Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2295130, 19 pages
https://doi.org/10.1155/2021/2295130

Research Article

Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication Security

Yifeng He, Nan Ye, and Rui Zhang

Xi'an Institute of Space Radio Technology, Xi'an 710100 Shaanxi, China

Correspondence should be addressed to Yifeng He; yifenghe@mail.nwpu.edu.cn

Received 27 July 2021; Revised 16 September 2021; Accepted 22 September 2021; Published 13 November 2021

Academic Editor: Zhihan Lv

Nowadays, the development of information technology can be described as extremely rapid, especially with the widespread use of the Internet; the security of communications in the network has become an important issue we are facing. The purpose of this article is to solve the problems in today's network security data encryption algorithms. Starting from the computer network communication security data encryption algorithm, we discuss the effects of several different encryption methods on improving network security. The research results show that it is known that the application of link encryption algorithm in network communication security encryption algorithm can increase the security index by 25%, the node encryption algorithm can increase the security index by 35%, and the end-to-end encryption algorithm can make the cyber activity safety index to increase by 40%. Among them, RSA algorithm and DES algorithm are two very representative algorithms; they represent different encryption systems. From the perspective of network data link, there are three methods of encryption algorithm, namely, link encryption algorithm, node encryption algorithm, and end-to-end encryption algorithm.

1. Introduction

Since the beginning of the new century, with the rapid development of modern computer information technology, computers have gradually entered thousands of households, becoming a necessary for modern people to engage in communicative work such as cooperation and business negotiation, entertainment education and learning, and daily life [1], although computer network wireless communication has various advantages, such as instant, convenient, fast, no working time, and network space restrictions [2]. But they often have pros and cons in all things. While achieving good convenience for people's lives and work, security technical problems such as network security vulnerabilities, virus software intrusions, hacker vulnerability intrusions, and network server security information system leaks also frequently broke out [3, 4]. The security of the wireless communication system of the multicomputer network has been greatly reduced, which has caused serious threats to the legitimate rights and interests of network users and the security of citizens' personal information [5]. Therefore, the prevention of computer network communication security risks is an important academic research topic [6]. The practical application of data information encryption technology [7] provides useful theoretical reference and technical reference [8].

Data plaintext encryption, in brief, is to convert those plain digital plaintext information changes into digital ciphertext that ordinary people cannot easily understand by using certain encryption technology [9]. In turn, it cannot be decrypted. In this concept, the technical staff first mentioned that the basic meaning and functional difference between the plaintext of the password and the ciphertext should be correctly distinguished [10]. The opposite is the ciphertext, which is something that ordinary people cannot easily understand, and it has been used by transformation processing [11]. When technicians are preparing for network data security encryption, they may also need to figure out the data sender and data receiver separately [12, 13].

In order to discuss the role of the latest encryption technology in network security protection. Computer expert Liu

gave a detailed introduction to computer data encryption technology and method principles, analyzed the problems in the computer field under the current scientific and technological limitations, and elaborated related research methods and technologies [14]. In their article, Wang et al. proposed the research significance and research status of computer network security encryption algorithm and expounded the relevant technical theoretical basis. In addition, it showed the significance and importance of security secret technology in the network operation platform [15]. In the article, Yang et al. elaborated the methods and methods of data encryption technology application and proposed the advantages and advantages of this technology [16]. Ruslan and Tsouri said that data encryption technology greatly protects the privacy of information and improves the confidentiality of data transmission in a networked system, which has a positive effect on improving the security of computer network communications [17].

In short, this article discusses the application of network security data encryption technology in practical applications. Specifically, the main research content of this article is roughly divided into five parts: the first part is the introduction part, which aims to make a systematic review of the main research content of this article from the research background, research purpose, and research ideas and methods; the second part is the theoretical basis, a detailed and systematic summary of the current research status of network security data encryption technology, and the introduction of existing scientific and technological means. The third part is related research, through inquiring information and conducting relevant experiments to explain the advantages of the latest network security data encryption technology compared with the traditional protection mode. The fourth part is the analysis of the data. Through specific investigation data and research results, the specific application of network security data encryption technology is obtained, and it has better effects on network security protection and personal privacy protection. The fifth part is the summary, and the recommendation part is a summary of the results of the article and the prospect of further application of network security data encryption technology in the future purification of the network environment.

2. Proposed Method

2.1. Research the Security Mechanism of Computer Network Communication Data. Data encryption is to take certain technical means to transform the easy-to-understand plaintext processing into ciphertext that outsiders cannot understand. The reverse process is decryption, that is, to use the technical means corresponding to encryption to transform the ciphertext into a readable plaintext. Here are some basic concepts involved: the first is plaintext and ciphertext. The plaintext is easy to understand and needs to be transformed. The corresponding is ciphertext. The ciphertext is not readable by outsiders and has been transformed. The second is the algorithm and the key, which is the technical means used to encrypt or decrypt the data. Among them, the keys are divided into symmetric keys and asymmetric keys. Symmetric key algorithms are algorithms that use the same key for encryption and decryption. Asymmetric key algorithms are also called public-key cryptosystems and dual-key cryptosystems. The principle is that the encryption key and the decryption key are different to form a key pair, and the result of encryption with one key can be decrypted with the other key; the third is the sender and the receiver, which process the plaintext into ciphertext and send it out called the sender. For the sender, the receiver who receives the ciphertext and transforms the ciphertext into plaintext is called the receiver. The encryption and decryption flowchart is shown in Figure 1.

AES is an iterative block encryption algorithm with variable length of data block and variable length of key. After several rounds of block transformation, an intermediate state transition is generated. This state can be expressed as a two-dimensional byte array with 4 rows and Nb columns (Nb = data block length divided by 32), and the key can also be expressed as a two-dimensional byte array with 4 rows and Nk columns (Nk = key divide the length by 32). The number of rounds of transformation Nr is determined by Nb and Nk, as shown in Table 1.

Each transformation ring contains four stages: byte replacement, row movement, hot obfuscation, and adding ring keys. Byte replacement is based on the replacement process of *S*-box. *S*-box is a nonlinear and reversible thief, which is composed of two reversible thieves. Row shifting is a row-based operation. The function of row shift is to realize the replacement between the internal bytes of a 4×4 matrix. The schematic diagram of the forward row shift is as follows (Figure 2).

Column confusion (MixColumn) is a replacement operation that uses the arithmetic characteristics of the GF(28) domain. The schematic diagram of the forward nematic confusion is as follows (Figure 3).

Column confusion transformation is to transform each column in the state matrix $s(x)$. The transformation process of each column is independent, so it can be processed in parallel. As shown in Equation (1),

$$s(x) = c(x)s(x) \bmod \left(x^4 + 1\right), \tag{1}$$

$$c(x) = (03)x^3 + (01)x^2 + (01)x + (02). \tag{2}$$

The numbers in (x) are all hexadecimal bytes. The above formula can be expressed as a matrix as

$$\begin{bmatrix} 02 & 03 & 01 \\ 01 & 02 & 03 \\ 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \end{bmatrix} = \begin{bmatrix} b0 \\ b1 \\ b2 \end{bmatrix}. \tag{3}$$

In the above formula, we can get

$$b_0 = (02)a0 + (03)a1 + (01)a2 + (01)a3. \tag{4}$$

Among them, a is the input data, and b is the output data after transformation. The calculation process involves the multiplication of the finite field GF(28). For the constant

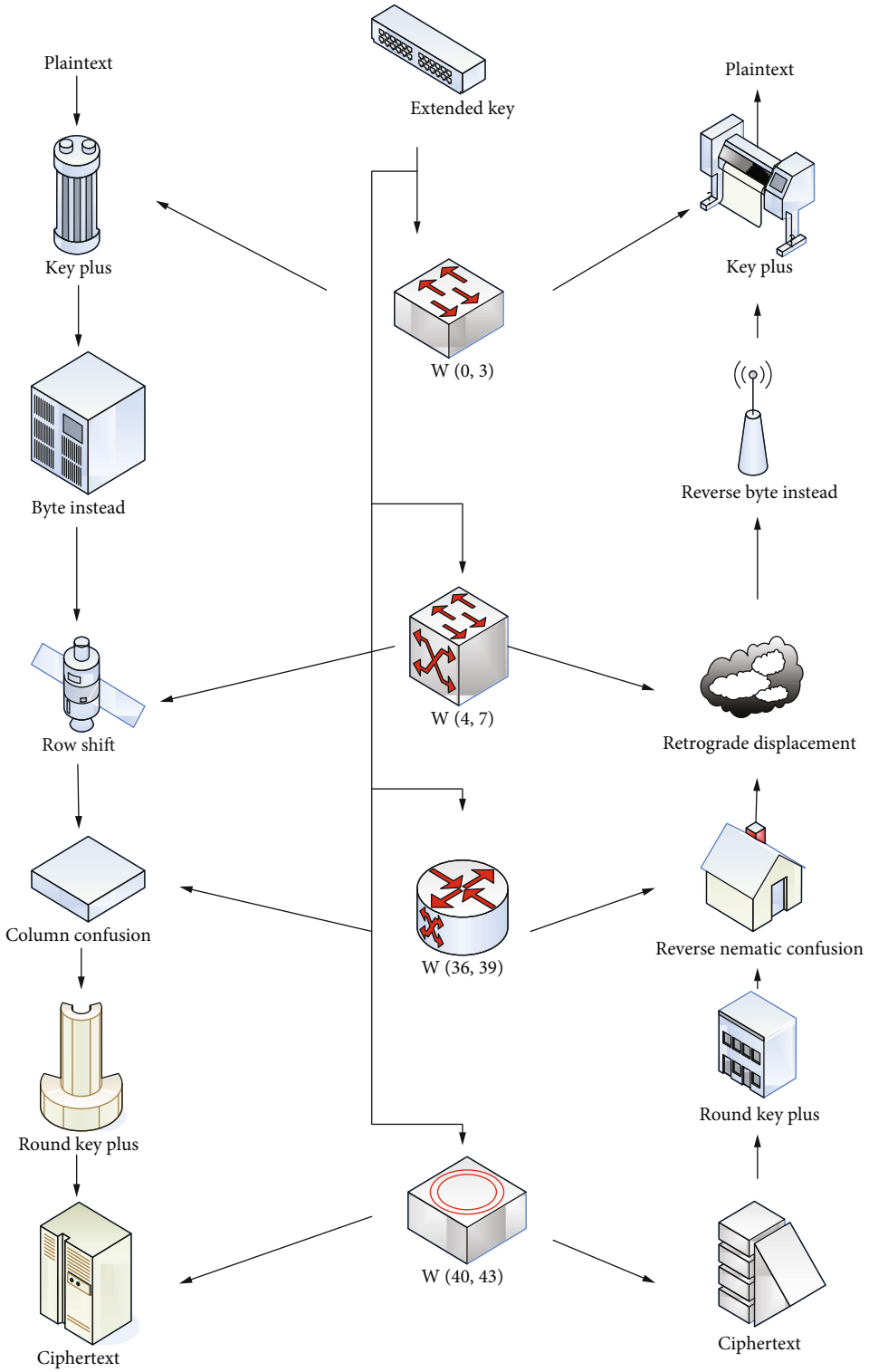

Figure 1: AES encryption and decryption flowchart.

