JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 739-757 (2023)
DOI: 10.6688/JISE.202307_39(4).0003

Research on Secure Transmission of Heterogeneous Network

MEI-RONG ZHENG[1] AND RU-CHUN JIA[2,+]
[1]*Fujian Chuanzheng Communications College*
Fujian Fuzhou, 350000 P.R. China
[2]*College of Computer Science*
Sichuan University
Chengdu, 610065 P.R. China
[+]*E-mail: jiaruchun@stu.scu.edu.cn*

With the continuous destruction of the data transmitted in the protection network system, data encryption is an important research object in the network security technology, and it is the core to ensure the correctness of the data transmitted in the network. Through further research and Analysis on the basic technologies of cryptography and data transmission, combined with several common data encryption algorithms and data communication methods, the Windows sock communication method and mixed encryption module of mixed encryption data transmission system are designed and studied. In this module, a pair of RSA keys are generated by the software system first, which are imported into the hybrid encryption process to encrypt the des keys randomly generated in the system, which optimizes the system design objectives and the main functions of the system. In this paper, through further careful and in-depth research on the two classical encryption algorithms DES (Data Encryption Standard) and RSA (Rivest-Shamir-Adleman), we propose and design a method of heterogeneous network data security transmission based on hybrid encryption. The experiment is programmed by visual c++, and the mixed encryption data transmission system is simulated and tested. The experimental results show that the design and implementation of the hybrid encryption data transmission system overcomes the shortcomings of the previous systems, such as slow speed and difficult key transmission.

Keywords: hybrid encryption, heterogeneous network, data security, transmission, system security

1. INTRODUCTION

In recent years, along with the combination of information and computer, e-commerce, electronic fusion, government office networking and so on have brought great convenience to our work and life, and the Internet has become an indispensable part of our daily work and life. However, while obtaining network resources, their own confidential resources and users' personal information have been stolen and attacked to varying degrees [2]. Therefore, the security of information and network is especially important in this era. Cryptography is the core technology of information security [3]. Therefore, facing the pressing situation, strengthening the research and development of cryptography technology has important theoretical significance and practical value [4].

Further in-depth analysis of various security issues in instant messaging systems, using symmetric encryption algorithm DES, asymmetric encryption algorithm RSA and Hash algorithm, a hybrid encryption application model in instant messaging is proposed. The model integrates the features of symmetric encryption algorithm DES, which can judge whether the transmitted information has been tampered with or not, and improve the transmission efficiency.

Received April 25, 2022; revised June 13 & September 19 & November 5, 2022; accepted November 24, 2022.
Communicated by Rung-Ching Chen.
[+] Corresponding author.

With the rapid development of communication technology and obvious network characteristics, and many years of reform and innovation, the transmission rate of wireless access technology has gradually approached the limit. In order to meet various business needs, multi-network collaboration is required. However, traditional network data transmission cannot effectively guarantee efficient transmission services, and will increase the energy consumption problems in transmission, resulting in interference problems in the transmission process. Therefore, this paper carries out the research on the secure data transmission method of heterogeneous network with mixed encryption.

2. THE PRINCIPLE OF THE COMMON ENCRYPTION ALGORITHM

2.1 DES Algorithm

2.1.1 DES algorithm

The database are using the most common encryption – data encryption standard (DES (Data Encryption Standard) is the classification login password algorithm, its specification form uses 64 bit key, 56 bits arbitrary choice, the remaining 8 bits (each bit check 56 bits arbitrary value 7 bits), the algorithm uses 64 bits as an enterprise to classify and decrypt data information. Milphertext and text have the same length, both 64 bits [5]. The encryption algorithm converts the 64-bit input to a 64-bit derivation, through a series of processes, using the same method steps and the same key during the decryption operation, and the basic idea is to select the combination and iteration of the transformation to turn each group in the ciphertext into a cipheric group [6].

In 1973, the National Bureau of Standards has gradually conducted scientific research on the data and information encryption specifications for computer software in units other than the Minister of Defense. Between May 15, and August 27,1974, two rounds of the negotiated encryption algorithm were sent to the public on May 15,1973. The announcement. The key purpose of the encryption algorithm lies in the following four points: (1) providing high-quality personal information protection from uncertified leakage and undetected changes in data information; (2) with very high diversity, the probability of promoting cracking should not exceed the possible rights and grasp; and (3) the security factor of the DES login password system should not rely on the confidentiality of the algorithm information, which only depends on the encryption key; (4) Complete economic development, reasonable operation, and apply a variety of completely different applications [7, 8].

The actual encryption process of a DES can be divided into the following processes:

Initial replacement. Given a plaintext X, the 64-bit ciphertext was rearranged after passing through an original poll IP throughout the original displacement process. Permuted input X was generated 0. Write it as $\chi_0 = IP(\chi) = L_0R_0$, L_0 is the left of 32 bit of χ_0, and is the right of 32 bit of χ_0. The original replacement IP (Initial Permutation) is shown in Table 1.

(1) Iteration process

After the primary replacement process, the 16 cycles of the same function formula is calculated by the following criteria: L_iR_i, $1 \le i \le 16$.

$$L_i = R_{i\text{-}1}$$
$$R_i = L_{i\text{-}1} \oplus f(R_{i\text{-}1}, k_i) \quad (1)$$

Table 1. The initial replacement IP.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	4
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

The derivation of the last cycle system (cycle 16) consists of 64 bits and is the cipheric and cipheric function formula. The whole process of a full round of DES encryption is shown in Fig. 1 below.

