International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at :www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET25121171

A Comprehensive Review on Cryptography Algorithms: Methods and Comparative Analysis

Donia Fadil Chalob[1], Rusul Hussein Hasan*[2], Suaad M. Saber[1]

[1]Computer Science Department, Mustansiriyah University, Baghdad, Iraq

*[2]University of Baghdad, Baghdad, Iraq

ARTICLEINFO

Article History:

Accepted : 16 Jan 2025
Published: 18 Jan 2025

Publication Issue :
Volume 12, Issue 1
January-February-2025

Page Number :
275-282

ABSTRACT

The evolution of cryptography has been crucial to preservation subtle information in the digital age. From early cipher algorithms implemented in earliest societies to recent cryptography methods, cryptography has developed alongside developments in computing field. The growing in cyber threats and the increase of comprehensive digital communications have highlighted the significance of selecting effective and robust cryptographic techniques. This article reviews various cryptography algorithms, containing symmetric key and asymmetric key cryptography, via evaluating them according to security asset, complexity, and execution speed. The main outcomes demonstrate the growing trust on elliptic curve cryptography outstanding its capability and small size, while highlighting the requirement for study in the post-quantum cryptographic field to address the threats rising from quantum computing. The comparative analysis shows a comprehensive understanding that combines classical cryptography algorithms with up-to-date approaches such as chaotic-based system and post-quantum cryptography, confirming that the study addresses the future of cryptography security in the aspect of emerging challenge like quantum computing.

Keywords: Symmetric Key, Asymmetric Key, Post-Quantum Cryptography, Chaos-Based Systems.

INTRODUCTION

Cryptography is the skill of secure communication, and its roots date back to earliest civilizations like Egypt and Rome. Simple ciphers, e.g. the Caesar cipher, were utilized in the early algorithms, which substituted for each letter in a plaintext with alternative letter at a permanent number of places before or after it. Cryptography achieve military importance, and the Allied determinations to decipher it were vital. The basics of recent cryptography were formerly made via the effort of Withfield Diffie and Martin Hellman, who presented in 1976 the idea of public-key cryptography, a concept that was tracked by the improvement of the first applications of this idea RSA algorithm. Subsequently, cryptography algorithms have experienced incessant enhancement in reply to the requirements of secure digital communications and the complication of cyber-attacks., cyber-attack –e.g. identity theft, data breaches, and eavesdropping– have become extra public with the extensive consumption of the Internet, building strong cryptography crucial to confirming the integrity, authenticity, and confidentiality of digital information. Cryptography displays a fundamental part in keeping information secure in transmission (e.g. TLS/SSL protocols), securing saved data (for example, through file encryption), and assisting to prove the authenticity of digital communication (e.g. through the usage of digital signatures). Digital systems will be susceptible to attacks without actual encryption techniques, leading to a loss of trust and privacy [1-3].

1.1 Objectives and scope

The article highlights three main types of cryptography algorithms, which are:

- Symmetric key cryptography: Stream cipher and block cipher.
- Public key cryptography: RSA, ECC, and Diffie-Hellman algorithms.
- Recent trends: Review up-to-date advances in the field of cryptography.

The study aims to compare these algorithms based on several criteria including resistance to attacks (security), execution speed and resource consumption (performance) and ease of use and scalability (implementation complexity).

The content of the study is arranged as follows: Section 2 explains symmetric key cryptography techniques. Section 3 discusses asymmetric key cryptography. Section 4 provides recent developments. Section 5 delves into a comparative analysis of algorithms with recommendations. Section 6 concludes and future directions.

SYMMETRIC KEY CRYPTOGRAPHY

There are two common types of symmetric cipher clarified in the next subsections:

2.1. Stream Cipher

Streaming ciphers encrypt data incrementally, bit-by-bit or byte-by-byte, utilizing a produced continuous series of keys. This series is often produced via a pseudo randomness number generator that is delivered with a secret key. These ciphers are significant in circumstances where prompt cipher is necessary, e.g. live video streaming or voice communication, the following algorithms are popular type of stream cipher:

