International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

Modern Cryptographic Techniques in Cybersecurity

K. Suganya[1], P. Yamuna[2]

[1,2]*Assistant Professor, Department of Computer Science, Mahalashmi Women's College of Arts and Science*

***Abstract*— Modern cryptographic techniques are essential for protecting sensitive information in today's digital world. As cyber threats become increasingly sophisticated, organizations rely on advanced cryptographic algorithms to ensure the confidentiality, integrity, authentication, and non-repudiation of data. These techniques are widely used in secure communication, cloud computing, financial transactions, IoT, blockchain, and digital identity management. This article discusses the principles of modern cryptography, major cryptographic techniques, applications, advantages, challenges, and future trends in cybersecurity.**

***Keywords*—Cryptography, Cybersecurity, Encryption, Digital Signature, Hash Function, Public Key Infrastructure (PKI), AES, RSA, ECC, Post-Quantum Cryptography.**

I. Introduction

Cybersecurity aims to protect computer systems, networks, and digital information from unauthorized access, attacks, and data breaches. Cryptography plays a vital role in achieving this objective by transforming readable information (plaintext) into an unreadable format (ciphertext), ensuring that only authorized users can access the original data.

Modern cryptography combines mathematical algorithms with computational techniques to provide secure communication across various platforms. With the rapid growth of cloud computing, mobile devices, artificial intelligence, and the Internet of Things (IoT), cryptographic techniques have become indispensable in securing digital infrastructure.

Objectives of Modern Cryptography

The primary objectives of cryptography include:

Confidentiality: Prevents unauthorized access to sensitive information.

Integrity: Ensures that data has not been altered during transmission.

Authentication: Verifies the identity of users or systems.

Non-repudiation: Prevents the sender from denying the transmission of a message.

Availability: Supports secure access to information whenever required.

II. Hash Functions

Hash functions convert input data into a fixed-length value known as a hash. A **hash function** is a cryptographic algorithm that converts data of any size into a **fixed-length output**, called a **hash value**, **message digest**, or **checksum**. Hash functions are **one-way functions**, meaning it is computationally infeasible to reconstruct the original input from the hash value.

III. Digital Signatures

Digital signatures ensure message authenticity and integrity. A **Digital Signature** is a cryptographic technique used to verify the **authenticity**, **integrity**, and **origin** of a digital message or document. It uses **asymmetric (public-key) cryptography**, where the sender signs the message with a **private key**, and the receiver verifies it using the corresponding **public key**.

IV. Public Key Infrastructure (PKI)

PKI manages digital certificates and public keys. **Public Key Infrastructure (PKI)** is a framework of technologies, policies, procedures, and digital certificates that enables secure electronic communication using **public-key (asymmetric) cryptography**. PKI manages the creation, distribution, storage, and revocation of digital certificates and cryptographic keys, ensuring that users and devices can securely exchange information.

V. Elliptic Curve Cryptography(Ecc)

ECC provides strong security using smaller key sizes. **Elliptic Curve Cryptography (ECC)** is a modern **public-key (asymmetric) cryptographic technique** based on the mathematical properties of **elliptic curves over finite fields**. It provides the same level of security as traditional algorithms like RSA but with **much smaller key sizes**, making it faster and more efficient.

VI. Quantum Cryptography

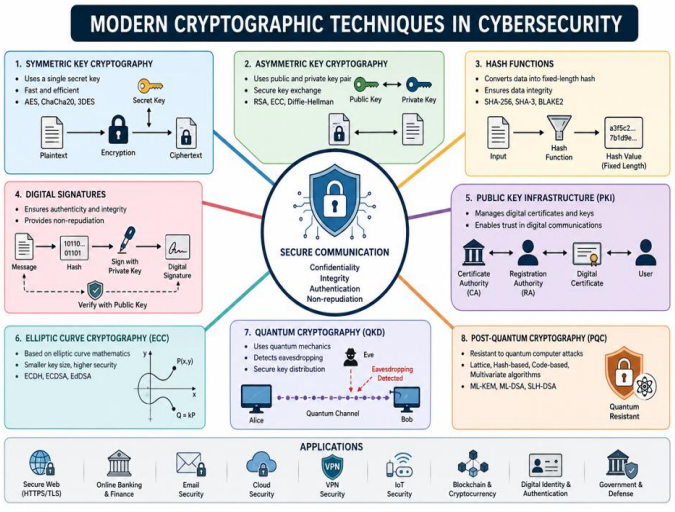
Quantum Cryptography is an advanced cryptographic technique that uses the principles of **quantum mechanics** to provide highly secure communication. Unlike traditional cryptography, its security is based on the laws of physics rather than computational complexity.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

The most widely used application of quantum cryptography is **Quantum Key Distribution (QKD)**, which enables two parties to securely exchange encryption keys.