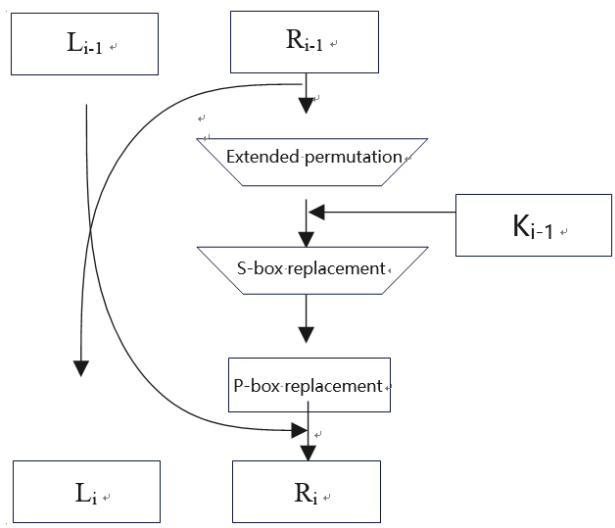


Fig. 1. Encryption process for the DES.

(2) IP-1handle

Inverse permutation IP was deduced according to the original permutation IP-1 Form a 64-bit ciphertext *y*, where *y* = IP-1(R16L16). That is, the ciphertext obtained after the DES encryption is derived. Inverse arrangement IP-1. This is shown in Table 2.

Table 2. Inverse initial displacement IP-1.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	4	9	49	17	57	25

The biggest flaw of the DES algorithm is that the key k is caused by the secret promise according to the secret method, only communication can master the key k, it is difficult to crack the ciphertext [9, 10]. Hybrid encryption gets rid of this flaw in DES and encrypts the DES key so that the ciphertext cannot be decrypted even if the key is captured [11].

2.1.2 Triplex DES algorithm

Although DES is a classical classification encryption algorithm, it appears relatively sensitive under exhaustive attacks due to the limitations of the key length [12]. Tuchman considers a new encryption method of three encryption using two keys, the 3DES algorithm. The actual calculation process is: first use K, conduct the DES encryption algorithm for the cipheric information P, and then apply K, decrypt the results of the first encryption, and finally apply k again. Encryption, which is described by mathematical thinking as:

$$C = E(K_1, D(K_2, E(K_1, P))). \tag{2}$$

This algorithm uses 2 keys. That is, the triple DES exhaustive attack cost is 2,112. At this stage, there is no triple DES attack method in the world [13]. For better compatibility with DES algorithms, the triple DES also has an algorithm for selecting three keys, as described in mathematical thinking:

$$C = E(K_3, D(K_2, E(K_1, P))). \tag{3}$$

If here $K_3 = K_2$, or $K_1 = K_2$, the triple DES algorithm is exactly the same as the single DES algorithm.

2.2 RSA Algorithm

The safety coefficient of RSA algorithm is based on the following views and basic theory in number theory: it is easy to calculate the product of two large prime numbers, but the need to resolve the product of the two is very difficult to estimate to find their prime factors [14]. The solving problem of large integer factor is a well-known mathematical thinking problem. So far, there is no best way to deal with it, so the safety factor of the RSA algorithm is guaranteed.

The RSA algorithm can be divided into the following processes:

(1) Each multiplication was calculated by randomly selecting two large primes P and q

$$n = pq. \tag{4}$$

(2) Select the encryption key e so that e and (n) are mutually prime, here φ

$$\phi(n) = (p - 1)(q - 1). \tag{5}$$

Called the Euler donkey function.

(3) Using the Euclidean algorithm, the encrypted public key d can be obtained according to the inverse operation of the multiplication and division of computing e:

$$d = e^{-1} (\text{mod } \phi(n)) \tag{6}$$

perhaps

$$ed = 1(\text{mod } \phi(n)). \tag{7}$$

The decryption keys d and module n are also prime numbers. The numbers e and n are called public keys, and the numbers d are called public keys.

(4) Encryption message m, ciphertext

$$c = m^e(\text{mod } n). \tag{8}$$

(5) Decrypt the ciphertext c, and restore the message

$$m = c^d(\text{mod } n). \tag{9}$$

There are usually three types of attacks:

(1) The forced attack only needs to choose a long enough key in the algorithm, and the forced attack is very difficult, but if the key length is increased, the encryption and decryption speed will be slow down [15]. Therefore, the selected key is moderate to prevent forced attacks without causing slow operations [16]; (2) According to the public key, so far, this type of attack has not been completed for RSA algorithms, which is the main factor that RSA algorithms are often attacked flourishing [17]; (3) The message format is very likely to be attacked. If the other party knows that the encrypted ciphertext of the RSA is a 56-bit DES encryption key, then the public key of the RSA is used to encrypt all possible keys. The text will decipher the key [18]. Regardless of the RSA key size, attacks can be attributed to a forced attack using a 56-bit key. This attack can be avoided by adding any number of bitdogs to the message format.

3. SEVERAL DATA TRANSMISSION AND COMMUNICATION METHODS

3.1 Hardware Communication Mode

With the development trend of electronic equipment, electronic computers and information content technology progress, the rapid development of communication systems is also very rapid, from cable TV to wireless network, from voice to data information, image, from LAN to multimedia sources. Many modes of network communication and communication are used in the transmission data system software. The main communication modes of the current hardware configuration and transmission data are as follows:

3.1.1 Radio communication

The software of the radio communication system uses the common frequency bands to transmit the data, and the communication security channels and communication equipment have the characteristics of small investment and simple maintenance [19]. However, due to the blockage of tall and large engineering buildings in large cities, the transmission distance is somewhat limited. Therefore, it is suitable to transmit data in second-and third-tier cities with small radii and small total numbers.

3.1.2 Cable communication (telephone line, special line)

The key to the communication network is the use of the network line communication and the establishment of the special line transportation and communication mode. Network line: with the existing public network as the auxiliary, choose the public network modem and network exchange system software, so as to establish a communication security channel between the two physical communication entity lines. Special line transmission mode: communication Internet is suitable for places where data transmission is not large and processing speed is not high [20].

3.1.3 Optical fiber communication

From the operation of the site, the data information is stable when using the fiber communication system and is resistant to interference. This method has a relatively large investment in the early stage of the project, but with the continuous decline of optical communication equipment prices, this method may become a more suitable for on-site communication mode.