- RC4: While RC4 is one of the supreme common stream ciphers, it has been revealed to have some flaws, particularly in the initial phases of the key sequence, creating it inappropriate for recent cryptography applications. RC4 involves two phases, a key scheduling algorithm (KSA) which transforms a random key whose distinctive size is 40-256 bits into an initial permutation S of $\{0,\ldots,N-1\}$, and an output production phase (PRGA) which utilizes this permutation to create a pseudorandom outcome series [4].
- Salsa20/ChaCha20: Chacha20 is an enhanced development of Salsa20, providing sophisticated security and quicker rapidity likened to RC4. It has been implemented in Android systems and TLS protocols to defending data saving. The 8-round cipher Salsa 20/8 is the base for ChaCha8, which is a 256-bit stream cipher. The modifications made from Salsa20/8 to ChaCha8 aim to enhance diffusion per round, potentially raising resistance to cryptanalysis, while maintaining and frequently enhancing time per round. The 12- and 20-round ciphers Salsa20/12 and Salsa20/20 are modified by ChaCha12 and ChaCha20 in an analogous manner. [5].

Pros:

- Provides quick cryptography thanks to its simple scheme.
- Appropriate for instantaneous application e.g. stream services and VPNs.

Cons:

- Susceptible to issues such as key reuse attack and utilize of weak initial vector.
- The weakness in RC4 have managed to its neglect in applications that require a high level of security.

2.2. Block Cipher

Block ciphers encrypt data via separating it into fixed blocks sizes, where every block of the plain text is transformed into a ciphertext of the similar size. Diverse operating modes are utilized, e.g. ECB (electronic cipher mode), CBC (cipher block chain), and CTR (counter mode), to handle plaintext of flexible length, the following algorithms are the most popular block ciphers:

- AES (Advanced Encryption Standard): AES is the strongest block cipher algorithm. It is commonly employed for securing communications like HTTPS, disk encryption like BitLocker, and file encryption. AES has verified its robust against general cryptanalysis. The AES fixes the block size to 128 bits, and maintenances key sizes of 128, 192 or 256 bits [6].
- DES (Data Encryption Standard): DES was once commonly implemented, but has become insecure since the 1990s because of its 56-bit key size, which leads it to be vulnerable to brute force attack. The block size is 64 bits. The utilized key via the DES contains 64 bits, but just 56 bits are utilized and 8 bits are for check parity [7].
- Blowfish: Blowfish was designed as a quicker substitute to DES, the encryption operation needs a function that repeats the network 16 times. For every round comprises a key and data-dependent permutation transformation and a key and data dependent substitution transformation. All processes are XORs and additions for 32-bit words. Four indexing matrix data recovery banks are the only additional processes for each cycle. The x is a 64-bit communication-instrumental variable’s data. Gap x is split up into two 32-bit parts: xR and xL. [8].

Pros:

- Offers a high level of security when utilizing an appropriate key.
- Flexible due to its maintenance for various modes of operations.

Cons:

- Slower than stream cipher, which can be a drawback in applications that require real-time cryptography.

PUBLIC KEY CRYPTOGRAPHY

Asymmetric cryptography is known as Public key cryptography techniques which rely on mathematic problems that are difficult to solve in computation. E.g., the security of ECC algorithms is based on the difficulty of deciphering the discrete logarithm problem on elliptic curve, while the security of RSA is relied on the hardness of factorizing a large complex number into its prime factors.

3.1. Rivest-Shamir-Adleman (RSA)

Computationally challenging mathematic problems are the foundation of public key cryptography techniques. The mathematical complexity of factoring two large prime numbers is what RSA relies upon. The process of generating the key involves choosing two large prime numbers and multiplying them to obtain a value that is utilized in both public and private keys. The use of RSA is widely observed in the security of communications, the creation of digital signatures, and the exchange of key protocols. RSA's security is based on the difficulty in factoring large numbers, but modern computational threats require keys with at least 2048 bits. The message should be represented as an integer between 0 and n - 1. After that, cipher the plaintext message M via raising it to the eth power modulo n. The outcome (ciphertext C) is the remainder when Me is divided via n. To decipher the ciphertext, raise it to a different power d, once more modulo n [9].

