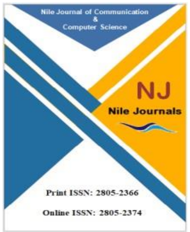
Nile Journals

Nile Journal of Communication & Computer Science

Volume 8, December 2024

Journal Webpage: https://njccs.journals.ekb.eg



Evaluation of Encryption Algorithms: A Comparative Approach over 6G Networks

Hesham.A. Sakr
Assistant Professor- ECE department-Nile Higher Institute for Engineering and Technology

Abstract

The protection of data, particularly sensitive information, has become increasingly crucial with the rapid expansion of digital storage platforms. As 6G networks emerge, offering ultra-low latency, large-scale connectivity, and high bandwidth, safeguarding data transmission poses new challenges. This research presents a comparative analysis of encryption algorithms such as DES, RSA, AES, Blowfish, ECC, and 3DES, assessing their efficiency in addressing security issues within 6G networks. The study examines the strengths and limitations of these algorithms in the context of fast, scalable, and energy-efficient communications. With the integration of advanced technologies like AI and IoT in 6G, the need for adaptive and resilient encryption solutions is rising. This paper aims to determine the most appropriate encryption techniques to ensure data security and confidentiality in 6G networks, offering valuable insights for optimizing cryptographic approaches in next-generation communication systems.

Keywords: Data Security; 6G Networks; Encryption Algorithms; AI ; IoT.

1. Introduction

Encryption is an essential method used by individuals and organizations to protect data when transmitting it over insecure networks or storing it on online platforms. As cyber threats become increasingly advanced, encryption plays a key role in safeguarding sensitive information from unauthorized access. Within organizations, encryption helps to maintain the confidentiality, integrity, and authenticity of data, making it a vital tool for securing valuable assets. The encryption process transforms readable data (plaintext) into an unreadable format (ciphertext) using specific algorithms and keys. Only individuals with the correct decryption key can convert the ciphertext back to its original form, ensuring that the data remains secure from unintended recipients [1-5].

There are several encryption methods available, each with its own advantages and disadvantages. While encryption can secure data for a period of time, it is important to recognize that no encryption method can guarantee perpetual security. The level of security provided by encryption is heavily influenced by the algorithm used, the key's length and complexity, and how effectively the keys are safeguarded. Managing encryption keys is a significant challenge, as the security of the data depends on securely sharing the key between the sender and recipient. If the key is compromised, the encrypted data becomes vulnerable.

In more complex systems, encrypted data is often passed through multiple nodes or stations. Each node may re-encrypt the data using new keys, replacing the previous ones. This multi-layered encryption approach enhances overall security by adding additional barriers for attackers. Encryption methods range from traditional algorithms like DES (Data Encryption Standard) and RSA (Rivest-Shamir-Adleman) to more modern techniques like AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography). Choosing the right encryption algorithm depends on the desired level of security, available computational resources, and the specific requirements of the application.

Encryption relies on the principle of converting plaintext into ciphertext using a key, which is then used at the receiving end to restore the original data. This process is central to cryptography, which includes both encryption (encoding) and decryption (decoding). The strength of this process is crucial for securing data during transmission or while at rest, ensuring protection against unauthorized access or tampering.

Despite advancements in encryption technology, cryptanalysis, or the practice of code-breaking, remains a threat. Attackers continually develop new techniques to crack encryption and access protected data. As shown in Figure 1, cryptanalysis methods can sometimes reveal encrypted information, emphasizing the ongoing battle between enhancing encryption methods and adapting to the evolving strategies of attackers [6-10].

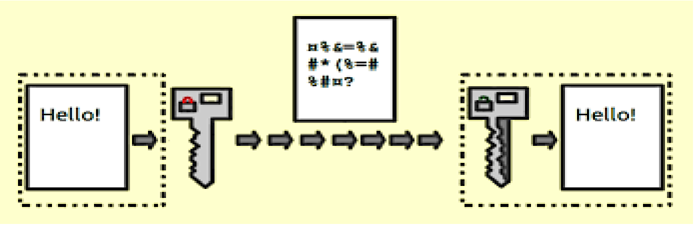


Figure 1. Encryption Process

Data security is vital for protecting sensitive information. As digital platforms continue to expand and data storage grows, encryption becomes increasingly important for safeguarding confidential business and personal data. In 6G networks, the scale, speed, and complexity demand advanced encryption methods to ensure security. Cryptography plays a crucial role in maintaining the confidentiality and integrity of information within communication systems. Encryption algorithms are integral to securing data transmission in high-speed 6G networks. Symmetric encryption methods like DES, AES, and Blowfish are commonly used due to their balance of speed and efficiency. This section reviews the performance of these algorithms in high-speed communication environments. Asymmetric algorithms, including RSA and ECC, are examined based on their application in 6G networks, with particular attention to key management, security, and computational efficiency. The performance of these algorithms is assessed by comparing their speed, security, energy consumption, and scalability in 6G environments. Research also explores their implementation challenges and benefits, especially in ultra-low latency and high-speed systems.

