Pisco Med Publishing

# Research on Data Encryption Technology

**Hongjiang Duan, Weilong Huang, Guangxu Zhu**

Information Technology Engineering College, Foshan University of Science and Technology, Guangdong, China

***Abstract:*** Data cryptography is the core technology of network and information security. Its basic design idea is to use the carrier form (called cipher text) after the various transformations (called encryption algorithm) to send the message (plaintext) For the storage and transmission, the authorized recipient with the corresponding transformation (known as the decryption algorithm) to restore the plaintext, the illegal interceptors are not visible or understand the plaintext, so as to achieve the purpose of information security.

***Keywords*:** Plaintext; Encryption Algorithm; Cipher Text; Decryption Algorithm

# 1. Introduction

## 1.1 Background of the times

In the information age, information security issues are increasingly important. We often need a measure to protect our data, to prevent some people with bad intentions to see or destroy. Therefore, there is a need for a strong security measure to protect confidential data from theft or tampering. The way to solve this problem is data encryption. An encrypted network, not only to prevent unauthorized users of eavesdropping and network, but also to deal with malicious software, one of the eff ective ways. In some cases, users may need to encrypt some confidential files, not because they want to transfer the file on the network, but worry about someone stealing a computer password to obtain the confidential file. Identity authentication is based on encryption technology; its role is to determine whether the user is true. In the transmission process to encrypt the data, you can protect the data in the transmission process security. Network security requires confidentiality, integrity, availability, can be achieved using cryptographic techniques. It can be said that cryptography is one of the practical means of protecting information on large-scale communication networks[1].

## 1.2 The meaning of the times

With the rapid development of modern information and the popularity of the network, people cannot go out to understand the world events and learn some important information. At the same time, the negative impact: people in this rapid development today no longer have their own secret, has become a 'naked'. For our personal privacy is not leaked, so to protect their personal information. So the encryption of the data is very important to us, the data encryption can be used in various fields, it aff ects all aspects of our lives.

# 2. Data encryption

## 2.1 Overview of cryptography

Cryptography[2] is an ancient and esoteric discipline, for the average person is very strange. For a long time, only in a very small range, such as military, diplomatic, intelligence and other departments. Computer cryptography is a science that studies the encryption, decryption and transformation of computer information. It is an interdisciplinary subject of mathematics and computer. It is also a new discipline.

Copyright © 2019 Hongjiang Duan *et al*.
doi: 10.18282/ics.v1i1.590
This is an open-access article distributed under the terms of the Creative Commons Attribution Unported License (http://creativecommons.org/licenses/by-nc/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of computer network and computer communication technology, computer cryptography has received unprecedented attention and has been rapidly popularized and developed. In foreign countries, it has become the main research direction of computer security. The history of cryptography is relatively long. Four thousand years ago, the ancient Egyptians began to use the password to keep the message secretly. Two thousand years ago, King Julius Caesarea (Caesar) began to use the current password system called 'Caesar Password'. But the password technology until the 20th century, 40 years after a major breakthrough and development. Especially in the late 1970s, due to the widespread use of computers and electronic communications, modern cryptography has been unprecedentedly developed.

## 2.2 Messages and encryption

Encryption and decryption can be translated into 'Encipher' and 'Decipher', and can be named: 'Encrypt' and 'Decrypt' The

The message is called plain text, and the process of using a method to disguise the message to hide its contents is called encryption[3]. The secret message is called cipher text, and the process of converting the cipher text into a plaintext is called decryption. The process of encryption and decryption is shown in **Figure 1** below:

The plaintext is represented by M (Message, Message) or P (Plaintext), which may be a bit stream, a text file, a bitmap, a digitized speech stream, or a digitized video image.

Cipher is expressed in C (cipher), but also binary data, sometimes as large as M, sometimes slightly larger. By combining the compression and encryption, C may be smaller than P.

The encryption function E acts on M to get the cipher text C, expressed as a mathematical formula:

E (M) = C (1)

The decryption function D acts on C to produce M, expressed as a data formula:

D (C) = M (2)

First encrypted and then decrypt the message, get the original plaintext, with the data formula expressed as:

D (E (M)) = M (3)

The nature of cryptography

In addition to providing confidentiality, cryptography needs to provide three functions: authentication, integrity, and non-repudiation. These functions are through the computer for social communication, is an important social needs.

Identification: The recipient of the message should be able to confirm the source of the message; the intruder cannot disguise himself.

Integrity: The recipient of the message should be able to verify that the message was not modified during the transfer; the intruder could not use a fake message instead of a legitimate message.

Anti-repudiation: It is impossible for a sending message to falsely deny the message he sent.

