Encryption and Decryption by using RC5 And DES Algorithms for Data File

Hnin Yu Wai, Khine Myat Nwe
University of Computer Studies, Magway
hninyuwai.cumg@gmail.com , khinemyatnwemdy@gmail.com

Abstract

Today, it is important that information is sent confidentially over the network without fear of hackers or unauthorized access to it. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. The proposed cryptographic system is reconfigurable for the number of block bits and the number of cryptographic rounds. In this system, many files types can encrypt and decrypt by using RC5 and DES algorithm. The secret key of DES is transformed into 16 sub keys and consequently DES takes 16 rounds to perform an encryption. For RC5 algorithm, rounds key is more than 16. But this system uses just only 16 rounds. In this system shows the tables and has included different time for DES and RC5.

1. Introduction

Today more and more sensitive data is stored digitally. Bank accounts, medical records and personal emails are some categories that data must keep secure. The science of cryptography tries to encounter the lack of security. Data confidentiality, authentication, non-reputation and data integrity are some of the main parts of cryptography. The evolution of cryptography drove in very complex cryptographic models which they could not be implemented before some years. The use of systems with increasing complexity, which usually are more secure, has as result low throughput rate and more energy consumption. Encryption is the process of converting from plaintext to ciphertext. Decryption is the process of restoring the plaintext from the ciphertext. Symmetric key cryptosystems are much faster than public key cryptosystems. The system is that many files are encrypted, transferred and decrypted between the network computers for the network security by using the block cipher encryption algorithms, DES and RC5. It transfers the secret file from one computer and another within the network. And then the files are encrypted and decrypted in only computer and processing times are saved. So it displays the encryption and decryption time of each encryption algorithm to study the variety of the processing time.

2. Cryptography

A cryptographic algorithm, also called cipher, is the mathematical function used for encryption and decryption. Modern cryptography can be divided into two main subfields of study: Symmetric-key (private key) and Asymmetric-key (public key) cryptography. Symmetric-key can be divided into block ciphers and stream ciphers. Asymmetric-key algorithms are RSA and others. Block Cipher consists of five majors algorithms. They are RC2, AES, DES, Blowfish and RC5 algorithms. Stream Cipher consists of RC4.

2.1 Symmetric Cryptography Algorithms

The terminology of symmetric cryptography algorithms mainly includes the following:

(i)Plaintext: Plain text is the ordinary information which the sender wishes to transmit to the receiver(s) [6].

(ii)Cipher text: The encrypted text is called Cipher text.

(iii)Encryption and Decryption: Encryption is the process of converting plain text into ciphertext. Decryption is the reverse process, moving from ciphertext back to the original plain text.

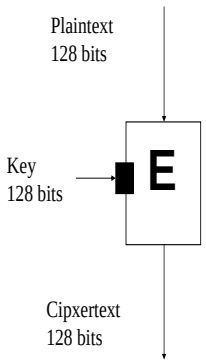

Figure 1: A Typical Encryption Procedure

(iv) Cipher: A cipher is a pair of algorithms which ensure the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and by a specific key.

(v) Key: The key is a secret parameter for encrypting or decrypting a specific message exchange context. Keys are important, as ciphers without keys are trivially breakable and therefore less than useful for most purposes.

2.2 Block Cipher

The block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plain text data into a block of cipher text data of the same length. This transformation takes place under the action of a user-provided secret key. Decryption is performed by applying the reverse transformation to the cipher text block using the same secret key. The fixed length is called the block size and, for many block ciphers, the block size is 64 bits [2].

2.3 Stream Cipher

Stream ciphers are typically much faster than block ciphers [6]. A stream cipher generates a key stream (a sequence of bits or bytes used as a key). The plaintext is combined with the key stream, usually with the XOR operation.

Generating the key stream may be independent of the plaintext and ciphertext, to give a synchronous stream cipher. Alternatively it may depend on the ciphertext, in which case the stream cipher is self-synchronizing. Nearly all stream cipher is of the synchronous type.

3. RC5 and Data Encryption Standard (DES)

3.1 RC5

In, R.Rivest proposes RC5 block cipher, which is a value transformation cipher. The RC5 encryption algorithm is a fast symmetric block cipher suitable for hardware or software implementation. A noval feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable word size, a variable number of rounds, and a variable-length secret key. The encryption and decryption algorithms are exceptionally simple [3].

