Based on The DES_RSA Encryption Algorithm Improvement and Implementation

Hao Wang

Changchun University of science and technology

Abstract

with the rapid development of information technology and net work,our life become more and more inseparable from the Internet .Network life has become apart of daily life is very important. RSA algorithm and DES algorithm are two very tepresentative algorithms ,they represent different encryption system , has its own advantages. This paper made analysis and comparison of them, and then to fuse, complement each other, their algorithm and the simple implementation is put forward. DES algorithm is the typical representative in the symmetrical encryption system, the RSA is representative of the symmetric encryption algorithm. At the end of the paper designed a kind of based on 2 sieve encryption algorithm des and RSA hybrid encryption system, and the simple implementation, its encryption efficiency test and analysis.

Keywords

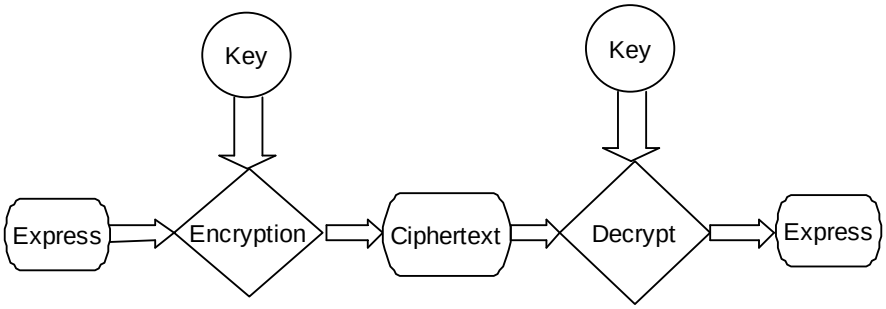
RSA algorithm, DES algorithm, 2DES-SIEVE algorithm.

1. Introduction

With the progress of the times, the continuous development of industrial technology, the computer from the original high-end equipment, has been into Into ordinary people's home. With the development of computer, the network is also following the pace of rapid development, and now the network is more and more convenient, people from the beginning of the online news, watching video, and gradually developed to online shopping, online banking transactions, etc.. Because of these, the security of the network is also increasingly high, the most basic is that people want the network is at least relatively safe, their personal information and information will not be stolen and used. Encryption is one of the effective means to protect information security.

Extraordinary significance. With the development of information technology, computer and network, the amount of data stored in the computer is increasing. How to protect the data is not illegal access, illegal modification, etc., are all computer users to consider the problem.

So we are here to introduce cryptography ,Cryptography is a kind of science and technology to write passwords and passwords. Writing code is to put the original information, through the transformation of the password to form another form, so as to ensure the safety of communication; and to crack the password is just the opposite, it from the information found in the law, so as to restore the original text, get the real meaning of information. Cryptography involves many disciplines, including information theory, mathematics, computer science, and so on. In computer field, we study how to encrypt data, so as to ensure information security in the process of network communication. The process is shown in figure



2. Analysis of encryption algorithm

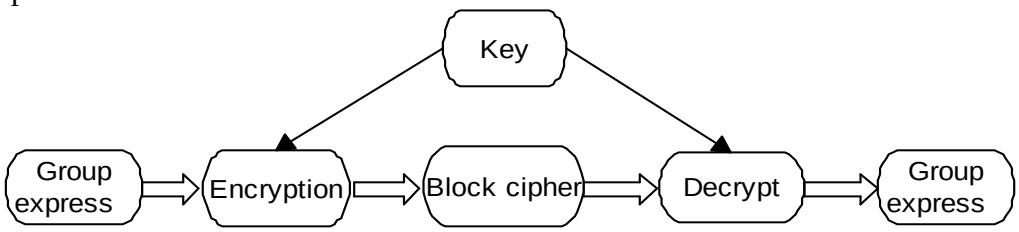
RSA was born early, in 1977 by the Rivest Adi, Shamirh Len and Adleman Ron, in the United States, the development of the Massachusetts Institute of Technology completed. RSA belongs to public key cryptography. The public key system is to generate two keys, one for encryption, one for decryption, and not according to the algorithm and one of the key, and to launch another key. In use, the public key is public, the other uses public key encryption data, the encrypted text back, and then use the other key to decrypt, so as to restore the clear text. RSA encryption and decryption of the use of the public key KP is open, that is, a lot of people can get, the third party is also very easy to steal the value of E and n. So the key is to crack, from E and n these two values, to find a way to get the value of D, if you can get the value of D, it is able to find the private key, then you can crack the corresponding information, to achieve the purpose of information theft.

