Hindawi
Security and Communication Networks
Volume 2023, Article ID 9873584, 1 page
https://doi.org/10.1155/2023/9873584

Retraction

Retracted: Application Research of Data Encryption Technology in Computer Network Information Security

Security and Communication Networks

Received 25 July 2023; Accepted 25 July 2023; Published 26 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. Wang, "Application Research of Data Encryption Technology in Computer Network Information Security," *Security and Communication Networks*, vol. 2022, Article ID 6485195, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6485195, 7 pages
https://doi.org/10.1155/2022/6485195

Research Article

Application Research of Data Encryption Technology in Computer Network Information Security

Meilin Wang

Inner Mongolia Preschool Education College for the Nationalities, Ordos, Inner Mongolia 017000, China

Correspondence should be addressed to Meilin Wang; 11231416@stu.wxic.edu.cn

Received 6 July 2022; Revised 5 August 2022; Accepted 13 August 2022; Published 6 September 2022

Academic Editor: C. Venkatesan

In order to ensure the rights and interests of computer users, a method of data encryption technology in computer network information security is proposed. According to the symmetric encryption AES algorithm, the ECC system has higher security, slower decoding speed, smaller storage space occupation, and lower bandwidth requirements. The experimental results show that the safety mode length can reach 5 : 1, 6 : 1, 10 : 1 or even 35 : 1. *Conclusion*. The use of a hybrid cryptosystem based on MD5, AES, and elliptic curve keys can effectively make up for various problems and loopholes encountered in data transmission in current network security, and improve the security of information transmission in today's social network.

1. Introduction

At this stage, the computer network has long become a part of the public's daily life, and the ensuing network information security problems also threaten the public's property security and social stability. Among the numerous computer network production security technologies, the data information encryption technology is a more common and effective optimization. The algorithm encryption technology can effectively maintain, eliminate, and resist many behaviors that harm network security. With the development of computer technology, the total number of applications for electronic computers is gradually increasing, and the issue of computer network information security is becoming more and more serious [1, 2]. Computer network information security can only be placed at the forefront of development. The computer network develops better and faster, and provides more convenient services to citizens. In short, data encryption technology is an innovation to maintain computer network information security technology. It can transform the information data transmitted by the computer into confidential information. This kind of encryption method can prevent hackers from stealing the original records, and can maintain and ensure the security of Internet information to a certain extent. The key is a kind of reference data information that will be used in the process of encryption and decoding. Using traditional computer technology to encrypt data information generally involves very complex optimization calculation methods. Secondly, the application of data encryption technology can not only achieve the expected effect of maintaining computer network information security but also will not cause any adverse impact on the operation of electronic computers. On the contrary, it will improve the operation speed of electronic computers to some extent. During the development of computers, there may be some loopholes in the transmission of computer information and related data [3, 4]. If the information security of computer network wants to be better guaranteed, it should be developed by using the technology of the new era. Through the computer data encryption technology, it can also ensure the communication between different industries and improve the accuracy of communication. Data encryption technology can effectively solve some problems existing in the computer itself, and put forward supplementary and perfect measures to give full play to the operation and scientific and technological functions of the technology, and provide technical support for social development and scientific and technological progress.

2. Literature Review

To solve this problem, Kiran and Nalini and others proposed the concept of public key cryptosystem, which has two requirements: first, even if the public key and encryption algorithm are public, the encrypted ciphertext is still secure; second, it is required that all those who hold the private key should have relatively simple computing power or processing power, but it should be very difficult and troublesome for those who do not hold the private key [5]. The cryptographic design idea proposed by Ramamoorthy and Jayagowri and others led to a revolution in cryptography, opened a new era of public key cryptography, was a major invention of modern cryptography, and took cryptography into a new direction [6]. DES, as the most widely used packet data encryption standard in the world, has existed for more than 20 years. DES has resisted cryptanalysis for a long time, but with the development of attack technology, DES was cracked in 1997. Later, deformed DES and triple DES that can resist differential analysis attacks were derived. Triple DES uses three different keys to encrypt data blocks three times, which is more effective than three times of ordinary encryption, and its strength is about the same as that of 112 bit keys. On October 2, 2000, NIST published the new Advanced Encryption Standard AES, and DES officially ended as a standard [7].

