Research on the Design of Lower Computer of Data Encryption System

Honghui Lai, Juan Zhong

College of Information Engineering, Gannan Medical University, Ganzhou, Jiangxi 341000

hunter2011@foxmail.com

Keywords: Data Encryption System; Lower Computer; Encryption Algorithm

Abstract. In the modern information and network society, the data security is very important to our daily lives. The data encryption system can help us to protect the security of personal information. This paper mainly introduces the hardware and software design of the lower computer of data encryption system, involving the communication interface design, memorizer design, circuit design, algorithm selection and algorithm design. After system testing, it has high success rates of encryption and decryption and improves the programming speed.

Introduction of Data Encryption System

With the development of computer network technology, computer network has penetrated into all areas of people's life. It not only greatly facilitates the exchange of information, but also brings about some security hidden dangers of the information. Nowadays, the loss caused by information leakage happens every day in our lives, such as personal account information leakage, the outflow of private personal documents, etc. Thanks to the digital certificate in the banking industry vigorously promote, inspired by the author developed a similar individuals in U disk encryption system, can at any time encryption of user's sensitive data, for each of us information security escort. Data encryption is a category of cryptography, including encryption and decryption. Encryption refers to the system through specific cryptographic algorithms and keys for encryption plaintext data conversion to cipher text data, then the cipher text without any meaning, commonly known as garbled; decryption refers to the system through specific decryption algorithm and key to decrypt cipher text data into plaintext data, only specified by the user or network to the correct execution of the decryption algorithm. If the same data has been performed in the process of encryption and decryption, the obtained final data is exactly the same.

As the Fig. 1 shows, the design of data encryption system mainly involves the software design and hardware design of the upper computer and the lower computer. This paper mainly introduces the software and hardware design of the lower computer.

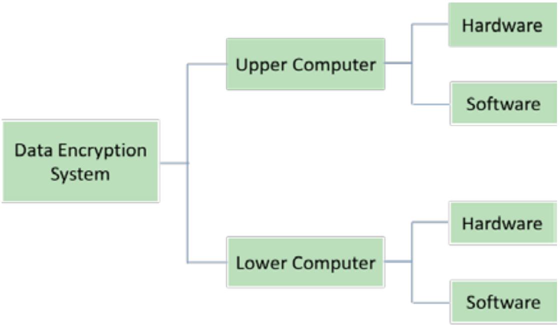

Fig.1 Content of the Design of Data Encryption System

Design Plan of Lower Computer of Data Encryption System

The core task of the lower computer is data processing. The hardware design of lower computer revolves around the single chip microcomputer, which mainly divides into three aspects: communication interface, memorizer and circuit. In order to make the design more practical, convenient, small, all of us use the current most popular USB interface communication, the host computer and the lower computer data exchange through the interface. If the independent design interface, it does not need to be equipped with the corresponding USB driver, in order to shorten the design cycle, this paper chose to bring a microcontroller C8051F340. In addition to having the general function of 51 single-chip, it comes with its own interface without its own development protocol to provide a microcontroller program and the host computer program development function library, which can directly call the library function, USB interface. With the C8051F340 microcontroller as the core, the hardware circuit design is very simple. Single chip microcomputer can be normal operation must design the peripheral circuit, including 3.3V power supply, design the external reset circuit. We connect two LED lights on the microcontroller. The first one stands for an indicator of whether the single chip is added; the other stands for an indicator of data transmission, when the USB in the data flow, the lights flashing. SCM program design by calling the software development kit, using C language to write function to realize the above functions including interface operation, and the host computer connection, send data, receive data, store data, call the encryption algorithm to deal with data. As the object of this paper is to design the object for individual users, it is necessary to use 3DES encryption algorithm, which has low cost and high encryption speed. In order to make the encryption speed faster, we use assembly language to write encryption function.