Because the theoretical basis of the RSA algorithm is a large number of the decomposition, it is recognized as the world's problem, which is the security of RSA, so it can resist all kinds of attacks, but it is not that RSA is perfect, it also has its own defects. RSA the biggest drawback is that it is slow encryption speed, is not suitable for a large number of data encryption.

3. DES algorithm analysis and research

DES algorithm is a symmetric cipher system developed by IBM. It should be able to prevent data from being modified and leaked without authorization, and the data can be obtained with high quality.Amount of protection. While the algorithm is easy to understand and master, but also to a considerable degree of complexity, so that the benefits of decoding the staff is far lower than the pay. The security of the algorithm is not dependent on the security of the algorithm itself, but on the basis of the security of the key.

DES algorithm is a kind of packet encryption mechanism, which will be divided into N group, then encrypt each group, form their own text, and then merge all the groups of the blocks to form the final text. In the encryption process, it is to be divided into groups, each group length is 64, then the individual packet and the key together as the parameter, the encryption algorithm, the encryption algorithm in the key role of the packet data encryption, so as to get the packet. DES encryption and decryption process as follows.

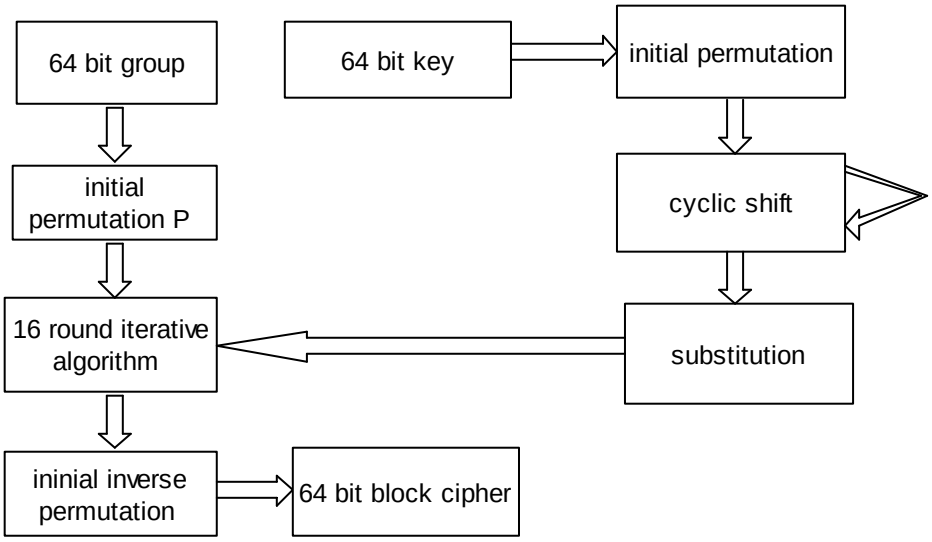


DES encryption is to encrypt each packet, so the input parameters for the group of clear and key, and the group need to be replaced and iteration, the key also need to be replaced and circular shift, the total flow as shown in Figure. In these iterative operations, the sub keys are applied to each group.Initial inverse permutation P,

DES encryption algorithm is a pioneering work in the field of data encryption, it not only has the advantages of safety coefficient is high, and the encryption speed is quick, suitable for large amounts of data encryption. But it is only a product of a period of time, with the development of modern technology, and the continuous development of it, the problem is gradually emerging. DES mainly has the following several problems.

DES is a kind of public encryption algorithm, its security depends on the secrecy of the key.