3.1.4 Cellular mobile communication mode

For remote data transmission, the communication network, wired communication and optical fiber communication systems are all classified as special mobile communication due to the harm of distance, natural environment, cost, processing speed regulation and other factors. Separate from a certain unit. Generally, only applicable to designated areas or institutions, with limited coverage. Therefore, they are not desirable in terms of the scope of application and economic development. Cellular mobile communication mode uses frequency reuse technology to reasonably realize the utilization of frequency resources, and has a high Internet penetration rate in domestic regions. Therefore, it is a reasonable and economical way to fully utilize the existing cellular network to complete the wireless data transmission business process.

3.2 Software Communication Method of using VC++

VC has an MFC (Microsoft Foundation Classes) class library that encapsulates almost all the programming resources for Windows to seamlessly integrate all Windows communication-related resources such as Socket, Serial Communication Control, Serial Communication API (Application Programming Interface) and its OPC (OLE for Process Control) sockets.

3.2.1 Serial port communication

The MSComm control can complete the serial communication. MSComm is the ActiveX control of Windows serial communication provided by Microsoft China, bringing the function of serial communication to the application software. Serial port communication with VC is a paired *t*-test for solving the serial port communication with MSCcomm. Each MSCcomm matches a serial port communication. If the application software has to browse through multiple serial port communications, you need to have multiple MSCcomm controls applied [21].

3.2.2 Socket communication

Due to the limitations, this communication is also used. Socket, the Chinese name Socket, was originally a communication network interface designed by the University of California for the UNIX system. It is a TCP / IP application software interface (API) created to better integrate TCP / IP into a UNIX system [22]. When the remote server / network server does not issue a unique program, a socket can be applied at the remote server and server and exchange the data information interface or data accordingly. In 1991, Microsoft cooperated with several enterprises to develop a network programming interface in Windows environment, making it a standard and universal TCP / IP programming interface under Windows system. In 1994 it was declared a specification, known as the Windows Sockets Standard, also known as the Windows Sock. Its range of application is widespread. Today, a variety of Internet and protocols, including PSTN (Public Switched Telephone Network), ISDN (Integrated Services Digital Network), wifi, all LAN protocols, asynchronous transmission mode ATM, are its application areas [23]. There are two different types of sockets: streaming sockets and datagram sockets.

(1) Flow Sockets: Flow Sockets provide dual, orderly, unrepetitive, and undocumented data flow analysis services for solving large amounts of data information. The Internet network layer can disperse or concentrate data information into the appropriate specifications. Flow sockets are connected to each other. Before communicating with each other, you need to create a path so that you can specify the routers between them and ensure that they are all active and can respond to each other.

(2) Datagram Sockets: Datagram socket is suitable for dual data flow analysis, but the stability, order and non-repetition of the transmitted data are not guaranteed. In other words, the process of receiving the data from the datagram socket may find that the contents of the messages are duplicate, or in a different order than when they were issued. Otherwise, a major feature of the datagram socket is that it retains the record boundaries. For this feature, the datagram socket uses an entity model that is very similar to many packet-exchange Internet networks (*e.g.*, Ethernet interfaces) today. The data message socket is disconnected, does not guarantee whether the recipient is monitored, similar to the postal express service items: the sender can put the letter into the mailbox, whether the recipient receives the letter or because the letter is not delivered to the recipient, the sender is unknown. Therefore, data information reporting is unreliable, and there must be reliable procedures responsible for arranging data information reporting.

3.2.3 The OPC and PLC communication mode

OPC (OLE for Process Contr01) is an OLE (Object Linking and Embedding) technology for process control. In this stage, the OPC, is an international industry standard. The specification defines the way that specific statistics of automation technology are exchanged between PC-based remote servers using the Microsoft real-world OS. The purpose of its development and design is to establish the interface specifications for the communication between the application software of the industrial control system, and to establish a unified information storage standard between the industrial production control sys-

tem and the management software. OPC objects provide an interface mode for data storage or communication networks. According to this interface, an OPC client program can connect to one or more vendor supplied OPC servers. The OPC standard gives two sets of interface schemes, namely the custom interface and the automation technical interface. Custom interface, highly efficient and efficient. According to this interface, the best features of the OPC network server can be fully exploited and expressed in C. Customers will usually choose a customized interface scheme. In addition, programs generally use VB language clients. The typical OPC system architecture is shown in Fig. 2 below:

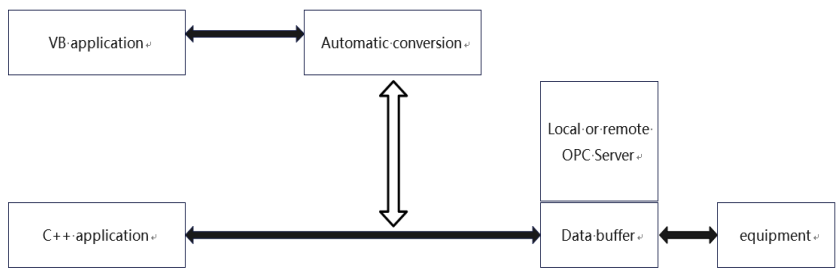


Fig. 2. Typical OPC architecture.

3.3.3 Confidentiality communication system model

The article is committed to building a perfect, secure and reliable confidential communication system. In order to better achieve the goal, we need to start from the overall scheme design. According to the requirements of the system infrastructure, carefully analyze the various hazards encountered by the system, integrate the main details of confidential communication, and formulate an effective system. In the overall scheme design of the safe communication system, the clear and detailed design concept and reasonable standards are the guarantee of the security and confidentiality of the system. In terms of post-hoc prevention measures, this will undoubtedly damage the safety of the system. The physical model of a secure communication system has the following key criteria:

(1) Security threat analysis and assessment principles

Conduct a full, comprehensive and detailed analysis, evaluation and inspection of the security risks of the system and the possible network security problems, so as to better discover the weak links and possible attacks of the system security level, and improve the safety factor of the whole system.