# 3. Key and algorithm

## 3.1 Key

K can be an arbitrary value in many values, and the range of possible values for key K is called the key space [4]. Encryption and decryption operations use this key, that is, the operation depends on the key, and K as the subscript expression, encryption and decryption function expression:

EK (M) = C (4)

DK (C) = M (5)

DK (EK (M)) = M (6)

Some algorithms use diff erent encryption keys and decryption keys, that is, the encryption key K1 is diff erent from the corresponding decryption key K2. In this case, the encryption and decryption function expressions are:

EK1 (M) = C (7)

DK2 (C) = M (8)

## 3.2 Caesar plus decryption algorithm implementation

Julius Caesar uses a simple replacement password - called Caesar cipher. Caesar is first applied to the military (Gallic Wars), his replacement rules: each letter with the subsequent third letter to replace.

Caesar password can be described as follows:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

'Caesar password' code is implemented as follows

```
Import java. util. Scanner;
Public class Caeser {
Private String table; // Define the key alphabet
Private int key; // define the key
Public Caeser (String table, int key) {
// Generate a new Caesar algorithm based on diff erent alphabets and diff erent keys to achieve common purpose
Super ();
His. Table = table;
This. Key = key;}
Public String encrypt (String from) {
// Caesar encryption algorithm, passing in a plaintext string, returns a cipher text string
String to = '';
For (int i = 0; i <from. Length (); i ++) {
To + = table.charAt ((table.indexOf (from.charAt (i)) + key)% table. Length ());}
Return to;
Public static void main (String [] args) {
Caeser = new Caeser ('abcdefghijklmnopqrstuvwxyz', 3);
Scanner = new Scanner (System.in);
System.out.println ('Please enter the string to be encrypted');
String str = scanner. next Line (); // Enter the string
String result = caeser. encrypt (str); / / call the encryption method for encryption
System.out.print (result); // get the result
Vhfxulwb}}
```

## 3.3 Symmetry algorithm

Key-based algorithms usually have two types: symmetric algorithms and public key algorithms (asymmetric algorithms). Symmetric algorithms are sometimes called traditional cryptographic algorithms, and the encryption key can be derived from the decryption key, which in turn is established.

In most symmetric algorithms, the encryption and decryption keys are the same. The symmetric algorithm requires the sender and the receiver to negotiate a key before secure communication. The security of a symmetric algorithm depends on the key, and the leaking key means that anyone can encrypt and decrypt the message. The encryption and decryption of the symmetric algorithm is expressed as:

EK (M) = C (9)

DK (C) = M (10)

## 3.4 Public key algorithm

The encrypted key of the public key algorithm (asymmetric algorithm) is diff erent from the decrypted key, and the decryption key cannot be calculated from the encryption key or cannot be calculated at least in the time that can be calculated.

It is called the public key algorithm because the encryption key can be made public, that is, the stranger can encrypt the information with the encryption key, but only with the corresponding decryption key to decrypt the information. The encryption key is called a public key (referred to as public key), and the decryption key is called a private key (referred to as a private key).

The public key K1 is encrypted as:

EK1 (M) = C (11)

Public key and private key is diff erent; the private key K2 decryption is expressed as:

DK2 (C) = M (12)

## 3.5 DES algorithm

The National Bureau of Standards (ISO) began investigating data encryption standards for computer systems in other sectors other than the Department of Defense, which issued a notice to the public on May 15, 1973 and August 27, 1974.

Encryption algorithm to achieve the purpose of four points:

1) to provide high-quality data protection, to prevent unauthorized disclosure of data and unaware changes;
2) has a very high complexity, making the cost of deciphering more than possible benefits, but also easy to understand and master;
3) the security of the cryptosystem should not depend on the confidentiality of the algorithm; its security is based only on the confidentiality of the encryption key;
4) to achieve economic, eff ective operation, and applies to a variety of completely diff erent system applications;

January 28, 1997, the United States RSA data security company on the Internet launched a 'key challenge' contest, reward 10,000 US dollars, crack with

a 56-bit key encryption encrypted cipher text. Plan announced after the strong response from the network users. A programmer named Rocke Verser designed a key exhaustive search program that could be run over the Internet, organized a search operation called DESHALL, and thousands of volunteers joined the program. On the 96th day of the plan, the 140th day of the Challenge Plan, at 10:39 pm on June 17, 1997, Michael Sanders, the staff member of Inetz in Salt Lake City, USA, successfully found the key, which was shown on the computer 'The unknown message is: Strong cryptography makes the world a safer place'. DES algorithm [5] is the work: If Mode is encrypted, then use the Key to the data encryption, generate data password form (64) as the output of DES; if mode is decrypted, then use key to password data in the form of data decryption, restore the data to the form of code (64) as the output of DES results.