DES encryption algorithm is the most important part of the 8 S boxes, and the design principle of these boxes, has never been announced, for the use of DES encryption, there is an unknown risk.

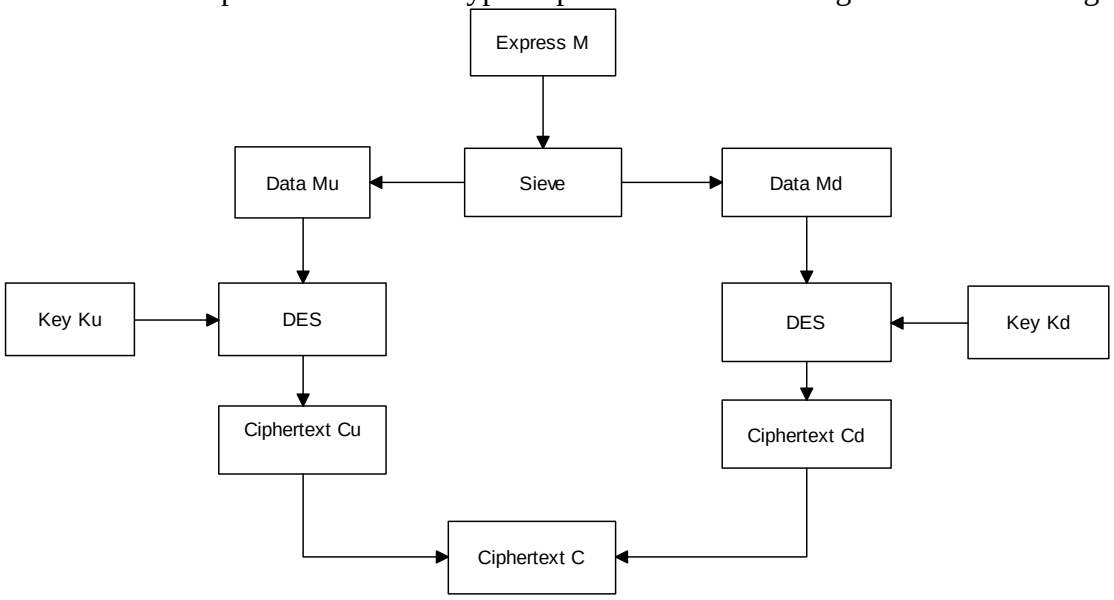


4. A 2DES encryption algorithm

After DES proposed, it is widely used, but with the development of society, it can not meet all the needs. At this time, there is no new encryption standard, that is, later AES. During this transitional period, it was suggested that 3DES. This chapter discusses the 2DES screen and 3DES encryption algorithm, encryption algorithm is very similar.

3DES (or DES Triple) is the three TDEA data encryption algorithm (Triple, Data Encryption Algorithm), which is the transition between DES and AES, which uses three times DES encryption, which is equivalent to increase the length of the key, thus increasing the security.

3DES encryption algorithm is a simple combination of DES algorithm. If you want to crack it, you must break the 3 keys. Only in this case, the entire cipher can be cracked, no doubt it is quite difficult. Also because of this, its security is much higher than DES. 2DES screen encryption algorithm, encryption algorithm and 3DES are the same as the combination of DES algorithm. The sieve 2DES encryption algorithm between the two combinations introduced a "sieve" and "screen" is a "two-dimensional" variables, it will clear the data into two layers, the upper data mu, the underlying data for MD, then use the DES algorithm for encryption, key for Ku and KD, encrypted by two layers of ciphertext Cu and CD, finally, the upper and lower two layers of ciphertext by combination of the formation of the final ciphertext C. Its encryption process schematic diagram .The following



2DES sieve the encryption algorithm both with respect to the DES encryption algorithm, and in comparison with RSA have their own advantages, which is reflected in the encryption speed and safety.

encryption speed.

key space has been greatly improved.

