Benha Journal of Applied Sciences (BJAS) **print: ISSN 2356–9751**
Vol. (10) Issue (4) (2025), (19- 25) **online: ISSN 2356–976x**
http://bjas.bu.edu.eg
engineering sciences

Hybridp Encryption Technologies in Wireless Network

Yassmin kh.Ahmed[2], Tamer O.Diab [2], Samah O.Mohamed[1]and Abd El- Hady M.Abd El- Hady [2]
Informatics Research Dept., Electronics Research Institute (ERI), Cairo, Egypt[1]
Electrical Engineering Dept., Faculty of Engineering, Benha, Egypt[2]
E-mail: yassmin.khairat@eri.sci.eg

Abstract
Securing Wireless Sensor Networks (WSNs) is essential to protect sensitive data and maintain privacy, particularly in applications where security is paramount, such as healthcare, military, and environmental monitoring. WSNs are susceptible to various security threats, including data tampering, unauthorized access, eavesdropping, and node compromise, which can have serious consequences. Ensuring the integrity, authenticity, and confidentiality of data transmitted through WSNs is crucial to maintaining trust in the network's performance. If security measures are not in place, critical services could be disrupted, leading to potential failures in systems like smart cities, agriculture, or disaster response. Additionally, since WSNs often operate in remote and untrusted environments, securing them against both internal and external attacks is vital. By implementing effective security protocols, WSNs can safeguard not only the data they transmit but also their overall functionality, making them reliable and trustworthy for various applications. This paper aims to discuss hybrid encryption methods which used in secure wireless sensor network based on co-operative communication. Hybrid encryption combining both symmetric and asymmetric methods of encryption using hybrid encryption offering balance between security and efficiency. Also has a lot of advantages such as enhanced security by using asymmetric key technique and symmetric block cipher such as Advanced Encryption Standard, for data transmission, hybrid type faster for encryption large amount of data, it supports secure communications between multiple parties without share all of Asymmetric Keys.

Key words: AES, block cipher, symmetric encryption, asymmetric encryption and RSA

Introduction

Hybrid encryption technology in wireless communication has become an essential mechanism to improve data security. This essay will examine the principles of hybrid encryption, assess its historical background, discuss its effects on wireless communication, and explore future advancements [1]. By concentrating on pivotal contributions from key individuals and analyzing various viewpoints, this analysis aims to deliver a thorough understanding of how hybrid encryption protects wireless communications.

Hybrid encryption merges the advantages of both symmetric and asymmetric encryption. Symmetric encryption uses the same key for both encryption and decryption [2], making it quicker but less secure during key distribution. Conversely, asymmetric encryption uses a pair of keys a public key for encryption and a private key for decryption offering a more secure method for key exchange but slower processing speeds. By combining both approaches, hybrid encryption takes advantage of the speed of symmetric encryption and the security of asymmetric encryption. This blend is particularly important in wireless communication, where data is vulnerable to eavesdropping and interception.

The demand for secure wireless communication has significantly increased with the rise of mobile technology [3]. As users become more reliant on devices like smartphones and tablets for personal and professional communication, worries regarding data privacy have heightened. Hybrid encryption effectively tackles these concerns, ensuring that sensitive information remains private during transmission. In recent years, encryption standards have been designed to meet the needs of contemporary wireless communication, including advancements in LTE and Wi-Fi technologies.

Numerous prominent individuals have greatly influenced the field of encryption, shaping its advancement. One of the most significant figures is Whitfield Diffie, who co-created the Diffie-Hellman key exchange protocol in 1976[4]. This groundbreaking method enabled two parties to securely exchange cryptographic keys over a public channel without the need for a previously shared key. This seminal work established the foundation for modern asymmetric encryption and created a framework for secure communication. Following this, researchers like Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA algorithm, which further popularized asymmetric encryption and solidified its use across various sectors.