The integration of AI, IoT, and large-scale data in 6G networks introduces new security challenges. This section analyzes studies that discuss encryption methods designed to mitigate risks in next-generation networks. Key features of 6G, such as ultra-low latency, high bandwidth, and massive connectivity, require optimization of existing encryption algorithms. Energy efficiency is another critical factor in 6G networks. Lightweight encryption algorithms like ChaCha20, Speck, and Simon are evaluated against traditional methods for their performance and scalability. These algorithms are essential for ensuring security in real-time 6G applications. As 6G continues to evolve, technologies such as post-quantum cryptography, AI-enhanced encryption, and other innovations will become increasingly significant.

The literature emphasizes the importance of selecting appropriate encryption algorithms for 6G networks based on specific use cases. The comparative analysis of DES, RSA, AES, Blowfish, ECC, and 3DES reveals important trade-offs between security, efficiency, and scalability. To summarize the findings from the literature review on encryption techniques for 6G networks, we can create a detailed table outlining the key features, benefits, limitations, and performance metrics of each encryption method [11-17].

Table1: a comprehensive overview of encryption techniques

Encryption Technique	**Algorithm**	**Key Features**	**Strengths in 6G Networks**	**Limitations**	**Performance Metrics**	**Application Areas in 6G Networks**
DES (Data Encryption Standard)	Symmetric	56-bit key, block cipher (64-bit blocks)	Fast encryption/decryption, suitable for legacy systems	Vulnerable to brute-force attacks, limited security in modern contexts	Moderate latency, low resource consumption	Not recommended for high-security applications in 6G due to limited key size

Encryption Technique	Algorithm	Key Features	Strengths in 6G Networks	Limitations	Performance Metrics	Application Areas in 6G Networks
AES (Advanced Encryption Standard)	Symmetric	128, 192, 256-bit key, block cipher (128-bit blocks)	High security, widely adopted, scalable	High computational requirements	Low latency, efficient with large data volumes	Secure data transmission, real-time IoT applications
RSA (Rivest-Shamir-Adleman)	Asymmetric	Key length varies (1024-4096 bits), public/private key pair	Strong security, widely used for key exchange	Slower than symmetric algorithms, high computational overhead	High latency, energy-intensive	Secure key management, digital signatures
Blowfish	Symmetric	Variable key length (32-448 bits), block cipher (64-bit blocks)	Fast encryption, flexible key size, efficient	Susceptible to weak key attacks, not optimized for 6G scalability	Low latency, high efficiency	Suitable for lightweight applications, limited by key management in large-scale 6G networks
ECC (Elliptic Curve Cryptography)	Asymmetric	High security with shorter keys, elliptic curve-based	Efficient for mobile devices, energy-efficient, scalable for 6G	Complex implementation, requires careful curve selection	Low latency, optimized for small data packets	Secure communication in IoT devices, mobile applications in 6G
3DES (Triple Data Encryption Standard)	Symmetric	168-bit key, three-stage encryption	Improved security over DES, backward compatibility	Slower performance, vulnerable to certain attacks	High latency, moderate resource consumption	Legacy systems, transition applications from older standards to 6G

This table 1 provides a comprehensive overview of encryption techniques, helping to assess the most suitable options for 6G network applications based on various performance and security factors [18-23].

2. Sixth generation Networks

The increasing demand for faster and more reliable wireless communication has driven the ongoing development of mobile networks. The introduction of 6G networks represents a major leap in communication technology, offering unparalleled capabilities and enabling revolutionary applications. To fully realize the potential of 6G, it is essential for researchers and industry professionals to thoroughly understand its core features and the challenges that must be addressed. This study aims to provide an in-depth analysis of 6G networks, shedding light on their unique attributes and possible applications. By evaluating emerging trends and requirements, the study identifies key obstacles that must be overcome for the successful implementation and deployment of 6G technology.

The vision for 6G networks includes delivering incredibly fast data rates, minimal latency, extensive connectivity, enhanced security, and immersive user experiences. With the ability to support data rates in the terabits per second range and reduce latency to sub-millisecond levels, 6G networks can enable groundbreaking applications such as augmented reality (AR), virtual reality (VR), smart cities, and autonomous systems. Successfully integrating these applications into everyday life requires a robust and streamlined communication infrastructure [24-33].

However, implementing 6G networks comes with significant challenges. Spectrum scarcity remains a major concern due to increasing demand for bandwidth. This challenge necessitates innovative approaches for spectrum allocation and utilization. Additionally, energy efficiency is crucial as the rapid growth of interconnected devices and data traffic puts pressure on energy resources. Network densification, through the use of technologies like small cells and massive multiple-input multiple-output (MIMO), introduces complications related to deployment, interference management, and backhaul connectivity. The use of millimeter-wave (mmWave) frequencies, while enabling high data transmission speeds, presents challenges such as limited signal range and increased path loss. To enhance network performance and manage the vast number of connected devices, intelligent network management and resource allocation become essential. Safeguarding user data within 6G networks is also a priority, given the massive amount of sensitive information being transmitted and stored. To address these challenges, researchers are exploring various technologies and solutions. One promising approach is dynamic spectrum sharing, which allows for the coexistence and optimal use of spectrum resources across multiple services. Energy-efficient network architectures aim to reduce energy consumption by incorporating strategies such as sleep modes and adaptive power control algorithms. Advanced antenna technologies, including beamforming and beam tracking, improve coverage and capacity in mmWave communications. The application of machine learning and artificial intelligence in network optimization offers exciting opportunities for the creation of intelligent, self-optimizing networks. Additionally, the integration of blockchain-based security solutions could enhance the trust and privacy features of 6G networks. This study also explores the future prospects of next-generation wireless networks beyond 6G. Key technologies such as terahertz communication, satellite networks, reconfigurable intelligent surfaces, edge computing, and AI-driven network optimization are examined in the context of ongoing research and future developments. By thoroughly analyzing the complexities of 6G networks and addressing the associated challenges, this study provides valuable insights for academics, industry professionals, and policymakers. Understanding the characteristics of 6G networks and envisioning their future trajectory will enable stakeholders to make informed decisions and contribute to the advancement of resilient, efficient, and groundbreaking wireless communication systems [34-36].