(2) Agree to the design principles

The formulation of the security system should be closely combined with the design scheme of the communication system. In the design scheme of the communication system, the design scheme of the security system should be fully considered to prevent the repair of the loopholes after the completion of the communication system is completed. Save the investment in construction projects and ensure the actual effect of confidential communication.

(3) Integrity principle of the system

In the design of the scheme, considering that the security communication system is unlikely to be hacked or damaged after the funds are put into operation, it stipulates that the security communication system must be equipped with security protection system, detection service system and security repair system. Security protection is the corresponding protection measures taken for the network security loopholes and security problems in the system. The detection service system is to monitor the operating status of the system in real time, and timely process or prevent various attacks on the system [24]. Security repair system is the emergency response when the system is attacked, and try to avoid the damage caused by the attack.

(4) Confidentiality and practical principle of the system

Confidentiality is the basis of the system. Various encryption algorithms can be used to ensure the confidentiality of the system. However, the economic development capacity and the applicability of the system builders should be fully considered.

(5) Design principle of system safety grade

The key levels of the communication content are classified into confidential, trade secrets and confidential according on the system customer management authority and work content. A full series of optional password algorithms and security systems are presented to meet the requirements of different levels in the system [25].

(6) General and dynamic principles

The security equipment in the system should be integrated into the technical development trend and update changes of the communication system, such as speed improvement, interface change, try to avoid the types of security equipment in the system, and improve the practical facilities. Confidential machines and equipment in the system should complete the dynamic selection and application of encryption technology, and fully allocate the work keys. Improve the security features of the system [26].

3.4 Technology for Communication using Windows Sock

3.4.1 The Windows sockets specification

Windows Sockets is a widely used network programming interface under Windows, open to the public and applicable to multiple protocols. From version 1.0 in 1991 to version 2.0.8 in 1995, it has become a practical standard for Windows network programming with strong support from Intel, Microsoft, Sun, SGI, Informix, Novell. Windows Sockets standard in U.C. Socket interface popular in Berkeley University BSDUNIX is, for example, with a network programming interface defined under Micosoft Windows. It contains not only the function library that we are familiar with in the BerkeleySocket design style, but also a set of extended function library for Windows, allowing programmers can make the most of the Windows information push system to write programs. The original intention of the Windows Sockets standards is to provide application developers with a simple set of API that every software platform distributor should follow. In addition, Windows Sockets defines a binary interface (ABI) based on a special version of Windows to ensure that applications using Windows Sockets API are available to all software platform publishers

that meet the Windows Sockets protocol. Therefore, the standard defines a set of library function calls and associated word meanings that can be supplied by program developers and implemented by software platform distributors. The software platform that follows this Windows Sockets standard is called Windows Sockets compatible, and Windows Sockets compatible service providers are called Windows Sockets service providers. Software platform dealers must 100% implement the Windows socket standard. Guaranteed for Windows Sockets compatibility. All applications that are compatible with Windows Sockets are considered to have a Windows Sockets interface. We call this type of application a Windows Sockets. The Windows Sockets specification defines and records how to use the API to interact with the Internet Protocol Suite (IPS, usually called TCP / IP), especially when emphasizing that all Windows Sockets implementations apply for streaming and data message reporting sockets. Application software to read Windows Sockets API to complete mutual communication. The Windows Sockets uses the next layer of the network communication protocol function and the actual operating system reading to complete the specific communication work [27-33].

3.4.2 The implementation principle of the Windows sock

The main problem with network process communication is process recognition. In the same server, different processes can be uniquely identified by the process number; in Internet, the application IP address represents the server. On the other hand, each Internet process in the host has a protocol marking the port number, so to uniquely identify a process in cyberspace, the IP address and port must be both. The Internet process also needs to specify which communication protocol in many communication protocols when creating communication protocols. Since the detailed address file formats of different protocols, port number assignments are independent of each other and work differently. In general, to globally mark a process in cyberspace, it must be a triad: protocol, local address, local port number, and such triples are called semicorrelated. A complete communication network must be marked with pentata: protocol, local address, local port number, remote detailed address, remote address, remote port, such pentata is called a relationship. When programming with Windows Socket, the communication must be separately applied for a node Socket, each using a semi-correlation description above, and a complete Socket connection using a correlation description. Socket is a design model for the remote server and server side, giving different socket function formulas for the remote server and client programs. The client program arbitrarily applies for a Socket, and the system dynamically assigns it a Socket number. The Client program has a globally recognized Socket to which all clients can send connection requirements and information content requirements. Whether streaming sockets or data message sockets, they generally use a remote server / server mode, and their whole operation process is basically similar. The TCP protocol is a stable protocol for analyzing the connected data streams. The TCP protocol must be used when the data must be transmitted reliably. The Windows Socket using the TCP protocol as the underlying protocol is a streaming socket that must be connected before the two servers can communicate. When the two servers are connected, they can push or stream data through socket. In this application system, select the Socket communication for the connection protocol [34-42]. The status diagram of the socket application software is shown in Fig. 3.

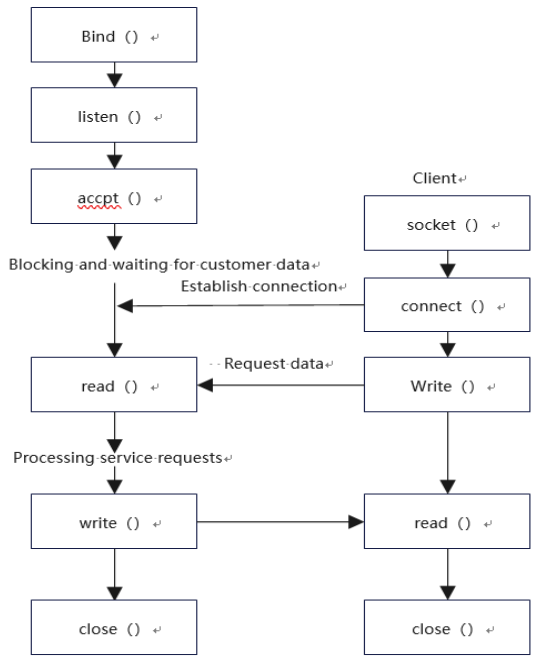


Fig. 3. Time diagram of the interface.

