Advances in Engineering Research, volume 122

7th International Conference on Applied Science, Engineering and Technology (ICASET 2017)

Research on Encryption Technology in Contactless IC Card

Mingxin Zhao[1, a]

[1] Computer Centre, Anshan Normal Collge Anshan China

[a]email：zhao_mx@hotmail.com

Abstract. This paper mainly researches the important value of encryption technology in contactless IC card in the practical application. In the paper, it is pointed out that the DES arithmetic algorithm and 3DES algorithm is by far the most suitable encryption method for encrypting contactless IC card data. The implementations of 3DES algorithm in the M1 card are described in detail, and the specific implementation process are provided. Finally, the development direction of the contactless IC card encryption technology in the future are pointed out.

Keywords: IC card security technology, DES algorithm, 3DES algorithm, M1 card

Introduction

In the next few years, China will be the biggest EPC (Electronic Product Code) user in the world along with the development of logistics network, and that contactless IC card (radio frequency card) encryption technology is the core of EPC technology , so the study of contactless card encryption technology is of great significance.[1].

Contactless IC card, also known as contactless integrated circuit card, rf (radio frequency card)card, is a new technology which is a combination of card technology and the radio frequency identification technology originated in the mid-1980s. As having no mechanical contact with read/write device, communicating with the help of "space medium" electromagnetic waves ,it has remained prominent advantages of traditional IC card, also. It has the characteristics of convenient operating, high reliability, long service life, good security, good safety, strong anti-jamming capability, and multi-purpose in one card, etc.

So it has developed rapidly and are widely used in the identification, logistics management, bus charging, highway tolls,, gas stations, parking lots, etc [2].

Widely use of contactless IC card has brought great convenience for the financial world and the user, but its defects of being modified, copied and imitated easily also brings a serious damage and threat. Rf card and reader communicate using radio communication technology, and the radio waves is open in space and can be intercepted by the invaders easily, therefore, Ordinary radio frequency card without logic encryption can't defend the most simple password attack, communication content can be stolen, rewrited, counterfeited, copied easily , it has less security assurance even than the general contact card with logic encryption. Therefore, only Rf smart card which is embedded with encryption technology and matched with the corresponding communication encryption technology, the security of the system can be guaranteed.

The attacker’s main purpose is to grab the information in the card, or illegal copying or tamper the contents in card, or illegally use other people’s cards, etc., and finally it damage the system. Modern cryptography provides some encryption/decryption systems specially designed, These standard password systems has a reliable theoretical basis, and has been tested in the application, also easily get the user’s trust. Through our extensive research on IC card application at home and abroad, we find DES arithmetic system is by far the most widely used, the most secure encryption system.

DES arithmetic algorithm and 3DES algorithm

DES arithmetic system is a typical representation of traditional grouping cryptography. The DES algorithm adopts basic hidden information technology in the design: spread and chaos. Many professionals have made a lot of research work for the security of DES arithmetic. Considering the

characteristics of DES arithmetic algorithm, theoretically the key can certainly found by exhaustive method, but it's hard to work out the encrypted data with the current hardware speed and price.

DES arithmetic algorithm

DES algorithm principles has been described accurately in detail in many books, because of the limited length, here only the main process of the algorithm is shown in figure 1.

