Encryption System Design Based On DES And SHA-1

Jian Zhang, Xuling Jin
School Of Science,Beijing University Of Civil Engineering And Architecture,Beijing, China
zhangjian@bucea.edu.cn, sahjxl@sina.com

***Abstract*—For modern society, The concealment and completeness of data is particularly important. To solve this problem, developed a mixed DES and SHA-1 encryption system based on VC + + environment. The system on the one hand by Triple DES and RSA algorithms for data encryption to hide, on the other hand, by the SHA-1 algorithm to validate the integrity of data, it has a wide range of practicality.**

***Keywords*—data encryption standard; public key cryptography; secure hash algorithm; data encryption system**

I. INTRODUCTION

The rapid development of information network creates favorable conditions for the rapid flow of data, the shadow of the figures can be found everywhere in people's lives, the relationship between people and the data becomes closer, and its position is gradually rising. For modern society, the concealment and integrity of data is extremely important. Therefore, important data files, usually require the encryption algorithm for processing to turn it into obscure "garbled", in order to achieve its secretive, calculation and check of the authentication algorithm to verify whether the data was falsified. This system uses DES (Data Encryption Standard) algorithm and SHA-1 hash function as a combination of methods to achieve this objective.

II. THE DESIGN OF THE DATA ENCRYPTION SYSTEM

A. Design Scheme

In order to achieve the concealment and security of data, we must increase the complexity and irreversibility of the algorithm. Data encryption system uses the Triple DES algorithm based on CBC mode to encrypt important data files and then get the encrypted file. Next, we can sign on the files by the hash function SHA-1 to get the corresponding hash sequence, and the bulk of the original file column hash value add to the end of the encrypted files; then decrypt the encrypted data file, remove the hash value attached to the end of the corresponding to get the decrypted file; and calculate the hash value of the declassified documents, compared with the original hash value, in order to verify whether The file has been falsified. Using Triple DES and RSA encryption algorithm in the system design, increase the key length to ensure the security; The authentication algorithm using SHA-1, as the irreversible algorithm, so that its safety can be guaranteed. The specific design shown in Figure 1:

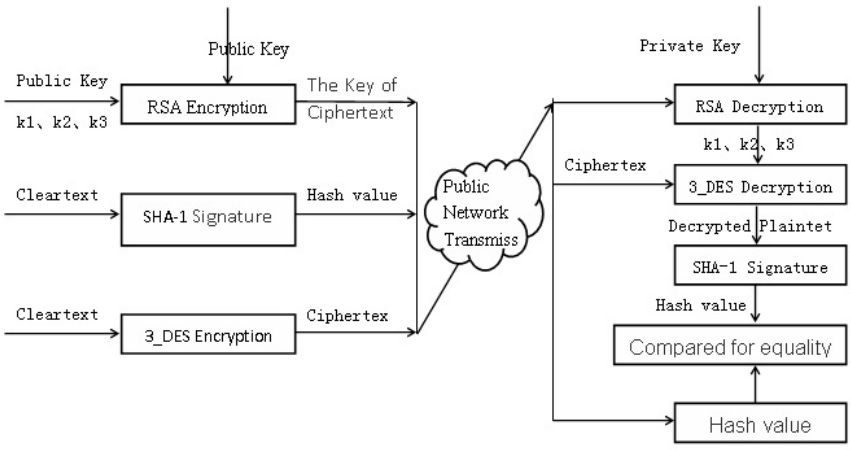

Figure 1. data encryption system design

B. Program analysis

1). Analysis of CBC mode

In CBC mode, before encryption, each plaintext group Pi should be added with the prior one ciphertext by bit mode 2, and then sent to the DES encryption, CBC mode overcomes the packet reorganizing disadvantage of ECB mode. This mode has a limited (two steps) error propagation characteristics, self-synchronization, and can not easily be attacked, etc.

978-0-7695-4818-0/12 $26.00 © 2012 IEEE
DOI 10.1109/DCABES.2012.42

2). Analysis of encryption algorithm

With the development of cryptanalysis techniques and computing capability, the security of DES is threatened. Short key is one of a main shortcoming of DES. The actual DES key length is 56 bits, the key quantity is only 256 ≈1017. As the computing capability of contemporary computers, DES can not resist exhaustive key search attack. In January 1999, the Electronic Frontier Foundation (EFF) successfully deciphered the DES in just 22 hours, 15 minutes.

However, triple DES can resist the half-way encounter attack:

$$y = DES_{k3}(DES_{k2}{}^{-1}(DES_{k1}(x)))$$

Where x represents the plaintext, y on behalf of the ciphertext, which is equivalent to the key length is extended from the original 56 bits to 168 bits, and these three keys have different arrangements, greatly improving the resistance to exhaustive key search attack. Although now a new Advanced Encryption Standard AES is announced, Triple DES is still widely in various fields of practical, such as encrypted the transmission of cardholder PIN, IC card and two-way authentication in POS, financial transactions, data packet MAC calibration, etc., all of them adopt the triple DES algorithm.