multiplication (02) operation, you can use the xtime function in the following formula to achieve. For any byte a, there is the formula:

$$(02)a = \text{xtime}(a) = (a[6:0], b0) \wedge (hlb\lambda[a[7]]). \quad (5)$$

For the multiplication {03} operation, we can derive it and convert the multiplication {03} into the multiplication {02} on the field GF plus the multiplication {01}, and we can get

$$(03)a = (02)a + (01)a. \quad (6)$$

Table 1: The relationship between the number of conversion rounds Nr, Nb, and Nk.

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	12	14	16
Nk = 6	14	14	16
Nk = 8	16	16	16

The addition in the finite field GF is a bitwise XOR, so substitute the transformation to get

$$(03)a = (a[6:0], (b_0) \wedge (8hlb\lambda 8a(7) \wedge a[7:0]). \quad (7)$$

The multiplication and addition of the state matrix are all based on the operation on the finite field GF, and the addition is equivalent to the XOR operation. The multiplication operation is as in Equation (5), and the operation is based on the column. The schematic diagram of reverse nematic confusion is shown in Figure 4.

Due to

$$\begin{bmatrix} 0E & 0B & 0D \\ 09 & 0E & 0B \\ 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 \\ 01 & 02 & 03 \\ 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} 01 & 00 & 00 \\ 00 & 01 & 00 \\ 00 & 00 & 01 \end{bmatrix}. \quad (8)$$

It shows that the two matrices are inverse to each other, and the original text can be restored after one inverse nematic confusion, and the inverse confusion change can be converted into

$$\begin{bmatrix} 0e & 0b & 0d \\ 09 & 0e & 0b \\ 0b & 0d & 09 \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \end{bmatrix} = \begin{bmatrix} b0 \\ b1 \\ b2 \end{bmatrix}. \quad (9)$$

Similarly, we can derive multiplication {09}, multiplication {0e}, etc., on the finite field GF, but the calculation process is more complicated. Later, we will deform the inverse confusion transformation to make it similar to the confusion transformation process. The AES algorithm includes 11 key addition operations, including the initial key and 10 rounds of function keys, a total of 11 subkeys. First, the initial key is divided into 16 groups and transformed into a state matrix according to the method in Figure 5. Each column of the state matrix is connected according to the byte connection method to obtain $W[0]$, $W[1]$, $W[2]$, and $W[3]$. These 4 arrays are the first round used in the key expansion secret key.

Then, perform ten rounds of calculation on the array W in the following way to obtain the required 11 rounds of subkeys:

(1) If i is not an integer multiple of 4, then the ith column is determined by

$$W[i] = W[i-4] \oplus W[i-1] \quad (10)$$

(2) If i is an integer multiple of 4, then the ith column is determined by

$$W[i] = W[i-4] \oplus T(W[i-1]) \quad (11)$$

The above subkey generation process can be represented by Figure 6.

Among them, the nonlinear function T has the following steps:

(1) Word cyclic shift cyclically shifts each state element of the array $W[4i-1]$ to the left, as follows:

$$[k0, k1, k2, k3] \longrightarrow [k1, k2, k3, k0] \quad (12)$$

(2) Byte replacement will replace the result obtained in (1) with an S-box replacement operation

(3) Round constant XOR the 128-bit data obtained in (2) change and the round constant $\mathrm{Rcon}[i]$ are XORed bitwise, where i represents the current round number, $\mathrm{Rcon}[i] = (\mathrm{RC}[i], 00,00,00)$ (all in hexadecimal); the value of $\mathrm{RC}[i]$ is shown in Table 2

The result of the exclusive OR of the round key plus any number and itself is 0. In the encryption process, the input of each round is XORed with the round key. Therefore, the input can be restored by XORing the key of the round during decryption. The formula is as follows:

$$a_{(i,j)_{4\times4}} \otimes k_{(i,j)_{4\times4}} = b_{(i,j)4\times4}, \quad (13)$$

where $a(i, j)$ is the data block of each byte, Nb = 4, $k(i, j)$ is the round key of each byte, Nk = 4, and $b(i, j)$ is the exclusive OR operation after the result. The round key is obtained by expanding the key through the key expansion process, and then, the plaintext is XORed with the corresponding subkey. A certain encryption algorithm is implemented. The process of recovering and transforming from ciphertext to plaintext is called decryption. If only one key is used, then this is a symmetric encryption technology using a symmetric key, and the shared key is K. This principle process is shown in Figure 7.

Foreign encryption technology has always been ahead of China, and we have been using foreign technology. However, considering the security of national information, our country began to design its own encryption algorithm and introduced the SM4 algorithm of symmetric block cipher to realize the encryption and decryption of information. The packet length of the SM4 algorithm is 128 bits, and the key length is also 128 bits. Similar to the structure of the AES algorithm, the structure of the SM4 algorithm is divided into two parts: the key expansion algorithm and the encryption and decryption algorithm. The algorithm process of SM4 is shown in Figure 8.

The SM4 algorithm is used as a symmetric round transform encryption algorithm, and the encryption and decryption process is 32 rounds in total. Each round of transformation transforms 128-bit data, but the data length

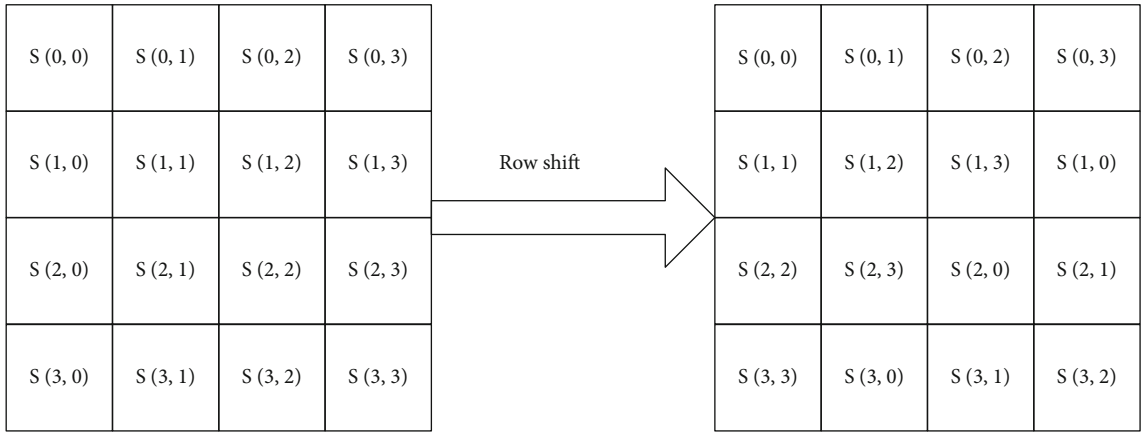

Figure 2: Row shift.

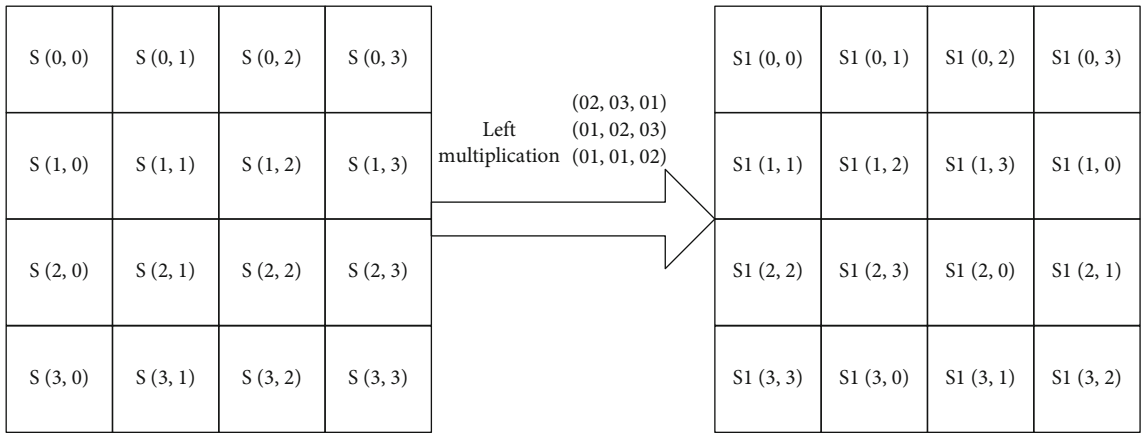

Figure 3: Column confusion.

