IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 12, December 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

Alternative Cryptographic Algorithms vs Traditional Cryptographic Algorithms A Critical Analysis

Shajahan S

Lecturer in Computer Engineering, Department of Computer Hardware Engineering, Government Polytechnic College, Nedumangad, India

ABSTRACT: Cryptography has evolved significantly over the past few decades, with traditional cryptographic algorithms like RSA, AES, DES, and SHA forming the backbone of digital security. However, with the rise of quantum computing, IoT expansion, big data applications, and cyber threats, these algorithms face increasing vulnerabilities and limitations. In response, alternative cryptographic techniques such as DNA cryptography, quantum cryptography, chaos-based cryptography, and lattice-based cryptography have emerged as promising solutions to address these security gaps. This article critically analyzes the limitations of traditional cryptographic systems and evaluates the advantages and challenges of alternative cryptographic techniques, discussing their real-world applications and future viability.

I. INTRODUCTION

Cryptography has undergone remarkable advancements over the past few decades, with traditional cryptographic algorithms like RSA, AES, DES, and SHA serving as the foundation of modern digital security. These algorithms, based on complex mathematical computations, have effectively protected sensitive data against cyber threats. However, with the rapid evolution of computing power, the rise of quantum computing, the proliferation of IoT devices, and the increasing complexity of big data applications, these traditional cryptographic methods face significant vulnerabilities. RSA and ECC, for example, rely on factorization and discrete logarithm problems, which quantum computers using Shor's algorithm could break efficiently. AES and SHA, while more resistant, also face potential risks as quantum advancements continue. Additionally, the growing need for lightweight and scalable cryptographic solutions for IoT and cloud computing further exposes the inefficiencies of traditional methods. To address these challenges, alternative cryptographic techniques such as DNA cryptography, quantum cryptography, chaos-based cryptography, and lattice-based cryptography have emerged as potential solutions. DNA cryptography leverages biological molecules for ultra-high-density data storage and parallel processing, offering unparalleled security but facing challenges in scalability and processing speed. Quantum cryptography, particularly Quantum Key Distribution (QKD), ensures unbreakable encryption using the principles of quantum mechanics, but its practical implementation remains limited due to expensive infrastructure and scalability concerns. Chaos-based cryptography exploits nonlinear chaotic systems to create highly unpredictable encryption, making it resistant to pattern-based attacks while being computationally lightweight and suitable for real-time applications. Meanwhile, lattice-based cryptography, a leading candidate for post-quantum security, provides robust encryption resistant to quantum attacks while maintaining efficiency, though it still requires extensive testing and optimization for widespread adoption. These alternative techniques offer innovative approaches to overcoming the shortcomings of classical cryptographic algorithms, providing enhanced security, efficiency, and resilience against emerging cyber threats. However, despite their advantages, challenges such as implementation costs, hardware constraints, standardization issues, and computational efficiency must be addressed before they can fully replace or complement traditional cryptographic systems. As digital security continues to evolve, the integration of these alternative cryptographic methods will play a crucial role in shaping the future of cybersecurity, ensuring robust protection against increasingly sophisticated attacks in an era of quantum computing, IoT expansion, and big data-driven environments.

II. GENERAL LIMITATIONS OF TRADITIONAL CRYPTOGRAPHIC ALGORITHMS

Traditional cryptographic algorithms have been designed based on mathematical hardness assumptions, providing security through complex computational problems. However, several emerging factors challenge their effectiveness:

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

Computational Vulnerabilities: RSA and ECC depend on the difficulty of factoring large prime numbers and solving the discrete logarithm problem. However, with Shor's algorithm on quantum computers, these problems become solvable in polynomial time, making these encryption schemes insecure in a post-quantum world. AES and SHA-256 are relatively secure today but require increasing key sizes to resist brute-force and collision attacks. This leads to higher computational costs.

Quantum Threats: Quantum computing is set to break asymmetric encryption (RSA, ECC, Diffie-Hellman) by solving problems exponentially faster than classical computers. Symmetric encryption (AES, 3DES) is more resistant but still requires doubling key sizes, making encryption computationally expensive for IoT and cloud computing.
Scalability & IoT Challenges: Resource-constrained devices (IoT, embedded systems) struggle with implementing strong encryption due to limited processing power and memory. Algorithms like AES and RSA require high computational power, making them inefficient for lightweight IoT applications.