Qiu et al. proposed that the process of chaotic encryption refers to using the chaotic sequence generated by the chaotic system as the key, then encrypting the information, and the receiving party of the ciphertext after channel transmission uses the method of chaotic synchronization to decrypt the ciphertext. In this way, the data encrypted by chaos makes it difficult for attackers to decipher the information or even analyze the data. Based on the above advantages, chaotic encrypted data are continuously improved and developed, which brings more convenience and value to our life. There are also many difficulties to be overcome. For example, many chaotic systems are difficult to realize, and the short period response will reduce the reliability of chaotic encryption systems; however, with the development of science and technology, these problems will be overcome one by one, so that the chaotic encryption system can serve the public more [8].

On the basis of the current research, this paper proposes to use the digital signature algorithm based on public key algorithm and one-way hash function to realize the authenticity and integrity verification of data, and uses database technology to realize the hierarchical management of user permissions, so that users with different permissions can only read different encrypted files. In this paper, the combined encryption scheme is described in detail and analyzed carefully in theory. The results show that the scheme has certain theoretical value and strong practical value in the field of secure communication to realize fast encryption and fast transmission of information.

3. Research Methods

The purpose of the digital signature is to enable the signer to sign the electronic file, and it cannot be denied, and the verifier cannot tamper with the file. After that, different digital signature schemes have been proposed [9]. Digital signature is an alphanumeric string obtained by the information sender through some processing of the information to be transmitted, which cannot be forged by any other person, and is used to authenticate the information source and verify whether the information has changed.

Digital signatures require the following features:

(1) Signature cannot be forged;

(2) The issuer cannot deny or repudiate the fact of issuing documents after signing;

(3) After the information is sent, no one can modify it;

(4) In case of any dispute over the signature between the two parties, the evidence that can be arbitrated can be provided to the third-party arbitration institution.

Generally speaking, digital signature should solve the problems of forgery, tampering, impersonation, and denial to ensure the authenticity, integrity, and nonrepudiation of electronic document transmission. Digital signature generally consists of signature algorithm and verification algorithm. Signature algorithms generally include public key algorithm, symmetric key algorithm, and one-way hash function. In the existing digital signature schemes, file messages are usually treated with one-way functions such as functions. A fixed length binary number is generated as a message digest, and the message digest is encrypted and sent with the file as a signature. As a one-way function is used, given a fixed length string, it is difficult to find a message with clear meaning, so that its function value is exactly the same as the "information summary" value of the string. Therefore, if the message is modified or destroyed in January, it will not match the original "information summary" value. The receiver can easily detect that the message has been tampered by illegal users by calculating the difference between the "information summary" value of the message and the function value transmitted [10, 11]. The signature and verification process is shown in Figure 1.

3.1. MDS Algorithm Overview. The full name of MDS is Message-Digest Algorithm 5 (Message-Digest Algorithm), an improved method derived from MD4. Its function is to "squeeze" large amounts of information into a secure format before signing a private key with the help of digital signature software, which converts a string of any length into a large integer of a certain length. Because the main idea of someone's original design was to have a system architecture based on 32-bit processors in mind. Therefore, all operations in MDS are based on a 32-bit word, the operating unit. MDS adds the concept of "safety zone" based on MD4. Although MD5 is slower than MD4, it is more reliable. Of course, this algorithm consists of four steps, slightly different from the MD4 model. For the MDS algorithm, the amount of the message fee and the conditions required for filling are exactly the same as for the MD4.