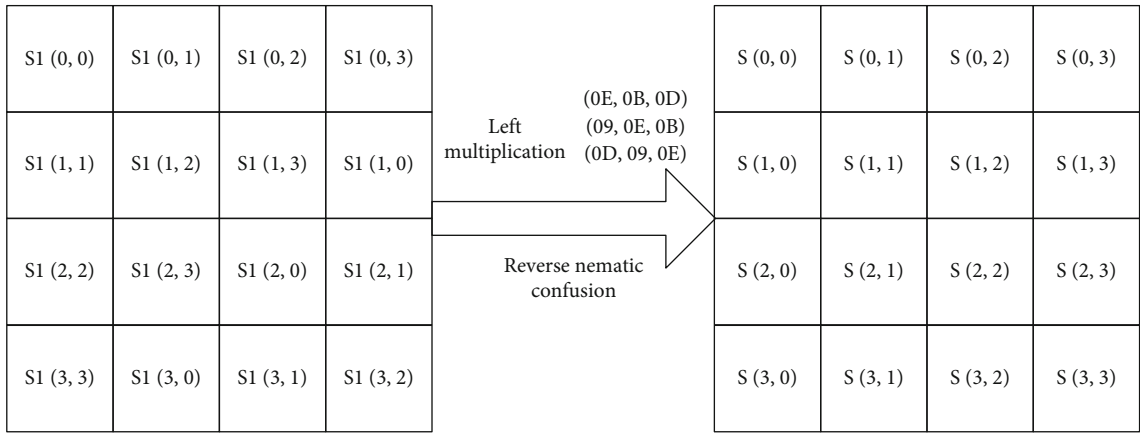

Figure 4: Reverse nematic obfuscation.

in the actual operation unit is only 32 bits. The change process of each round in SM4 is shown in Figure 9, where the process of the encryption algorithm can be expressed as the following formula:

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+2}, rki) \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3}). \end{aligned} \tag{14}$$

The data processed in the nonlinear function ✦ is 32 bits, so 4 parallel S-boxes need to be used. Suppose the input data $A\ (a0, a1, a2, a3)$ belongs to (Z8) 4, and the output data $B = (b0, b1, b2, b3)$ belongs to (Z8) 4. Then, there is the following formula:

$$\begin{aligned} B &= (b0, b1, b2, b3) \\ &= (S\text{-box}(a0), S\text{-box}(a1), S\text{-box}(a2), S\text{-box}(a3)). \end{aligned} \tag{15}$$

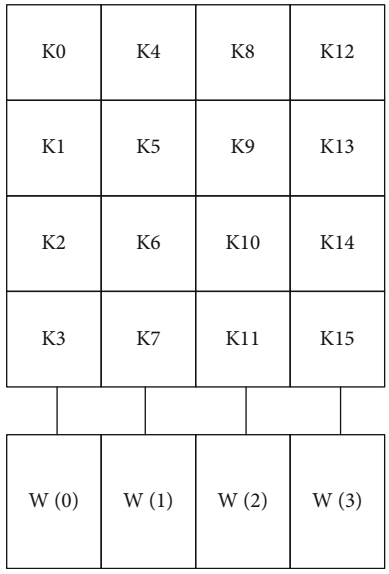

Figure 5: The first set of keys from the state matrix.

For the S-box data of the SM4 algorithm, the structure is similar to the S-box of the AES algorithm. For specific element values, please refer to the relevant literature, then

$$C = L(B) = B \oplus (B<<<2) \oplus (B<<<10) \oplus (B<<<18) \oplus (B<<<24). \quad (16)$$

After 32 rounds of iterative operations, the byte reverse order replacement is performed to obtain the final ciphertext, such as

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32}). \quad (17)$$

2.2. Principles of DES and RSA Encryption Algorithms. Both string encryption and file encryption of the DES algorithm require string encryption. The DES encryption method is widely used in the implementation of computer network information protection applications [18]. For example, the DES algorithm is used to encrypt a character string close to thirty bytes in length, where the key length is 64 bits. The generated ciphertext is expressed in hexadecimal. The encryption speed of the DES algorithm is very fast. It can be considered that if only a small amount of data is encrypted, the DES algorithm basically does not consume system time [19]. But the length of the DES key is an obvious limitation. As file encryption involves opening and closing of folders, it is relatively cumbersome. Therefore, this article uses MFC to establish a simple interface for easy operation. Create a test file in txt format on the computer desktop. The content of this file is English literature on the encryption algorithm; the size is 4.77 KB. After encrypting and decrypting the file with DES encryption technology, the encrypted file and the decrypted file perform corresponding encryption and decryption operations on the MFC interface. The encryption and decryption operations are fast and almost equal. List the source files, encrypted files, and decrypted files. It can be found that the file becomes a bunch of garbled characters after encryption, and the original text is restored after decryption [20]. The effects of encryption and decryption are very good [21]. The DES algorithm uses a variety of crystallographic techniques, including character replacement and scrambling. The main features of the DES encryption algorithm are fast encryption speed and high security. Compared with other encryption algorithms, it has great advantages in encrypting large amounts of data. Apart from the exhaustive method, there is no effective way to crack it. But DES has a fatal flaw, that is, key management, because DES uses single key encryption, and the key length is only 56 bits. Therefore, it is usually adopted to secretly distribute keys before communication and use different keys for different objects [22]. This greatly increases the additional overhead of the system. Finally, the string encryption and file encryption are merged. Use VC ++ to write the program and the main interface and generate an executable file from the interface, which is equivalent to encryption software that can encrypt characters and files.

DES is a symmetric cryptographic algorithm, and the basic algorithm of the encryption method and decryption method is the same (the order of using the subkeys is different, and the subkeys are reversed). The number of initial secret keys entered in the DES algorithm is 64 bits, which are divided into 8 groups in order, and the last bit of each group is the parity bit. In this way, only the 56-bit secret key of the initial key is actually used in the encryption process. The specific operation of DES encryption and decryption is shown in Figure 10.

The specific encryption and decryption process of the DES algorithm is as follows. The first step is to perform the initial replacement operation by bit XOR to obtain 64-bit new data and then take the 64-bit high 32-bit data as $l0$ and the low 32-bit data as $P0$. In the second step (F0, P0), a new set of 64-bit data $(L1, R1)$ is obtained through a series of transformations such as S-box transformation, replacement, and round key addition. The first round of transformation is completed, and then, $(F1, P1)$ performs the same series of transformations to get $(F2, P2)\cdots$; similar operations until the last set of data $(F16, P16)$ is obtained, a total of 16 rounds of transformations. Finally, perform the inverse transformation of the initial permutation on $(F16, P16)$ to obtain a 64-bit ciphertext. Among them, the iterative processing expression for each round is as follows:

$$P_i = F_{i-1} \oplus f(P_{i-1}, K_i), \quad F_i = P_{i-1}. \quad (18)$$

In the formula, the f function has two variables set as a and j, denoted as $f(a, j)$. Among them, a is 32-bit data and j is 48-bit data. In the ith round of iterative calculation process, $a = P(i-1)$, J refers to the subkey, and 32-bit data is output after processing. The given E transformation for the first variable A is shown in Figure 11.

Change from 32-bit data to 48-bit data output. Then, calculate

$$E(A) \wedge j = B. \quad (19)$$

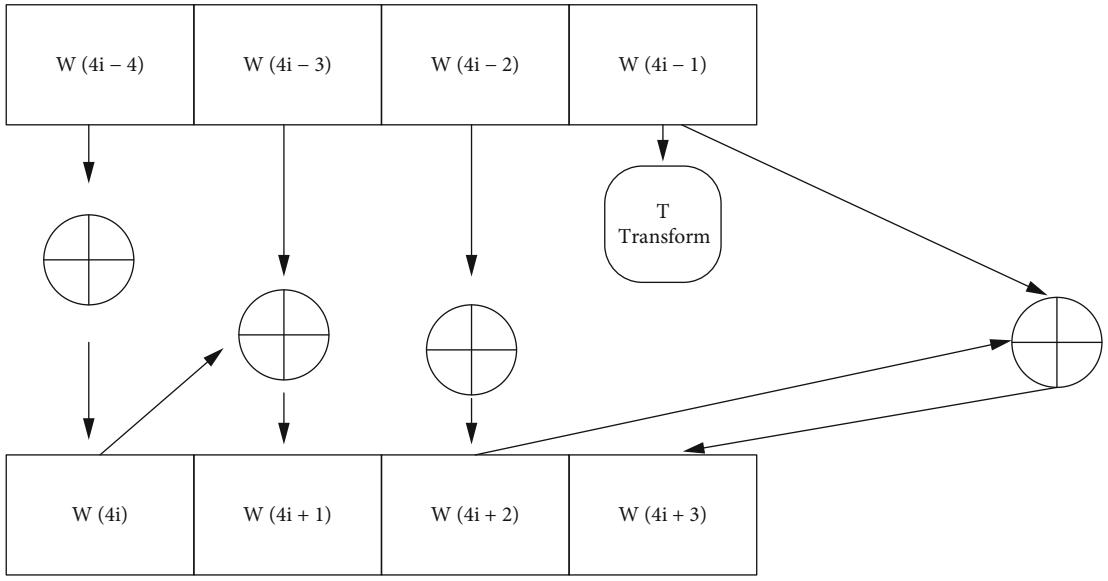

Figure 6: Round key transformation process.

Table 2: Wheel constant RC[i] value table.

i	1	2	3	4	5	6	7	8	9	10
RC[i]	01	02	04	08	10	20	40	80	1B	36

Write the result as a continuous 8 groups of data, each group of 6 bits of data, namely, $Bi = B1B2B3B4B5B6B7B8$; each Bj contains 6 bits, namely, $Bi = b1b2b3b4b5b6$, $i = 1, 2, 3, 4, 5, 6, 7, 8$. After the above calculation, the S-box transformation operation is performed on B. The S-box transformation is the only nonlinear transformation component in the DES algorithm, and its security strength also determines the overall strength of the encryption algorithm. Each S-box is a fixed 4×16 matrix, and its element value is decimal, as shown in Table 3.

When calculating, use the highest bit and the lowest bit in B as the number of rows in the S-box to select $h\,(0 \le h \le 3)$; use the 2nd to 5th bit as the column to find the S-box number $r\,(0 \le r \le 15)$. Finally, P is a fixed permutation, as shown in Figure 12, where E and P transformations only need to be used to increase the diffusion effect of the algorithm.

In the DES algorithm, the first replacement processing IP replacement and the last processed IP inverse replacement belong to a simple correspondence relationship, and the specific correspondence relationship is known and has no specific meaning in cryptography. Its main function is to change the ASCII value of the input x that is scrambled, and the IP replacement and its inverse replacement are shown in Table 4.