3). Analysis of key management algorithm

Its biggest flaw for DES is the shortage of key. For the purpose of enhancing the anti-attack capability of encryption algorithm, although it can not increase the length of the key, it can be processed to enhance the difficulty of exhaustive key search attack on DES key. The system uses the RSA asymmetric encryption algorithm to manage the keys for the following reasons:

a) The RSA encryption algorithm is based on the puzzle of large prime integer decomposition, in order to decipher the RSA, they must decompose a large prime integer, but there is not a confirmed algorithm yet to achieve this factorization. It can only be tested by quotient test method, so that the difficulty of deciphering greatly increased;

b) RSA as a asymmetric encryption algorithm, is in line with the encrypted during transmission very well. Public key is open to the public as a key transport user; private key is kept secret by the individual, only the recipient know the encryption key used in the algorithm; thus it can avoid the DES symmetric key of falsified and intercepted during the process of recipient and transmission, and greatly improving the safety performance of the key;

c) Although the RSA algorithm is complex, has large consumption of computer memory and time, while applied to the 64-bit DES key, it can just reduce its disadvantage in the encryption process. On one hand, it could save time and memory space for the system. On the other hand, it greatly improved the security of the encryption algorithm, the encryption algorithm of the anti-attack capability.

4). Analysis of authentication algorithm

SHA-1 is the national standards promulgated by the American Standards and Technology (NIST), it is the most widely used hash function algorithm. The password community, which has been published, is a strict inspection and has not been found unsafe, it is now considered security.

SHA-1 is similar to the MD-5 algorithm and is based on the same principle with MD4 same in the design, and imitate the MD4 algorithm. The algorithm is designed to used in conjunction with the Digital Signature Standard (DSS). Therefore, the anti-exhaustive is better. It is currently the most advanced encryption technology, used by government departments and private owners to deal with sensitive information, to prevent information from being maliciously falsified.

C. Functional design

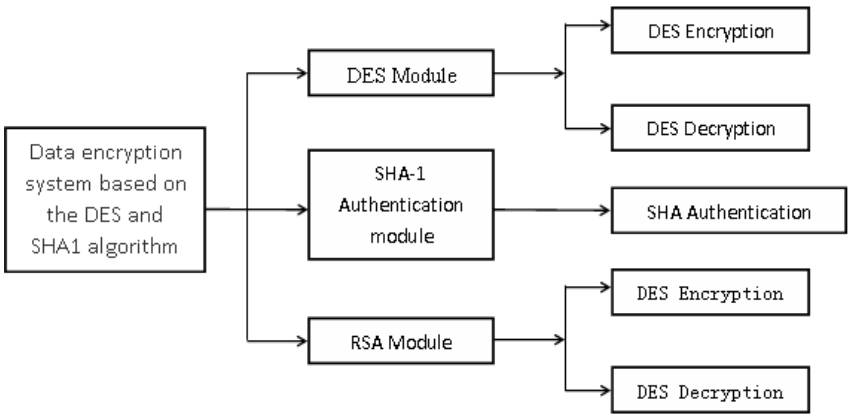

Figure 2. Functional block diagram

III. THE KEY TECHNOLOGIES OF MIXED ENCRYPTION SYSTEM

A. Processing of Word documents

Visual C + + Class Wizard mechanisms, from the Office type library to generate a wrapper class, and then call the appropriate library functions of word reading and writing. Required to read and write word documents Application class, Document class, the Selection class. Documents class and Selection class in accordance with the steps to add Application class, is added to the application.

B. System integration

1). Analysis on the interface

Three algorithms 3-DES、RSA、SHA-1 Input, output and actions. Such as table1

TABLE 1. INFORMATION OF THREE ALGORITHMS

Algorithm	Function	Input	Output	Actions
3-DES	Plaintext encryption、Ciphertext decryption	Plainte、Ciphertext、k1、k2、k3	Ciphertext 、Decrypted plaintext	Encrypt、Decrypt
RSA	Key encryption Key decryption	Prime number Status P 、Q	P 、Q 、M 、N 、Public key 、Private key	Prime number generate、Key generate、Encrypt、Decrypt
SHA-1	Plaintext signature 、Authentication	Binary plaintext	Hexadecimal Hash value	Sign、Authenticate

The link between the relevant functional modules, as well as the interface between the module and the module can be seen through the table. for example, the interface between the 3-DES and RSA module three key DES module.

2). Module integration

Through the analysis of the above interfaces, has been associated with the interface between the related modules, Figure 3 shows the module inputs and outputs and the behavioral characteristics of the interface design:

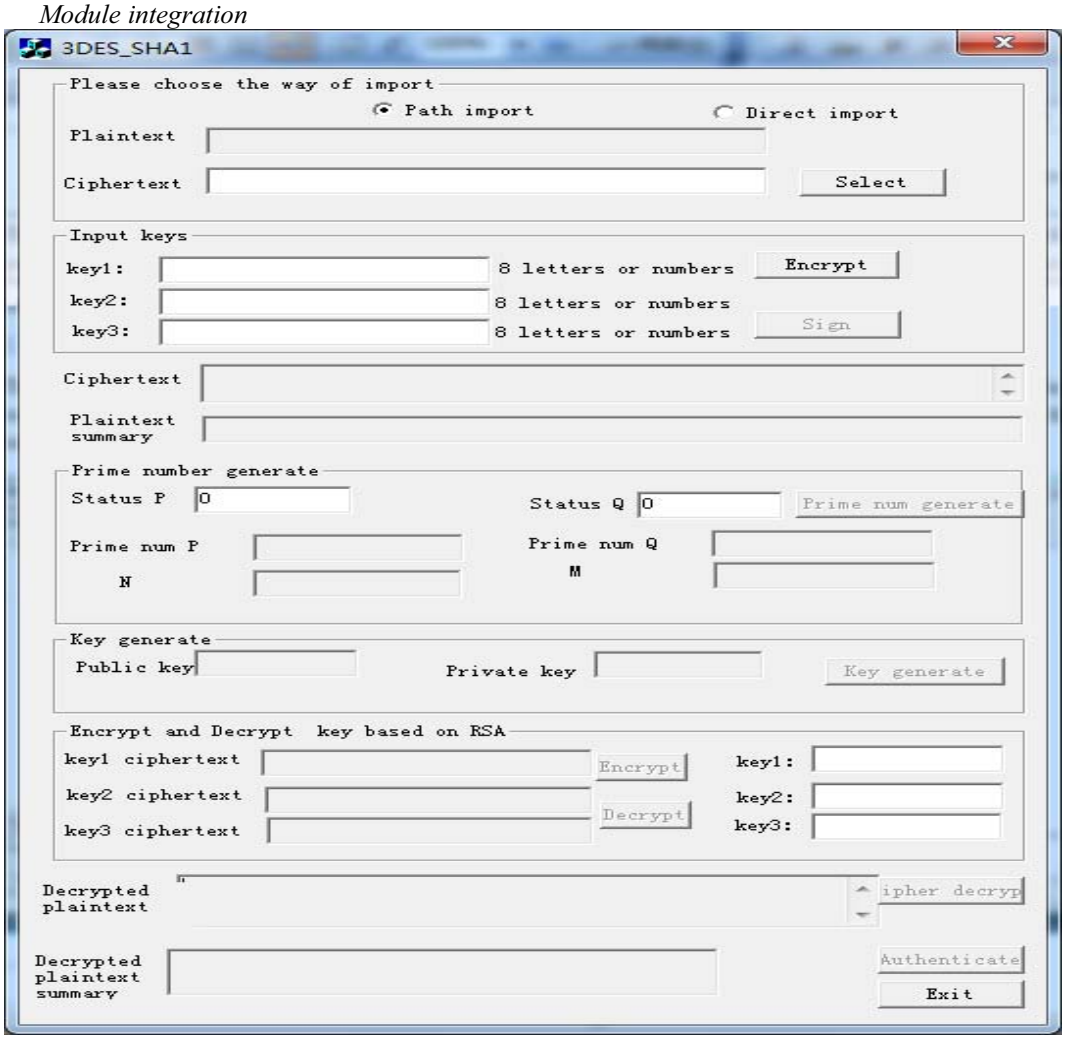

Figure 3. Interface design

IV. SOFTWARE FUNCTIONAL VERIFICATION

A. The operating environment test

Test environment: Windows XP operating system, VC6.0 development environment

Test method: according to the workflow of the software system, each module to be tested.

Test Conclusion: friendly software interface, the various functions operating normally. The overall operating condition is fine.

B. The encryption and decryption functional test

Test environment: Windows XP operating system, VC6.0 development environment

Test method: the traditional encryption of files on local computer. Test the decryption functions under the mode local storage system.

Test results: the files under operation can be selected correctly and encrypted. When the keys are error or changed, it can be reported immediately. So the encryption to the files could fulfil the requirements of system.

C. The software efficiency test

Test environment: Windows XP operating system, VC6.0 development environment

Test method: test the speed of encryption and decryption of the files in different size while under the same environment. Then, record the time of encryption and decryption.

In the same environment, the use of three encryption methods to encrypt different document, collecting some of the encryption/decryption time, can demonstrate the superiority of mixed algorithm in the encryption and decryption speed.

V. CONCLUSION

The system is suitable for the transmission of important data between companies. When company A needs to transfer data to company B, company A can use the system for data encryption package, and then transmit over the Internet to company B, company B authenticate via the same system to decrypt the file, and get the corresponding data. At the same time, they could identify whether the data has been tampered during the transmission, thus the security and integrity of the data transfer process can be ensured.

REFERENCES

[1] Aqi Zheng、Youhe Ding VC++ Tutorial 1st Edition Beijing, Tsinghua University Press, 2005: 49-132

[2] Haoqiang Tan C Programming 3rd Edition Beijing, Science Press, 2008: 49-175

[3] Hong Yan Data Encryption Technology And Its Development Trend Computer and Modernization, 2005, Total 115: 1-3

[4] Tuhao Shen WORD Documents Created With VC + + Language Computer Engineering and Design, 2004, 6 of 25: 1-3

Remark--The paper is supported by BMEC(KM201010016003)