2.1. Reflective Analysis of 6G Networks

The emergence of 6G networks signifies the beginning of a new chapter in the evolution of wireless communication technology. The purpose of this section is to provide a detailed understanding of the components, key characteristics, and potential applications of 6G networks. By 2030, 6G mobile communication technology is expected to drive the realization of the Internet of Everything. While the global rollout of 5G is still in progress, Beyond 5G (B5G) developments are already well underway. Researchers have begun planning, envisioning, and outlining the requirements for the future 6G network. Additionally, several countries have already initiated investigations into 6G technologies [37-38] .

2.2 An Overview of 6G Networks

It is essential to establish a clear and precise definition of a 6G network. Sixth Generation (6G) refers to the next evolution of mobile networks following 5G technology. While there is not yet a universally agreed-upon definition, 6G is envisioned as an advanced wireless communication system that surpasses its predecessors in terms of data transmission speed, reduced latency, connectivity, security, and enhanced user experiences [39].

2.3 Fundamental Attributes of 6G Networks

Building on the advanced capabilities introduced by 5G, 6G networks are expected to bring forth groundbreaking functionalities that will significantly reshape the wireless communication landscape. One of the primary goals is to achieve extremely high data rates, potentially reaching terabits per second, to support bandwidth-intensive applications and allow seamless streaming of high-definition content. Another crucial goal is to achieve ultra-low latency, reducing delays to sub-millisecond levels. These advancements will enable instantaneous interactions for a variety of applications, including remote surgery, autonomous vehicles, and virtual reality gaming [40-42].

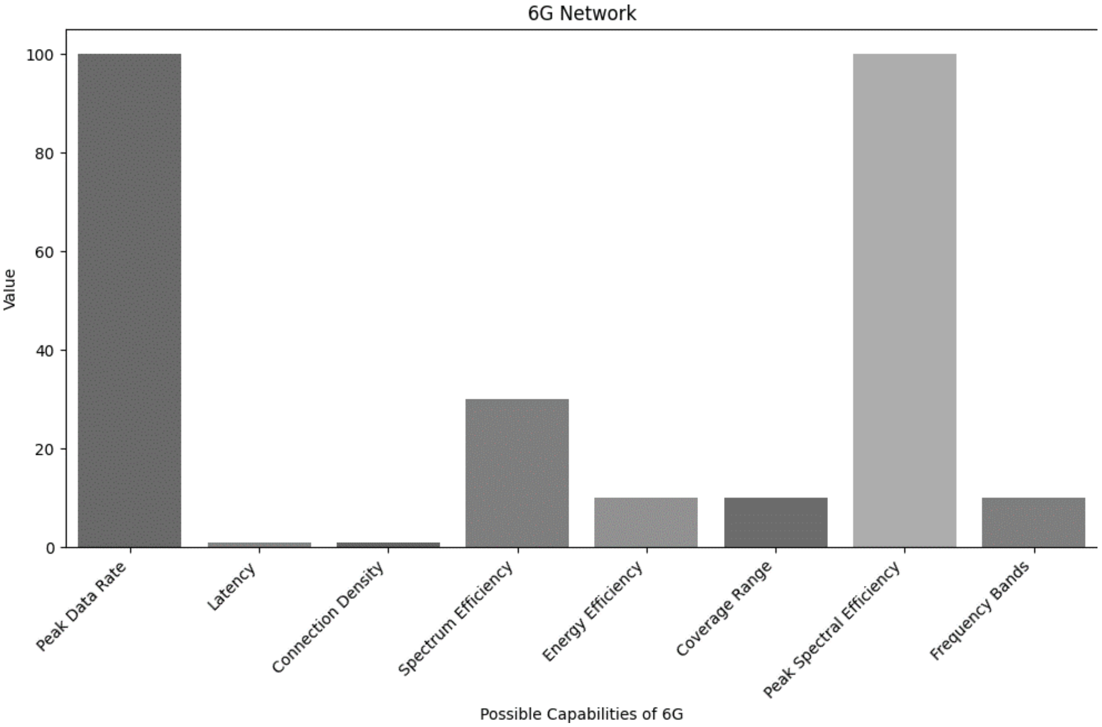


Figure 2. 6G network fields of source

2.4. Overview of Potential Applications of 6G Networks

The vast capabilities of 6G networks open up numerous opportunities for the development of innovative applications across various industries. The integration of augmented reality (AR) and virtual reality (VR) has the potential to revolutionize entertainment, gaming, and education by allowing users to interact with immersive virtual environments. In the healthcare sector, 6G networks could enable remote surgeries, telemedicine, and real-time patient monitoring, expanding healthcare access and improving patient outcomes.