3.2. Elliptic Curve Cryptography

Elliptic curve cryptography (ECC)depends on on the algebra possessions of elliptic curves defined over determinate arenas to make protected public key system. ECC is sole in that it delivers an identical criteria of security to RSA utilizing minor keys, creating it more effective. ECC is progressively vital in situations where computation properties are narrow, e.g. mobile devices and Internet of Things IoT systems. The analog of the discrete logarithm problem on elliptic curves is harder than the classical discrete logarithm problem, particularly over GF (2"). ECC has gained more significance since the starter of the peer-to-peer electronic cash system Bitcoin, by Satoshi Nakamoto in 2008 [10,11].

3.3. Additional Asymmetric Algorithms

- Diffie-Hellman: The Diffie–Hellman protocol is known for its minimalism and still the common protocol after many years for producing a shared secret key for encryption for e-trading and different applications [12].
- ElGamal: El-Gamal is an enhanced type of Diffie-Hellman utilized in digital signature and encryption which is a public key cryptography scheme. It is proven on the one-way characteristics, which approves that cipher approaches are accomplished separately [13,14].

UP-TO-DATE DEVELOPMENTS IN CRYPTOGRAPHY

The next subsections highlight the most common directions in encryption techniques:

4.1. Chaos Cryptography

The application of chaos theory in cryptography have approved developing consideration in latest years, mainly in the pseudo-randomness number producers design (PRNGs) and key generation. The Chaos system is extremely sensitive to initial values, meaning that tiny alters in the input can produce to totally dissimilar output, a property that is important in generating unpredictable cryptographic keys [15-19]:

- Linear Congruential Generators (LCGs) and Logistic Map: LCG and Logistic Map, these implements are extensively employed in chaotic-based cryptography to create random series. LCGs are depended on a linear repetition association, while logistic map is a nonlinear function that harvest output that is high sensitive to initial conditions.
- Exclusive-OR Operations: Exclusive-OR operations are utilized to improve the random of series made via chaotic methods, and are regularly joint with scramble techniques to confirm that the ultimate production still secure even if the plain text is vulnerable to some without knowing the cipher key.
- Study: New articles have highlights the possible of implementing chaotic maps and systems in image cryptography and further applications, establishing that chaotic-based ciphering schemes can improve security while preserving high computation competence.

4.2. Post-Quantum Cryptography ((PQC)

Quantum computers utilize quantum mechanism ideologies to achieve computations. Quantum computers utilize quantum bits or qubits, which can be in various situations concurrently, unlike the classical computers, which utilize bits that equal either 0 or 1. Qubits have the characteristic that permits quantum computers to accomplish specific calculations much quicker. Developing methods in this field embrace code-based encryption, polynomial systems, and lattice-based encryption as shown in Fig. 1; these systems display pronounced potential as future cryptography criterions. Lattices have been generally used in cryptography, and these approaches have been used in: (a) lattice approximation for crypto analysis; and (b) encryption by employing non-deterministic polynomial time hardness lattice problems to build steady cryptography functions. The arrival of quantum computing inquires imperative development of encryption algorithms that can endure quantum attacks [20-23].

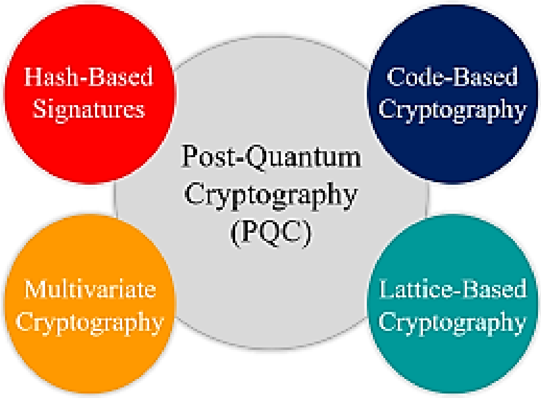
Hash-Based Signatures
Code-Based Cryptography
Post-Quantum Cryptography (PQC)
Multivariate Cryptography
Lattice-Based Cryptography

Figure 1. Basic categories of Post-Quantum cryptography.

COMPARATIVE ANALYSIS AND RECOMMENDATIONS

This section addresses a comprehensive overview of the pros and cons of the cryptography algorithms discussed, focusing on sides of security, performance, and implementation complexity. Table 1 summarizes the main aspects of every algorithm, highlighting the benefits and regions for upgrading.

Table 1. Comparative analysis summary.