3.2. MD5 Encryption Algorithm Description. The brief description of MDS algorithm can be as follows: MDS

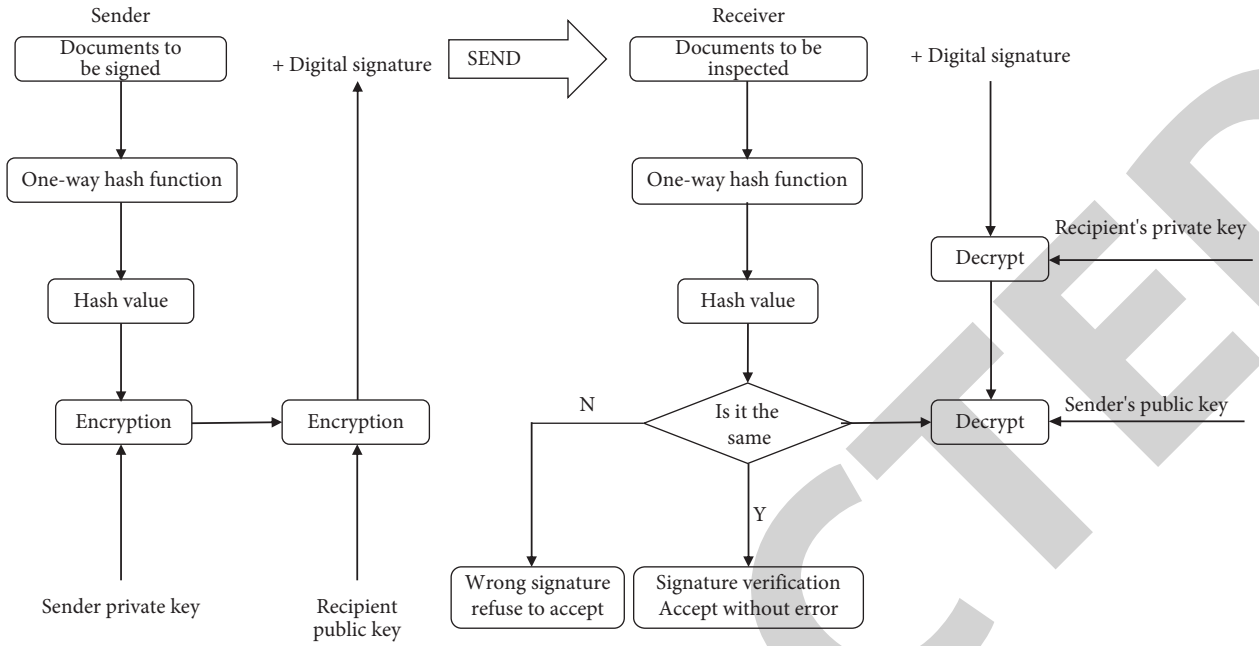

Figure 1: Signature and verification process.

processes the input information in 512 bit packets, and each packet is divided into 16 32-bit sub packets. After a series of processing, the output of the algorithm is composed of four 32-bit packets, which will be cascaded to generate a 128-bit hash value. In the MD5 algorithm, the information needs to be filled first, so that the result of the byte length of 512 is equal to 448. Therefore, the bits length of information will be extended to $n * 512 + 448$, that is, $n * 64 + 56$ bytes, where n is a positive integer. The method of filling is as follows: fill a 1 and countless after the information. Do not stop filling information with 0 until the above conditions are met [12]. The result is then appended with a length of pre fill information in 64-bit binary. After these two steps, the current information byte length $= n * 512 + 448 + 64 = (n + 1) * 512$, that is, the length is exactly an integer multiple of 512. The reason for this is to meet the requirements for information length in subsequent processing.