In smart cities, 6G technology could enhance urban infrastructure, optimize transportation systems, and support efficient energy management. Autonomous systems, such as self-driving vehicles and unmanned aerial vehicles (UAVs), could benefit from the low latency and reliable connectivity of 6G networks, ensuring secure and efficient operations.

2.5. Challenges in Implementing 6G Communications

The implementation and development of 6G networks present numerous challenges that must be addressed to fully leverage the potential of this advanced wireless communication technology. This section of the study aims to explore the key obstacles, as illustrated in Figure 3 [43-47].

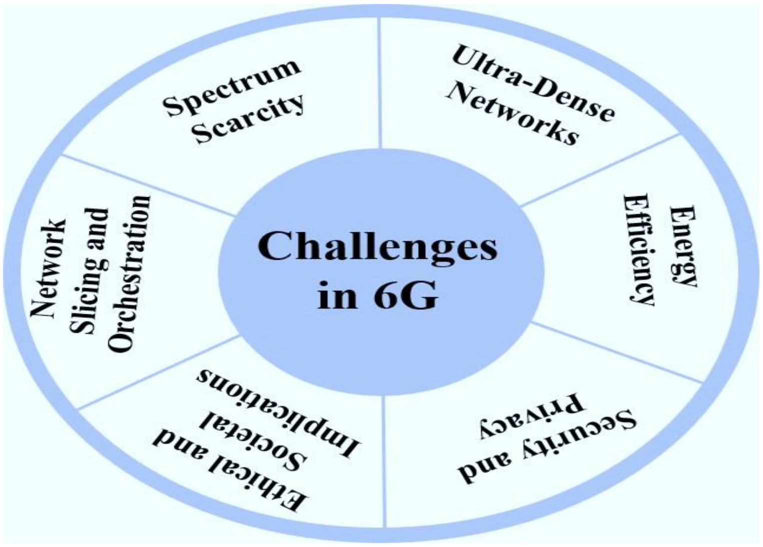


Figure 3. 6G Challenges

2.6. Limited range of frequencies

One of the main challenges in 6G communications is the scarcity of available spectrum. As the demand for faster data rates and improved connectivity continues to grow, the frequency spectrum becomes an increasingly limited resource. To tackle this issue, researchers are exploring innovative solutions, including spectrum sharing, dynamic spectrum allocation, and the use of underutilized frequency bands. Additionally, it is essential to enhance spectrum management policies and regulations to efficiently allocate and utilize the existing spectrum resources [48].

3. Cryptography Components

A. *The organization of cryptography terminology*

It is essential to comprehend this language because it accurately describes every algorithm we will discuss. We will focus on Common terms are used to illustrate encryption-related terminology in figure 4.

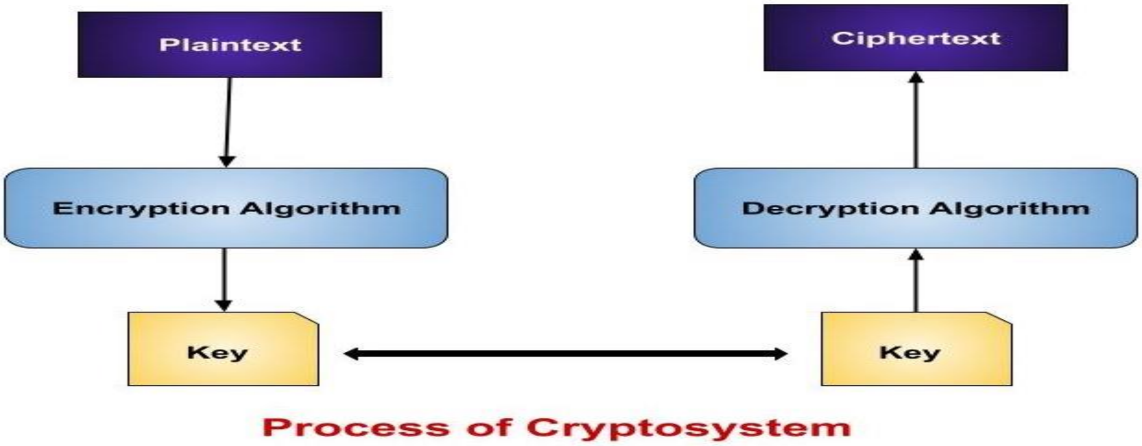


Figure 4. Encryption process

B. Plain Text or Normal Text

Plain text refers to text that is not formatted and lacks any special styling. The term "undisputed text" is used to describe the original text or message being discussed.

C. Cipher Text

Cipher text is the result of transforming plain text through encryption, rendering the original message unreadable.

D. ***Encryption***

Encryption is the process of transforming plain or original text into ciphertext, rendering it unreadable to unauthorized users.

E. Decryption

Decryption is the process that reverses encryption, converting cipher text back into its original readable form.

F. Key

A key is a sequence that can be numerical or alphanumeric, often represented as a mathematical formula. In an encryption system, the plain text undergoes encryption, while the decoding process applies to the cipher text [49].