The subkey Ki is generated according to the design of the DES algorithm. The encryption process in the algorithm corresponds to 16 subkeys $K1, , ,, ,K16$. The length of the subkey Ki is 48 bits. The bit operation is obtained, and the flow chart of key generation is shown in Figure 13.

Execute according to the flow of Figure 10 to find the last set of word secret keys $K16$. The number of left shifts in each round is different. Specifically, the number of cyclic shifts in the first, second, nineteenth, and 16th rounds is 1 bit, and the number of cyclic shifts in the other rounds is 2. The replacement option 1 operation is to remove the parity bit from the 64-bit key and replace it with 56 bits. The output is shown in Table 5.

The DES decryption and decryption process is similar. The use order of the generated subkeys can be reversed. The ith round of transformation uses the ith round of subkeys during encryption, and the ith round of transformation uses the 17th round of decryption. The subkey is generated by iteration i.

The RSA algorithm is also one of the commonly used algorithms. Random large prime numbers need to be generated in the RSA algorithm, because the number of RSA prime numbers determines the security of the RSA algorithm and is also the key to ensuring the security of password encryption. Therefore, how to quickly generate large prime numbers restricts the efficiency of the algorithm [23]. In the actual RSA algorithm, the method of random generation is usually used, first generating a large random number, and then determining whether it is a prime number, so the method of determining the prime number determines the speed of the algorithm [24]. Judging a prime number with a probabilistic algorithm is a very fast algorithm, because in computer judgment, there is a very small probability to determine the composite number as a prime number. This method generates a prime number very quickly and then uses some algorithms to determine whether the number is a prime number; if it is not, continue to judge the next random number until there is a random number that is a prime number. The algorithm can be divided into three stages in the algorithm: the selection of large prime numbers, the generation of public and private keys, and encryption and decryption operations. In the network communication optimization encryption process, the RSA encryption prepossessing process expresses the reconstruction of the encryption algorithm through the setup

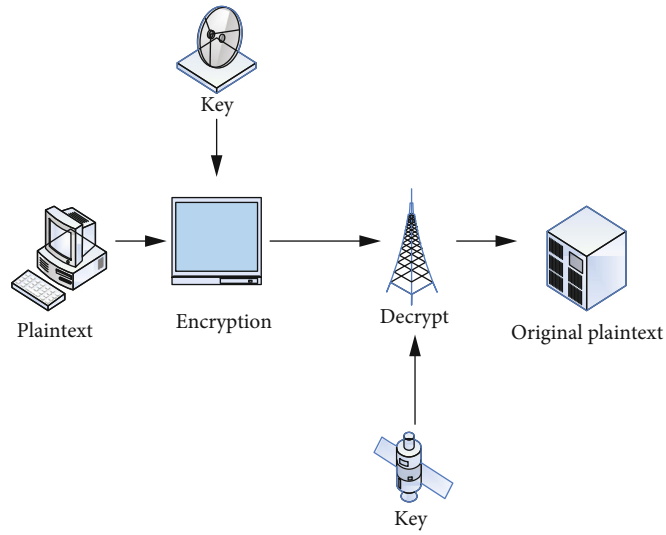

Figure 7: Encryption principle model using the same key.

function, and the parameter area needs to be set, as shown in formulas (1), (2), (3), and (4).

$$y = \min\left[\sum_{i=1}^{nl}\left(y_i^{\,2} - 2y_i y_l + y_l^{\,2}\right) + \sum_{im+1}^{n_l+n_R}\left(y_i^{\,2} - 2y_i y_R + y_R^{\,2}\right)\right], \tag{20}$$

$$x\text{best} = \min\left[\sum_{yeD_1}(y - y_L)^2 + \sum_{yeD_2}(y - y_R)^2\right], \tag{21}$$

$$F\left(X^i\right) = \frac{\sum_{j=0}^{\text{num}} C_{nj}\left(uj^i - u^i\right)^2}{\sum_{j=0}^{\text{num}} C_{nj}\left(dj^i\right)^2}, \tag{22}$$

$$\text{WOE}_i = \text{In}\frac{B_i/B_t}{G_i/G_t}. \tag{23}$$

The purpose of DES and RSA encryption algorithms is to maintain data security methods and methods and to achieve network information security and network device security through encryption technology [25]. The computer data encryption technology incorporates password-related technologies. The password-related technologies encrypt various information in the computer. The main method of implementation is to replace the internal information of the computer by function shift replacement and encryption key information that cannot be obtained by others; only the user knows the decryption function can view and modify the information; this way can improve the security of computer security information [26]. In actual use, only users who know the password can access the computer's data information.

Computer data encryption technology can be divided into symmetric encryption technology and asymmetric encryption technology. Computer information encryption the former means that the information sender and receiver use the same key to decrypt the data information, while the latter is the information sender and the receiver uses different information keys to encrypt and decrypt the data [27]. The difference between these two methods is whether the same key is used to encrypt the data. During the process of encrypting and decrypting the data of the computer, we need to ensure that the receiver and sender of the sent information can keep the decoding completely; the key is the only way to improve the confidentiality and security of data information. Computer data encryption requires the joint use and maintenance of users and encryptions to create a healthy computer environment and ensure the safety and reliability of computer information data [28].

2.3. Key Design Method of Encryption Algorithm. When we use a computer at home, we will inevitably need to use a lot of computer software, and to fully use this data security encryption in computer software, we need to create safe computer network security surroundings. Therefore, the key system of information encryption algorithm came into being. Although encryption algorithms have a wide range of applications, with the continuous research on large number decomposition technology, people can decompose more and more numbers. The length of the key also increases [29]. Due to the limitations of traditional encryption methods, the choice of large prime numbers becomes difficult and its efficiency is reduced. It is difficult to achieve a one-time encryption system, which results in complicated operations during encryption and decryption, which will greatly affect the efficiency of the algorithm. The generation of these problems will bring many restrictions to the application of encryption algorithms. The two basic elements of the most advanced encryption system are encryption algorithms and key management. The key in the encryption algorithm is some formulas and rules, which stipulate the conversion method between plaintext and ciphertext. Due to the repeated use of cryptosystems, it is difficult to rely on encryption algorithms to ensure the security of information. In fact, the security of encrypted information can depend more on the security management of the key. The key is the key

information to control the encryption algorithm and decryption algorithm, so its generation, transmission, storage, and other work are very important. Particularly in the case where multiple users share a computer, if each user lacks perfect management measures for the keys used, there will be no secure password system available. With the continuous breakthroughs in encryption technology, the creation of a public-private key system provides theoretical support for the security of computer encryption algorithms. A key is required for encryption and decryption: a public key and a private key. The user must ensure the security of the private key, and the public key can be released. The public key and the private key are closely related, and the information encrypted with the public key can only be decrypted with the private key, and vice versa. Since the receiver of the public key cryptosystem only needs to save a private key, there is no need to allocate additional management space in key management, so the key transmission is quite safe. Only the corresponding private key can decrypt the ciphertext encrypted by the public key. This is the principle of encryption algorithm key application. In order to ensure the complexity of the encryption algorithm, in the communication of computer network data, the data can be encrypted by the encryption algorithm operation formula, and the encryption process can be expressed as shown in formulas (5), (6), (7), and (8).

$$\text{Splitinfoa}(D) = -\sum_{j=1}^{v} \frac{D_f}{D} * \log 2\left(\frac{D_f}{D}\right), \tag{24}$$

$$V_{jk}(N+1) = V_{jk}(N) + a_1 d_k(N) h_j, \tag{25}$$

$$e_j = \left(\sum_{k=1}^{n} d_k v_j\right) * h_j * \left(1 - h_j\right) j = 1, 2, \tag{26}$$

$$\text{CRF}_t(b) = \sum_{t=1}^{k} F(t_b - t_{b1}). \tag{27}$$

Modern cryptography is two major aspects, that is, coding and analysis. The former is committed to establishing a secure cryptographic system that is difficult to be broken by the enemy or opponent, that is, "knowing oneself"; the latter is trying to decipher the existing cryptographic system of the enemy or opponent, that is, "knowing the enemy." These two aspects can be described as one main offense and one main defense, which are equally important. In detail, coding alone involves many aspects, such as the encryption and authentication of the most common information that is closely related to our lives, such as the use of digital signatures on Taobao, and the most important and most important. One aspect of difficulty: key management. This content is the core research point involved in PKI mentioned in the last chapter of this paper. Cryptography emphasizes that encryption and decryption algorithms can be made public, but it is obvious that private keys are strictly confidential, so obviously, key management is the most important part. Modern cryptography is in a vigorous development stage, and some new theories, new algorithms, and new implementation methods will constantly emerge, which all require us to continue to dig deeper to find better ways. Solve all kinds of problems in the future. The data encryption standard, DES, was developed by IBM. There are two types of data encryption technology, symmetric encryption technology, and the corresponding one is naturally asymmetric encryption technology. Of course, there are many algorithms now, and there is no conclusion, or a strict implementation of a standard. Algorithms are always evolving and always being optimized. If they are easy to use under certain circumstances in a certain period, they are good standards that can be used.

