Security Application of Encryption Technology in Network Communication

Jin Jin¹², Lipeng Zhao*, Guoquan Zhang³, Shenguo Zhang¹ and Shengui Zhang¹

¹School of Electrical Engineering, Northwest Minzu University, Lanzhou, Gansu, 730030, China
²Key Laboratory of China's Ethnic Languages and Information Technology of Ministry of Education, Northwest Minzu University, Lanzhou, Gansu, 730030, China
³School of Mathematics and Computer Science, Northwest Minzu University, Lanzhou, Gansu, 730030, China

*Corresponding author’s e-mail: Y200130485@stu.xbmu.edu.cn

Abstract. With the development and maturity of science and technology and the arrival of the Internet era, instant messaging software has become an indispensable communication method in people's life due to its comprehensive functions, high performance and high stability. However, due to the open, interactive and global nature of the Internet, there are a series of security problems that cannot be ignored, such as information leakage and virus transmission. Information security is particularly important to us and directly affects whether our personal interests can be effectively protected. Therefore, strengthening information protection and avoiding information leakage are important issues that need to be solved urgently. This paper designs a system based on hybrid encryption by using symmetric encryption original AES and improved symmetric encryption AES to ensure the efficiency of people in the process of information transmission and communication.

1. Introduction

Cryptography is a discipline that is both young and old. As early as thousands of years ago, people full of wisdom have sprouted the idea of keeping communication confidential and have proposed various encryption methods including translocation method. In 1949, after extensive and in-depth research, Sharon found that ciphertexts generated by conventional encryption methods can basically be quickly decoded in a short time, posing a series of severe challenges to the development and application of cryptography. Beginning in the 1960s, with the strong rise of computer technology and the improvement of related theories such as structural algebra, cryptography began to break the bottleneck and made great progress. Especially after the United States formulated the public secret password system, cryptography began to be vigorously promoted and actively applied in more fields and aspects.

The National Institute of Technology and Standards (NIST) launched a campaign to solicit AES (Advanced Encryption Standard) algorithms. NIST began to choose DES as its replacement. This alternative is the advanced encryption standard, AES. NIST announced 15 AES candidate algorithms at the "First AES Candidate Conference" on August 20, 1998. Rijndael was chosen as the advanced encryption standard in April 2000[1]. The main reasons for selection are its strong economy, high
safety factor, reliable and stable performance, etc. The most prominent advantage lies in its strong adaptability to the environment. No matter how harsh the environment is, it still maintains high encryption/decryption efficiency. In addition, from the aspect of operator design, it can withstand all kinds of intense and cruel complete search attacks, thus further prolonging the security period.

2. Method adopted
It mainly discusses several encryption algorithms which are widely used at present in detail and comprehensively. At the same time, it reveals comprehensively and objectively the problems existing in the distribution and management of each method, and formulates strict and reasonable improvement schemes according to the actual situation.

bullet This paper mainly discusses and analyzes several encryption technologies currently used and their application status.
bullet The working principles of the two algorithms are mainly discussed objectively.
bullet The mixed encryption system of the original AES symmetric encryption and the improved AES symmetric encryption is defined, thus not only overcoming the problem of asymmetric encryption and decryption time of the AES algorithm, but also improving the implementation efficiency of the AES algorithm.

3. Design PROCESS of symmetric encryption and decryption AES
Encryption: Each round of encryption is the same and consists of 4 parts: byte replacement, row shift, column mixing, and round key addition. However, it is very clear that the last round does not need to be implemented (column confusion transformation).

Decryption: There is a big difference between decryption algorithm and encryption. In the basic operation process, only (round key addition) remains the same, and the rest needs to be subjected to inverse transformation processing, i.e., InvSubBytes (inverse byte substitution), InvShiftRows (inverse shift), InvMixColumns (inverse column confusion).

C language code is as follows:

```c
Void Cipher()
{
    KeyExpansion();
    AddRoundKey(0);
    for(int round=1;round<=(Nr-1);round++)
    {
        SubByte(State);
        ShiftRow(State);
        MixColumn(State);
        AddRoundKey,RoundKey);
    }
    SubBytes();
    ShiftRows();
    FinalRoundKey(Nr)
}
```

AES decryption process is as follows: decryption and encryption process adopt the same encryption structure, but they are opposite and adopt the inverse algorithm of encryption algorithm.

4. Design PROCESS of asymmetric encryption and decryption ECC
bullet the user A selects an elliptic curve \( E_p(a,b) \), and randomly selects a point on the curve as a base point \( G(x,y) \);
bullet User A selects a private key \( K \) to obtain a public key \( K = k G \);
bullet User a sends \( E_p(a,b) \) and points \( K,G \) to user B;
User B after successfully obtaining the information, transmits the plaintext code to point M on
\( E_p(a,b) \), and generates a random integer \( r(r < n) \);

- User B calculation point \( C_1 = M + rK \); \( C_2 = rG \);
- User B transmits C1 and C2 to User A.
- After receiving the information, user A calculates \( C_1 - K C_2 \) that the result is point M. Because
  \( C_1 - K C_2 = M + rK - K (rG) = M + rK - r(kG) = M \);
- Decode M again to obtain plaintext.

5. Improvement of AES algorithm
In this graduation project, symmetric encryption AES algorithm studies 128-bit encryption. The
algorithm performs 10 rounds of encryption. Except for the last round of encryption, the first 9 rounds
are all the same and are all the same encryption steps. Byte substitution, row shift, column mixing and
round key addition are performed in sequence. Therefore, the round transformation function is the
most important thing in AES algorithm. Its efficiency determines the encryption and decryption speed
of the whole algorithm. Therefore, I intend to improve the matrix used in column mixing by analyzing
the four-step operation of round transformation and aiming at the problem of unequal encryption and
decryption time. Then, the simplified round function can quickly realize round transformation by
looking up tables, which improves the implementation speed and efficiency of AES algorithm.