DES algorithm to achieve encryption requires three steps[6]:

(1) Change the plaintext. X0 = IP (x) = L0R0, where L0 represents the first 32 bits of x0, and R0 is the x2 of the 64-bit bit, and then the first 32 bits of x0 are represented by a replacement IP table for a given 64-bit plaintext x Represents the last 32 bits of x0.

(2) According to the rules iteration [7]. Li = Ri-1; Ri = Li + f (Ri-1, Ki) (i = 1, 2, 3 ... 16) The value of L0 and R0 has been obtained by the first step transformation, where the symbol '+' The operation is exclusive OR, f represents a permutation, is replaced by an S-box, and Ki is a bit block generated by a key choreography function.

(3) On the L16R16 use IP-1 for the reverse replacement, to get the cipher text y. The encryption process is shown in the figure

DES algorithm has a relatively high security, so far, in addition to exhaustive search method to attack the DES algorithm, but also did not find a more eff ective way. While the 56-bit key's exhaustive space is 256, which means that if the speed of a computer is one million seconds per second, it searches for a full key for nearly 2285 years The It can be seen that this is diffi cult to achieve, of course, with the development of science and technology, when the emergence of ultra-high-speed computer, we can consider the length of the DES key to grow some, in order to achieve a higher degree of confidentiality.

# 4. Office file encryption

## 4.1 Word document encryption

(1) To create a Word document, as shown in **Figure 3**

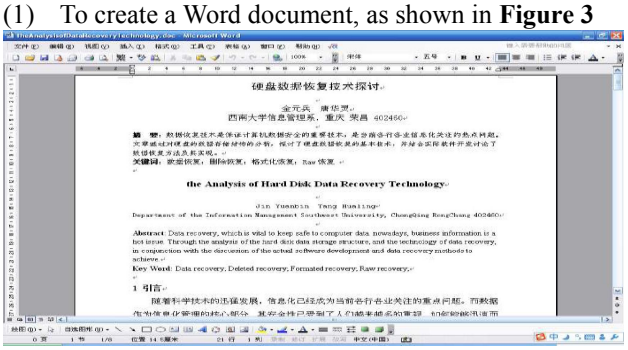


**Figure 3**; Word document establishment**.**

(2) Right mouse button, open the 'Tools' in the 'Options', click 'Security', set the password, the operation shown in **Figure 4** and **Figure 5**:

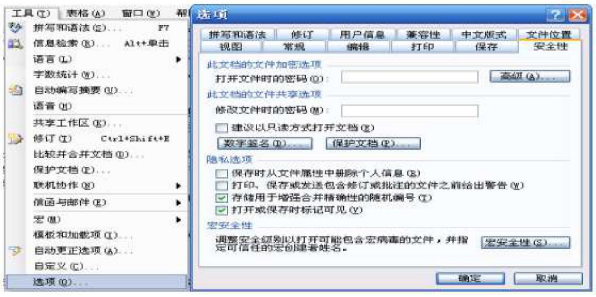

**Figure 4**; Tools and options**.**


**Figure 5**; Verification after password setting**.**

Office software is one of the most used software in daily work. In order to work better, familiar with offi ce software encryption and decryption, can help us work better, but also can eff ectively prevent our data

information is leaked.

Office software encryption and decryption is relatively simple, in the above I only for everyone to demonstrate the word encryption and decryption, the other commonly used ppt, excel and other software encryption and decryption process similar to the word, we refer to the word demonstration process can easily get their own The.

There are a number of related software, their ideas are generally used in a large dictionary of data cycle with the same algorithm encryption and password after the cipher text match, until the same time that has found a password. You can go to find these software, of course, some software is a back door, such as DOS under the WPS, Ctrl + qiubojun is a universal password.

# 5. Encryption software

## 5.1 Common fi le encryption and decryption tools

the king of encryption and decryption master 7.85;

(1) J. Hong folder encryption;
(2) password master V5.0;
(3) universal Encryptor V5.5;
(4) file password boxes 2012;
(5) PGP encryption software

PGP, full name: Pretty Good Privacy, is also a hybrid encryption system called. Usually only understood as the PGP company's series of software. Can be on the mail, files, folders, the entire hard disk encryption, the entire network segment encryption authority and access control.

PGP[8] can provide independent information protection on the computer, making the security system more complete. Its main function is: data encryption, including e-mail, any stored files and so on.