3. Experiments

3.1. Experimenter Information and Related Data. In order to verify the accuracy of the DES encryption method, taking real data as an example, a data encryption experiment was carried out, and the network Web communication data was selected in the experiment. Under the MATLAB environment, a network data communication encryption experiment simulation platform was formed, and fuzzy parameter proofing encryption algorithms and the proofreading algorithm to determine the threshold parameter are used to encrypt the computer network data. In the simulation, the vertex coordinates of the communication area of 3 network data are selected, the unit is km, which are $x1 = 0.415$, $x2 = 0.438$, and $x3 = 0.558$. Design 10 MB computer network communication data as the specific experimental data for comparing different methods. Contains redundant data, and then compares the time spent in data encryption and decryption under different algorithms. It is necessary to count the results of the number of parameter calibrations. The method of determining fuzzy parameters will not appear much during the DES encryption process. The problem of the second iteration, because the judgment can be completed quickly under the premise of the ambiguity of the parameters, the encryption speed, and the number of iterations is better than the judgment algorithm with fixed parameters, to ensure the efficiency of improved algorithm encryption. In order to further prove the effectiveness of the DES encryption method in computer network data encryption, this article conducted multiple experiments and analyses, using 10 MB of computer network communication data as the basis to compare the experimental data, and using different algorithms to encrypt experiments based on multiple experiments. Key generation time, the time of encrypted data, and the time of decrypt data are compared, respectively. The experimental comparison A results. The algorithm of this paper is superior to the traditional algorithm in the time of key generation, encrypted data, and decrypted data. The fuzzy interval theory first defines the data sequence to be encrypted as a random sequence and then confirms the parameters through multiple fuzzy functions. The single threshold is no longer used to confirm the parameters, which avoids the repeated calibration process. Based on several proofreading, the plaintext in the computer network can be encrypted, and on this basis, fully constrained multiple encryption attributes can be imported to

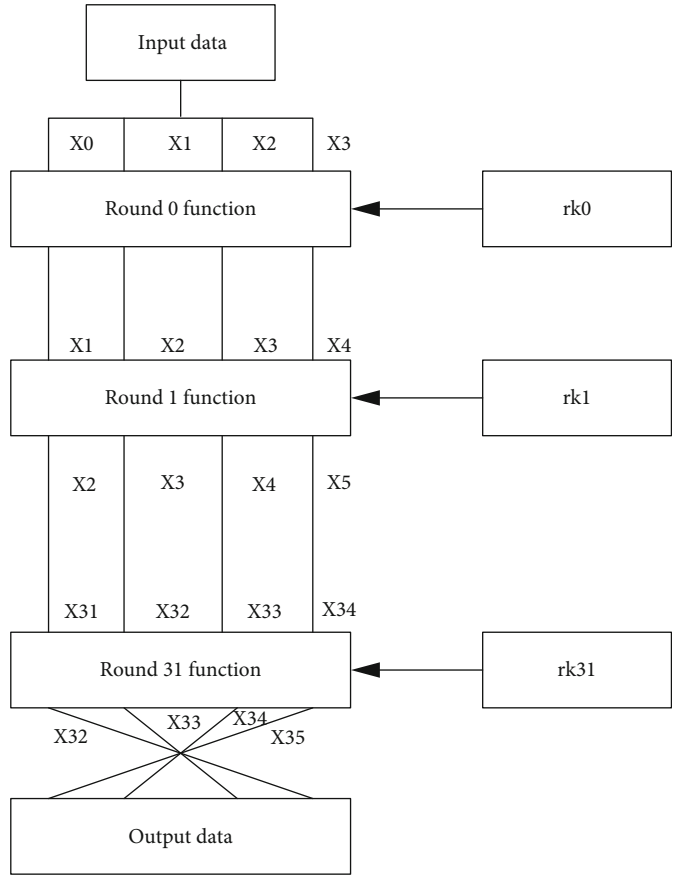

Figure 8: SM4 algorithm implementation process.

ensure the effectiveness and efficiency of improved algorithm encryption, while traditional algorithms generate and encrypt data 2. The time spent decrypt data has increased and cannot meet the demand.

The standard objects of this encryption experiment are DES, which can also be called a standard in data symmetric encryption. This is also a very practical classic symmetric data encryption standard algorithm. Its main feature is that it was developed and succeeded by the IBM team put forward. After a long period of research and development, the United States and RSN directly write DES as the main standard for encrypting data. Using its DES encryption algorithm can be used to encrypt plaintext databases, first, we should deal with each group of plaintext data. Perform a grouping, set the length of each plaintext in the same group to 64 bits, and then, perform an encryption and deletion operation on each binary plaintext data in each same group, so that the data in each group can be encrypted. After being processed by encryption software, a set of 64-bit long digital ciphertext will be automatically formed. Finally, all the ciphertexts of each ciphertext group are spliced in everything. You can directly get the ciphertext of the entire group. Here, in an algorithm that uses integer DESE, since the algorithm uses a 64-bit integer as the parity group check unit, one thing that needs special attention is that 8 bits must not be used as a parity unit. CDESD is used although the

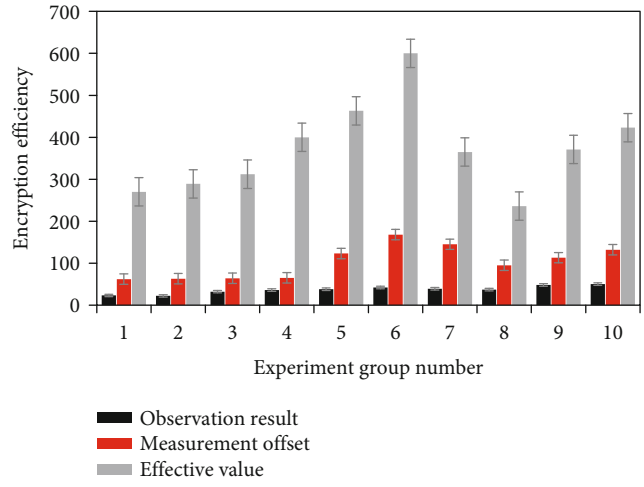

Figure 9: The computing speed of the MD5 algorithm encryption technology will be greatly improved.

specific process of the ciphertext encryption technology such as the algorithm enters the run-time; this is the case, but when the computer switches from the ciphertext work processing mode when entering the ciphertext encryption processing mode, you can still directly use the per-predicted key to perform confidential password processing on the

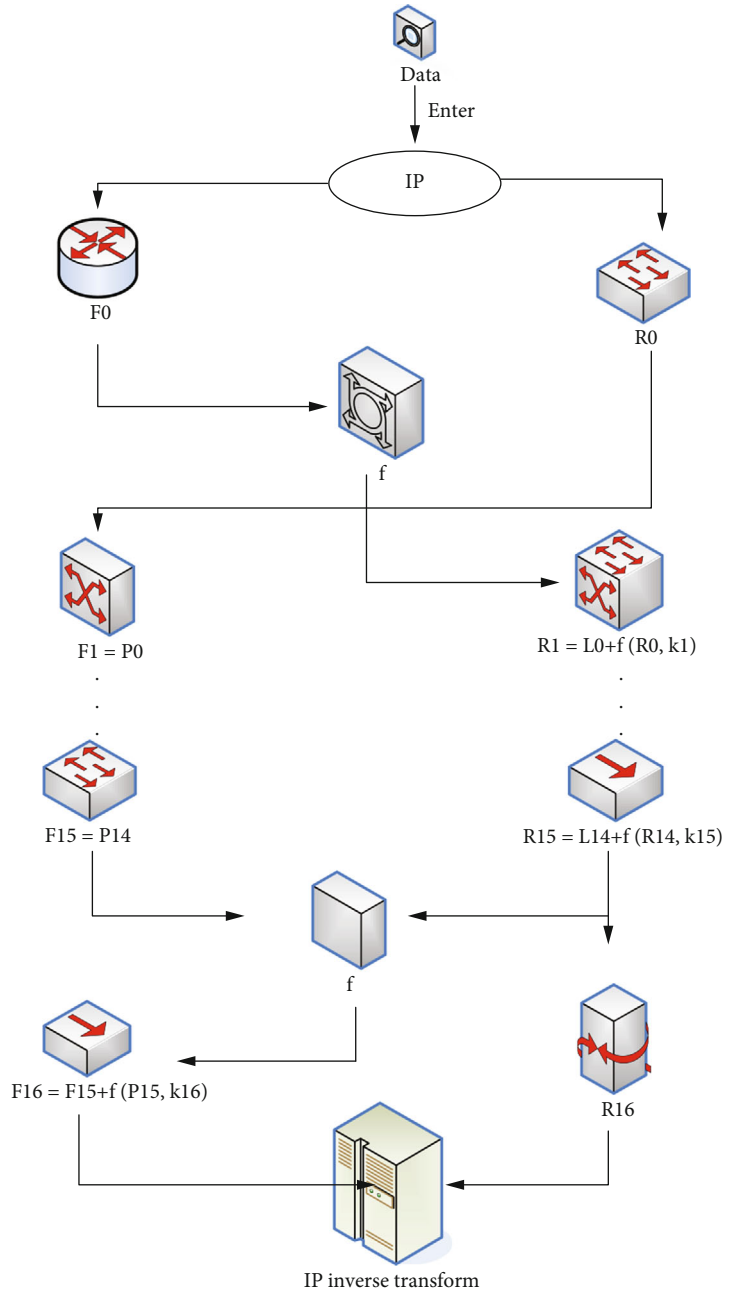

Figure 10: The basic operation process of DES encryption and decryption.

relevant plaintext data and directly produce and output the relevant ciphertext, and one point that needs special attention at this time is, before the ciphertext data is transmitted, the receiver and the data sender must reach some kind of coordination or unification in advance, obtain a corresponding plaintext key, and use it to decrypt it in plaintext. Through such data encryption technology, the encrypted data information is transmitted in real time to any place the user needs and effectively guarantees the security of user data information transmission.