Hardware Design of Lower Computer of Data Encryption System

Communication Interface Design. In order to complete the function of the upper computer and the lower computer, the system is equipped with a RS-422 interface. RS-422 is a full duplex communication interface. The maximum transmission distance of up to 1200m and the maximum transmission speed can reach 10Mb/s. RS-422 interface is generally used to match the final resistance, but in the low rate and short distance cannot consider the terminal matching. RS-422 standard only on the interface electrical characteristics specified does not involve the connector, cable or agreement, so that the user can establish their own high-level communication protocol. RS-422 in order to achieve full duplex requires two channels, respectively, responsible for sending and receiving. The transmission channel is mainly composed of a transmitter and a balanced connection cable, etc. the receiving channel is composed of a receiver and a cable terminal load, etc. Because of the differential interface, each channel should be accounted for two of the signal lines. RS-422 communication interface in the system is used to transmit the control commands and parameters from the upper machine to the lower machine and transmit the return state parameters and operation results from the lower machine to the upper machine.

Memorizer Design. Considering the scalability of the system, the system needs to be equipped with memorize for the image processing algorithm. The DDR2 is high-speed and large capacity storage, which can provide a cost-effective solution, in the FPGA to achieve the DDR2 control, can reduce the system power consumption and development costs, shorten the development cycle. Therefore, the system can be disassembled and replaced the DDR2 memory module (SODIMM DDR2), that is, DDR2 memory. DDR2 (Data Rate Double 2) is a new generation of memory technology standards developed by the electronic equipment Engineering (JEDEC), which is the biggest difference between DDR2 and DDR, although it has been used in the rise and fall of the clock along the way data transmission, but it has two times the memory of the DDR. In addition, the DDR2 memory standard provisions of all DDR2 memory should be used to have better electrical performance and thermal performance of the FBGA package. So in the lower power and lower heat condition, DDR2 memory can get faster frequency, which lays a solid foundation for the lower machine memory function.

Circuit Design. Data encryption system needs to encrypt and decrypt the data in the microcontroller, so the core of the hardware device is C8051F340 microcontroller chip. The C8051F340 itself has a universal serial bus controller, and its own USB transceiver, pin settings, internal matching, pull resistance and so on are consistent with the USB2.0 specification, while in the project we just use the basic functions of the C8051F340 microcontroller, the circuit design is relatively simple, thus ensuring the stability of the system. In addition to ensure that the normal work of the external chip design, the only need to configure the USB connector, set the USB self-power supply and two LED light-emitting tube. In the C8051F340 microcontroller built in a voltage regulator, when it is enabled, to provide an external +5V power supply. The system selects the USB bus powered, to connect REGIN and VBUS, which is connected to a pin 11 and pin 12, and then connected to the USB pin 1 pin, to obtain the +5V voltage. Pin 10 requires external +3.3V voltage. +3.3V voltage is provided by an external regulator AS1117 chip, the chip is divided into three pins, wherein the 1 ground pins are connected to the ground; the +5V voltage is provided by the USB pin 1; the +3.3V output voltage of the is provided to the microcontroller 10. Pin 3 and the ground are connected with electrolytic capacitor to filter the interference.

Software Design of Lower Computer of Data Encryption System

Algorithm Selection. We select the encryption algorithm to realize the function that it can transmit the data to the cipher text that the outsiders cannot read the data, and then transferred to the right receiver. Encryption algorithm should also realize transmit the cipher text to plaintext data that the receiver can read the meaning. So even if the cipher text is intercepted, it is unable to read the information after the interception because the interceptor has no corresponding decryption algorithm. Encryption algorithm has two major categories. A class is used earlier not based on the key, the premise of this algorithm is confidential, as countersign a truth, the disadvantage is obvious if the algorithm is disclosed or decoded, then it is not available. Another kind of nature is based on the key, which is what we are now commonly used. Key is generated by the algorithm, the algorithm is open, but key is a secret, so only for key, no change in the algorithm, so much more flexible. That security is guaranteed to fall on the key; the length of the key determines the security. Symmetric encryption and asymmetric encryption are two major classes of key based encryption algorithm. The previous chapters have talked about, here is not much. This paper introduces several commonly used encryption algorithms, and selects the encryption algorithm to encrypt the client.