The key length used by the DES algorithm is 64 bits, and the effective key length is 56 bits. Because the key is small, it cannot provide enough security. Now this algorithm has been used as a new data encryption standard, and has been widely used in various industries and fields. Although some people have different opinions on AES, generally speaking, as a new generation of advanced encryption standard, AES has the characteristics of high security, high operation efficiency, strong performance, and flexible use. Relatively speaking, aes128-bit key is 1021 times stronger than des56 bit key [13]. AES is a new symmetric encryption algorithm, which is used to ensure the security of electronic information. To be exact, AES belongs to an iterative packet encryption algorithm. The data are grouped by 128 bits, i.e., 16 bytes. Encrypt and decrypt packet data using 128, 192, and 256 bit keys. Unlike asymmetric encryption that uses two keys, AES symmetric encryption uses the same key to encrypt and decrypt the data. The number of ciphertext data obtained through AES packet encryption is the same as that of the input data, and the algorithm is easily implemented by various hardware and software. Symmetric encryption algorithms can be divided into flow encryption and block encryption according to different encryption methods. Block encryption divides a plain text message into blocks of constant length, and the length of the output ciphertext block is the same as the length of the input plain text block. The Rijndael algorithm is a repeating block encryption algorithm that can specify block lengths of 128 bits, 192 bits, 256 bits, and key lengths of 128 bits, 192 bits, and 256 bits. In other words, you can change both the block length and the key length. In the general structure of the Rijndael algorithm, a substitute network is used to form a loop function, and multiple iterations are used [14–16] ,as shown in Figure 2.

Each circle consists of three layers. In order to realize the wide trajectory strategy, each of the three layers of the wheel function has its own function:

(1) Linear mixing layer: ensure high diffusion over multiple wheels;

(2) Nonlinear layer: parallel use of S-boxes with optimal and worst-case nonlinear characteristics;

(3) Key adding layer: the single wheel key is simply XOR to the intermediate state to realize one-time masking.

3.3. Status, Seed Key, and Rounds. Rijndael's encryption and decryption will go through many data transformation operations. After each transformation operation, an intermediate result will be generated, which is called the state. Where Nb is used to indicate the number of data words contained in the ciphertext; Nk refers to the number of data words contained in the key; Nr represents the number of iterations. Specific values are shown in Table 1.

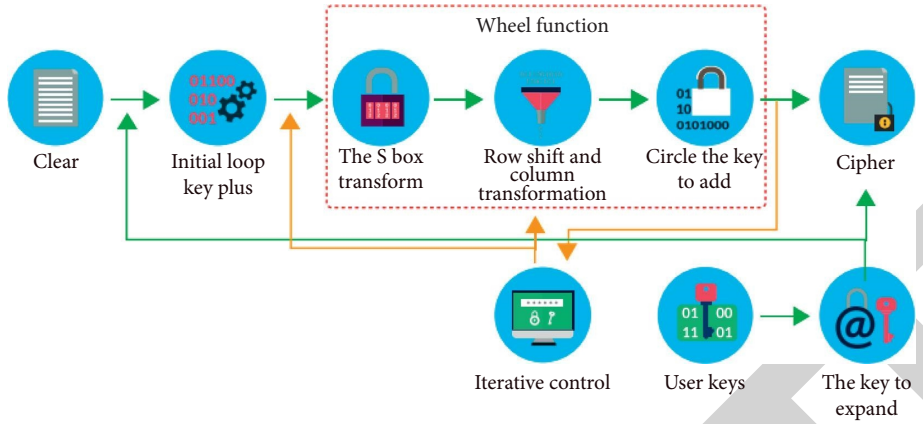

Figure 2: Change process.

Table 1: Number of turns of algorithm transformation.