Security Risks in Data Integrity & Authentication: Hash functions (SHA-1, MD5) have been broken due to collision attacks, leading to security breaches. Digital signatures and authentication protocols based on RSA and ECC face threats from quantum computing.

Traditional cryptographic systems are facing obsolescence due to quantum threats, inefficiency in IoT, and security vulnerabilities, necessitating the need for alternative cryptographic techniques.

III. LIMITATIONS OF TRADITIONAL CRYPTOGRAPHIC ALGORITHMS: A DETAILED ANALYSIS

(i) RSA (Rivest-Shamir-Adleman) – Increasingly Insecure in the Quantum Era

Limitation	Impact
Vulnerable to Quantum Attacks (Shor's Algorithm)	Quantum computers running Shor's Algorithm can factor large prime numbers in polynomial time, rendering RSA insecure.
Requires Large Key Sizes	To match the security level of 256-bit ECC, RSA requires 3072-bit keys, making encryption computationally expensive.
Computationally Slow	Key-generation, encryption, decryption take significant processing power, making RSA inefficient for IoT and mobile devices.

RSA relies on the difficulty of factoring large prime numbers. Classical computers struggle with this, but quantum computers can break RSA in seconds, making it unsuitable for future security applications. In 2017, researchers factored a 768-bit RSA key, indicating that 1024-bit RSA may soon be broken. NIST (National Institute of Standards and Technology) is pushing for post-quantum cryptographic standards due to RSA's vulnerabilities.

(ii) AES (Advanced Encryption Standard) – Powerful but Not Quantum-Resistant

Limitation	Impact
Requires Secure Key Exchange	Secure key distribution mechanisms are necessary, increasing complexity and risk.
Quantum Computers Could Break AES-128	Grover's Algorithm reduces AES-128's effective security to AES-64, making it vulnerable.
High Processing Power Needed for IoT Devices	AES encryption and decryption require significant computational resources, making it unsuitable for low-power IoT applications.

While AES is still considered secure, quantum attacks could eventually reduce its effectiveness. AES-128 is particularly at risk, and AES-256 is recommended for future security. AES is widely used in TLS, VPNs, and encrypted storage, but secure key exchange is a major challenge. IoT devices struggle with AES due to power and memory constraints.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

(iii) DES (Data Encryption Standard) – Completely Obsolete

Limitation	Impact
Easily Broken by Brute Force	DES's 56-bit key size is too small and can be cracked within hours using modern computers.
Replaced by AES Due to Weak Security	DES is no longer used for encryption due to its vulnerabilities and inefficiency.

In 1999, a brute-force attack cracked DES in 22 hours. Modern GPU clusters can break DES keys in minutes. The US government replaced DES with AES in 2001 due to its weak security. Many legacy systems still use DES, creating security risks.

(iv) 3DES (Triple DES) – Too Slow & Marginally Secure

Limitation	Impact
Slow and Inefficient	Encrypting with three DES iterations makes it significantly slower than AES.
Only Marginally More Secure than DES	3DES can be attacked using Meet-in-the-Middle techniques, reducing its effectiveness.

3DES uses three rounds of DES encryption, but it is still slower and weaker than AES. NIST deprecated 3DES in 2023, advising organizations to transition to AES.

(v) SHA-1 & SHA-256 (Cryptographic Hash Functions) – Collision Attacks & Quantum Threats

Limitation	Impact
SHA-1 is Broken (Collision Attacks Found)	Google's "SHAttered" attack (2017) proved SHA-1 collisions, making it insecure.
SHA-256 May Be Vulnerable to Quantum Attacks	Grover's Algorithm reduces SHA-256's security from 256-bit to 128-bit, potentially making it weak.

SHA-1 is completely broken; major organizations like Google and Microsoft have abandoned it. SHA-256 remains secure today, but quantum threats could force a shift to SHA-512 or post-quantum hash functions. In 2017, Google and CWI Amsterdam demonstrated a SHA-1 collision, proving its insecurity. Most systems now use SHA-256 or SHA-3 instead.