Comparison of Cryptographic Techniques

Technique	Key Type	Speed	Security	Common Applications
AES	Symmetric	Very Fast	High	File encryption, VPNs
RSA	Asymmetric	Slow	High	Secure communication
ECC	Asymmetric	Fast	Very High	Mobile security
SHA-256	Hash	Very Fast	High	Password hashing
Digital Signature	Asymmetric	Moderate	High	Document authentication
PKI	Hybrid	Moderate	High	SSL/TLS Certificates
Quantum Cryptography	Quantum	Moderate	Very High	Secure communication



Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a **symmetric-key encryption algorithm** used to securely encrypt and decrypt digital data. It was developed by the U.S. National Institute of Standards and Technology (NIST) and became the official encryption standard in **2001**, replacing the older DES (Data Encryption Standard).

Rivest-Shamir-Adleman (RSA)

RSA (Rivest–Shamir–Adleman) is an **asymmetric encryption algorithm** developed in **1977** by Ron Rivest, Adi Shamir, and Leonard Adleman. It uses **two keys**: a **public key** for encryption and a **private key** for decryption. RSA is based on the mathematical difficulty of factoring large prime numbers. It provides **confidentiality, authentication, integrity, and digital signatures**. Although RSA is slower than AES, it is widely used in **HTTPS, SSL/TLS, digital certificates, email encryption, online banking, and secure communication**.

Secure Hash Algorithm (SHA)

The **Secure Hash Algorithm (SHA)** is a family of **cryptographic hash functions** designed by the **National Security Agency (NSA)** and standardized by the **National Institute of Standards and Technology (NIST)**. SHA converts data of any size into a **fixed-length hash value (message digest)**. It is mainly used to ensure **data integrity** and **authentication**.

Digital Signature Algorithm (DSA)

The Digital Signature Algorithm (DSA) is an asymmetric cryptographic algorithm used to create and verify digital signatures. It was developed by the National Institute of Standards and Technology (NIST) in 1991. DSA ensures the authenticity, integrity, and non-repudiation of digital documents and messages.

Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to remain secure against attacks from both **classical computers** and **quantum computers**. Unlike quantum cryptography, PQC uses conventional computer systems but employs new mathematical algorithms that are resistant to quantum attacks. It is being developed to replace vulnerable public-key algorithms such as RSA and ECC.

Applications in Cybersecurity

Modern cryptographic techniques are used in:

A. E-commerce
B. Cloud security

C. Virtual Private Networks (VPNs)
D. Blockchain and cryptocurrency
E. Internet of Things (IoT)

VII. Conclusion

Modern cryptographic techniques form the backbone of cybersecurity by ensuring confidentiality, integrity, authentication, and non-repudiation of digital information. Techniques such as AES, RSA, ECC, SHA-256, digital signatures, and PKI are widely deployed to secure communications and protect sensitive data across industries. As emerging technologies like quantum computing introduce new security challenges, organizations are increasingly adopting post-quantum cryptography and advanced privacy-preserving methods to safeguard future digital systems. Continuous research and innovation in cryptography will remain essential for building resilient cybersecurity infrastructures.

REFERENCES

[1] National Institute of Standards and Technology (NIST), "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," Gaithersburg, MD, USA, Aug. 2024.

[2] National Institute of Standards and Technology (NIST), "FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)," Gaithersburg, MD, USA, Aug. 2024.

[3] National Institute of Standards and Technology (NIST), "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)," Gaithersburg, MD, USA, Aug. 2024.

[4] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, Version 0.6, 2024.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 9th ed. Pearson, 2024.

[6] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, "Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey," *arXiv preprint arXiv:2510.10436*, Oct. 2025.

[7] A. Kudaloor and A. Aijaz, "Toward Quantum-Safe 6G: Experimental Evaluation of Post-Quantum Cryptography Techniques," *arXiv preprint arXiv:2605.06881*, May 2026.

[8] M. Toruan, R. D. N. Shakya, S. Tseitkin, R. K. Zhao, and N. Arachchilage, "When Security Meets Usability: An Empirical Investigation of Post-Quantum Cryptography APIs," *arXiv preprint arXiv:2602.14539*, Feb. 2026.

[9] A. C. H. Chen, "NIST Post-Quantum Cryptography Standard Algorithms Based on Quantum Random Number Generators," *arXiv preprint arXiv:2507.21151*, Jul. 2025.

[10] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography," National Cybersecurity Center of Excellence, 2024.