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

3.3.1. AES Algorithm Encryption and Decryption. From the above four transformations, we can know that the decryption process of AES algorithm is to convert the transformation of each round of function into the corresponding inverse transformation, and transform the state matrix obtained from the ciphertext mapping in the reverse order [17, 18]. The encryption and decryption block diagram of AES is shown in Figure 3:

The implementation of AES encryption is very easy, because it gives most of the work to the four different computing components of the round function, namely, SubByte, shiftrow, MixColumn, and addroundkey. Since all operations used in AES encryption algorithm are reversible, the decryption algorithm is essentially the reverse operation of all operations performed by the encryption algorithm. The structure of AES algorithm is compact and standard. Each round of transformation is basically consistent. The algorithm is easy to be implemented by various hardware and software. It is the most secure encryption algorithm available at present. It has been listed as a more secure algorithm than any other encryption algorithm today. On the basis of theory and practice, AES is considered "secure," because the only effective way to crack it is to forcibly generate all possible keys. If the key length is 256 bits, no known attack can crack AES in an acceptable time. Even on today's fastest system, it will take several years [19].

3.3.2. Algorithm Principle on Elliptic Curve

(1) The Weierstrass equation of elliptic curve e is:

E: $\{(x, y)|y^2 + a_1xy + a_3y = x^3 + a_2x_2 + a_4x + a_6\} \cup \{0\}$

Let $p_1 = (x_1, y_1), p_2 = (x_2, y_2)$ be two points on the curve, then $p_1 = (x_1, y_1 - a_1x_1, a_3)$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2, \\ \dfrac{3x_1^2 + 2a_2x_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2. \end{cases} \quad (1)$$

(2) If $p_s = (x_3, y_s) = p_1 + p_2 \neq$ infinity point is 0, x_s, y_3 can be given by the formula: $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$

$$y_3 = \lambda(x_1 - x_3) - a_1x_3 - y_1 - a_3. \quad (2)$$

Elliptic curves on different fields have different algorithms:

(1) Elliptic curve on real field R:

The characteristic of real number field R is not, so Weierstrass equation of elliptic curve E on real number field R can be set as:

E: $y^2 = x^3 + a_4x + a_6 \triangle = -16(4a_4^3 + 27a_6^2) \neq 0$. The operation rule of E on R is:

Let $p_1 = (x_1, y_1), p_2 = (x_2, y_2)$ be two points on curve E, and 0 be infinity, then $0 + p_1 = p_1 + 0$; $-p_1 = (x_1, -y_1)$;

If $p_3 = (x_3, y_3) = p_1 + p_2 \neq$ infinity point 0, $x_3 = \lambda^2 - x_1 - x_2 y_3 = \lambda(x_1 - x_3) - y_1$

Where: $\lambda = \begin{cases} y_2 - y_1/x_2 - x_1, & x_1 \neq x_2, \\ 3x_1^2 + a4/2y_1, & x_1 = x_2. \end{cases}$

(2) Elliptic curves over prime field $GF(p)(p > 3)$.

The characteristic of prime field $GF(p)(p > 3)$ is not 2 or 3, so the Weierstrass equation of elliptic curve E on prime field $GF(p)(p > 3)$ can be set as:

E: $y^2 + xy = x^3 + a_2x^2 + a_6 \triangle = -16(4a_4^3 + 27a_6^2) \neq 0$ 。 The operation rule of E on $GF(2^n)$ is: set up $p_1 = (x_1, y_1), p_2 = (x_2, y_2)$ are the two points on curve E, 0 is the infinity point, then:

$0 + p_1 = p_1 + 0 - p_1 = (x_1, -y_1)$;

