Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2527–2537
DOI : 10.47974/JDMSC-2337

Exploration and comparison of cryptographic algorithms for security

Rekha Jain [#]
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Aditya Vikram Agarwal [†]
Orbit Systems Inc
Columbus 43235
Ohio OH
United States

Rajat Goel [§]
V. Jeyakrishnan [‡]
C. S. Lamba [@]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Linesh Raja *
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[#] *E-mail:* Rekha.jain@jaipur.manipal.edu
[†] *E-mail:* adityavagarwal.research@gmail.com
[§] *E-mail:* rajat.goel@jaipur.manipal.edu
[‡] *E-mail:* jeyakrishnan.v@jaipur.manipal.edu
[@] *E-mail:* cs.lamba@jaipur.manipal.edu
* *E-mail:* linesh.raja@jaipur.manipal.edu (Corresponding Author)

Abstract

Cryptography is one of the cornerstones of secured communication in the digital age, enabling confidentiality, integrity, and authentication in various applications. This paper provides an exploration and comprehensive review of cryptography algorithms, discussing their underlying principles, strengths, weaknesses, and areas of application. The review covers classical algorithms like RSA, DES, and AES, as well as modern advancements, including elliptic curve cryptography and post-quantum cryptography. Additionally, it addresses the challenges faced by cryptography in the era of evolving technological threats.

Subject Classification: *Primary 68R01, Secondary 97N70.*

Keywords: *Cryptography, AES, DES, Security, RSA algorithms.*

1. Introduction

Cryptography is a crucial component in securing data in an increasingly digital world. As data breaches, cyber-attacks, and digital espionage continue to rise, robust cryptographic algorithms are essential to protect sensitive information. It is an essential discipline in securing digital communications and data, forming the backbone of modern information security systems. As technology advances, cryptographic algorithms have evolved to address emerging threats and vulnerabilities.

This paper reviews the key cryptographic algorithms, analyzing their effectiveness in various contexts and their resilience against emerging threats. It is a fundamental technology that underpins the security of digital communications, data storage, and authentication. Over the era, several cryptographic algorithms have been developed, each with distinct features, advantages, and vulnerabilities. The proposed work support secure institutions and digital justice which is related to SDG 16. Section 2 focuses on literature survey. Section 3 describes classical cryptography algorithms whereas modern cryptography algorithms are mentioned in section 4. Section 5 provides comparative study of cryptography algorithms. Challenges faced in cryptography are discussed in section 6. Finally, paper concludes with section 7.

2. Literature Survey

Cryptography has evolved significantly over the past few decades, driven by the need for secure communication and data protection. This literature survey provides an overview of key developments, foundational algorithms, and current research trends in cryptography. Cryptography

has long been a fundamental pillar in ensuring secure communication in the digital era.

One of the most notable advancements in modern cryptography is the implementation of the Data Encryption Standard (DES), which became a widely adopted encryption algorithm. However, with advancements in computational power, DES's vulnerability to brute-force attacks became apparent, prompting the need for more secure algorithms. This led to the creation of the Advanced Encryption Standard (AES), now established as encryption standard globally due to its robustness and efficiency.

Diffie and Hellman announced public key cryptography in 1976. They marked another significant milestone in this field. This approach allowed for secure key exchange over insecure channels, addressing one of the major limitations of symmetric key cryptography [1]. The RSA algorithm, developed by Rivest and colleagues in 1977 and is a widely known implementation of public key cryptography and is still extensively used today for securing sensitive data [2].

With the expansion of the internet and e-commerce, the importance of cryptography has only grown. The "SSL (Secure Sockets Layer) and TSL (Transport Layer Security)" are the protocols that rely on cryptographic techniques to secure online communications, making them essential for activities such as online banking and shopping.

The DES algorithm, standardized in 1977 by the NIST (National Institute of Standards and Technology), was a pioneering block cipher with a "56-bit" key length. DES uses a Feistel network and has 16 rounds of encryption. Despite its initial strength, DES was ultimately deemed insecure because of its limited key length, which made it susceptible to brute-force attacks [3,4]

RSA is introduced in 1977, as public-key algorithm that depends on the mathematical challenge of factoring of large integers. RSA provides both encryption as well as digital signatures. It remains widely used for secure communications and digital authentication. Its security is based on the factorization problem [2,5]

Daemen and Rijmen introduced AES in 2001 as an auxiliary for DES [6]. It functions on "128-bit" blocks with key sizes of "128, 192, or 256" bits. Substitution-permutation network is the basis, and it is renowned for its security and efficiency. AES's robustness against cryptanalytic attacks has made it the standard encryption algorithm for modern applications [7].