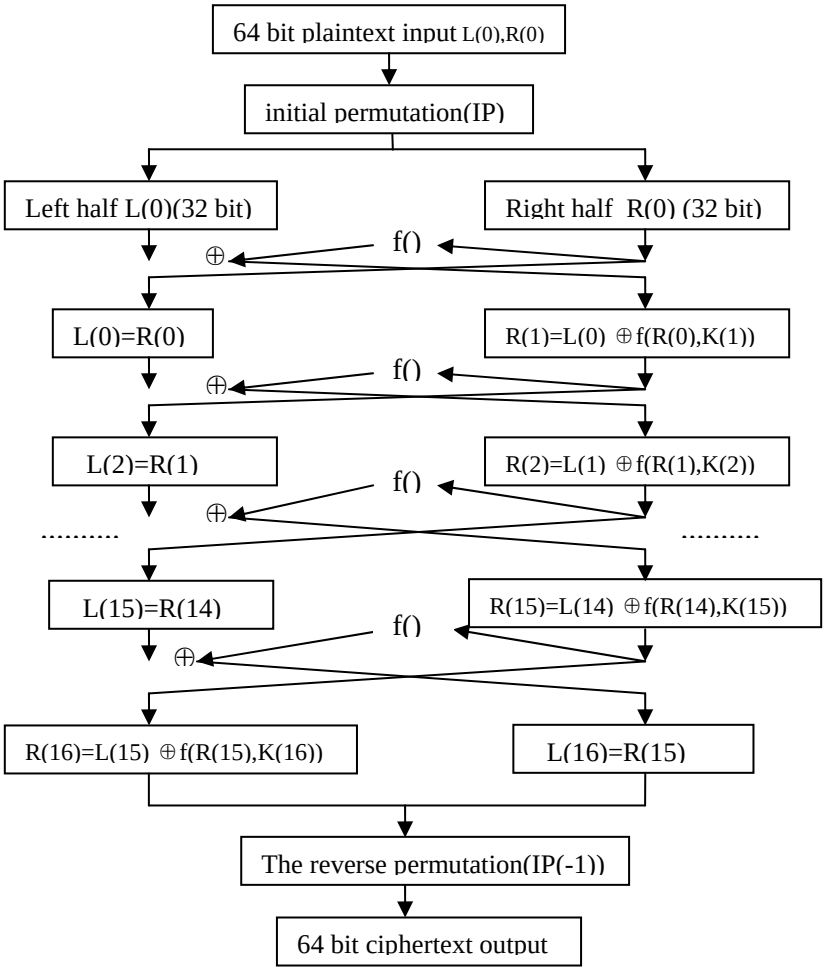

Fig.1 the main process of the DES algorithm

The entrance of the DES arithmetic algorithm has three parameters: Key、Data and Mode. The Key with length of 8 bytes ,64bits, are working Key of the algorithm; The Data with length of 8 bytes ,64bits also, is to the data to be encrypted or decrypted. The Mode is the DES working mode, there are two, encryption or decryption [3]. This algorithm works, for example: If the Mode is encryption, the DES algorithm encrypts the Data with the Key and generates cipher text of Data(64bits) as the output of DES. :If the Mode is decryption, the DES algorithm decrypts the encrypted data with the Key and generates plaintext of Data(64 bits) as the output of DES. Both ends of the IC card reader and the card have the same Key, the IC card reader encrypts the core data with the Key, and transfers the cipher text to card, When receiving the cipher text the card decrypts the data and recreates the plaintext, In this way, DES algorithm can guarantees the core data transmission security and reliability in the IC card system.

In DES arithmetic algorithm, the main operation is substitution, shifting and binary addition ,any computer language can implements shifting and binary addition easily, while substitution requires more complex processing to complete.

substitution is a more unique step in the DES algorithm. Assume that the input A = a1a2a3a4a5a6 ,a2a3a4a5 = k, a1a6 = h, finding B at line h column k in S box, B is between 0 ~ 15 and B = b1b2b3b4 expressed in binary, this is a output of S box; For example, assume that binary input of S box is 111010, according to the above algorithm, B is at line 2 column 13 in the S box, finding the number 9 along the table, it is 1001 with binary representation, that is the output is 1001.

3DES algorithm

The key of DES algorithm is too short (only 56bits effective data),So it can not rule out that the data will be broken out by the "brute force" method as the developing of computer hardware technology. In order to guarantee higher safety and reliability of data in IC card , considering the problem such

as the speed of encryption and decryption at the same time ,the DES algorithm must be improved. Using 3 DES (Triple DES) algorithm to encrypt the data in card is a very practical, reasonable and effective method.

On the basis of the DES algorithm, 3DES algorithm has 8 bytes length encrypted data packet ,encryption and decryption keys are the same. It encrypts the plaintext through three times DES processing, using K1, K2, K3,three different keys (8 bytes length).It works like this, encrypts the original data with K1 first ,then decrypts it with K2, encrypts it with K3, finally generates the final cipher text [4];The Decrypting process accord to opposite order, that is, decryption with K3-encryption with K2- decryption K1, then restore the original plaintext. In order to reduce the system overhead in terms of key generation and management, K1 and K3 can be set to the same value ,in this way , only two keys (K1 and K2) are in use actually. But K1 and K2 should never be the same, or 3DES algorithm will lose its meaning. 3DES algorithm program flow chart is shown in figure 2.

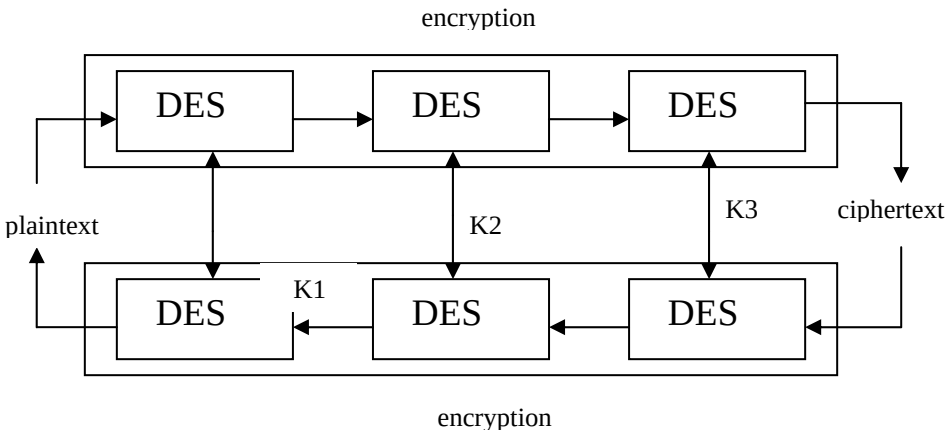

Fig.2 the main process of the 3DES algorithm

3DES encryption /decryption algorithm, Adopt dual keys, The key length is 112 - bit, doubled than DES algorithm. Although the operation speed reduce to a certain extent, , but security has been greatly enhanced.