(vi) ECDSA (Elliptic Curve Digital Signature Algorithm) – At Risk from Quantum Computing

Limitation	Impact
Secure Today but May Be Broken by Quantum Algorithms	Quantum computers running Shor's Algorithm can break ECC, making ECDSA signatures insecure.

ECDSA relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which quantum computers can solve efficiently. Post-quantum alternatives like CRYSTALS-Dilithium are being explored. Bitcoin and blockchain security rely on ECDSA, raising concerns about post-quantum attacks. Many governments are investing in post-quantum cryptography to replace ECC.

(vii) Diffie-Hellman (Key Exchange Protocol) – Vulnerable to MITM Attacks

Limitation	Impact
No Authentication Mechanism	Diffie-Hellman alone does not verify identities, allowing Man-in-the-Middle (MITM) attacks.

Attackers can intercept and modify key exchange processes, posing a security risk. Quantum computers can solve the Diffie-Hellman problem efficiently. In 2015, researchers found that many VPNs used weak Diffie-Hellman key exchange, making them vulnerable to nation-state attacks.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

Why Traditional Cryptography Needs to Evolve

Traditional Algorithm	Major Limitation	Future Risk
RSA	Slow, quantum-vulnerable	Quantum computers will break it
AES	Secure, but quantum threats exist	AES-128 is at risk
DES / 3DES	Completely obsolete	Already broken
SHA-1	Broken (collision attacks)	No longer safe
ECDSA	Quantum-vulnerable	Needs post-quantum replacement
Diffie-Hellman	MITM attacks possible	Quantum attacks will break it

To address these limitations, modern security systems must adopt alternative cryptographic techniques, such as: Post-quantum cryptography (Lattice-based, Hash-based, Code-based encryption), Quantum cryptography (Quantum Key Distribution - QKD), DNA cryptography (Biological encryption techniques). Organizations must transition towards quantum-safe encryption to future-proof their security infrastructure.

IV. ALTERNATIVE CRYPTOGRAPHIC ALGORITHMS OVER TRADITIONAL CRYPTOGRAPHY

The rapid evolution of computing power, quantum computing, IoT devices, and cyber threats has exposed major limitations in traditional cryptographic algorithms like RSA, AES, DES, SHA, and ECC. These conventional algorithms rely on mathematical complexity, but emerging threats—such as quantum attacks, brute force advancements, and scalability challenges—demand alternative cryptographic solutions. Alternative cryptographic algorithms—including DNA cryptography, quantum cryptography, chaos-based encryption, lattice-based cryptography, and lightweight cryptography—are being developed to address the weaknesses of traditional methods.

(i) DNA Cryptography (DNAC) Over RSA & AES

Traditional Algorithm	Alternative Algorithm	Advantages
RSA, AES	DNA Cryptography	Ultra-high data density, biological security, parallel computing

DNA cryptography uses biological DNA molecules as the medium for encryption. DNA consists of four nucleotide bases—Adenine (A), Thymine (T), Cytosine (C), and Guanine (G)—which can be mapped to binary data.

1. Mapping Binary to DNA Sequences
    a. A = 00, T = 01, C = 10, G = 11
    b. Example: 110100 → GTC
2. Encryption Using DNA Operations
    a. DNA techniques such as Polymerase Chain Reaction (PCR), DNA sequencing, and complementary pair matching ensure secure encryption.
3. Decryption via DNA Analysis
    a. Reverse sequencing translates DNA back to binary format.

Merits of DNAC: (a) Resistant to Brute Force & Quantum Attacks: DNA encryption is computationally infeasible to break. (b) Higher Storage Density: DNA can store exabytes of data per gram. (c) Parallel Processing: DNA reactions occur simultaneously, accelerating encryption speed.

Challenges of DNAC: (a) Expensive: DNA synthesis and sequencing are costly. (b) Slow Biochemical Processes: DNA reactions take longer than digital computing.