4. Main Objectives of Cryptography

Encryption, or cryptography, must fulfill specific requirements to benefit consumers. Modern cryptography focuses on achieving four main objectives:

1. **Privacy**
   Information should be unintelligible to anyone for whom it was not intended.
2. **Integrity**
   Data must remain tamper-proof during storage and transmission, with any modifications easily detectable.
3. **Non-repudiation**
   This guarantees that a party cannot deny the authenticity or integrity of a message or action they have executed. The creator or issuer of the data cannot later deny their intentions related to the creation or distribution of the information.
4. **Authentication**
   Both the sender and receiver are able to verify each other's identities, along with the source and destination of the information.
5. **Access Control**
   Access to data is limited to authorized users only to prevent unauthorized access.

The process of encrypting plain text utilizes a method called an "encryption algorithm," while the decryption of cipher text involves a technique known as a "decryption algorithm." A key is crucial in both the encryption and decryption processes. The security level of cryptography is determined by the key space or key length, which refers to the size of the key. [50-53].

5. Encryption Algorithms

This section will explore various cryptographic algorithms to assess their performance. Before diving into the evaluation, it's crucial to define what an algorithm is. An algorithm is a finite set of clear instructions designed to generate a specific output for any valid input within a designated timeframe. The encryption techniques we will examine include DES, RSA, AES, BLOWFISH, ECC, and 3DES.

A. DES (Data Encryption Standard)

The Data Encryption Standard, abbreviated as DES, was developed in the early 1970s at IBM laboratories under the supervision of Horst Feistel. It received initial approval from the National Bureau of Standards (now known as NIST, the National Institute of Standards and Technology) in 1978. DES was standardized by the American The Data Encryption Standard (DES) was adopted by the National Standards Institute (ANSI) under the designation ANSI X3.92 and is commonly referred to as the Data Encryption Algorithm (DEA). However, it is now considered outdated for symmetric key encryption. The DES process involves 16 rounds of encryption on each 64-bit block of data. Despite using a 64-bit key, the effective key length is 56 bits, meaning that only 56 bits are actively used in the encryption process.

B. Triple Data Encryption Standard (3DES)

In cryptography, a range of techniques and methodologies are employed to secure data. The Triple Data Encryption Standard (3DES), also known as the Triple Data Encryption Algorithm (TDEA), is a symmetric-key block cipher that enhances the security of DES by applying it three times to each data block. Introduced by IBM in 1978 as a more secure alternative to DES, 3DES uses the DES encryption method three times on the same data, which is why it is sometimes referred to as T-DES. This repeated application strengthens the encryption, as depicted in Figure 5.

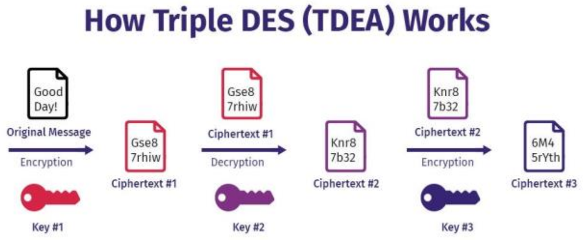


Figure 5. 3DES Structure

C. RSA (Rivest-Shamir-Adleman Algorithm)

The RSA algorithm, also known as the Rivest-Shamir-Adleman algorithm, is one of the most significant public-key cryptosystems. Widely utilized and highly regarded for its effectiveness, RSA is a well-known public-key encryption scheme. It operates with large integers, typically 1,024 bits in size, and performs a single round of encryption, resulting in a non-uniform cipher. RSA is employed by modern computers for both encryption and decryption of messages. Classified as an asymmetric cryptography algorithm, it utilizes two distinct keys—one for encryption and another for decryption, as illustrated in Figure 6 [54-57].

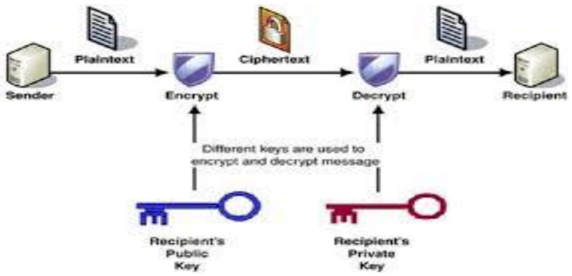


Figure 6. RSA Algorithm

D. ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) was developed in 1985 by Victor Miller from IBM and Neil Koblitz from the University of Washington, serving as a modern alternative to conventional public-key encryption techniques. ECC leverages the mathematical properties of elliptic curves over finite fields, relying on elliptic curve theory. Compared to other encryption algorithms, ECC offers faster key generation, smaller key sizes, and greater efficiency. The encryption process is based on the elliptic curve equation, represented by a mathematical formula, as depicted in Figure 7.