Algorithm	Security	Performance	Complexity	Application	Key Space
RC4	Low- key scheduling vulnerability)	Very fast	Low	Real-time stream, VPNs	Variable
DES	Low- deprecated, 56-bit key	Moderate	Moderate	Historic utilize in file cipher	56 bits
ChaCha20	High- more secure compare to RC4	Very fast	Moderate	Safe communication (TLS/SSL), file encryption	256 bits
Blowfish	Moderate- fast but less secure compare to AES)	High	Low	Disk cipher, VPNs	32-448 bits
AES	High- NIST standard	Moderate	Moderate	File cipher, safe communication	128, 192, 256 bits
RSA	High- but quantum vulnerable, key dependent	Moderate	High	Digital signature, safe key exchange	2048, 3072 bits
Diffie-Hellman Key Exchange	High- based on discrete logarithm	Moderate	Moderate	VPNs , Safe key exchange	2048 bits
ECC	High- effective	High	Moderate	SSL/TLS, IoT,	256 bits

Algorithm	Security	Performance	Complexity	Application	Key Space
	security with minor keys			cryptocurrency, blockchain	
Code-based Cryptography	High- quantum resistant	Moderate	High	Post quantum cipher	Varies by algorithm
Lattice-based Cryptography	High- quantum resistant	Low- now high computation rate	High	Post quantum cipher, safe communication	1024-4096 bits
Multivariate Polynomial System	High- quantum resistant	Moderate	High	Post quantum cipher	Varies by algorithm
Chaos-based Cryptography	High- if applied with high randomness	High- if optimized	Moderate	Real-time stream, image encryption	Variable

When selecting a cryptographic algorithm, the choice should be guided by several factors, including security requirements, performance considerations, and computational resources. Below are general recommendations:

1. General data
   - AES is optimal because of its security, common availability, and flexibility. A 256-bits key is favored for maximum security.
   - Blowfish may be utilized in environments that need speed, in another side its 64-bits block leads it to be susceptible to specific attacks, therefore AES is the favored choice.
2. Instant communication
   - Chacha20 is the perfect choice for instant communication, e.g. live video streaming, since its high speed and capability to deliver well security compared to RC4 the older stream encryption algorithms, particularly in environments where AES may not be substantially maintained.
3. Digital Signature
   - With a key of at least 2048-bits essential to confirm adequate security, RSA is commonly utilized.
   - The devices with restricted computing power (e.g. IoT and mobile phones), ECC is placed growing approval because of its competence.
4. Key Exchange
   - Elliptic Curve offers a protected approach for key exchange, offering security similar to RSA while utilizing minor keys.
   - Diffie–Hellman remains a feasible choice for key exchange, but involves cautious managing of transaction size and key.
5. Post Quantum Cryptography
   - The quantum computing may pose to present criterions given the probable dares, it is desirable to begin embracing post-quantum cryptography schemes. ECC and RSA-based algorithms should be assessed one more time in light of modern progresses, e.g. Shor's algorithm. Quantum-resistant replacements like lattice-based cryptography should be discovered to safe future systems.

CONCLUSION

The arena of cryptography is continuously developing in reaction to evolving intimidations and technology advances. While classical algorithms AES and RSA persist the backbone of secure communication, modern improvements in machine learning techniques, post-quantum cryptography and chaotic-based encryption, are escalating the prospect of security potentials. Chaos theory has presented new approaches for producing pseudo-randomness sequences, which has facilitated enhance cipher operations and form more robust approaches. It will be authoritative to accept quantum-resilient methods as the era of quantum computing schemes. Future principles are probable to unite hybrid methods that syndicate classical algorithms with progressive quantum-resistant machineries, confirming strong security in the varying digital scenery.

REFERENCES

[1]. Schneier, B. (1996). Applied Cryptography. John Wiley & Sons.

[2]. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice, 7th ed., Pearson.

[3]. M. Husam, A. Kamel, D. F. Chalob, and Z. M. Abood. (2020). "Safe Fingerprint Analysis Technique Employed in Passport Verification for Sustainable Development". Journal of Green Engineering, vol. 10, no. 9, pp. 6103–6114.

[4]. Fluhrer, S., Mantin, I., & Shamir, A. (2001). "Weaknesses in the key scheduling algorithm of RC4." Proceedings of the 8th Annual International Workshop on Selected Areas in Cryptography.