Recent advancements in wireless communication technologies have highlighted the importance of hybrid encryption. The rollout of 5G networks has opened new paths for increasing data transmission speeds while expanding the number of connected devices. However, such progress presents new security challenges. Hybrid encryption becomes vital in

these situations, offering strong security mechanisms to safeguard data integrity and privacy as more devices get connected through the Internet of Things (IoT) [5]. With these devices transmitting sensitive information, utilizing hybrid encryption protects against possible cyber threats.

Critics of hybrid encryption frequently point out its complexity and the challenges related to implementation. While the combination of symmetric and asymmetric encryption provides security advantages, the integration process can be complicated. Organizations may need considerable resources and expertise to implement hybrid encryption systems effectively [6]. Additionally, the reliance on both types of encryption requires clearly defined protocols to securely manage key generation, exchange, and storage. Consequently, maintaining a balance between security, functionality, and user experience continues to be a challenge in many applications.

The significance of regulations in affecting the deployment of hybrid encryption cannot be ignored. As governments worldwide implement stricter data protection laws, compliance has become essential for organizations. Hybrid encryption solutions must comply with these regulations to guarantee that sensitive information is sufficiently safeguarded [7]. Looking to the future, the significance of hybrid encryption in wireless communication is expected to increase even more. With the ongoing advancement of quantum computing, the security environment will encounter new obstacles. Quantum computers have the capability to compromise numerous traditional cryptographic algorithms currently employed. As researchers delve into post-quantum cryptography, the hybrid encryption strategy may require adjustments to preserve its effectiveness. Future cryptographic systems may combine quantum-resistant algorithms with current hybrid methods to ensure strong security for wireless communication. This paper divided into four sections, first section was the introduction, second section is the description of advanced encryption standard, while the third section is Ron Rivest, Adi Shamir, and Leonard Adleman Algorithm by the end of the paper was the last section conclusion.

Advanced Encryption Standard

The Advanced Encryption Standard, often referred to as AES, is a symmetric encryption algorithm that acts as the foundation of contemporary data security. This essay will examine the historical background of AES, its technological implications, key figures who played a role in its creation, and future developments in encryption technology. By recognizing AES's importance, we can gain a greater understanding of its part in safeguarding information in an increasingly digital environment.

AES was instituted by the National Institute of Standards and Technology, or NIST, in 2001[7, 8]. The algorithm was created to succeed the Data Encryption Standard, known as DES, which was considered insecure because of its short key lengths and susceptibility to brute-force attacks. The necessity for a strong encryption standard became crucial as digital data grew more widespread. The process of selecting AES commenced in 1997, during which several candidates were assessed based on performance, security, and efficiency of implementation. Ultimately, the Rijndael algorithm, crafted by Belgian cryptographers Vincent Rijmen and Joan Daemen, was selected as the AES after thorough analysis and multiple rounds of public evaluation.

The influence of AES on technology and information security is significant. Currently, AES is an international standard utilized in a variety of applications, spanning from securing sensitive information in government communications to safeguarding personal data in mobile devices and financial transactions. Its symmetric nature implies that the same key is employed for both encryption and decryption, offering a straightforward yet effective means of securing data. AES accommodates key sizes of 128, 192, and 256 bits, which present different levels of security. The greater the key size, the longer it takes to breach the encryption, thereby rendering AES remarkably strong against attacks [9].

Key individuals have influenced the creation and implementation of AES. Vincent Rijmen and Joan Daemen, the developers of Rijndael, made significant contributions to the mathematical principles that support AES [10]. Their design included a series of transformations, such as substitution, permutation, and mixing of input data, which bolster security. Additionally, the standardization of AES was backed by a worldwide cryptographic community that offered essential feedback, ensuring that the algorithm stayed resilient against emerging threats.