3.2. Experimental Conditions and Operation Plan. This article uses the latest scientific and technological means to observe and analyze the current network data encryption algorithm. This experiment is based on the well-known American network information encryption algorithm SNYLE technology. In the process of conducting computer network data information encryption experiments, a theoretical model that can be freely calculated can be created for the information encryption reaction group. They can expand and infer some objective data through experiment expansion, which can better the relevant theory of computer information encryption and methods to understand and learn. Practicality is an important characteristic to distinguish computer encryption from other disciplines. Practical learning includes the design, implementation, and

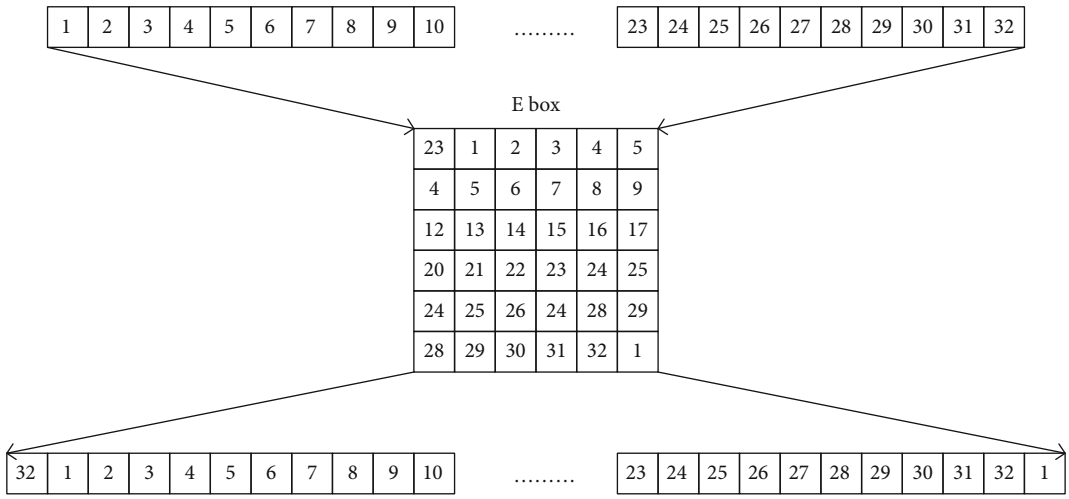

Figure 11: *E* transformation in DES.

debugging of software and hardware. If we can effectively improve the quality and effectiveness of the computer encryption algorithm experiment teaching activities, then the students themselves can also complete the theoretical knowledge learning more specifically. Based on satisfying knowledge exploration and current market demands, improving its security and controllability as much as possible, and doing well computer encryption algorithm experimental teaching, can also promote the effective training and development of researchers' creative thinking ability. By participating in experimental learning, relevant technical personnel themselves can carry out certain innovations and explorations and explore the relevant skills they have learned from a subjective level. After continuous practice and thinking, the encryption algorithm experiment itself can eventually form the development of innovative ability. With the development of the current era, computer encryption technology is also undergoing rapid progress. The emergence of many new technologies requires the frontline researchers to have a good innovative ability and learning ability to accept. In the process of actual computer encryption algorithm experiment teaching activities, we can apply the theoretical knowledge learned through hands-on operation, so that they can test the correctness of the learned knowledge theory and improve their knowledge understanding. At the same time, it can also form developmental thinking, which is also of positive significance for the improvement of one's own scientific literacy. The structure of the computer data node encryption experiment information table used in this paper is shown in Table 6.

During the current computer encryption technology practice activities, the housekeeper network data encryption security experiment group attaches relatively limited importance to the computer encryption algorithm experiment and still uses the previous research methods in the development of related experimental activities. Under such a prerequisite, the top IT research talents themselves will lose enough interest in participating in computer encryption experiment

Table 3: *S*-box replacement.

S	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	19	5	3	8
	4	1	14	8	14	6	2	10	15	12	9	6	4	10	2	5
	14	11	8	2	4	9	2	7	5	12	15	7	10	5	0	13

learning. Because the teaching system is not scientific and advanced enough, it affects the rationality of the evaluation of students' academic performance, and it is difficult to better consider the development of students' computer practice ability. At the same time, during the current encryption experiment, it also has higher requirements for the professional quality of the IT elite, and some high-end encryption technology companies have relatively limited mastery of practical training, which affects the encryption experiment. Specific effects. In the current new development environment, in the course of the development of computing encryption experiment activities in colleges and universities, we should objectively analyze the deficiencies of the current encryption experiment mechanism, make reasonable arrangements for practical teaching activities, and enhance professional capabilities and qualities. It can better meet the task of the current network computer encryption experiment.

4. Discussion

4.1. Analysis of Computer Data Communication Security Data Encryption Algorithm. This article discusses the two most used algorithms. The DES algorithm is a typical representative in a symmetric encryption system, and RSA is a representative in an asymmetric encryption algorithm. The DES algorithm uses the same key for encryption and decryption. It is fast and efficient, suitable for the encryption of large amounts of data, but the key length is short and the security is slightly worse; RSA is the representative of asymmetric encryption algorithm, and its encryption and

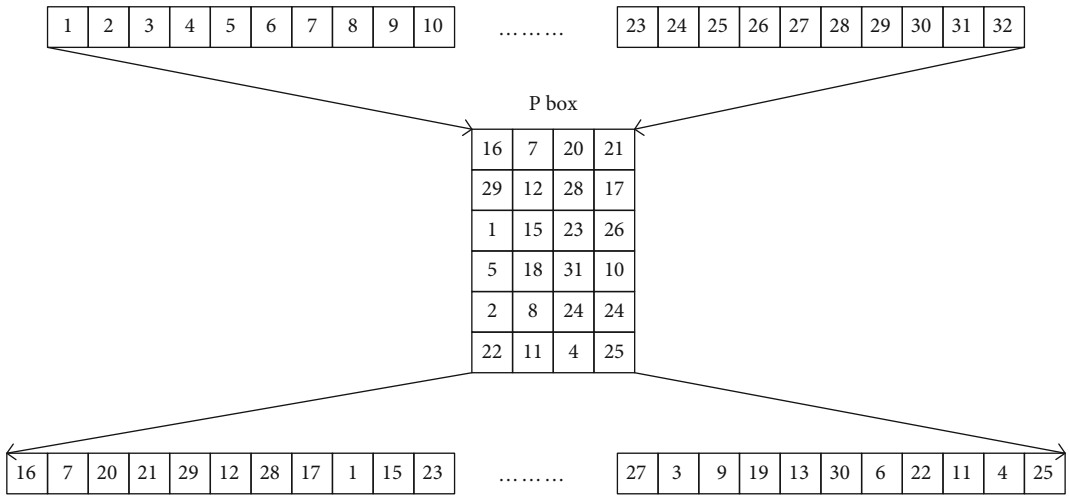

Figure 12: *P*-box substitution table in DES.

decryption are the use of different keys that is not easy to crack, but the operation is slow and is not suitable for encrypting large amounts of data. In this algorithm, the concept of "sieve" is introduced, "sieve" is a "two-dimensional" variable, and the plaintext is split and then separately encrypted by DES, which not only ensures the efficiency of encryption but also overcomes to a certain extent. The shortcoming of DES key is short. In the end, this paper simply designs and implements a hybrid encryption system based on 2DES sieve encryption algorithm and RSA algorithm and tests and analyzes its encryption efficiency. This article compares the results of the two algorithms, as shown in Table 7.

Compared with other encryption standards such as DES and 3DES, the AES standard has a long enough key, flexible design of packet length and key length, and an open algorithm, which makes the cracking takes a long time, fast calculation speed, and very low memory requirements. In a restricted environment, it has a better avalanche effect characteristic. The AES standard supports variable packet length. The packet length can be set to any multiple of 32 bits, with a minimum value of 128 bits and a maximum value of 256 bits. The key length of AES is larger than DES, it can also be set to any multiple of 32 bits, the minimum value is 128 bits, and the maximum value is 256 bits, so it is impossible to crack by exhaustive method, so the AES standard is now more extensive application in various fields. The results of comparison between the latest encryption technology and traditional encryption technology are shown in Table 8.

The advantage of the traditional two-tier architecture mode is simplicity, which can make the information transmission efficient. The disadvantage is that the analysis and discrimination ability is low in the process of information transmission, and the input information instructions can not be classified accurately. The new three-tier architecture is conducive to improve the efficiency of information use and ensure the security of information transmission and use. In order to improve the security and stability of the database and to ensure the integrity of the database content, the previous two-layer architecture model was improved, and a business layer was added between the computer and the server, using the relevant procedures of the business layer to access the information timely classification, judging the security of the information source, and sending the information after screening. The business layer can classify and analyze a large amount of data, reducing the workload of the original architecture and improving the security during information transmission. By setting the corresponding operation instructions, a large amount of data can be exchanged between the server and the computer, and the integrity of the data transmission process is guaranteed, the value of the information is improved, and the information content will not be maliciously attacked and destroyed. The results of the latest MD5 algorithm encryption technology are shown in Figure 9.

Table 4: IP replacement.

IP					IP^{-1}				
58	42	26	10	2	40	8	48	16	56
60	44	28	12	4	39	7	47	15	55
62	46	30	14	6	38	6	46	14	54
64	48	32	16	8	37	5	45	13	53

From the data in Figure 1, the latest MD5 algorithm encryption technology has a 40% increase in computing power and a 55% increase in computing speed over traditional data encryption technology. The setting of the computer programming language is the prerequisite for ensuring work efficiency. People use the programming language to complete the communication and exchange with the computer, so that a large amount of database information can be edited, to rationally modify and organize the contents of the database. For the choice of programming language, you can filter from two levels of PHP and NET. According to the advantages and content of a specific