DES is often called the data encryption standard, which is a very classic "symmetry" encryption algorithm. It is initially developed by IBM, which is developed as a data encryption standard by the United States. MD5 main purpose is to ensure that the information is correct, and so on. The concrete implementation process is like this: for example, I created a text file, and then generate a MD5 value. I released this file for others to download and use, when the download is not sure if this file is safe, and that it can be used to verify the virus, if the value of the same, then it is safe, if not the same, is to be modified, there is a danger in it. On the network there are a lot of MD5 small programs, mainly used to verify data integrity. This shows that the MD5 application is more extensive, its security and reliability are also more mature. At present, the most of the RSA public key encryption algorithm is proposed in 1977. Its developers are three young students in the United States. They were using a number theoretic structure asymmetric key, because of its unique advantages, popularization and later called RSA cryptosystem. The RSA algorithm is also called by their name. It is clearly not a symmetric cryptosystem due to the double keys.

Algorithm Design. Encryption program is an existence of the function named DES (). After the completion, the program has to be downloaded to the microcontroller running. Encryption algorithm uses DES encryption algorithm and the deformation of the 3 DES encryption algorithms. The program calls the function DES () three times, has used a different key, enhanced encryption strength. DES encryption algorithm for the 64 bit encryption, the key is up to 64, after dropping 8, the effective key is 56, that is, 8 characters. If you want to be cracked, it is only the 256 time you can try to enumerate the entire key, which is not difficult for the current supercomputer.

In this paper, we use three DES, that is, the clear text is used different key encryption for three times, such an effective key for 168, a total of 24 characters. If you try to break the code, you must try 23 x 56 (2168) a key, so that the password strength has increased a lot of times, can effectively prevent violence. Three DES is a very popular DES algorithm deformation, in the network security, data transmission and other aspects of a wide range of applications, simple and easy to use, low-cost, low hardware requirements. The encryption process has a standard DES deformation. K1, K3, DES are independent 64 bit key, each containing 8 characters, respectively for the encryption, 1 and 2 K2, the final text in the program design, only call three DES () function. Three the decryption process of the heavy DES and the encryption process are inverse operation, we must still use K1, K2, and K3 64 three bit key. The cipher text is 2, the key K2 is encrypted by the key K3, and the key K1 is 1, which is the original text. Each decryption process is the decryption process of DES algorithm. Because the DES algorithm is a symmetric encryption and decryption algorithm, so the DES encryption and decryption implementation method is almost the same, only one difference, namely in the round of 16 key shift operation, after expansion transformation of 48 bit plaintext and after compression permutation of 48 bit key to XOR calculation. In the encryption, the I wheel is shifted to the I round of the express and the next to the I wheel; however, the I wheel is displaced by the I wheel and the key of the 17-i wheel is used. In the program design, encryption and decryption need the same procedure, that is, DES () function. The procedures of the encryption and the decryption is 16 rounds of the “if” statement.

System Test

After the design of the data encryption system, the running environment, the stability and the execution speed of the system are tested. The results show that the whole system design is reliable, stable and two-way communication smooth. The success rates of encryption and decryption are high and have achieved the anticipated results. As the Tab. 1 shows, the improved DES encryption algorithm has increased the programming speed by 20% compared with the traditional DES implementation method.

Table 1 Speed Comparison

File Type	Size of the File	Processing Time(second)	
		DES	Improved DES
MP3	3.10M	7	4
EXE	6.34M	13	9
ZIP	899M	400	340

References

[1] X. Zhao. Analysis and Improvement of Data Encryption Algorithms. Harbin Institute of Technology, 2012.

[2] Y.H. Meng, Y.X. Wang, T.Y. Ni. Design and implementation of data encryption systems. Journal of Shenyang University of Technology, 2009, 06: 340-343.

[3] X.Z. Zhao, Y.J. Xi. Research on Data Encryption Algorithm on Basis of Chaos Theory. Computer Simulation, 2011(28)2:120-123.

[4] Y. Li. Research on Data Encryption Decryption in Mobile Application. Coal Technology, 2013, 32(4):185-187.

[5] J. Shi, Z. Wu, L. Tan, H.P. Wang, N. Wang. Analysis and Improvement of RSA Data Encryption Algorithm. Journal of University of Jinan (Sci. & Tech.), 2013,27(3): 283-286.

[6] X.C. Wang. The Application of the Data Encryption Technology in the Network Communication Security. Software Guide, 2011, 10(3): 149-150.