3.4.3 Design of the Windows Sock based on the TCP / IP protocol

The Windows Sock gives the application of the TCP (transmission control protocol). Under the TCP protocol, we can create a server with a specific IP address, while using the created connection to double exchange data information. It is simple to use C Socket to control the data transmission of the connection, but in the connected communication, one party must play the role of the network server, and wait for the connection request from the other party (customer), so the network server must build a monitoring socket, and then wait for the connection on this socket. When a connection is created, a new socket is formed for communication. And after the customer sets up the socket, they simply read the connection function formula to establish the connection. For the connected communication, the order of push or push and reception of data information is guaranteed. To create a Windows Socket environment, the Windows platform should first apply the TCP / IP protocol. The system software is run on Windows XP system software and designed with VC 6.0. Starting with VC 6.0, the MFC gives you two New classes, namely: CAsync Socket and C Socket, to encapsulate the Socket API function. The C Socket class is an advanced goal inherited from the CAsync Socket class. Suitable for synchronous control, it is becoming more and more effective. We have introduced the basic principles of C Socket programming before, here we introduce the completion method of this operating system. Due to the mobile phone software regulations, the server and the mobile phone client are combined in one. A connection to each other is a point-to-point relationship that can receive and send data information to each other. In network communication, due to the Internet congestion or too much data information pushed at one time, the exchanged data in-

formation is often not transmitted in a short time, unable to return the function formula for receiving and sending data information, which is called blocking. Windows Sock provides two ways to handle blocked and non-blocking. In blocking mode, the function formula for receiving and sending data information is not returned until the transmission ends or after an error is read. During the blocking period, the blocked variable will constantly read the system software function formula GetMessage0 to maintain the normal development of the information circulation system. For the non-blocking mode, the function formula is returned immediately after reading, and the Windows Sock sends a pre-promised message to the program flow. A non-blocking method should be used when programming whenever possible [43-47].

4. HYBRID ENCRYPTION MODULE DESIGN

4.1 Large Prime Generation and Key Pair Generation in the RSA Algorithm

Before communicating with the RSA encryption algorithm, both the sender and the receiver must create a pair of keys (public and private keys). The RSA algorithm is based on selection of large prime mes P and q. Its choice of public and private key depends on the subprime P and q. To prevent network attacks, the values of P and q should be obtained by exhaustive. P and q are selected from sufficiently large combinatorial masks so that how methods to generate and test primes on electronic computers is crucial. If you create any alternative and then try to break them down to find the prime that is wrong. The usual practice is to select a singular number large enough and then test if it is sufficient prime. The method of testing the number of cables at this stage is as follows:

(1) The Solovag-Strassren method

It is a probabilistic basic test algorithm proposed by Rober Solovag and Volker Strassen.

(2) Miller-Rabin algorithm

This is also a faster prime test algorithm at this stage. The mechanism is based on two properties of prime *mes*. The first property is that if P is a prime and a is an integer less than P, then

$$\alpha^2 = 1(\text{mod } p) \Leftrightarrow \alpha = 1(\text{mod } p) \text{ or } \alpha = -1(\text{mod } p). \tag{10}$$

The second property is that if P is a prime on 2, there is $P - 1 = 2k$. The q, $k > 0$, and q are singular. Let a be an integer and $1 < a < P - 1$, then one of the following two criteria holds:

$a^q = 1(\text{mod } p)$①; ② in the integer aq, $a2q$, $a4qa^{2k-1q}$. There is a number in the module P and -1 identity. That is, there is $a\ j$ $(1\ j\ k)$ satisfaction.

$a^{2k-1q} = (-1)\ (\text{mod } p)$, $a^{2j-1q} = p - 1(\text{mod } p)$ or $a^{2k-1q} = -1(\text{mod } p)$.

(3) The Lehmann method

This approach is sufficient for Lyman to conduct scientific research alone and is suitable for checking primes on electronic computers. This system adopts this method, and the main basis for checking the prime number is: ① chooses a random number less than P a.

The ② computes $t = a(p-1)/2(\text{mod } p)$. ③ If $t = 1$ or -1, then P is undoubtedly not a prime. ④ If $t = 1$ or -1, then the probability of P being not a prime is at most 50%. Pick n different arbitrary values for a, and this type of test is repeated n times. If this value is equal to 1 or-1, but not always 1, P may be prime and the risk of incorrect does not exceed $1/2n$.

In the specific implementation of the algorithm, the prime formation is very fast. To implement the algorithm in a computer system, the key steps are as follows: ① creates an 11-bit random number P. ② sets the low and low to 1 (low is set to 1 because the prime is guaranteed to reach the specified length and the minimum to 1 because the guaranteed prime is singular 1. ③ inspection ensures that P cannot be divided by all small primes: such as: 2,3,5,7,11. This procedure tests P for the division of all primes below 4000.The ④ runs the Lehmann test on the random number a. If you press test P, it also causes a random number of a', the run test again selects a smaller a value to ensure a fast processing speed for five Lehmann tests, and if one of the P tests does not succeed, create P again and run the test again.

The above algorithm found 256 bits in 2.8 seconds, 512 bits in 24 seconds, 768 bits in 2 minutes, and the 1024-bit prime range in 5.1 minutes.