Different viewpoints exist regarding the security of AES. Some specialists maintain that the algorithm is strong, while others voice concerns about possible vulnerabilities. A notable issue is the potential of quantum computing to undermine classical encryption methods. Quantum computers function based on principles that allow them to solve particular problems much more rapidly than

conventional computers. These developments create a challenge for AES [11], particularly for key sizes below 256 bits. As a result, researchers are investigating post-quantum cryptography to create encryption algorithms that can withstand quantum attacks. This encompasses the ongoing advancement of alternative schemes that could either complement or supplant AES in a future where quantum computing is prevalent.

Another factor to take into account is the legal and ethical consequences of encryption. Governments globally confront the challenge of finding a balance between national security and personal privacy. While AES offers crucial security protections, it simultaneously raises concerns about surveillance and backdoors in encryption. Law enforcement agencies contend that access to encrypted information is essential for fighting crime and terrorism. Conversely, privacy advocates emphasize the potential for misuse and infringements on civil liberties. This ongoing discussion highlights the importance of creating a clear framework for the use of encryption and governmental oversight.

In recent times, the field of cybersecurity has changed significantly due to the rising occurrence of cyberattacks and data breaches, which underscores the demand for strong encryption standards like AES [12]. Notable incidents have shown the vulnerabilities that organizations encounter, stressing the importance of implementing strong encryption methods. For instance, the 2017 Equifax data breach revealed sensitive personal details of over 147 million individuals. Such incidents emphasize the vital role that AES plays in protecting sensitive information and sustaining consumer confidence in digital services.

As we look ahead, various trends and innovations in encryption technology are surfacing. The drive for enhanced cybersecurity measures is leading more organizations to adopt AES and investigate multifactor authentication, alongside hybrid encryption solutions that merge symmetric and asymmetric algorithms. Additionally, machine learning and artificial intelligence are starting to play significant roles in refining encryption processes and boosting threat detection capabilities. These technologies may result in the creation of adaptive encryption that reacts in real-time to new threats.

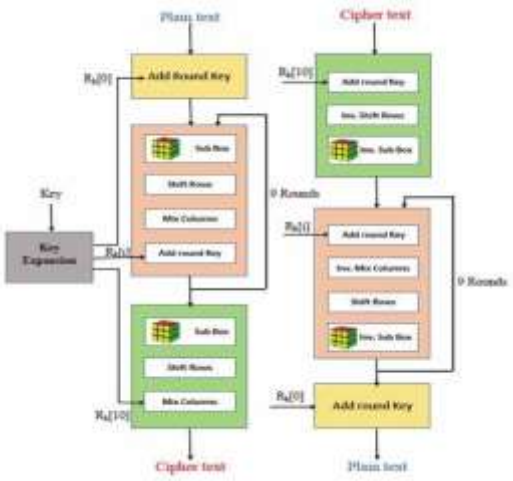

Fig. 1. Block diagram of advanced encryption standard (AES)

Ron Rivest, Adi Shamir, and Leonard Adleman Algorithm

The RSA algorithm constitutes one of the essential foundations of contemporary cryptography. It enables secure data transmission and acts as the core for a range of applications [14], from safe emails to internet transactions. This essay will examine the RSA algorithm, its mathematical principles, and its historical importance, the impact of key individuals, various uses, and future possibilities in the realm of cryptography.

The RSA algorithm was created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology. This groundbreaking algorithm is notable for its asymmetrical characteristics. In contrast to symmetric cryptography, which necessitates a single key for both encryption and decryption, RSA employs a public key for encryption and a private key for decryption [15]. This difference permits secure communications without the need to exchange secret keys.

The mathematical foundation of the RSA algorithm consists of several steps that are vital for ensuring security. The algorithm commences with the choice of two large prime numbers, referred to as p and q. These are multiplied to compute n, which is utilized in the public key. The totient function phi (n) is determined as (p-1) (q-1). A number e is subsequently selected such that it is coprime to phi (n). The public key is established from the pair (n, e), while the private key d is computed to fulfill the equation ed ≡ 1 (mod phi (n)). The encryption of a message m is performed using the formula c ≡ m^e (mod n), and decryption is accomplished through c^d ≡ m (mod n).