As compared with RSA, ECC provides a high level of security. It has shorter key lengths that makes it efficient for restricted environments like mobile devices. The basis of it is the Elliptic Curve Discrete Logarithm

Problem and it has become increasingly popular for both encryption as well as digital signatures [6,8,9].

Twofish, designed by B. Schneier and his team, is a symmetric block cipher that offers a key length of up to "256 bits" and operates on "128-bit" blocks. It is known for its speed and security and was a finalist in the AES competition. It is particularly used in software implementations [10].

SHA-2 is introduced in 2001. It is a family of hash functions including "SHA-224, SHA-256, SHA-384, and SHA-512" [11]. It replaced the aging "SHA-1" due to vulnerabilities. "SHA-3", released in 2015, is based on the Keccak sponge construction and provides an alternative to "SHA-2", offering similar security with different internal structures [10] [6].

With the emergence of quantum computing, traditional cryptographic algorithms face new challenges [12]. "Post-Quantum Cryptography (PQC)" objects to develop algorithms that are impervious to quantum attacks [13]. Some cryptography techniques like Lattice-based cryptography and hash-based signatures are promising approaches in this field [14,15].

Cryptographic algorithms are fundamental to blockchain technology and cryptocurrencies like Bitcoin. They ensure transaction integrity, security, and decentralization. SHA-256 is used in Bitcoin's proof-of-work algorithm, and elliptic curve cryptography secures digital wallets and transactions [16].

3. Classical Cryptographic Algorithms

3.1 *RSA Algorithm*

It was introduced by Rivest, Adleman and Shamir in 1978. It is based on key concepts like: Public and Private Keys. Its security is contingent on key length, and with the onset of quantum computing, its long-term viability is under threat. Shor's algorithm, a quantum-based method can efficiently factor large integers, which could potentially render RSA obsolete [5].

Figure 1 shows the functioning of RSA algorithm. RSA's key generation is computationally expensive, and its security is threatened by potential quantum computing advancements. The challenge of factoring large integers ensures the security of the RSA algorithm. As long as sufficiently large key sizes are used, RSA is resistant to brute-force attacks. RSA is implemented in many security protocols, incorporating SSL/TLS to ensure secure web browsing and is used for securing emails, software, and digital certificates.

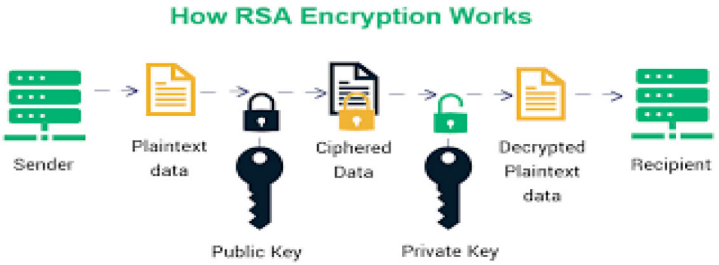

Figure 1

Functioning of RSA algorithm [17]

3.2 *DES (Data Encryption Standard)*

The DES is called as Data Encryption Standard. It was embraced by the "U.S. government" in 1977. It is used for encryption of digital data [3]. DES operates on "64-bit" blocks of data using a "56-bit" key, utilizing the sequence of permutations and substitutions. Despite its initial robustness, DES's relatively short key length made it vulnerable to exhaustive key search attacks. Its vulnerability led to the development and adoption of more secure alternatives like the Advanced Encryption Standard (AES) [6].

Relatively the short key length of DES makes it susceptible to brute-force attacks [7,18], resulting in its gradual replacement by more secure algorithms such as AES. Data Encryption Standard is relatively simple to implement and was widely adopted in hardware and software for secure data transmission. It set the standard for cryptographic security in the late 20^{th} century and influenced the design of later encryption algorithms. The encryption process in DES is based on a Feistel network, which consists of multiple rounds of processing. Each round involves permutations and substitutions that scramble the input data to produce the ciphertext.