If $p_3 = (x_3, y_3) = p_1 + p_2 \neq$ infinity point 0,

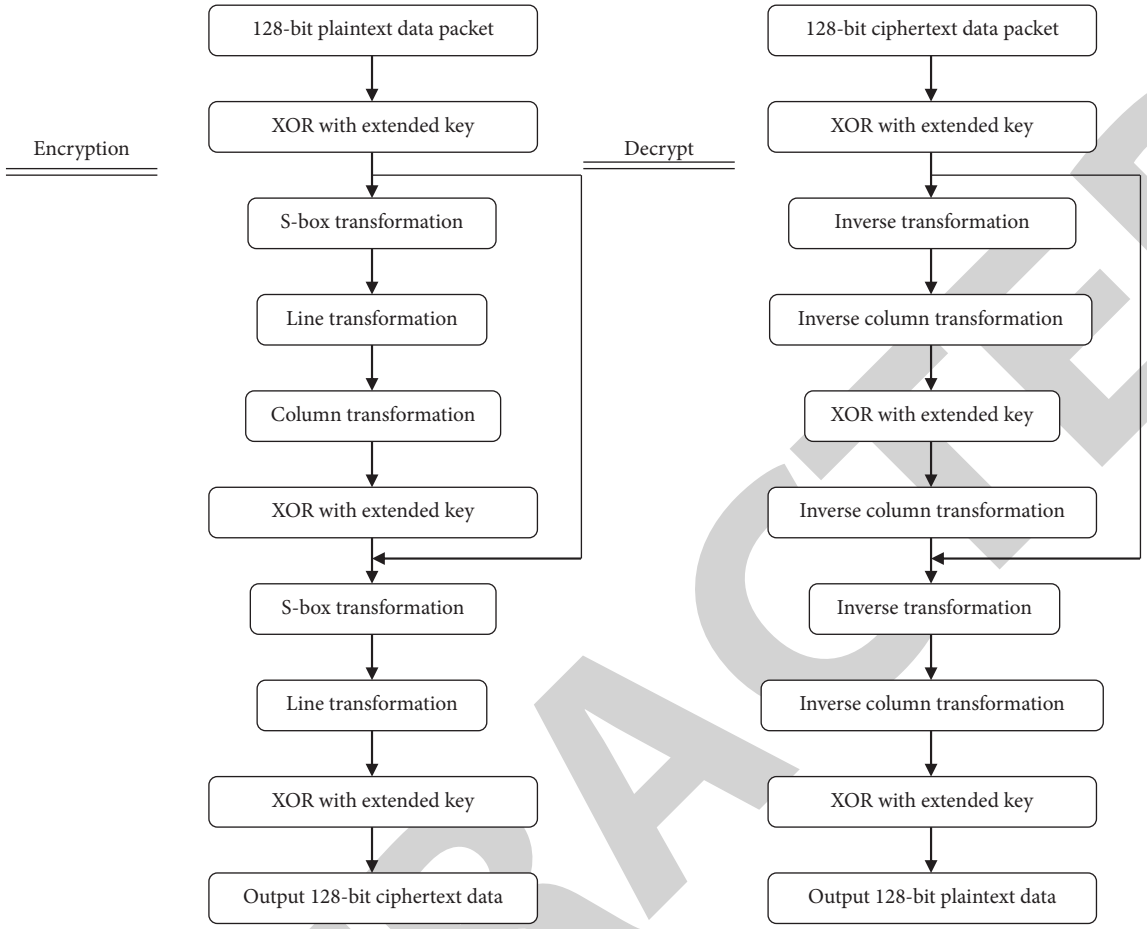

Figure 3: Encryption and decryption block diagram of AES.

Table 2: Comparison of RSA and ECC safety module length.

Breakthrough time MIPS year	RSA/DSA Key length	ECC key length	RSA/ECC Key length ratio
10^4	512	106	5: 1
10^8	768	132	6: 1
10^{11}	1024	160	7: 1
10^{20}	2048	210	10: 1
10^{78}	21000	600	35: 1

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1, \quad (3)$$
$$\text{where : } \lambda = \begin{cases} y_2 + y_1/x_2 + x_1, & x_1 \neq x_2, \\ x_1 + y_1/x_1, & x_1 = x_2. \end{cases}$$

4. Results and Discussion

Elliptic curve public key system has the following advantages:

(1) Higher security performance: Elliptic curve cryptosystem comes from the study of elliptic curve. There is no effective method to solve this problem based on the elliptic curve discrete logarithm problem, so the security of ECC system is very high. See Table 2 and Figure 4:

(2) Small storage space: The storage size is much smaller because the basic size of the ECC and the system parameters are much smaller than RSA and DSA [20].