The range of integers available to a 32-bit computer is-231To 231-1 For bits, the necessary large prime in the RSA algorithm used in this paper is at least 400 bits. Data types, produce a large number of custom basic data types, the design scheme must be in accordance with the algorithm, to achieve addition, subtraction, multiplication, division, value and other calculation of large integer numbers.

To create a key, you must first select two large prime numbers, P and q. To better obtain a greater degree of safety, the two numbers have the same length, and generally decimal prime numbers of 100 to 200b.The calculation is multiplied by $n = pq$ and then arbitrarily select the encryption key e so that e and mutin. The decryption key d is then computed with the Eucliverde extension algorithm, satisfied. The d and n are also mutin. The flowchart of RSA large prime generation is shown in Fig. 4.

$$(p-1)(q-1)ed = 1\text{mod}((p-1)(q-1)).$$

4.2 Specific Design of Hybrid Encryption System Module

The mixed encryption system module can also be divided into two parts, one is the mixed encryption part and the other is the asymmetric encryption algorithm key generation part. The mixed encryption part mainly includes:

(1) DES key generation. The system software automatically generates the DES key to achieve the real purpose of “one key” information confidentiality;
(2) DES plus and decryption function formula. Since DES is a symmetric encryption algorithm, the entire encryption and decryption processes are completely similar, and DES algorithm can be performed by reversing the 16-wheel key encoding sequence.
(3) The RSA encryption function formula. For RSA encryption, the first ciphertext intelligence, the length is less than log2, the n-bit data is used as cipheric blocks (here $n = pq$).
(4) RSA decrypt function formula. The decryption algorithm is performed with part of the RSA (*i.e.* module n). The feature settings for partial control hybrid encryption are shown in Table 3.

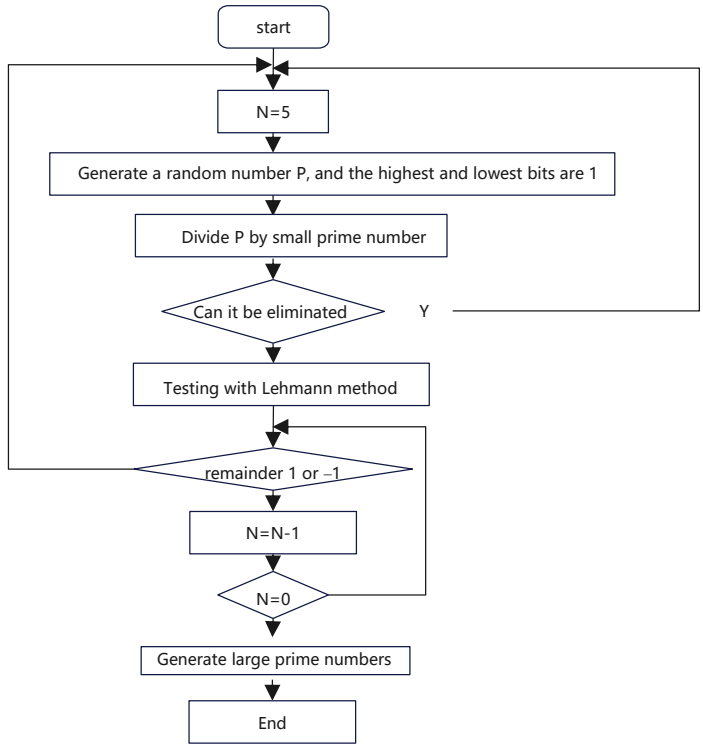


Fig. 4. Flow diagram of human prime generation.

Table 3. Main control property settings for the Hybrid Encryption module.

Control type	ID	name
Static Text		input file
		output file
		RSA Key (0)
		RSA module *n* (0)
Edit Box	IDCInput	input file
	IDC_Output	output file
	IDC_RsaKey	Enter the RSA key
	IDC_RsaMod	Enter the module for the RSA
	IDC_Browse	Browse the file
	IDC_OutFolder	Select the daily record
Bottom	IDC_InputRsaKey	leading-in
	IDC_InputRsaMod	leading-out
	IDCRun	Mixed encryption
	1D_EXIT	withdraw from

The SA key generation part mainly includes: (1) can be converted into large prime with clear length; because the security factor of the RSA algorithm is based on what cannot be resolved by large prime numbers, it must be converted to large prime before generating

the key, and then calculate the public key *n*, *e* and public key *d*. (2) The prime number can be exported as text files file or the stored prime; (3) After the prime number is created, the system software can create key pairs, which can export the moduli, public key and private key respectively. And import, encryption is easy to apply. The RSA key generation control property settings are shown in Table 4:

Table 4. RSA Key Generation primary control property settings.

Control type	ID	name
Static Text		prime number *p* prime number *q* public key *d* model *n* public key *e* private key *d*
Button	IDC _GetP IDC_InputP IDC_OutputP IDC _GetKey IDC_OutputE IDC_OutputE	produce leading-in leading-out produce leading-out leading-out

5. COMMENT

In summary, the design of mixed encryption and secure transmission method for heterogeneous network data in this study has less latency and packet loss than the traditional two transmission technologies. The data transmission system with mixed encryption is simulated and tested by two computers. The experiment shows that the design of the mixed encryption algorithm module avoids the shortcomings of a single encryption algorithm in transmission by programming with VisualC++. The experimental results show that the design and implementation of the data transmission system with mixed encryption is successful, which overcomes the shortcomings of slow speed and difficult key transmission in the previous system.

6. CONCLUSION

In this paper, two classical encryption algorithms, DES and RSA, are studied carefully and deeply. A design of secure transmission method for heterogeneous network data based on hybrid encryption is proposed. A hybrid encryption system which combines DES algorithm with RSA public key cryptography is presented. Clear text data is encrypted by symmetric encryption algorithm DES, key is generated by RSA and DES key is encrypted by RSA. Experiments are programmed by VisualC+. The data transmission system with mixed encryption is simulated and experimented. The experimental results of data optimization show that the design and implementation of the data transmission system with mixed encryption overcome the shortcomings of the previous system, such as slow speed and difficult key transmission. Thus, the information encryption process in the network com-

munication system is more efficient, and the problem that speed and security cannot be considered in the cryptography system is solved.