The importance of the RSA algorithm goes well beyond its mathematical sophistication. It transformed digital communications and continues to be a benchmark for securing sensitive data [16]. Before RSA, secure digital communication heavily depended on symmetric key algorithms, which presented

significant logistical obstacles for key distribution. RSA addressed this issue with its pioneering approach of public and private key pairs, thus simplifying the secure exchange of information.

Key individuals like Rivest, Shamir, and Adleman have profoundly impacted the advancement of cryptography. Their contributions established a foundation for additional progress in the field. Numerous other researchers have expanded upon their basic principles, improving security measures and increasing the complexity of cryptographic techniques [17]. Throughout the years, various implementations of RSA have surfaced, benefiting industries such as finance, healthcare, and e-commerce by facilitating secure transactions and protecting personal data.

As digital technology continues to grow swiftly, different applications of the RSA algorithm have become increasingly significant. One prominent application is in secure web browsers, where RSA supports the HTTPS protocol. This protocol encrypts communication between users and web servers, ensuring that sensitive information like credit card details remains confidential [18]. Furthermore, RSA is utilized in digital signatures, which verify the origin and integrity of messages. In a time when information security is crucial, RSA maintains its relevance due to its ability to safeguard sensitive information.

In recent years, quantum computing has surfaced as a possible risk to established cryptographic algorithms, including RSA. Quantum computers have the capability to resolve intricate problems at faster rates through algorithms such as Shor's algorithm, which can efficiently factor large integers. The consequences for RSA are significant, as the security of the algorithm depends on the challenge of factorizing large numbers [19]. This has inspired researchers to investigate post-quantum cryptography, with the goal of creating algorithms that remain secure in the face of quantum computing capabilities.

Despite these obstacles, the RSA algorithm is still progressing. Cryptographers are striving to bolster the algorithm against possible threats, such as introducing larger key sizes and enhancing the mathematical foundation of RSA. Current guidelines frequently suggest key sizes of 2048 bits or more to improve security against sophisticated computational attacks. Additionally, as digital communication increasingly converges with new technologies, the need for robust cryptographic methods is expected to grow.

Looking forward, the trajectory of the RSA algorithm and cryptography overall will be influenced by continuous advancements in both computational capability and research [20]. As more organizations shift to cloud-based solutions and the Internet of Things widens, the necessity for secure communication will become even more crucial. Thus, RSA's function in ensuring security will likely keep evolving in tandem with these technological advancements.

RSA Operation

The RSA algorithm involves four steps: key generation, key distribution, encryption, and decryption.

A basic principle behind RSA is the observation that it is practical to find three very large positive integers *e*, *d*, and *n*, such that for all integers *m* ($0 \leq m < n$), both $(m^e)^d$ and m have the same remainder when divided by n (they are congruent modulo *n*),

$$(m^e)^d = m \ (mod\ n)$$

However, when given only *e* and *n*, it is extremely difficult to find *d*.

The integers *n* and *e* comprise the public key, *d* represents the private key, and *m* represents the message. The modular exponentiation to *e* and *d* corresponds to encryption and decryption, respectively.

In addition, because the two exponents can be swapped, the private and public key can also be swapped, allowing for message signing and verification using the same algorithm.

Key generation

The keys for the RSA algorithm are generated in the following way:

1. Choose two large prime numbers p and q.
   - To make factoring harder, p and q should be chosen at random, be both large and have a large difference. For choosing them the standard method is to choose random integers and use a primality test until two primes are found.
   - P and q are kept secret.
2. Compute n = p q.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
   - n is released as part of the public key.
3. Compute λ(n), where λ is Carmichael's totient function. Since n = pq, λ(n) = lcm(λ(p), λ(q)), and since p and q are prime, λ(p) = φ(p) = p − 1, and likewise λ(q) = q − 1. Hence λ (n) = lcm (p − 1, q − 1).
   - The lcm may be calculated through the Euclidean algorithm, since lcm (a, b) = □|ab|/gcd (a, b) □.
   - Λ (n) is kept secret.
4. Choose an integer e such that 1 < e < λ (n) and gcd (e, λ (n)) = 1; that is, e and λ (n) are coprime.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – the most commonly

chosen value for e is 216 + 1 = 65537. The smallest (and fastest) possible value for e is 3, but such a small value for e has been shown to be less secure in some settings.[15]

- e is released as part of the public key.