(3) Low bandwidth requirements: Low bandwidth requirements make the ECC a widely used prospect. These features of the ECC can replace RSA and become a general public key encryption algorithm.

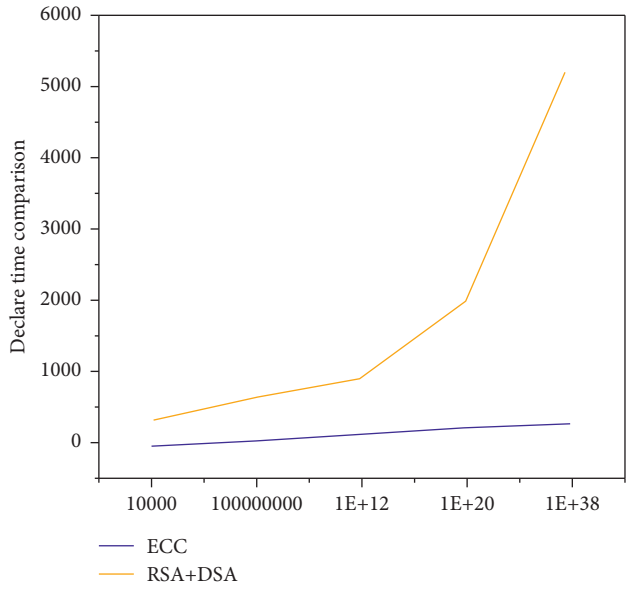

Figure 4: Comparison of decoding time.

5. Conclusion

This paper studies, analyzes, and compares various encryption algorithms. A hybrid cryptosystem based on MD5, AES, and elliptic curve key is proposed. AES encryption is fast and suitable for encrypting long messages. MD5 can generate a 128-bit message summary from any long message, which improves the speed and security of data encryption, realizes digital signature, and greatly improves the speed of signature. This paper introduces several commonly used encryption algorithms, including the basic ideas, methods, and characteristics of symmetric encryption algorithm and asymmetric encryption algorithm. This paper introduced the characteristics of the AES algorithm and analyzed its encryption, decryption algorithm, and security. Finally, the relevant operations of the ellipse curve cryptosystem are introduced and its performance is analyzed, and the advantages over RSA and DSA are that it is faster, more convenient, and more difficult to decipher.

This paper combines the current advanced encryption technology to design the network file encryption system, which provides a basic mode, and also provides a practical basis for the safe transmission of network files. However, there are still some areas to be improved and ex.anded in its functions and applications: as the secure transmission of network files is paying more and more attention, the system can be embedded in the Windows operating system, In this way, the operation of file encryption and decryption can become a part of the operation of the operating system.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] I. D. Reshetnikova and P. D. Dunaev, "Academician andrei dmitrievich ado and the kazan scientific research institute of epidemiology and microbiology," *Kazan medical journal*, vol. 102, no. 1, pp. 115–122, 2021.

[2] P. Amudha, J. Jayapriya, and J. Gowri, "An algorithmic approach for encryption using graph labeling," *Journal of Physics: Conference Series*, vol. 1770, no. 1, p. 9, Article ID 012072, 2021.

[3] R. E. Christenson and M. J. Harris, "Real-time hybrid simulation using analogue electronic computer technology," *International Journal of Lifecycle Performance Engineering*, vol. 4, no. 1/2/3, p. 25, 2020.

[4] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications," *Vehicular Communications*, vol. 28, no. 1, Article ID 100306, 2021.

[5] G. M. Kiran and N. Nalini, "Enhanced security-aware technique and ontology data access control in cloud computing," *International Journal of Communication Systems*, vol. 33, no. 23, Article ID e4554, 2020.