6. Comparison of operation efficiency between symmetric encryption AES and asymmetric
encryption ECC
The two encryption test environments are: the operating system is Windows Home Chinese version,
the system type is 64-bit operating system, the CPU model is INTERCELEON 3160, the CPU main
frequency is 1.6GHz, his disk size is 512G, the memory size is 2G, and the programming language
C++. Table 1 below:

| Operating system     | Windows10 family chinese version |
|----------------------|----------------------------------|
| System type          | 64-bit operating system          |
| CPU model            | Inter Celeron N3160              |
| CPU frequency        | main 1.60GHz                     |
| Disk size            | 512G                             |
| Memory size (RAM)    | 2.00G                            |
| Simulation software  | Visual Studio 2019               |
| Programming language | C++                              |

Test data for different file sizes are shown in Table 2 below:

| algorithm | 1000bit Encryption | Decryption | 2000bit Encryption | Decryption | 3000bit Encryption | Decryption |
|-----------|--------------------|------------|--------------------|------------|--------------------|------------|
| AES       | 0.83s              | 0.78s      | 1.73s              | 1.72s      | 2.45s              | 2.49s      |
| ECC       | 1.12s              | 4.35s      | 2.27s              | 8.79s      | 3.39s              | 13.66s     |

Make the above data into a chart as follows:
According to figures 1 and 2 of the data chart, the red curve represents the encryption and decryption of elliptic curve encryption ECC, and the blue curve represents the encryption and decryption of advanced encryption standard AES. It can be understood from this that ECC consumes significantly more time than AES in the encryption and decryption process with the same bit, regardless of whether ECC is encrypted or decrypted. This figure also directly reveals that ECC uses two keys in the data transmission process. In public key encryption system, information needs to be encrypted and decrypted by different keys. Encrypted data can be successfully decrypted only by its unique decryption key. Among them, the most difficult problem is that it is difficult to obtain the corresponding decryption key directly by the encryption key. Therefore, ECC encryption takes a long time and is slow.

7. Comparison of original AES and improved AES and mixed encryption efficiency
The two encryption test environments are: the operating system is Windows Home Chinese version, the system type is 64-bit operating system, the CPU model is INTERCELERON 3160, the CPU main frequency is 1.6GHz, his disk size is 512G, the memory size is 2G, and the programming language C++. Test data for different file sizes are shown in Table 3 below. AAES is after improving AES. MAES is mixed encryption of original AES and improved AES.
Table 3. Test Data for Files of Different Sizes

| algorithm | 1000bit Encryption | 1000bit Decryption | 2000bit Encryption | 2000bit Decryption | 3000bit Encryption | 3000bit Decryption |
|-----------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| AES       | 0.79               | 0.85               | 1.57               | 1.72               | 2.38               | 2.49               |
| AAES      | 0.44               | 0.42               | 0.82               | 0.83               | 1.20               | 1.23               |
| MAES      | 0.58               | 0.54               | 1.08               | 1.11               | 1.53               | 1.58               |

Make the above data into a chart as follows:

Figure 3. Comparison of Original AES and Improved AES and Their Mixed Encryption Efficiency

Figure 4. Comparison of Original AES and Improved AES and Their Mixed Decryption Efficiency

From the above data chart, the encryption and decryption efficiency has been greatly enhanced without changing the internal structure of the S-box. Compared with the encryption process of the original AES algorithm, the newly improved D-box look-up table method has the characteristics of fast processing speed and high calculation efficiency, and also solves the problem of different encryption and decryption times of the symmetric encryption algorithm AES.

8. Conclusion

This paper describes the relevant background development and significance of encryption technology, and then begins to explain in detail the theoretical knowledge of AES and ECC encryption algorithm, including basic mathematical theorem and algorithm process analysis. The information is encrypted by the original AES algorithm, the matrix used for column mixing in the AES algorithm is improved, and then the round function is simplified to rapidly realize round transformation by looking up a table,
so that the efficiency of the AES algorithm can be improved. Therefore, a mixed encryption algorithm based on the original AES and the improved AES is designed, which not only can ensure the efficiency, but also can solve the problem of unequal encryption and decryption time of the AES algorithm.

Acknowledgements
This work was supported by the Central Universities of China for Northwest Minzu University (Grant No. 2018xjipzygxk-21), the Major horizontal project for Northwest Minzu University (Grant No. XBMU-2020-BC-28) and the Fundamental Research Funds for the Introduction of Talent Project for Northwest Minzu University (Grant No. Z14011).

References
[1] Qingyu Ma, Dong Zhang. research and implementation of telemetry data encryption technology based on AES and ECC [J]. naval electronic engineering, 2015,35(04):78-81.
[2] Hongzhen Wang, Zhulin Li. Design and Implementation of Hybrid Encryption System Based on AES and ECC [J]. Electronic Design Engineering, 2012,20(04):9-11.
[3] Liang Wang. Research on ECC and AES Hybrid Encryption Algorithm Based on WSN [D]. Jiangxi University of Technology, 2013,24(09):26-27.
[4] Hongjun Liu. Using C# to Realize AES Encryption Algorithm to Encrypt Text Information [J]. Information Security and Technology, 2012,3(07):14-16.
[5] Xiujuan Zhang. Implementation and Application of AES-Based Encryption Algorithm [J]. Digital Technology and Application, 2011(12):128-131.
[6] Chunao Wang. Implementation of Elliptic Curve Encryption Algorithm Based on VC++ [D]. Jilin University, 2016(13):65-68.