Implementation of 3DES algorithm in the M1 card

Mifarel contactless IC card (also called Mifare1 rf card, referred to as Ml card below) is divided into 16 sectors, each sector have 4 blocks, each block have 16 bytes, store/fetch data based on block. The last block of each sector is used to store the sector's physical password and access control information, therefore, blocks used to store user data is 47 blocks in all.

Two kinds of password are stored in EEPROM inside the read/write device, one is the the physical password needed by verification while reading the M1 card ,the another kind is the logic password used by 3DES algorithm to encrypt/decrypt data. When read/write device detects card, it authenticate the password settled on a sector in card. If the certification is past, read/write device is allowed to read and write data on the sector. Otherwise new certification is needed.

3DES algorithm has 16 bytes length logic password. When writing data into M1 card, the read/write device move 16 bytes of the logical key stored in EEPROM in advance into the array password [16] then encrypt the data according to 3DES algorithm encryption, eight bytes as a group, write it to the specified sector block when having achieved 16 bytes, if the encrypted data is less than eight bytes, supplementary zero is needed in accordance with requirement of 3DES algorithm.

When read/write device read the M1 card data, and physical password authentication is finished, the read/write device decrypt the data according to 3DES algorithm encryption, eight bytes as a group,and return plaintext data to user. Plaintext data will not be achieved even if someone has read the data in the M1 card because the absence of 16 bit logical key, so as to prevent data be cracked.

In addition, although the plaintext data cann't be gutted out, the attacker can completely copy the card, including copying card serial number in sector 0, block 0 and other information if the cipher text data is stolen.

In order to prevent the attacker copies the data in M1 card into another M1 card, system tables storing card serial number and time stamp ,each 4 bytes is needed in EEPROM or external memory. Once the read/write device read or write the card, after the, a new time stamp will be written into the card and system table. No matter how many identical cards the attacker copy, only the one being read by system first can be admitted, thereby preventing the card to be copied. Timestamp is unsigned variables, four bytes length, generated by shifting and compounding data of year, month, day, hour, minute, second read by read/write device. Timestamp synthesis algorithms can be done with the following statement:

```
ts =(( INT 32U ) yr  < < 2 6 ) | ((INT32U)month << 22) | ((INT32U)day << 17);
ts|=(( INT 32U ) hr  < < 1 2 ) | ((INT32U)min << 6)|(INT32U)sec;
```

The time and date also can be gained through system timer or other methods.

The tendency of IC card encryption technology

Due to the limitation of CPU and memory capacity, 3DES arithmetic is the best choice of IC card encryption/decryption system. But it can be expected, more ideal public cryptosystem can be in used with more powerful CPU and large capacity of storage, such as the RSA (asymmetric encryption algorithm or public key cipher algorithm).

Card manufacturer may set sensing network on the outside of the chip when the card is produced, when detecting the attack on card, it should immediately turn to chip self-destruct or effective protection status. Also a electromagnetic shield layer could be added around the integrated circuit, which can avoid information leaks caused by electromagnetic radiation, and can also ensure that the chip is not affected by external interference signal.

Personnel management should become the core of the management system. Improving the management system, strengthening safety education and safety supervision , especially improving the quality of the staff, carrying out responsibility system of personnel can reduce the possibility of internal crime.

The use of IC card becoming more and more popular, so the security problem it will faced with is more and more complex, the measures above can prevent attacks to card system to a certain extent, but the IC card security is still a process of finding problems and solving the of problem constantly.

References

[1] J. ZHANG ,H. ZHANG. Design and Implementation of Sales Management Information System. Modern Applied Science, 2009, (01): 23-25

[2] R. BARSKAR, A. J. DEEN, Y. BHARTI. The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology .International Journal of Computer Science and Information Security, 2010, (06): 307-312

[3] L.ZHANG, J.S.JIANG, L.N.LIU. Design of Field Irrigation Multi-purpose Control Device Based on Idle Work Compensation. International Journal of Image, Graphics and Signal Processing, 2011, (03): 38-44

[4] R. BARSKAR, A. J. DEEN, Y. BHARTI. The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology .International Journal of Computer Science and Information Security, 2010, (06): 307-312