[6] A. Ramamoorthy and P. Jayagowri, "A secure public key cryptosystem based medical records using non-commutative group," *Journal of Physics: Conference Series*, vol. 1964, no. 2, Article ID 022011, 2021.

[7] F. Ramzan, S. Klees, A. O. Schmitt, D. Cavero, and M. Gultas, "Identification of age-specific and common key regulatory mechanisms governing eggshell strength in chicken using random forests," *Genes*, vol. 11, no. 4, p. 464, 2020.

[8] G. Qiu, C. Wang, S. Luo, and W. Xu, "A Dual Dynamic Key Chaotic Encryption System for Industrial Cyber-Physical Systems," *IEICE Electronics Express*, vol. 17, no. 24, 2020.

[9] M. Arun, S. Praveenkumar, P. S. Rajakumar, and P. Thamizhikkavi, "Cbca: consignment based communal authentication and encryption scheme for internet of things using digital signature algorithm," *IOP Conference Series: Materials Science and Engineering*, vol. 1074, no. 1, p. 16, Article ID 012003, 2021.

[10] T. Iwase, L. Pusztai, K. Blenman et al., "Validation of an immunomodulatory gene signature algorithm to predict response to neoadjuvant immunochemotherapy in patients with primary triple-negative breast cancer," *Journal of Clinical Oncology*, vol. 38, no. 15, p. 3117, 2020.

[11] A. Urbschat, S. Uppenkamp, and J. Anemüller, "Searchlight classification informative region mixture model (scim): identification of cortical regions showing discriminable bold patterns in event-related auditory fmri data," *Frontiers in Neuroscience*, vol. 14, Article ID 616906, 2020.

[12] D. E. Kurniawan, M. Iqbal, J. Friadi, F. Hidayat, and R. D. Permatasari, "Login security using one time password (otp) application with encryption algorithm performance," *Journal of Physics: Conference Series*, vol. 1783, no. 1, Article ID 012041, 2021.

[13] Y. Lu, N. Xie, D. Yang, and X. Lei, "Can brand sharing change consumers' brand attitudes? the roles of agency-communion orientation and message length," *Journal of Business Research*, vol. 128, pp. 350–359, 2021.

[14] O. A. Dawood, O. I. Hammadi, K. Shaker, and M. Khalaf, "Multi-dimensional cubic symmetric block cipher algorithm

for encrypting big data," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 6, pp. 2569–2577, 2020.

[15] H. S. Lee, M. H. Hwang, and H. R. Cha, "Development of an Optimal Power-Distribution-Management Algorithm for Four-Wheel-Drive Electric Vehicles," *IEEE Access*, vol. 9, no. 99, pp. 99731–99741, 2021.

[16] B. H. Rong, "Discussion and Analysis of Computer Information Data Security and Encryption Technology," *Journal of Physics: Conference Series*, no. 3, Article ID 032005, 1601.

[17] M. Bradha, N. Balakrishnan, S. Suvi et al., "Experimental, Computational Analysis of Butein and Lanceoletin for Natural Dye-Sensitized Solar Cells and Stabilizing Efficiency by IoT. Environment, Development and Sustainability," *Environment Development and Sustainability*, vol. 24, no. 7, 2021.

[18] A. Sharma, "An optimal routing scheme for critical healthcare HTH services – an IOT perspective," in *Proceedings of the 2017 International Conference on Image Information Processing*, Beijing, China, September 2017.

[19] P. Ajay, B. Nagaraj, R. A. Kumar, R. Huang, and P. Ananthi, "Unsupervised hyperspectral microscopic image segmentation using deep embedded clustering algorithm," *Scanning*, vol. 2022, pp. 1–9, Article ID 1200860, 2022.

[20] G. Veselov, A. Tselykh, A. Sharma, and R. Huang, "Special issue on applications of artificial intelligence in evolution of smart cities and societies," *Informatica*, vol. 45, no. 5, p. 603, 2021.