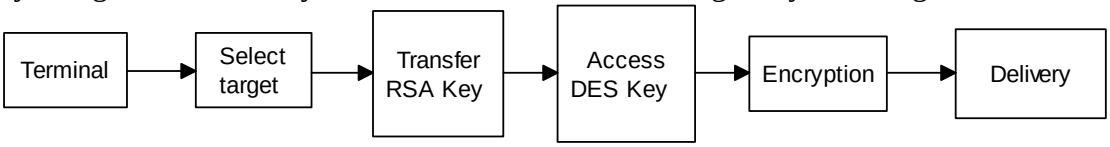
Has a strong practical

5. A 2DES algorithm with RSA hybrid encryption design

2DES sieve encryption algorithm in pure DES algorithm on some improvement, it belongs to symmetric encryption algorithm system, has some of the characteristics of symmetric encryption algorithm; RSA asymmetric encryption algorithm, is obviously different from the former. They each have their own advantages and disadvantages, this paper by comparing their, take each other's method, so as to obtain their hybrid encryption.

2DES sieve algorithm and RSA Security are high, their security depends on the security of the key, 2DES encryption speed of efficiency is high, suitable for large amounts of data encryption; RSA encryption speed and large prime numbers P and Q is related to the size, due to the use of power and modular arithmetic, because of its slow speed of this it, does not apply in the large amounts of data. On the other hand, key distribution, RSA has obvious advantages compared to the 2DES screen encryption. Therefore, in the process of encryption and decryption, if we can learn from each other, will receive good results.

This system is mainly used for the security of data file transfer. After the system is opened, it is connected with the selection process terminal. After the connection is good, the user can send the RSA key and get the 2DES key, and then send the data file. Figure system diagram



Key less easy to keep. In communication with multiple people, the RSA public key system is used to obtain the encryption key, as long as the public / private key of a pair of RSA can be obtained, and then the encryption key of the data can be acquired in real time. Through the above analysis, we can know that this hybrid encryption algorithm not only can play the characteristics of 2DES fast encryption, it can carry out a lot of data encryption, but also on the security of the encryption, or the key security, there is a lot of high. The mixed encryption method can complement each other by using two kinds of encryption effect.

6. The algorithm and implementation of RSA hybrid encryption 2DES encryption.

2DES sieve encryption algorithm implementation, mainly includes three parts: sieve, the realization of DES encryption, and a is des decryption implementation. In order to make the running faster, the implementation of these parts are used in pure C. In this system, we must select the other users, and then exchange RSA and 2DES key, to send the file to be encrypted and sent, without the need to encrypt a user to encrypt once, then click send. Use a sieve in 2DES encryption algorithm and RSA hybrid encryption, combines the advantages of two kinds of encryption system. In the encryption security have greatly improved the encryption efficiency but no significant decline. Truly learn from each other.

7. Conclusion and Prospect

Along with the development of information technology, the increasing of the amount of data is increasing, and the security of data is received more and more attention. Research and application of encryption algorithm is also in constant depth, in order to meet the needs of the industry. The

emergence of DES is a milestone, its efficiency and security has been recognized by the world. But due to the length of the key, it can no longer meet the needs of modern society, and on this basis, this paper put forward the 2DES sieve encryption algorithm, the sieve is introduced and two times using DES encryption, effectively overcomes the defects des caused because the key is too short.

Reference

[1] Su Kaiyuan.DES_RSA RSA mixed data encryption and transmission realization [D]. Jiangsu: Nanjing University of Posts and telecommunications, electronics and communication engineering specialty, 2012:

[2] Zhang Xuefeng.AES and DES algorithm analysis [R]. Shaanxi: Xi'an University of Posts and Telecommunications,.2010:

[3] peak.RSA encryption scheme security research [J]. technology vision.2012, 18:187-188.

[4] Sheng Zhong Biao. [J]. RSA algorithm of encryption algorithm.2012 Henan science, 30 (11):167-169.

[5] Haobing Mongolia, Lu Xiaoya.DES algorithm analysis of [J]. computer security.2012, 9:43-46.

[6] Rong Kevin. About DES difference [J]. Journal of Institute of education of the Jia musi.2012, 5:419-422.

[7] Liu, Zhou Xin Wei. DES symmetric encryption system of [J]..2012 based on 10:10-13. Technology Square,