PGP's main function:

(1) Encrypt / sign and decrypt / verify in any software. With PGP options and e-mail plug-ins, you can use PGP functionality in any software.
(2) Create and manage the key. Use PGPkeys to create, view, and maintain your own PGP key pair; and add any person's public key to your public key library.
(3) Create a self-decrypting archives (SDA). You can create an auto-decrypted executable file. Any person does not need to install PGP in advance, as long as that the file encryption password, you can decrypt this file. This feature is particularly useful when you need to send files to people who do not have PGP installed. And, this function can also be embedded in the file compression, compression rate and ZIP similar to RAR slightly lower. In general, the function is quite good.
(4) Can create a pgd file, this file with PGP Disk function will be loaded, will appear in the form of a new partition, you can put in this partition need to keep any files. It uses the private key and password to share the two ways to save encrypted data, confidentiality indestructible, but need to pay attention to, be sure to reload the system before you remember to back up the 'My Documents' in the 'PGP' folder all the files, to reinstall your private key after reloading. Remember to remember that otherwise it will never be possible to open any encrypted files that were once created under the system!
(5) You can use the PGP crush tool to permanently remove those sensitive files and folders without leaving any data snippets on the hard disk. You can also use the PGP free space crusher to clean up the hard disk space that has actually been deleted.
(6) PGP can encrypt all the data on your entire hard disk, even the operating system itself. Provide a high degree of security, no password of the people is impossible to use your system or view the hard disk inside the files, folders and other data. Even if the hard disk is removed to another computer, the function will still faithfully protect your data, encrypted data to maintain the original structure, file and folder location will not change.
(7) This feature can be supported by the instant messaging tool (M, also known as instant messaging tools, chat tools) to send the information entirely through the PGP processing, and only have the corresponding private key and password the other party can unlock the contents of the message to anyone who intercepts does not make any sense, just a pile of garbled.
(8) Can use PGP to take over your shared folder itself and its files, the security is much higher than the operating system itself provides account

verification function. And it is easy to manage the actions that an authorized user can do. Greatly facilitate the need to often share files in the internal network of business users, from worms and hackers.

# 6. Encryption tips

In the process of using the computer, we are dealing with the password all the time. If you set the password by someone else guess or decipher, then it will lead to important information, personal privacy is leaked. So how to set a safe password is a major event associated with each. Here we introduce you to set the password in the process must comply with the ten military regulations[9].

(1) as long as possible;
(2) as unfamiliar as possible;
(3) as complex as possible;
(4) from the front to the previous order;
(5) easy to forget the password;
(6) do not use the same password;
(7) frequent replacement of the password;
(8) do not save the password;
(9) the correct password;
(10) the most important self-safety awareness;

# 7. Conclusion

With the continuous development of Internet technology and scale, the scope and field of its application in the continuous expansion and promotion of security issues, but also gradually become increasingly prominent. Especially in the financial, e-commerce, database areas, the security requirements are higher. On the basis of demand, with the traditional method to solve the security problem, there are great drawbacks. More and more users are aware of the importance of data confidentiality. Data sensitivity, confidentiality will have a means or method to solve, so the use of data and dissemination of encryption is very important, must greatly guarantee their encryption reliability and security.

But security is a combination of technology, management and regulation, and absolute security is not the only way to minimize the potential threat of the network through all eff orts. So encryption is the core of network security, file security, e-commerce security. Encryption algorithm, key management, field type processing problem is an important research topic of network database encryption and file encryption.

In this paper, the data confidentiality technology is studied under such a premise, and the key technologies of data encryption, encryption method, data encryption technology and data encryption are analyzed. After analysis and comparison, the advanced encryption technology is selected, encrypt the data. This will maximize the protection of our data security.

# References


1. SY Wang. Talking about data encryption technology [J]. Journal of Chaohu University, 2013 (6): 88-89.
2. Y Zheng, CS Yang. Encryption and decryption combat entry [M]. Beijing: Electronic Industry Press, 2006.
3. GP Zhang. Network security in the application of information encryption [J]. Consumer Guide, 2008.
4. [XY Xie, BF Wei. Analysis of network information encryption technology [J]. Technology Square, 2007 (5): 129.
5. YH Li. Application of DES encryption algorithm in data security protection in file transmission [J]. Hubei: School of Electric Power and Electronic Engineering, North China Electric Power University, 2012, (3): 06-009.
6. XL Cao. DES-based encryption algorithm [J]. Henan Vocational and Technical College, 2011, (4): 295-296,309.
7. J Li , XY Li. Data encryption in the DES encryption algorithm [J]. 2012, (2): 82-84.
8. XL Zhao. Network security technology course [M]. Beijing: National Defense Industry Press, 2014, (6): 93-95.
9. JW Hu. Network security and confidentiality [M]. Xi'an: Xi'an University of Electronic Science and Technology Press, 2013, (3): 112-114.