(ii) Quantum Cryptography (QC) Over AES & RSA

Traditional Algorithm	Alternative Algorithm	Advantages
RSA, AES	Quantum Cryptography (QKD - Quantum Key Distribution)	Unbreakable security, quantum entanglement-based key distribution

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

Quantum cryptography leverages the principles of quantum mechanics to secure encryption:

1. Quantum Key Distribution (QKD) via BB84 Protocol
    a. Qubits are sent using random polarization states.
    b. Any eavesdropper's attempt disturbs the qubits, revealing the attack.
2. Uncertainty Principle-Based Security
    a. Heisenberg's Uncertainty Principle ensures encryption is unbreakable.

Merits of QC: (a) Provable Security: Based on physics, not mathematical complexity. (b) Immune to Brute Force & MITM Attacks: Eavesdropping detection is automatic. (c) Future-Proof Against Quantum Computers.

Challenges of QC: (a) Expensive: Requires advanced quantum hardware. (b) Not Yet Scalable: Limited to high-security environments.

(iii) Chaos-Based Cryptography (CBC) Over Blowfish & Twofish

Traditional Algorithm	Alternative Algorithm	Advantages
Blowfish, Twofish	Chaos-Based Cryptography	Highly unpredictable encryption, resistant to pattern-based attacks

Chaos-based cryptography utilizes chaotic mathematical functions like Logistic Map, Henon Map, and Lorenz Attractor for encryption.

1. Chaotic Key Generation
    a. The encryption key is derived from nonlinear chaotic systems.
    b. A tiny change in the key creates drastically different outputs, making it unpredictable.
2. Encryption with Chaotic Functions
    a. Unlike traditional ciphers, chaos-based cryptography uses nonlinear transformations, making attacks impractical.

Merits of CBC: (a) Extremely Unpredictable: Chaos functions ensure high entropy. (b) Low Computational Cost: Ideal for real-time encryption. (c) Efficient for Cloud Security, IoT, and Streaming.

Challenges of CBC: (a) Difficult to Standardize: No universal encryption model yet. (b) Sensitive to Key Variations: Small errors in key input can affect encryption.

(iv) Post-Quantum Cryptography (PQC) Over RSA & ECC

Traditional Algorithm	Alternative Algorithm	Advantages
RSA, ECC	Lattice-Based Cryptography (NTRU, Kyber, Dilithium)	Resistant to quantum attacks, efficient key sizes

Lattice-based cryptography relies on hard mathematical problems in high-dimensional lattices, which even quantum computers cannot efficiently solve.

1. Algorithms like Kyber, Dilithium, and Falcon
    a. These are being standardized for post-quantum security.
    b. Used in secure communication and authentication protocols.

Merits of PQC: (a) Quantum-Resistant: Does not rely on prime factorization or elliptic curves. (b) Smaller Key Sizes: More efficient than RSA. (c) NIST Standardization Underway.

Challenge of PQC: Still Under Research - Needs further testing and real-world deployment.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

(v) Lightweight Cryptography Over Triple DES (3DES)

Traditional Algorithm	Alternative Algorithm	Advantages
Triple DES (3DES)	Lightweight Cryptography (PRESENT, SIMON, SPECK)	Optimized for IoT & embedded systems

Lightweight cryptographic algorithms are designed for low-power, resource-constrained devices (IoT, RFID, smart sensors).

1. Smaller Key Sizes & Simpler Rounds
    a. PRESENT, SIMON, and SPECK use optimized encryption for embedded systems.
    b. Efficient for smart devices, medical implants, and industrial control systems.

Merits of LC: (a) Low Power Consumption: Ideal for battery-operated devices. (b) Faster Encryption for Real-Time Processing. (c) More Secure Than Legacy Systems Like 3DES.

Challenge of LC: Trade-off Between Security and Performance.

V. CONCLUSION

Why Alternative Cryptographic Algorithms Are the Future

Traditional Algorithm	Alternative Algorithm	Why It's Better?
RSA, AES	DNA Cryptography	Ultra-secure, high-density storage
AES, RSA	Quantum Cryptography (QKD)	Unbreakable key distribution
Blowfish, Twofish	Chaos-Based Cryptography	Unpredictable and highly secure
RSA, ECC	Lattice-Based Cryptography	Post-quantum resistant
3DES	Lightweight Cryptography	Ideal for IoT & embedded devices

Alternative cryptographic methods are the future of cybersecurity, offering resilience against quantum computing, better efficiency for IoT & real-time processing, and enhanced security for next-gen applications. To future-proof cybersecurity, organizations must transition to post-quantum cryptography, DNA encryption, and chaos-based methods to protect against emerging threats.