[5]. Bernstein, D. J. (2008). "ChaCha, a variant of Salsa20". The Second Open Workshop on the Cryptography and Security of TLS.

[6]. Daemen, J., & Rijmen, V. (2002). "The Design of Rijndael: AES – The Advanced Encryption Standard. Springer". Berlin.

[7]. W. A. Shukur, L. K. Qurban, and A. Aljuboori. (2023). "Digital Data Encryption Using a Proposed W-Method Based on AES and DES Algorithms". Baghdad Sci.J [Internet], vol. 20, no. 4, pp. 1414-1424. doi:10.21123/bsj.2023.7315.

[8]. Adeniyi, A.E.; Misra, S.; Daniel, E.; Bokolo, A., Jr. (2022). "Computational Complexity of Modified Blowfish Cryptographic Algorithm on Video Data". Algorithms, vol. 15, no. 373. doi:10.3390/a15100373.

[9]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM, 21(2), 120-126.

[10]. Koblitz, N., "Elliptic Curve Cryptosystems. (1987). " Mathematics of Computation, 48(177), pp. 203-209.

[11]. Jebrane, J.; Chhaybi, A.; Lazaar, S.; Nitaj, A. (2025). "Elliptic Curve Cryptography with Machine Learning". Cryptography, Vol. 9, No. 3. doi:10.3390/ cryptography9010003.

[12]. E. Järpe. (2020). "An Alternative Diffie–Hellman Protocol". Cryptography, vol. 4, no. 1, Art. 5. doi: 10.3390/cryptography4010005.

[13]. Adeniyi, E.A.; Falola, P.B.; Maashi, M.S.; Aljebreen, M.; Bharany, S. (2022). "Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions". Information, 13, 442. Doi:10.3390/ info13100442.

[14]. Steichen, M.; Fiz Pontiveros, B.; Norvill, R.; Shbair, W. (2018). "Blockchain-Based, Decentralized Access Control for IPFS". In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, pp. 1499–1506.

[15]. Zhang, B.; Liu, L. (2023). "Chaos-Based Image Encryption: Review, Application, and Challenges". Mathematics, 11, 2585. Doi:10.3390/math11112585.

[16]. D. F. Chalob, R. H. Hasan, and R. F. Yaser. (2024). "Image Cryptography Based on Confusion and Diffusion Using 6D Hyper Chaotic System and Fibonacci Q-matrix".

International Journal of Intelligent Engineering and Systems, vol. 17, no. 4, pp. 944-956. doi:10.22266/ijies2024.0831.71.

[17]. D. F. Chalob, R. H. Hasan, & F. N. Abbas. "Image Encryption based on Chaotic Blocks Shuffling and RC4. " Baghdad Sci.J [Internet]. [cited 2025 Feb. 8];22(6).

[18]. D. F. Chalob, A. A. Maryoosh, Z. M. Essa, and E. N. Abbud. (2020). "A New Block Cipher for Image Encryption Based on Multi Chaotic Systems". TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no. 6, pp. 2986-2994. doi: 10.12928/TELKOMNIKA.v18i6.13746.

[19]. Talha Umar, Mohammad Nadeem, Faisal Anwer. (2024). "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage". Expert Systems with Applications, Vol. 257, 125050. doi: 10.1016/j.eswa.2024.125050.

[20]. Dam, D.-T.; Tran, T.-H.; Hoang, V.-P.; Pham, C.-K.; Hoang, T.-T. (2023). "A Survey of Post Quantum Cryptography: Start of a New Race". Cryptography, 7, 40. doi: 10.3390/cryptography7030040.

[21]. Asif, R. (2021). "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms". IoT, 2, 71–91. doi.org/10.3390/iot2010005.

[22]. G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone. (2022). "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process". NIST Interagency or Internal Report NIST IR 8413 upd1, 102 pp. doi:10.6028/NIST.IR.8413-upd1.

[23]. Moody, D. , Alagic, G. , Apon, D. , Cooper, D. , Dang, Q. , Kelsey, J. , Liu, Y. , Miller, C. , Peralta, R. , Perlner, R. , Robinson, A. , Smith-Tone, D. and Alperin-Sheriff, J. (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. doi.org/10.6028/NIST.IR.8309.