FUNDING

China University industry university research innovation fund 2020ita03033.

REFERENCES

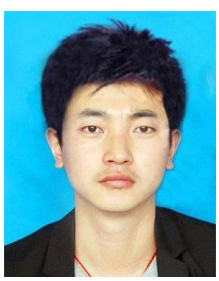
1. H. L. Liu, "Research on quantitative method of data transmission security in heterogeneous super density network," *Computer Simulation*, Vol. 38, 2021, pp. 150-153.
2. M. Pajany and G. Zayaraz, "A robust lightweight data security model for cloud data access and storage," *International Journal of Information Technology and Web Engineering*, Vol. 16, 2021, pp. 39-53.
3. B. Zhang, K. Huang, S. Lin, M. Yi, and Y. Chen, "A robust secure transmission scheme based on artificial noise for resisting active eavesdropper in MIMO heterogeneous networks," *Journal of Electronics and Information*, Vol. 42, 2020, pp. 2186-2193.
4. Y. Guan and Y. Jiang, "Design of ciphertext anti loss transmission system in communication network based on hybrid encryption algorithm," *Modern Electronic Technology*, Vol. 43, 2020, pp. 64-66.
5. H. Zhang, "Research on transmission optimization of encrypted information resources in ship network," *Ship Science and Technology*, Vol. 42, 2020, pp. 139-141.
6. G. Chang, "Design of network link transport layer key database security encryption system," *Modern Electronic Technology*, Vol. 43, 2020, pp. 74-77+81.
7. X. Zhang, Y. Liu, T. Liu, G. Lin, and H. Huang, "Research on buoy data security management system based on hybrid encryption," *Journal of Tropical Oceanography*, Vol. 39, 2020, pp. 117-123.
8. L. Xu, "Design of wireless sensor big data cross domain transmission security control system in heterogeneous environment," *Computer Measurement and Control*, Vol. 28, 2020, pp. 17-121.
9. A. Kakkar, "A survey on secure communication techniques for 5G wireless heterogeneous networks," *Information Fusion*, Vol. 62, 2020, pp. 89-109.
10. D. Deng, X. Li, M. Zhao, K. M. Rabie and R. Kharel, "Deep learning-based secure MIMO communications with imperfect CSI for heterogeneous networks," *Sensors*, Vol. 20, 2020, pp. 1730.
11. L.-L. Shi and J.-Z. Li, "Research and design of secure data transmission mechanism in heterogeneous network," *Microelectronics and Computer*, Vol. 36, 2019, pp. 84-88.
12. Z. Bo, H. Kaizhi, Z. Zhou, and C. Yajun, "Artificial noise assisted robust energy and information security transmission scheme in heterogeneous energy carrying communication networks," *Journal of Communications*, Vol. 40, 2019, pp. 60-72.
13. G. Xu and D. Wang, "Secure network coding scheme against eavesdropping based on Chaotic Encryption," *Computer Applications*, Vol. 39, 2019, pp. 1374-1377.
14. J. Zhou and C. Chen, "Design of a data security model based on heterogeneous network," *Computer Engineering and Science*, Vol. 41, 2019, pp. 2160-2165.

15. Y. Zhang, G. Luo, H. Wang, and X. Liu, "Provably secure TPKC-CLPKC heterogeneous hybrid signcryption scheme under 5G network," *Information Network Security*, 2019, pp. 30-37.
16. Y. Zhang, X. Liu, X. Lang, Y. Zhang, and C. Wang, "Security analysis and improvement of a heterogeneous hybrid group signcryption scheme," *Journal of Electronics and Information*, Vol. 41, 2019, pp. 2708-2714.
17. X. Jin, B. Ren, H. Li, X. Gong, and F. Dong, "Research on forward link secure transmission scheme of satellite ground hybrid communication network," *Journal of Astronautics*, Vol. 40, 2019, pp. 1444-1452.
18. B. Zhang and K. Huang, "Robust secure transmission scheme based on artificial noise-aided for heterogeneous networks with simultaneous wireless information and power transfer," *Journal of Electronics and Information Technology*, Vol. 41, 2019, pp. 1-8.
19. B. Zhang, K. Huang, Z. Zhong, and Y. Chen, "Artificial noise-aided robust secure information and power transmission scheme in heterogeneous networks with simultaneous wireless information and power transfer," *Journal on Communications*, Vol. 40, 2019, pp. 60-72.
20. L. Duan, X. Sun, and Z. Wang, "Heterogeneous network selection algorithm for secure application message transmission," *Computer Science and Exploration*, Vol. 12, 2018, pp. 595-607.
21. M. Jiang, "Design of network information security encryption system based on chaotic sequence," *Modern Electronic Technology*, Vol. 41, 2018, pp. 76-80.
22. G. Zhang, L. Kong, H. Yao and H. Pan, "Research on secure transmission of network communication based on reverse training model," *Computer and Digital Engineering*, Vol. 46, 2018, pp. 313-317.
23. T. Kunchok and V. B. Kirubanand, "A lightweight hybrid encryption technique to secure IoT data transmission," *International Journal of Engineering & Technology*, Vol. 7, 2018, pp. 236-240.
24. N. Wu, X. Zhou, and M. Sun, "Secure transmission with guaranteed user satisfaction in heterogeneous networks: A two-level stackelberg game approach," *IEEE Transactions on Communications*, Vol. 66, 2018, pp. 2738-2750.
25. B. Li, Z. Fei, Z. Chu, and Y. Zhang, "Secure transmission for heterogeneous cellular networks with wireless information and power transfer," *IEEE Systems Journal*, Vol. 12, 2017, pp. 3755-3766.
26. T.-X. Zheng, H.-M. Wang, and J. Yuan, "Secure and energy-efficient transmissions in cache-enabled heterogeneous cellular networks: Performance analysis and optimization," *IEEE Transactions on Communications*, Vol. 66, 2018, pp. 5554-5567.
27. N.-N. Chen, X.-T. Gong, Y.-M. Wang, C.-Y. Zhang, and Y.-G. Fu, "Random clustering forest for extended belief rule-based system," *Soft Computing*, Vol. 25, 2021, pp. 4609-4619.
28. R. Cheng, W. Yu, Y. Song, D. Chen, X. Ma, and Y. Cheng, "Intelligent safe driving methods based on hybrid automata and ensemble cart algorithms for multihigh-speed trains," *IEEE Transactions on Cybernetics*, Vol. 49, 2019, pp. 3816-3826.
29. H. Cheng, L. Wu, R. Li, F. Huang, C. Tu, and Z. Yu, "Data recovery in wireless sensor networks based on attribute correlation and extremely randomized trees," *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, 2021, pp. 245-259.