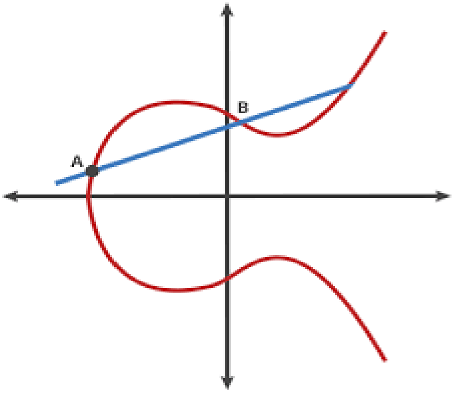


Figure 7. Elliptic Curve Representation

E. AES (Advanced Encryption Standard)

In 1997, the National Institute of Standards and Technology (NIST) initiated a program to identify a successor to the Data Encryption Standard (DES), with the goal of completing this selection by 2001. The Advanced Encryption Standard (AES) was ultimately selected to replace both DES and 3DES. Designed by Vincent Rijmen and Joan Daemen, AES was established in 2001 as a symmetric block cipher employed by the U.S. government to secure classified information. It is widely utilized around the world in both software and hardware for the encryption of sensitive data. AES consists of three distinct block ciphers: AES-128, AES-192, and AES-256. Each of these ciphers processes 128-bit data blocks and utilizes cryptographic keys of 128, 192, and 256 bits, respectively. The encryption and decryption processes involve a series of rounds: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, as depicted in Figure 8 [58].

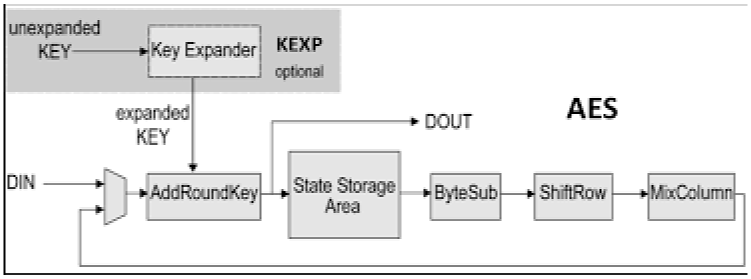


Figure 8. AES Algorithm

F. Blowfish

Blowfish was developed by Bruce Schneier in 1993. It is a symmetric block cipher that accommodates key sizes ranging from 32 bits to 448 bits, operating with a block size of 64 bits. Blowfish is a Feistel cipher that performs 16 rounds and employs S-Boxes that depend on a large key. As shown in Figure 9, each S-box contains 32 bits of data.

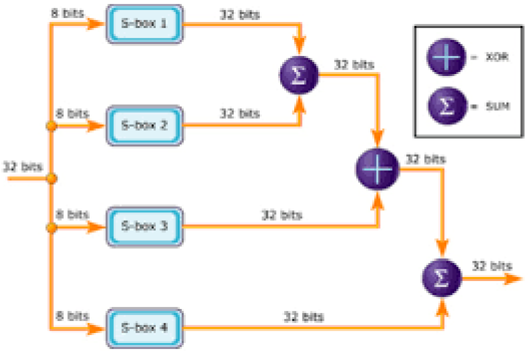


Figure 7. Blowfish Function F.

Conclusion

This study emphasizes the vital role of strong encryption methods in protecting data within the rapidly advancing realm of 6G networks. Given that these networks offer ultra-low latency, extensive connectivity, and high bandwidth, securing data transmission has become increasingly complex yet essential. Our comparative analysis of various encryption algorithms—such as DES, RSA, AES, Blowfish, ECC, and 3DES—demonstrates that each method possesses unique strengths and weaknesses. Therefore, the selection of an encryption technique should align with the specific requirements of 6G communication.

The study highlights that while traditional encryption algorithms are effective in many situations, they may need enhancements or alternatives to tackle the distinctive challenges presented by the fast and scalable nature of 6G networks. Algorithms like AES and ECC, recognized for their robust security and efficiency, stand out as particularly viable options for future applications. Additionally, the incorporation of advanced technologies such as AI and IoT further intensifies the necessity for adaptive and resilient cryptographic solutions.

Our findings offer valuable insights into optimizing encryption strategies to fulfill the evolving demands of 6G communication. By identifying the most appropriate encryption methods, this research contributes to improving data confidentiality and security, ensuring that as 6G networks progress, they are built on a strong foundation of data protection.

REFERENCES

1. Zahoor, M.M.; Khan, S.H.; Alahmadi, T.J.; Alsahfi, T.; Mazroa, A.S.A.; Sakr, H.A.; Alqahtani, S.; Albanyan, A.; Alshemaimri, B.K. Brain Tumor MRI Classification Using a Novel Deep Residual and Regional CNN. Biomedicines 2024, 12, 1395. https://doi.org/10.3390/biomedicines12071395

2. H.A. Sakr and M.A. Mohamed. "Handover Management Optimization over LTE-A Network using S1 and X2 handover," Proc. of The Seventh International Conference on Advances in Computing, Electronics and Communication - ACEC 2018, ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-11, pp. 58–64, 2018.

3. Giordani, M., Polese, M., Roy, A., Zorzi, M., & Mezzavilla, M. (2020). Toward 6G networks: Use cases and technologies. IEEE Communications Magazine, 58(3), 55-61.

4. Amin, R., Rehman, A., & Khan, I. (2021). A comprehensive study on security challenges in 6G networks. IEEE Access, 9, 148051-148067.

5. Alouini, M.-S. (2020). Towards 6G networks: Application of communication technologies beyond 5G. IEEE Communications Magazine, 58(3), 56-62.

6. Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Ghafoor, M. I., & Sakr, H. A. (2023, January). "In MANET: An Improved Hybrid Routing Approach for Disaster Management". In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-6). IEEE.