5. Determine d as d ≡ e−1 (mod λ (n)); that is, d is the modular multiplicative inverse of e modulo λ(n).

- This means: solve for d the equation de ≡ 1 (mod λ(n)); d can be computed efficiently by using the extended Euclidean algorithm, since, thanks to e and λ(n) being coprime, said equation is a form of Bézout's identity, where d is one of the coefficients.
    - d is kept secret as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the private (or decryption) exponent d, which must be kept secret. P, q, and λ (n) must also be kept secret because they can be used to calculate d. In fact, they can all be discarded after d has been computed.

In the original RSA paper, the Euler totient function φ (n) = (p − 1) (q − 1) is used instead of λ (n) for calculating the private exponent d. Since φ (n) is always divisible by λ (n), the algorithm works as well. The possibility of using Euler totient function results also from Lagrange's theorem applied to the multiplicative group of integers modulo pq. Thus any d satisfying d·e ≡ 1 (mod φ (n)) also satisfies d·e ≡ 1 (mod λ (n)). However, computing d modulo φ (n) will sometimes yield a result that is larger than necessary (i.e. d > λ(n)). Most of the implementations of RSA will accept exponents generated using either method (if they use the private exponent d at all, rather than using the optimized decryption method based on the Chinese remainder theorem described below), but some standards such as FIPS 186-4 (Section B.3.1) may require that d < λ(n). Any "oversized" private exponents not meeting this criterion may always be reduced modulo λ(n) to obtain a smaller equivalent exponent.

Since any common factors of (p − 1) and (q − 1) are present in the factorization of n − 1 = pq − 1 = (p − 1)(q − 1) + (p − 1) + (q − 1),[17][self-published source?] it is recommended that (p − 1) and (q − 1) have only very small common factors, if any, besides the necessary 2.

Key distribution

Suppose that Bob wants to send information to Alice. If they decide to use RSA, Bob must know Alice's public key to encrypt the message, and Alice must use her private key to decrypt the message.

To enable Bob to send his encrypted messages, Alice transmits her public key (n, e) to Bob via a reliable, but not necessarily secret, route. Alice's private key (d) is never distributed.

Encryption

After Bob obtains Alice's public key, he can send a message M to Alice.

To do it, he first turns M (strictly speaking, the un-padded plaintext) into an integer m (strictly speaking, the padded plaintext), such that 0 ≤ m < n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c, using Alice's public key e, corresponding to C = m^e *(mod n)*

This can be done reasonably quickly, even for very large numbers, using modular exponentiation. Bob then transmits c to Alice. Note that at least nine values of m will yield a cipher text c equal to m, but this is very unlikely to occur in practice.

Decryption

Alice can recover *m* from C by using her private key exponent *d* by computing

$C^d = (m^e)^d = m \ (mod\ n)$

Given *m*, she can recover the original message M by reversing the padding scheme.