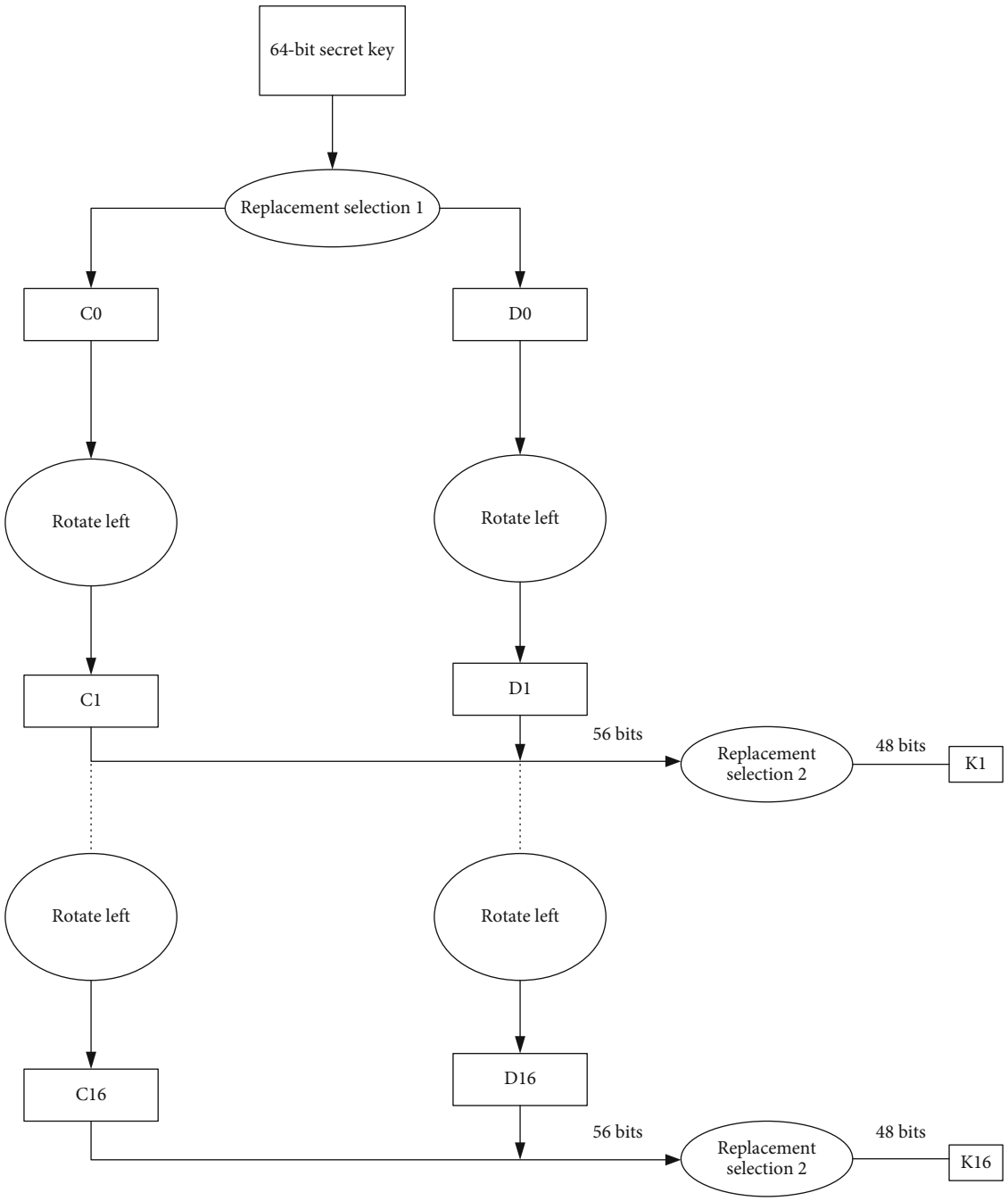

Figure 13: Key generation.

Table 5: PC1 and PC2 transformation.

PC-1						PC-2			
57	49	33	17	18	14	17	11	1	5
1	58	42	26	9	3	28	15	21	10
10	2	51	35	27	23	23	12	26	8
19	11	60	23	15	16	7	27	13	2
63	25	36	37	22	30	52	31	47	48
7	62	45	12	29	14	42	51	33	53

Table 6: Data node encryption experiment information table structure.

Experimental information	Statistical data	Conclusion data
Cryptography	The first stage	Strengthen
Defense ability	Second stage	Point-to-point defense failure
Operating frequency	The third stage	Conversion rate
Cycle	The fourth stage	Data information update time

Table 7: Computer encryption technology security feasibility index.

Node encryption	Calculating speed	Safe range	Use range value	Replacement interval
Execution space	18.57 s	105.47-123.58	23.48-24.26	65.32-66.35
Period value	21.55 s	203.11-247.36	24.32-24.96	39.32-40.21
BB\UP	36.78 s	-352.74-89.25	0.115/0.956	0.152/0.75

environment, use a specific language programming mode, while paying attention to the security issues in the language programming process. Compared with the above two programming modes, the overall security of the Java programming language is higher, and it can be accurately classified according to different types of languages, and the programming content can be structured to allow users to edit website content more conveniently. At the same time browsing the specific information, its security is also improved. The application effect of RSA algorithm encryption technology is shown in Figure 14.

From the data in Figure 2, the RSA algorithm is the most used algorithm, reaching 46% of the total application volume, and its security performance is improved by 30% compared with the traditional algorithm.

4.2. Contrast Analysis and Analysis of the Security Performance of Data Encryption Algorithms for Computer Network Communication Security. Through the research of this paper, we know that the improved 2DES encryption algorithm is a linear operation with fast operation speed. On the other hand, the sum of its encrypted data is still the original key length, which is different from 3DES encryption three times, which is equivalent to using one DES. The three lengths of data in plaintext are encrypted, so the improved algorithm can be well-secured and suitable for the encryption of large amounts of data. The key space has been greatly improved. 2DES encryption uses DES encryption twice, effectively preventing illegal theft in the network. Because the original data has been split, when the data is transmitted on the network, the data carried in each data packet is incomplete, so when the data is illegally stolen, the stolen person cannot crack the original key. It has strong practicality. Since the DES algorithm is already very mature in various fields, there are many corresponding encryption chips. The 2DES sieve encryption algorithm is based on DES and only undergoes a simple split. Therefore, the original DES resources can be used well without the need for excessive investment and change. It is very resistant and can resist all cryptography attacks known today, and because of this, it can become the standard for public key data encryption. We attach equal importance to the RSA algorithm. This article has made in-depth research and proposed many new public-key cryptosystems based on RSA. According to different industries, many encryption software based on the RSA algorithm have been developed to meet the different encryption requirements of different industries. RSA belongs to the public-key cryptosystem. The public key system is to generate two keys, one for encryption and one for decryption, and cannot derive another one based on the algorithm and one of the keys. When in use, the public key is disclosed. After the other party encrypts the data with the public key, the ciphertext is sent back, and then, the private key is decrypted with another one, thereby restoring the key. But at the same time, the development and application of two encryption algorithms are very difficult, as shown in Figure 15.

Table 8: Operating space value tablet.

Serial number	Corresponding parameters	Adoption rate	Number of attributes
One	Tic-tac-toe	35%	8
Two	Lymphography	46%	9
Three	Vote	55%	15

From the data in Figure 3, the application and development of data encryption algorithm technology for computer network communication security is very difficult. Compared with traditional development, the development difficulty has increased by 25%, and the investment development cost has increased by 35%. There is a specific relationship between computer databases, servers, and the Internet. They are uniformly protected by the system firewall, so that the corresponding programs can run normally. At present, the general security precautions are to set up a system firewall, filter all kinds of information under the protection of a specific firewall, and at the same time complete the instruction setting and target selection. During the application of firewall technology, with different systems, a hardware firewall and a software firewall are set. Although there is a name distinction between the two, their work content is aimed at improving the integrity of the computer database to ensure that the internal information is not stolen; at the same time, the internal information is analyzed and distinguished, so that the valuable information continues to be stored and used. When performing database command operations, specific operation logs are kept. Based on this data information, the actual operation process of the management personnel can be understood, and the monitoring ability of the firewall can be judged. The use of computer network communication security data encryption algorithm has a good effect on preventing virus intrusion, as shown in Figure 16.

It can be seen from the data in Figure 4 that the software protection strength of the data encryption algorithm technology using computer network communication security can be increased by 36%, and the rate of data encryption algorithm technology adopted when developing software is

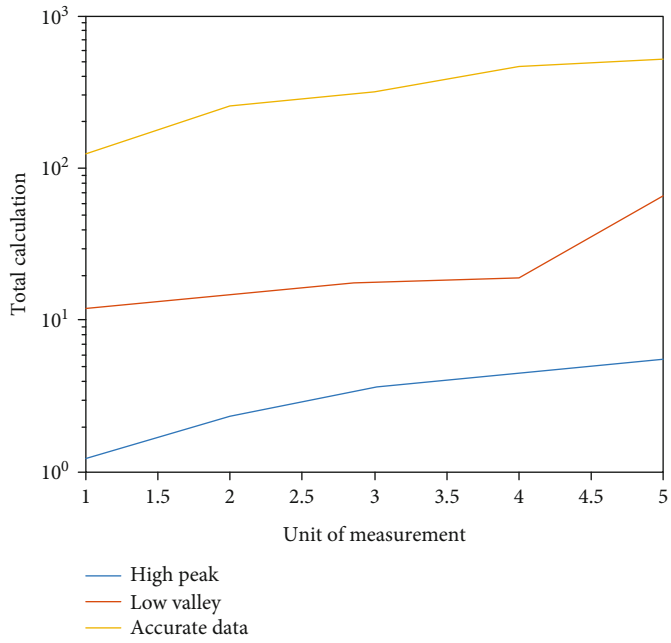

Figure 14: RSA algorithm encryption technology is the most applied and safest calculation method.

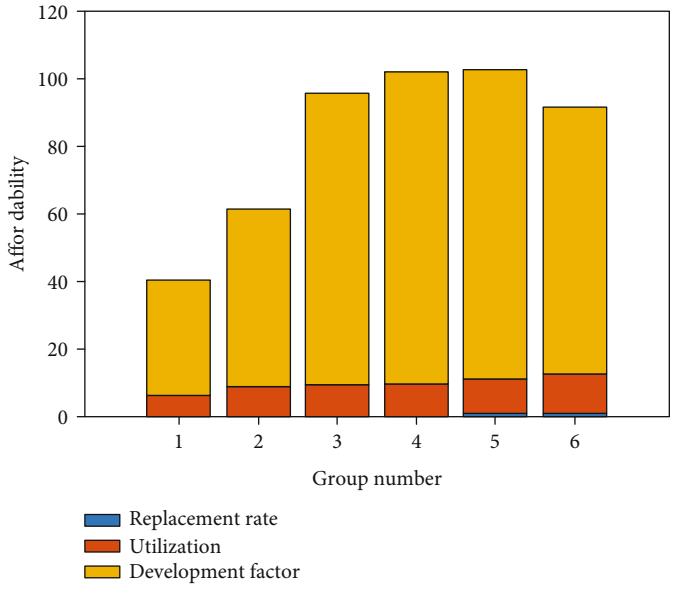

Figure 15: Computer network communication security data encryption algorithm technology application development is very difficult.