7. Sakr, Hesham A., and Magda I El-Afifi. "Mechanisms of system penetration." Nile Journal of Communication and Computer Science (2023).

8. Saad, W., Bennis, M., & Chen, M. (2019). AI and IoT in 6G: New challenges for security. IEEE Communications Standards Magazine, 3(4), 66-72.

9. Miller, V. (1985). Security Implications of Elliptic Curve Algorithms.

10. Khan, S. H., Alahmadi, T. J., Alsahfi, T., Alsadhan, A. A., Mazroa, A. A., Alkahtani, H. K., ... & Sakr, H. A. (2023). COVID-19 infection analysis framework using novel boosted CNNs and radiological images. Scientific Reports, 13(1), 21837.

11. Bernstein, D. J. (2008). Cryptographic Solutions for Real-Time 6G Systems.

12. Zhao, Z., et al. (2020). Next-Generation Encryption for Ultra-Low Latency Networks.

13. H.A. Sakr, A. I. Abdel-Fatah, A. T. Khalil. "Performance Evaluation of Power Efficient Mechanisms on Multimedia over LTE-A Networks," International Journal on Advanced Science, Engineering and Information Technology (IJASEIT), vol. 9, no. 4, pp. 1096-1109, 2019.

14. Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Maaliw, R. R., & Sakr, H. A. (2023, January). "Constructor Development: Predicting Object Communication Errors." In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-7). IEEE.

15. Zong, B., Fan, C., Wang, X., Qin, Y., & Wang, Z. (2019). 6G vision and requirements: Is it truly 6G? IEEE Network, 33(4), 138-145.

16. Giordani, M., et al. (2020). Securing Massive Connectivity in 6G Networks.

17. El-afifi, Magda I., and Hesham A. Sakr. "Intelligent Traffic Management Systems: A review." Nile Journal of Communication and Computer Science (2023): 1-16.

18. H.A.Sakr, and M.A.Mohamed. “Performance Evaluation Using Smart: HARQ Versus HARQ Mechanisms Beyond 5G Networks”, Wireless Personal Communications (Springer), pp. 1-26, ISSN: 1572-834X, June 2019.

19. Abdel-Azim, M., Awad, M. M., & Sakr, H. A. “VoIP versus VoMPLS Performance Evaluation”, International Journal of Computer Science Issues (IJCSI), 11(1), 194, 2014.

20. Rivest, R. L., et al. (1978). Public-Key Cryptosystems in Modern Communication.

21. Zhao, Z., Li, Z., Chen, Y., & Zhou, Y. (2020). 6G mobile communication technology: Vision, trends, and challenges. China Communications, 17(11), 2-12.

22. Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., ... & Fan, P. (2019). 6G wireless networks: Vision, requirements, architecture, and key technologies. IEEE Vehicular Technology Magazine, 14(3), 28-41.

23. Grover, L. K. (1996). Quantum Security Considerations in 6G Networks.

24. Saad, W., Bennis, M., & Chen, M. (2019). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network, 34(3), 134-142.

25. Abeer Twakol Khalil, A. I. Abdel-Fatah and Hesham Ali Sakr. “Rapidly IPv6 multimedia management schemes based LTE-A wireless networks", International Journal of Electrical and Computer Engineering (IJECE), vol. 9, no. 4, pp. 3077-3089, 2018.

26. Beaulieu, R., et al. (2015). Evaluating Lightweight Block Ciphers for High-Efficiency Applications.

27. Alouini, M-S. (2020). Adapting Cryptography to 6G Requirements.

28. Stallings, W. (2017). Evolving Cryptographic Standards for 6G.

29. Amin, R., et al. (2021). Towards a Secure 6G Future: Emerging Threats and Solutions.

30. M. Abdel-Azim, M., Awad, M. M., & Sakr, H. A. “RSVP Based MPLS versus IP Performance Evaluation”, Mediterranean Journal of Computers and Networks (MEDJCN), 10(2), 2014.

31. Mansour, Nehal A., and Hesham A. Sakr. "The Role of data mining in healthcare Sector." Nile Journal of Communication and Computer Science 4.1 (2023): 1-11.

32. Sakr, H. A., H. M. Ibrahim, and A. T. Khalil. "Impact of Smart Power Efficient Modes on Multimedia Streaming Data Beyond 5G Networks." Wireless Personal Communications (2022): 1-37.

33. ALMEIDA, FRIBAN, Hesham A. Sakr, et al.. "Detecting Three Different Diseases of Plants by Using CNN Model and Image Processing." J. Electrical Systems 20.2 (2024): 1519-1525.

34. Ibrahim, M., Bajwa, I. S., Sarwar, N., Hajjej, F., & Sakr, H. A. (2023). “An Intelligent Hybrid Neural Collaborative Filtering Approach for True Recommendations”. IEEE Access.

35. Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., ... & Fan, P. (2019). 6G wireless networks: Vision, requirements, architecture, and key technologies. IEEE Vehicular Technology Magazine, 14(3), 28-41.

36. Zhao, Z., et al. (2020). Next-Generation Encryption for Ultra-Low Latency Networks.

37. A. A. Eladl, M. E. El-Afifi, and M. M. El-Saadawi, "Optimal Power Dispatch of Multiple Energy

Sources in Energy Hubs" 2017 Nineteenth International Middle East Power Systems Conference (MEPCON), Cairo, Egypt, 19-21 Dec. 2017, pp. 1053-1058.