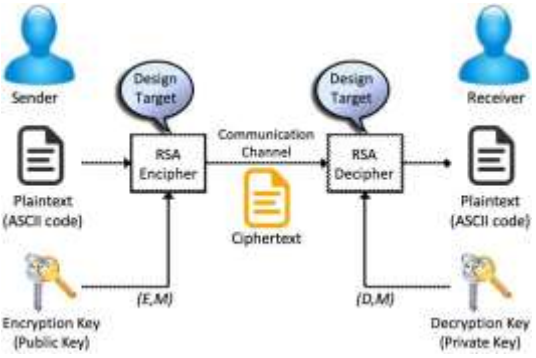

Fig. 2. RSA Process Diagram

Hybrid Cryptography in the Quantum Era: Trends and Applications (2024–2025)

1. Crypto Chaos: Chaos-Based Hybrid Cryptography (April 2025)

Researchers introduced **Crypto Chaos**, a hybrid cryptographic framework that combines deterministic chaos theory with modern cryptographic primitives. It utilizes chaotic maps (e.g., Logistic, Chebyshev) to generate high-entropy keys, which are then used in AES-GCM encryption. This approach enhances resistance against quantum attacks, particularly those leveraging Grover's algorithm [24].

2. 5G-AKA-HPQC: Quantum-Resilient 5G Authentication (February 2025)

A new protocol, **5G-AKA-HPQC**, was proposed to enhance 5G authentication mechanisms by integrating classical Elliptic Curve Integrated Encryption Scheme (ECIES) with post-quantum Key Encapsulation Mechanisms (KEMs). This hybrid approach ensures forward secrecy and quantum resistance in 5G networks [25].

3. Hybrid Encryption for Smart Home Healthcare (October 2024)
An optimized hybrid encryption framework combining ECC-256r1 and AES-128 in EAX mode was developed for smart home healthcare systems. This solution offers enhanced data confidentiality, low energy consumption, and resilience against quantum computing threats, making it suitable for IoT devices in healthcare settings [26].
4. Hybrid Cryptographic Approach Using Block Ciphers (August 2024)
A study presented a hybrid cryptographic algorithm that leverages both symmetric (AES) and asymmetric (ECC) encryption techniques, along with Digital Signature Algorithm (DSA), to secure data communication. This approach aims to provide robust and adaptable security solutions for various applications [27].
5. Enhancing Cloud Security with Hybrid Encryption (February 2024)
Researchers proposed a hybrid encryption technique combining homographic encryption with the Squirrel Search Algorithm (SSA) to improve cloud security for web applications. This method enhances data protection in cloud environments by optimizing encryption processes [28].

Future Trends in WSN Security:

1. **Lightweight Cryptography**
- Efficient encryption tailored for low-power sensor nodes.
2. **AI-Based Intrusion Detection**
- Machine learning to detect attacks and anomalies.
3. **Trust & Reputation Systems**
- Nodes evaluate neighbor behavior to reduce insider threats.
4. **Blockchain Integration**
- Secure, tamper-proof data sharing and authentication.
5. **Cross-Layer Security**
- Coordinated defense across multiple network layers.
6. **Secure & Energy-Aware Routing**
- Resilient routing protocols that save energy and block attacks.
7. **Edge Computing & 5G Integration**
- Local processing boosts security in large-scale networks.
8. **Post-Quantum Cryptography**
- Preparing for quantum threats with future-proof encryption.

Conclusion
Hybrid encryption technology signifies a crucial advancement in securing wireless communication. By integrating the efficiency of symmetric encryption with the robustness of asymmetric encryption, this method responds to the escalating demand for data protection in an increasingly interconnected world. In this work, we have examined two critical areas: Hybrid Cryptography in the Quantum Era: Trends and Applications (2024–2025), which explores the integration of classical and post-quantum encryption to strengthen security in fields such as telemedicine, 5G, and IoT; and Future Trends in Wireless Sensor Network (WSN) Security, which focuses on the development of lightweight, energy-efficient, and AI-driven encryption strategies tailored for resource-constrained environments. The contributions of researchers and innovators in these areas have significantly influenced the security technologies we depend on today. As cyber threats continue to evolve particularly with the rise of quantum computing hybrid encryption will undoubtedly play a central role in protecting sensitive data and ensuring secure wireless communication in the years ahead.