68%. In the application of computer communication networks, the types of software are increasing and have been fully developed and applied. However, there are still viruses or hackers who steal user data through software, which in turn leads to abnormal user usage. To this end, it is necessary to encrypt the application software. The application of data encryption technology can ensure the quality of the software encryption process and ensure that the user data information will not be leaked. At the same time, the early warning system can be used to feedback the upcoming network security problems and take precautionary measures. In addition, users should regularly check to ensure that the application software is safe, effectively deal with potential viruses, and improve information security. Computer network communication security data encryption algorithm is very effective in protecting personal privacy, preventing virus infection, and preventing financial fraud and information leakage, as shown in Figure 17.

From the data in Figure 5, the data encryption of computer network communication security can reduce personal privacy leakage by 25%, intercept 80% of hacker attacks, and reduce the success rate of financial fraud by 64%.

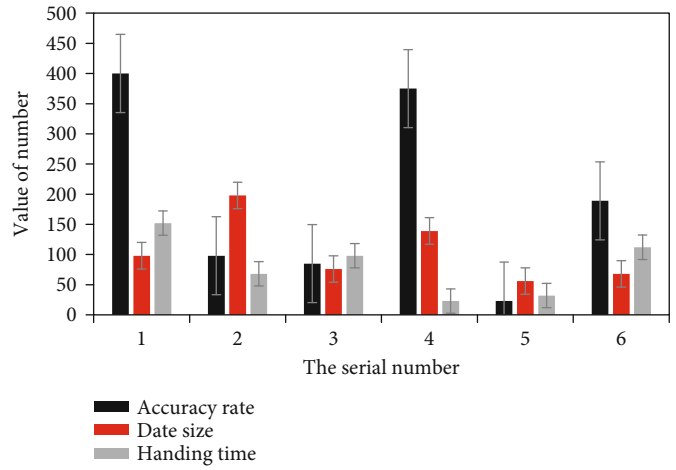

Figure 16: The software protection intensity of the data encryption algorithm technology using computer network communication security has been greatly improved.

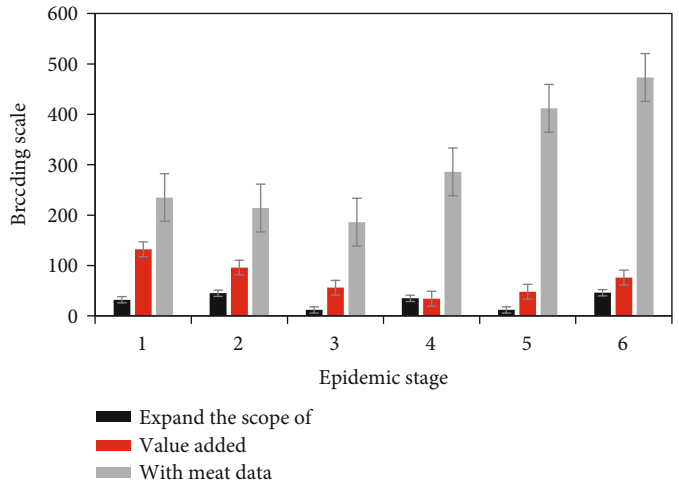

Figure 17: Data encryption software using computer network communication security has a good effect in protecting financial fraud, privacy leakage, and hacking.

5. Conclusions

(1) This article analyzes the ways and means to ensure the security of computer communications under the current network environment. The problems of current network data encryption technology are discussed. Although encryption technology has many deficiencies in practical applications, technical staff have optimized and studied it. To this end, the issues related to computer communication security data encryption technology are elaborated in detail, hoping to provide valuable theoretical basis for the application of data encryption technology in computer communication security through the above research and discussion

(2) This paper analyzes the encryption security performance of computer network security communication machine and conducts many experiments for many users. From the perspective of network data link, there are three encryption algorithms, namely, link encryption algorithm, node encryption algorithm, and end-to-end encryption algorithm. The results of the study show that the use of link encryption algorithms in network communication security encryption algorithms can increase the security index by 25%, node encryption algorithms can increase the security index by 35%, and end-to-end encryption algorithms can increase network activity. Safety index increased by 40%

(3) This article discusses and verifies the feasibility and superiority of computer network security communication machine encryption. After experimental verification, the latest MD5 algorithm encryption technology has a 40% increase in computing power and a 55% increase in computing speed over traditional data encryption technology. The RSA algorithm is the most used algorithm, reaching 46% of the total application volume, and its security performance is improved by 30% compared with the

traditional algorithm. The software protection strength of data encryption algorithm technology using computer network communication security can be increased by 36%, and the rate of data encryption algorithm technology adopted when developing software is 68%. Computer network communication security data encryption can reduce personal privacy leakage by 25%, can intercept 80% of hacker attacks, and can reduce the success rate of financial fraud by 64%. In short, due to the limited research time, ability, and energy, although the research content of this article has been successfully applied, it is still lacking in breadth and depth. In-depth research on this will be the focus of my work for a period of time in the future

Data Availability

This article does not cover data research. No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] W. H. Jeong, B. G. Yeo, K. H. Kim et al., "Performance analysis of the encryption algorithms in a satellite communication network based on H-ARQ," *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 15, no. 1, pp. 45–52, 2015.

[2] Y. Zhang, D. Zheng, Q. Li, J. Li, and H. Li, "Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing," *Security & Communication Networks*, vol. 9, no. 16, pp. 3688–3702, 2016.

[3] C. K. Ke and Z. H. Lin, "An optimal mobile service for telecare data synchronization using a role-based access control model and mobile peer-to-peer technology," *Journal of Medical Systems*, vol. 39, no. 9, pp. 101–105, 2015.

[4] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: a survey towards private and secure applications," 2021, https://arxiv.org/abs/2106.03785.

[5] B. A. Mahafzah and I. O. Alzoubi, "Broadcast communication operations for hyper hexa-cell interconnection network," *Telecommunication Systems*, vol. 67, no. 3, pp. 1–21, 2018.

[6] N. Yu, "Dynamic access network reorganization for the depopulation age," *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 45, no. 5, pp. 743–750, 2015.

[7] M. Jahanbakht, W. Xiang, L. Hanzo, and M. Rahimi Azghadi, "Internet of underwater things and big marine data analytics – a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 904–956, 2021.

[8] J. Cao and J. Liu, "A two-stage double-threshold local spectrum sensing algorithm research for the power private communication network," *Proceedings of the CSEE*, vol. 35, no. 10, pp. 2471–2479, 2015.

[9] H. Xu, J. Shen, L. Wen et al., "A system steady-state assessment-based routing algorithm for optical communication networks," *Study on Optical Communications*, vol. 12, no. 4, pp. 76–78, 2015.

[10] W. Dai and Y. Masayuki, "Key update mechanism using all-or-nothing transform for network storage of encrypted data," *Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences*, vol. 98, no. 1, pp. 162–170, 2015.

[11] M. Elhoseny, H. Elminir, and A. Riad, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 28, no. 3, pp. 262–275, 2016.

[12] A. Saraswat, C. Khatri, and Sudhakar, "An extended hybridization of Vigenere and Caesar cipher techniques for secure communication," *Procedia Computer Science*, vol. 92, no. 5, pp. 355–360, 2016.

[13] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 38, no. 5, pp. 968–979, 2020.

[14] X. Liu, "Research on data access control and encryption storage technology of internet of things in network communication," *Journal of Computational and Theoretical Nanoscience*, vol. 13, no. 12, pp. 9591–9595, 2016.

[15] X.-F. Wang, M. Yi, and R.-M. Chen, "An efficient privacy-preserving aggregation and billing protocol for smart grid," *Security & Communication Networks*, vol. 9, no. 17, pp. 4536–4547, 2016.

[16] H.-m. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A practical and compatible cryptographic solution to ADS-B security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3322–3334, 2019.

[17] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 1, pp. 135–142, 2016.

[18] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, "Cloud-based fine-grained health information access control framework for lightweightIoT devices with dynamic auditing andattribute revocation," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 532–544, 2018.

[19] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in LTE-advanced networks," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 29–39, 2016.

[20] G. Yadav and S. Dalal, "Improvisation of network security using encryption technique for big data technology," *International Journal of Computer Applications*, vol. 124, no. 11, pp. 27–30, 2015.

[21] W. Sun, J. Wang, N. Zhang, and S. Yang, "Scalable implementation of hippocampal network on digital neuromorphic system towards brain-inspired intelligence," *Applied Sciences*, vol. 10, no. 8, p. 2857, 2020.

[22] C. Longstaff and the subcommittee on fibrinolysis, "Development of Shiny app tools to simplify and standardize the analysis of hemostasis assay data: communication from the SSC of the ISTH," *Journal of Thrombosis & Haemostasis*, vol. 15, no. 5, pp. 1044–1046, 2017.

[23] B. P. Chaudhury and A. K. Nayak, "Energy saving performance analysis of hierarchical data aggregation protocols used in wireless sensor network," *Advances in Intelligent Systems & Computing*, vol. 309, no. 9, pp. 79–89, 2015.

[24] B. Fisher, "Addressing pressing cybersecurity issues through collaboration," *It Professional*, vol. 18, no. 4, pp. 66–69, 2016.

[25] I. Ostrowski, P. Szulewski, and A. Masłowski, "Analysis of WiFi communication (data interchange) for mobile robot in industrial environment," *Applied Mechanics & Materials*, vol. 817, no. 7, pp. 342–347, 2016.

[26] R. M. Larik, "Light and secure communication algorithm for cognitive radio network by using labyrinthine authentication formula," *Pediatrics*, vol. 102, no. 6, pp. 1432–1436, 2015.

[27] J. Li, "Research on the application of data encryption technology in network security transmission," *Revista De La Facultad De Ingenieria*, vol. 32, no. 5, pp. 595–604, 2017.

[28] H. S. Chang, "International data encryption algorithm," *Hepatology*, vol. 60, no. 6, pp. 2125-2126, 2016.

[29] R. V. Rose and J. S. Kass, "Mitigating cybersecurity risks," *Continuum Lifelong Learning in Neurology*, vol. 23, no. 2, pp. 553–556, 2017.