38. A. A. Eladl, M. E. El-Afifi, and M. M. El-Saadawi, " Communication Technologies Requirement for Energy Hubs: A survey " 2019 21st International Middle East Power Systems Conference (MEPCON), Tanta, Egypt, 17-19 Dec. 2019.
39. A. A. Eladl, M. E. El-Afifi, and M. M. El-Saadawi, "Optimal Operation of Energy Hubs Integrated with Renewable Energy Sources and Storage Devices Considering CO2 Emissions ", International Journal of Electrical Power & Energy Systems, 2020, 117, 105719
40. M. I. El-Afifi, M. El-Saadawi and A. A. Eladl, " Cogeneration Systems Performance Analysis as a Sustainable Clean Energy and Water Source based on Energy Hubs Using Archimedes Optimization Algorithm", Sustainability, 14(22), 14766, 2022.
41. A. A. Eladl, M. I. El-Afifi, M. El-Saadawi, and Bishoy E. Sedhom, "A Review on Energy Hubs: Models, Methods, Classification, Applications, and Future Trends" Alexandria Engineering Journal, Vol. 68, 1 April 2023, pp.315-342.
42. A. A. Eladl, M. I. El-Afifi, M. M. El-Saadawi and B. E. Sedhom, "Distributed optimal dispatch of smart multi-agent energy hubs based on consensus algorithm considering lossy communication network and uncertainty," in CSEE Journal of Power and Energy Systems, doi: 10.17775/CSEEJPES.2023.00670.
43. R. M. Ibrhim, M. M. Elkelany, M. I. El-Afifi, Trends in Biometric Authentication: A review. Nile Journal of Communication and Computer Science, 2023.
44. Magda I. El-Afifi, et al. An IoT-fog-cloud consensus-based energy management algorithm of multi-agent smart energy hubs considering packet losses and uncertainty. Renewable Energy, 2023, 119.
45. M. I. El-Afifi, H. A. Sakr, Security Issues and Challenges for IoT-based Smart Multi Energy Carrier Systems. Nile Journal of Communication and Computer Science, 2023.
46. M. I. El-Afifi, Walaa A. Abdelrazik, Renewable Energy Sources Applications in Currently Occupied Structures. Nile Journal of Communication and Computer Science, 2023.
47. H. A. Sakr et al., "Al-based Traffic System: A Novel Approach," 2023 24th International Middle East Power System Conference (MEPCON), Mansoura, Egypt, 2023, pp. 1-6, doi: 10.1109/MEPCON58725.2023.10462361.
48. M. I. El-Afifi, A. A. Eladl, and Bishoy E. Sedhom., " Smart Building Demand Side Management Using Multi-Objective Archimedes Optimization Algorithms," 2023 24th International Middle East Power System Conference (MEPCON), Mansoura, Egypt, 2023, pp. 1-6, doi: 10.1109/MEPCON58725.2023.10462410.
49. H. A. Sakr & M. I. El-Afifi. "A Framework for Confidential Document Leakage Detection and Prevention". Nile Journal of Communication and Computer Science, 2024.
50. S. Fawzy, E. E. Abd-Raboh, M. I. El-Afifi & A. A. Eladl, Optimal location and operation of energy storage and transmission switching for minimizing wind power spillage. Journal of Energy Storage,

2024, 90, 111925.

51. Magda I. El-Afifi, et al. "Demand Side Management Strategy for Smart Building Using Multi-Objective Hybrid Optimization Technique." Results in Engineering, 2024, 102265.
52. M. I. El-Afifi, SSAFR Team, & M. M. Elkelany, Development of Fire Detection Technologies. Nile Journal of Communication and Computer Science, 2024, 7(1), 58-66.
53. M. I. El-Afifi, Solar Energy: Our Future for Sustainable Energy. Nile Journal of Communication and Computer Science, 2024, 7(1), 67-83.
54. A. A. Eladl, M. I. El-Afifi, Saadawi, P. Siano, & B. E. Sedhom, Multi-Objective optimal scheduling of energy Hubs, integrating different solar generation technologies considering uncertainty. International Journal of Electrical Power & Energy Systems, 2024, 161, 110198.
55. M. I. El-Afifi, B. E. Sedhom, S. Padmanaban, S., & A. A. Eladl, A review of IoT-enabled smart energy hub systems: Rising, applications, challenges, and future prospects. Renewable Energy Focus, 2024, 100634.
56. H. A. Sakr, M. M. Fouda, A. F. Ashour, A. Abdelhafeez, M. I. El-Afifi, & M. R. Abdellah, M. R. Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. Egyptian Informatics Journal, 2024, 28, 100540.
57. El-Afifi, Magda I., et al. "Survey of technologies, techniques, and applications for big data analytics in smart energy hub." Energy Strategy Reviews 56 (2024): 101582.
58. Ibrahim, H. M., Khalil, A. T., & Sakr, H. A. (2024). Enhancing the Quality of Multimedia Streaming over Radio Resource Management and Smart Antennas of 5G Networks. *Wireless Personal Communications*, 1-36.