3.3 *AES (Advanced Encryption Standard)*

In 1999, Daemen and Rijmen introduced AES algorithm [19]. It was selected as the replacement for DES following a public race. It uses key sizes of "128, 192, or 256 bits", offering robust security against known practical attacks [20]. AES's design makes it extremely resistant to cryptographic attacks, including differential and linear cryptanalysis. It is efficient in both hardware and software deployment, making it widely

applied in various contexts, from securing internet communications for encrypting files and databases.

4. Modern Cryptographic Algorithms

4.1 *Elliptic Curve Cryptography (ECC)*

Elliptic Curve Cryptography offers a substitute to RSA by providing similar security with significantly shorter key lengths. This efficiency makes ECC especially attractive for application in constrained environments, like mobile devices and IoT applications [8,9]. The security of ECC depends on the elliptic curve discrete logarithm problem, that is currently considered hard to solve. However, as with RSA, ECC's security is threatened by quantum computing, which could solve these problems using algorithms like Shor's [5].

4.2 *Post-Quantum Cryptography (PQC)*

Post-Quantum Cryptography is a burgeoning field aimed at creating cryptographic algorithms which are resistant to quantum attacks. Cryptography, known as Lattice-based cryptography stands out as a highly promising approach, takes advantage of the difficulty of lattice problems, which are considered to withstand both classical and quantum attacks [15]. Research by Peikert highlights the potential of lattice-based schemes in achieving quantum-resistant security [14]. The NIST has also started a process to standardize PQC algorithms, further accentuating the importance of this research area. PQC is still in development, and many algorithms are yet to be fully standardized or optimized for practical use.

4.3 *BlowFIsh*

Blowfish is one of the symmetric-key algorithms that is based on block cipher, was designed by B. Schneier in 1993. It was developed as a fast and secure alternative to the then-ubiquitous DES, which was becoming susceptible to brute-force attacks because of its relatively short key length [21].

4.4 *TwoFish*

Twofish is an algorithm that uses symmetric keys based on block cipher and created by B. Schneier, along with a team of cryptographers, as a successor to the Blowfish algorithm. Twofish was one of the five finalists

in the competition to select the AES, ultimately losing to Rijndael (AES), but it remains a robust and widely respected encryption algorithm [10].

4.5 *SHA-256 (part of SHA-2)*

SHA-256 (Secure Hash Algorithm with 256-bit output) is a cryptographic hash function that is part of the SHA-2 (Secure Hash Algorithm 2) family, designed by the NSA (National Security Agency) and published by NIST in 2001. SHA-256 is extensively utilized in a range of security applications as well as protocols, such as SSL/TLS, digital certificates, and blockchain technologies like Bitcoin [11].

Table 1

Comparison of Cryptography Algorithms

Algorithm	Security Basis	Strengths	Weaknesses
RSA	Integer Factorization Problem	Widely adopted, proven security	Computationally expensive, vulnerable to quantum attacks
DES	Feistel Network	Simple and fast	Short key length, vulnerable to brute-force attacks
AES	Substitution Permutation Network	Highly secure, efficient in both hardware and software	Potential future vulnerability to quantum computing
ECC	Elliptic Curve Discrete Logarithm Problem	Efficient, small key sizes for high security	Complexity in implementation, quantum threat
Blowfish	Feistel Network	Fast, flexible key length	Weaknesses in certain applications, limited to smaller data blocks
Twofish	Feistel Network	More secure than Blowfish, flexible	Slower than AES in some implementations
SHA-256	Merkle–Damgård construction, Secure Hash Algorithm	Highly secure, widely used in digital signatures	Computationally intensive for some applications
SHA-3	Keccak algorithm, sponge construction	Secure, resistant to different attack vectors	Relatively new, less tested in real-world applications

4.6 *SHA-3*

SHA-3 (Secure Hash Algorithm 3) is a cryptographic hash function introduced by the National Institute of Standards and Technology (NIST) in 2015 [11]. It is a member of the SHA (Secure Hash Algorithm) group, but unlike its precursors, "SHA-1, SHA-2 and SHA-3" is based on a completely different construction [6]. It is known as the Keccak (pronounced "ketchak") algorithm, which was selected through an open competition held by NIST.

5. Comparison of Cryptography Algorithms

Table-1 compares various cryptographic algorithms based on their type, key length, security basis, strengths, weaknesses, and typical use cases. Each algorithm serves different purposes based on computational constraints and the security requirements of the application [12,18].