30. Y. Cheng, H. Jiang, F. Wang, Y. Hua, D. Feng, W. Guo, and Y. Wu, "Using high-bandwidth networks efficiently for fast graph computation," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 30, 2018, pp. 1170-1183.
31. Y. Dai, S. Wang, X. Chen, C. Xu, and W. Guo, "Generative adversarial networks based on Wasserstein distance for knowledge graph embeddings," *Knowledge-Based Systems*, Vol. 190, 2020, p. 105165.
32. Y.-G. Fu, H.-Y. Huang, Y. Guan, Y.-M. Wang, W. Liu, and W.-J. Fang, "EBRB cascade classifier for imbalanced data via rule weight updating," *Knowledge-Based Systems*, Vol. 223, 2021, p. 107010.
33. Y.-G. Fu, J.-F. Ye, Z.-F. Yin, L.-J. Chen, Y.-M. Wang, and G.-G. Liu, "Construction of EBRB classifier for imbalanced data based on Fuzzy C-Means clustering," *Knowledge-Based Systems*, Vol. 234, 2021, p. 107590.
34. Y.-G. Fu, J.-H. Zhuang, Y.-P. Chen, L.-K. Guo, and Y.-M. Wang, "A framework for optimizing extended belief rule base systems with improved ball trees," *Knowledge-Based Systems*, Vol. 210, 2020, pp. 106484.
35. L. Guo, M. Li, and D. Xu, "Efficient approximation algorithms for maximum coverage with group budget constraints," *Theoretical Computer Science*, Vol. 788, 2019, pp. 53-65.
36. X.-Y. Li, W. Lin, X. Liu, C.-K. Lin, K.-J. Pai, and J.-M. Chang, "Completely independent spanning trees on BCCC data center networks with an application to fault-tolerant routing," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 33, 2021, pp. 1939-1952.
37. G. Liu, X. Chen, R. Zhou, S. Xu, Y.-C. Chen, and G. Chen, "Social learning discrete Particle Swarm Optimization based two-stage X-routing for IC design under Intelligent Edge Computing architecture," *Applied Soft Computing*, Vol. 104, 2021, p. 107215.
38. G. Liu, Z. Chen, Z. Zhuang, W. Guo, and G. Chen, "A unified algorithm based on HTS and self-adapting PSO for the construction of octagonal and rectilinear SMT," *Soft Computing*, Vol. 24, 2020, pp. 3943-3961.
39. G. Liu, X. Zhang, W. Guo, X. Huang, W.-H. Liu, K.-Y. Chao, and T.-C. Wang, "Timing-aware layer assignment for advanced process technologies considering via pillars," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 41, 2021, pp. 1957-1970.
40. G. Liu, Y. Zhu, S. Xu, Y.-C. Chen, and H. Tang, "PSO-based power-driven X-routing algorithm in semiconductor design for predictive intelligence of IoT applications," *Applied Soft Computing*, Vol. 114, 2022, p. 108114.
41. N. Liu, J.-S. Pan, C. Sun, and S.-C. Chu, "An efficient surrogate-assisted quasi-affine transformation evolutionary algorithm for expensive optimization problems," *Knowledge-Based Systems*, Vol. 209, 2020, p. 106418.
42. Z. Lu, G. Liu, and S. Wang, "Sparse neighbor constrained co-clustering via category consistency learning," *Knowledge-Based Systems*, Vol. 201, 2020, pp. 105987.
43. S. Shen, Y. Yang, and X. Liu, "Toward data privacy preservation with ciphertext update and key rotation for IoT," *Concurrency and Computation: Practice and Experience*, Vol., 2021, p. e6729.

44. S. Wang, Z. Wang, K.-L. Lim, G. Xiao, and W. Guo, "Seeded random walk for multi-view semi-supervised classification," *Knowledge-Based Systems*, Vol. 222, 2021, p. 107016.
45. Z. Yu, X. Zheng, F. Huang, W. Guo, L. Sun, and Z. Yu, "A framework based on sparse representation model for time series prediction in smart city," *Frontiers of Computer Science*, Vol. 15, 2021, pp. 1-13.
46. H. Zhang, J.-L. Li, X.-M. Liu, and C. Dong, "Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection," *Future Generation Computer Systems*, Vol. 122, 2021, pp. 130-143.
47. Y. Zhang, Z. Lu, and S. Wang, "Unsupervised feature selection via transformed auto-encoder," *Knowledge-Based Systems*, Vol. 215, 2021, p. 106748.

Mei-Rong Zheng (郑美容) received the MS degree in Computer System Structure from Fuzhou University, Fujian, China. She is an Associate Professor in Fujian Chuanzheng Communications College. Her research interests include fuzzy information processing, machine learning and network security.



Ru-Chun Jia (贾如春) received the MS degree in Software Engineering from Sichuan University, Sichuan. His research interests include artificial intelligence, machine learning and network security.