REFERENCES

[1] K. SASIKUMAR AND SIVAKUMAR NAGARAJAN, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing", IEEE Access, Vol. 12, pp. 52325 – 52351, 2024.
[2] M. Sohal and S. Sharma, "BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Cloud Computing," J. King Saud Univ.- Comput. Inf. Sci., vol. 34, no. 1, pp. 1417–1425, 2022.
[3] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for Data Security in Cloud Computing," Int. J. Intell. Netw., vol. 3, pp. 16–30, Jan. 2022.
[4] A. A Fairosebanu and A. C. Febaseeli, "Enhanced Symmetric Encryption Technique for Securing Users' Data in Public Cloud Environment," Int. J. Comput. Sci. Netw. Secur., vol. 22, no. 4, pp. 785–791, Apr. 2022.
[5] S. Lu, J. Zheng, Z. Cao, Y. Wang, and C. Gu, "A Survey on Cryptographic Techniques for Protecting Big Data Security: Present and Forthcoming," Sci. China Inf. Sci., vol. 65, no. 10, pp. 201–301, Oct. 2022.
[6] Ratheesh Kumar R and Jabin Mathew, "Image Encryption: Traditional Methods vs Alternative Methods", IEEE, Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020), pp. 619-625, March 2020.
[7] Ratheesh Kumar R and Jabin Mathew, "How to Evaluate the Security and Performance of an Image Encryption System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Vol. 7 Issue 3, pp. 302-311, May-June 2020.
[8] Ratheesh Kumar R and Jabin Mathew, "A Mathematical Interpretation of Images and Image Encryption", International Journal of Mathematics Trends and Technology (IJMTT), Vol. 66.6 (2020):190-194.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212050 |

[9] Ratheesh Kumar R and Jabin Mathew, "A System with 5-Level Security for Cloud Data and a Comparison of AES and 3DES", International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 6, pp. 1046-1055, 2020.
[10] Ratheesh Kumar R and Jabin Mathew, "An Image Encryption Using Dynamic DNA Coding, Chaotic Map, And the Provision for Improved Robustness", Advances in Mathematics: Scientific Journal 9 (2020), no.10, pp. 8957–8967.
[11] Ratheesh Kumar R, "A Comparison of Two Image Encryption Algorithms with Chaotic Maps", International Journal of Scientific & Engineering Research Volume 12, Issue 12, December-2021, pp. 70-74.
[12] Ratheesh Kumar R, "A Comparison of Six DNA-based Cryptographic Methods", Science, Technology and Development, Volume X Issue XII DECEMBER 2021, pp. 358-361.
[13] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, and Muhammad Talha, "Robust Encryption of Quantum Medical Images", IEEE Access, vol. 6, pp. 1073–1081, 2017.
[14] Tian Tian Zhang, Shan Jun Yan, Cheng Yan Gu, Ran Ren and Kai Xin Liao, "Research on Image Encryption Based on DNA Sequence and Chaos Theory", Physics: Conf. Series, vol. 1004, pp. 1–6, 2018.
[15] Xing-Quan Fu, Bo-Cheng Liu, Yi-Yuan Xie, Wei Li, and Yong Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos", IEEE Photonics, vol. 10, no. 3, 2018.
[16] Xingbin Liu, Di Xiao, and Yanping Xiang, "Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map", IEEE Access, vol. 7, pp. 6937-6946, 2019.
[17] Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang, "Image Encryption with Double Spiral Scans and Chaotic Maps", Hindawi Sec.and Comm. Networks, vol. 2019, pp. 1-15, 2019.
[18] Yuling Luo, Xue Ouyang, Junxiu Liu, and Lvchen Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Cha-otic Systems", IEEE Access, vol. 7, pp. 38507–38522, 2019.
[19] Akram Belazi, Muhammad Talha, Sofiane Kharbech, and Wei Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA En-coding", IEEE Access, vol. 7, pp. 36667–36681, 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details