6. Challenges in Cryptography

6.1 *Quantum Computing and Cryptographic Vulnerabilities*

The advancement of quantum computers presents a serious threat to numerous commonly used cryptographic algorithms. Shor's algorithm could potentially compromise RSA and ECC encryption by efficiently solving the integer factorization and discrete logarithm problems [5]. This looming threat has accelerated research in PQC, as researchers seek to create algorithms capable of withstanding quantum attacks.

6.2 *Implementation Issues and Side-Channel Attacks*

Even secure algorithms can be compromised through poor implementation. Side-channel attacks, which take advantage of the physical characteristics of cryptographic operations (e.g., power consumption, timing), are a major concern [22]. These attacks emphasize the need not only for developing robust algorithms but also for ensuring their secure implementation in practical applications.

6.3 *Resource Constraints in Cryptographic Implementations*

As Internet of Things continues to grow, the need for lightweight cryptographic algorithms is becoming more pressing that can operate efficiently on resource-constrained devices [23]. Research into lightweight block ciphers, such as PRESENT, demonstrates the feasibility of achieving

a balance between security and performance in such environments. However, ensuring adequate security while minimizing computational overhead remains a significant challenge.

Conclusion and Future Directions

Cryptography is a dynamic field that must continually adapt to new challenges. While classical algorithms like RSA, DES, and AES have served well, the emergence of quantum computing necessitates a shift towards quantum-resistant algorithms. Furthermore, the secure implementation of these algorithms in diverse environments is crucial to ensure the ongoing protection of digital information.

As cryptographic research progresses, several key areas demand attention. The continued development of PQC is essential for maintaining data security in the face of quantum computing. Additionally, the design of lightweight cryptographic algorithms will be critical as the number of connected devices continues to grow. Finally, the implementation of cryptographic algorithms must be carefully managed to prevent vulnerabilities that could undermine even the most secure systems.

References

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO'96*, Berlin, Heidelberg: Springer, 1996, pp. 104–113.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[3] U.S. National Bureau of Standards, "Data encryption standard," *Federal Inf. Process. Standards Publ.*, vol. 112.3, 1999.

[4] B. Sun, Z. Xiang, Z. Dai, G. Liu, X. Shen, L. Qu, and S. Fu, "Feistel-like structures revisited: classification and cryptanalysis," in *Annual Int. Cryptology Conf.*, Cham: Springer Nature Switzerland, 2024.

[5] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Foundations of Computer Science (FOCS)*, 1994, pp. 124–134.

[6] C. Paar, J. Pelzl, and T. Güneysu, *Introduction to Cryptography and Data Security*. Springer Science and Business Media LLC, 2024, pp. 1–35.

[7] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Berlin, Heidelberg: Springer, 2002, pp. 1–8, doi: 10.1007/978-3-662-04722-4.

[8] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '85*, Berlin, Heidelberg: Springer, 1985, pp. 417–426.

[9] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[10] B. Schneier, "Twofish: A 128-bit block cipher," in *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, 1998.

[11] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 499–507, 2019.

[12] A. L. Imoize, W. Montlouis, M. S. Obaidat, S. I. Popoola, and M. Hammoudeh, *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, Boca Raton, FL: CRC Press, 2024, pp. 1–7.

[13] N. V. Y. Lankadasu, D. B. Pesarlanka, A. Sharma, and S. Sharma, "Security aspects of blockchain technology," in *IGI Global*, 2024, pp. 259–277.

[14] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, 2016.

[15] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 34, pp. 1–40, 2009.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[17] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 491–498, 2019.

[18] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed., Boca Raton, FL: Chapman and Hall/CRC, 2019, pp. 1–22.

[19] J. Daemen and V. Rijmen, "AES proposal: Rijndael," A report for NIST, Computer Security Resource Center (CSRC), 1999.

[20] M. S. Kamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, 2024.

[21] B. Schneier, "The IDEA encryption algorithm—The International Data Encryption Algorithm (IDEA)," vol. 18, pp. 50–57, 1993.

[22] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. CRYPTO'96*, Santa Barbara, Aug. 18–22, 1996, pp. 104–113.

[23] M. Gruber, P. Karl, and G. Sigl, "Algebraic fault analysis of Subterranean 2.0," in *Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, 2021.

Received March, 2024