References

[1] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.
[2] Diffie, W. , and Hellman, M. E. , "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.
[3] Rivest, R. , Shamir, A. , and Adleman, L. , "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
[4] Kaur, M. , and Singh, M. , "Hybrid Cryptosystem for Securing Data Communication," International Journal of Computer Applications, vol. 69, no. 6, pp. 1-6, 2013.
[5] Chen, L. K. , and Zhang, X. , "Post-Quantum Cryptography: How It Will Affect Hybrid Cryptography," IEEE Transactions on Information Theory, vol. 66, no. 5, pp. 3098-3114, 2020.
[6] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.
[7] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
[8] G. M. P. O. O. A. T. P. A. D. Wu, “A Hybrid Encryption Technology for Wireless Communication,” IEEE Access, vol. 7, pp. 64-72, 2019.
[9] “General Data Protection Regulation

(GDPR),” European Union, 2016.

[10] C. Z. Wu et al. , “Towards Post-Quantum Cryptography: Hybrid Encryption,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1234-1246, 2020.

[11] R. Rivest, A. Shamir, and L. Adleman, "Cryptographic Information Security," 1977.

[12] D. Boneh, "The Security of RSA and the Performance of RSA Implementation," 2010.

[13] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," 1994.

[14] NIST, "Post-Quantum Cryptography Standardization," 2020.

[15] M. A. Smith and J. R. Johnson, "Advancements in Cryptographic Standards and Practices," IEEE Trans. Inf. Forensics Security, vol. 11, no. 10, pp. 2324-2335, 2016.

[16] V. Rijmen and J. Daemen, "The AES Proposal: Rijndael," NIST, 2001.

[17] NIST, "Announcing the Advanced Encryption Standard (AES)," National Institute of Standards and Technology, 2001.

[18] S. Vaudenay, "On the security of AES," Journal of Cryptology, vol. 19, no. 2, pp. 207-224, 2006.

[19] D. J. Bernstein, "Post-quantum cryptography," Proceedings of the IEEE, vol. 106, no. 3, pp. 473-482, 2018.

[20] "2017 Equifax Data Breach," Federal Trade Commission, 2017.

[21] H. Su, W. Luo, and X. Zhang, "Research on Secure Encryption Communication Method for Unmanned Aerial Vehicle System Based on Hybrid Encryption Algorithm," in Proc. 2024 8th Int. Conf. Electron. Inf. Technol. Comput. Eng. (EITCE), 2024, pp. 477–480.

[22] A. Shafique, S. A. A. Naqvi, A. Raza, M. Ghalaii, P. Papanastasiou, J. McCann, Q. H. Abbasi, and M. A. Imran, "A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks," Sci. Rep., vol. 14, no. 1, p. 31054, 2024.

[23] Q. Chang, T. Ma, and W. Yang, "Low power IoT device communication through hybrid AES-RSA encryption in MRA mode," Sci. Rep., vol. 15, no. 1, p. 14485, 2025.

[24] K. Song, N. Imran, J. Y. Chen, and A. C. Dobbins, “A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications,” *arXiv preprint*, arXiv:2504.08618, 2025.

[25] Y. Ko, I. Pawana, and I. You, “5G-AKA-HPQC: Hybrid Post-Quantum Cryptography Protocol for Quantum-Resilient 5G Primary Authentication with Forward Secrecy,” *arXiv preprint*, arXiv:2502.02851, 2025.

[26] O. Popoola, M. A. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, “An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security,” *Internet of Things*, vol. 27, p. 101314, 2024.

[27] A. Gour, S. S. Malhi, G. Singh, and G. Kaur, “Hybrid Cryptographic Approach: For Secure Data Communication using Block Cipher Techniques,” in *E3S Web of Conferences*, vol. 556, p. 01048, EDP Sciences, 2024.

[28] R. S. Kanakasabapathi and J. E. Judith, “Improving cloud security model for web applications using hybrid encryption techniques,” *Int. J. Internet Technol. Secured Transact.*, vol. 13, no. 3, pp. 291–308, 2024.