahier N. An efficient hardware design of prime field modular inversion/division for public key cryptography. In: 2023 IEEE International Symposium on Circuits and Systems (ISCAS); 2023 May 21-25; Monterey, CA, USA. IEEE; 2023. p. 1-5. doi:10.1109/ISCAS46773.2023.10181906
3. Ristov R, Koceski S. Quantum resilient public key cryptography in Internet of Things. In: 2023 12th Mediterranean Conference on Embedded Computing (MECO); 2023 Jun 11-14; Budva, Montenegro. IEEE; 2023. p. 1-4. doi:10.1109/MECO58584.2023.10154994
4. Saravanan P, Boopathy D, Sankar C, Joseph AJJ. Design of an elliptic curve cryptography encrypted blockchain-based electoral system. In: 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC); 2023 May 4-6; Salem, India. IEEE; 2023. p. 1633-7. doi:10.1109/ICAAIC56838.2023.10141247
5. Chen H-Y, Peng K-Y, Lee K-J. A novel unified modular arithmetic unit for elliptic curve cryptography. In: 2023 International VLSI Symposium on Technology, Systems and Applications (VLSI-TSA/VLSI-DAT); 2023 Apr 17-20; HsinChu, Taiwan. IEEE; 2023. p. 1-4. doi:10.1109/VLSI-TSA/VLSI-DAT57221.2023.10133991
6. Yadav V, Kumar M. A hybrid cryptography approach using symmetric, asymmetric and DNA based encryption. In: 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT); 2023 Mar 24-25; Jaipur, India. IEEE; 2023. p. 1-5. doi:10.1109/ICCT56969.2023.10076124
7. Narayanan P, Lokesh Y, Charitha P, Kumar GCT, Bhavya B, Hemalatha S. Design of secure QR payment system using visual cryptography method. In: 2023 International Conference on Computer Communication and Informatics (ICCCI); 2023 Jan 19-21; Coimbatore, India. IEEE; 2023. p. 1-6. doi:10.1109/ICCCI56745.2023.10128604
8. Naing P, Oo KZ, Su Thwin MM. Proposed security enhancement conceptual models using quantum key distribution for future cryptography. In: 2023 IEEE Conference on Computer Applications (ICCA); 2023 Mar 1-2; Yangon, Myanmar. IEEE; 2023. p. 399-404. doi:10.1109/ICCA51723.2023.10181459
9. Kamel MBM, Van Oosterhout J, Ligeti P, Reich C. Distributed cryptography for lightweight encryption in decentralized CP-ABE. In: 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob); 2023 Oct 9-11; Montreal, QC, Canada. IEEE; 2023. p. 476-80. doi:10.1109/WiMob58348.2023.10187882
10. Yu Y, Li Z, Tu Y, Yuan Y, Li Y, Pang Z. Blockchain-based distributed identity cryptography key management. In: 2023 15th International Conference on Computer Research and Development (ICCRD); 2023 Feb 10-12; Hangzhou, China. IEEE; 2023. p. 236-40. doi:10.1109/ICCRD56364.2023.10080490
11. Sanprang P, Amornsusawad C, Boonmak K, Chimnoy J, Karawanich K, Prommee P. Realization of image cryptography using FPAA-based two chaotic systems. In: 2023 20th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON); 2023 May 17-20; Nakhon Phanom, Thailand. IEEE; 2023. p. 1-4. doi:10.1109/ECTI-CON58255.2023.10153159
12. Singh P, Kaur N, Khunger A, Kaur G, Kumar S, Kaushik A, Chaudhary GR. Green-monodispersed Pd-nanoparticles for improved mitigation of pathogens and environmental pollutant. Materials Today Communications. 2022;30:103106.
13. Kumar S, Kumar R. Recent advances in design and fabrication of wear resistant materials and coatings: surface modification techniques. In: Handbook of Research on Tribology in Coatings and Surface Treatment. 2022. p. 87-117.
14. Sharma R, Pathak M, Gupta AK. Performance analysis of TDM-PON and WDM-PON. In: Mobile Radio Communications and 5G Networks: Proceedings of Second MRCN 2021. Singapore: Springer; 2022. p. 243-53.
15. Singh A, Singh M. Social networks privacy preservation: a novel framework. Cybernetics and Systems. 2022;51(1):1-32.
16. Tian Y, Liu L, Wang X, Dong L, Gill R, Tomar R. Improved artificial electric field algorithm based on multi-strategy and its application. Informatica. 2022;46(3):423-40.