3.1.1 RC5 Algorithm

The RC5 algorithm, which consists of three components: a key expansion algorithm, an encryption algorithm, and a decryption algorithm. We present the encryption and decryption algorithms first.

Recall that the plaintext input to RC5 consists of two w-bit words, which we denote A and B. Recall also that RC5 uses an expanded key table, S [0...t−1], consisting of t = 2(r+1) w-bit words. The key-expansion algorithm initializes S from the user's given secret key parameter K [4].

RC5 uses only the following three primitive operations (and their inverses).

1. Two's complement addition of words, denoted by "+". This is modulo- 2w addition. The inverse operation, subtraction, is denoted "−".
2. Bit-wise exclusive-OR of words, denoted by $\oplus$.
3. A left-rotation (or "left-spin") of words: the cyclic rotation of word x left by y bits is denoted x <<< y. Here y is interpreted modulo w, so that when w is a power of two, only the lg (w) low-order bits of y are used to determine the rotation amount. The inverse operation, right-rotation, is denoted x >>> y .

3.1.2 RC5 Encryption

In this system**,** the input block is given in two w-bit registers A and B. We also assume that key-expansion has already been performed, so that the array S [0...t−1] has been computed.

Encryption algorithm

A = A + S [0];
B = B + S [1];
for i = 1 to r do
A = ((A $\oplus$ B) <<< B) + S [2 ∗ i];
B = ((B $\oplus$ A) <<< A) + S[2 ∗ i + 1];

The output is in the registers A and B. In figure 2 shows RC5 algorithm [8].

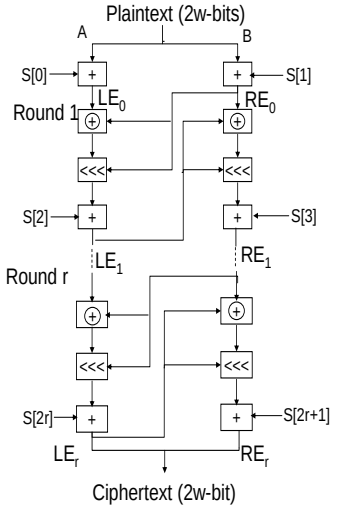

Figure 2: RC5 Encryption

3.1.3 RC5 Decryption

The decryption routine is easily derived from the encryption routine. In figure 3 shows the RC5 Decryption [8].

Decryption algorithm

for i = r down to 1 do

$B = ((B - S[2 * i + 1]) >>> A) \oplus A;$

$A = ((A - S[2 * i]) >>> B) \oplus B;$

$B = B - S[1];$

$A = A - S[0];$

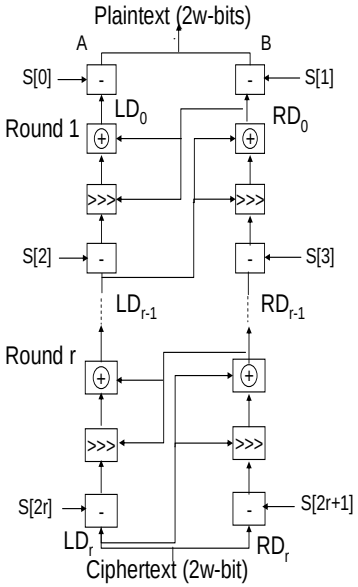

Figure 3: RC5 Decryption

3.2 Data Encryption Standard (DES)

In the case of DES, the block size is 64 bits (8 bytes) and the key is 56 bits presented as 8 bytes, the low order bit of each byte being ignored. It is usual to set every 8^{th} bit so that each byte contains an odd number of set bits. This process is known as DES key parity adjustment.

Most good block ciphers transform the secret key into a number of sub keys and the data is encrypted by a process that has several rounds (iterations) each round using a different sub key. The set of sub keys is known as the key schedule. In the case of DES the secret key is transformed into 16 sub keys and consequently DES takes 16 rounds to perform an encryption [7].

3.2.1 DES Algorithm

DES is a symmetric block cipher developed by IBM [7]. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1.

The algorithm is best suited to implementation in hardware, probably to discourage implementations in software, which tend to be slow by comparison. However, modern computers are so fast that satisfactory software implementations are readily available.

- **Key size:** The key originally consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective length is 56 bits, and it is usually used as such [5].
- **Block size:** The block size is 64 bits.
- **Rounds:** There are 16 rounds in the DES algorithms.

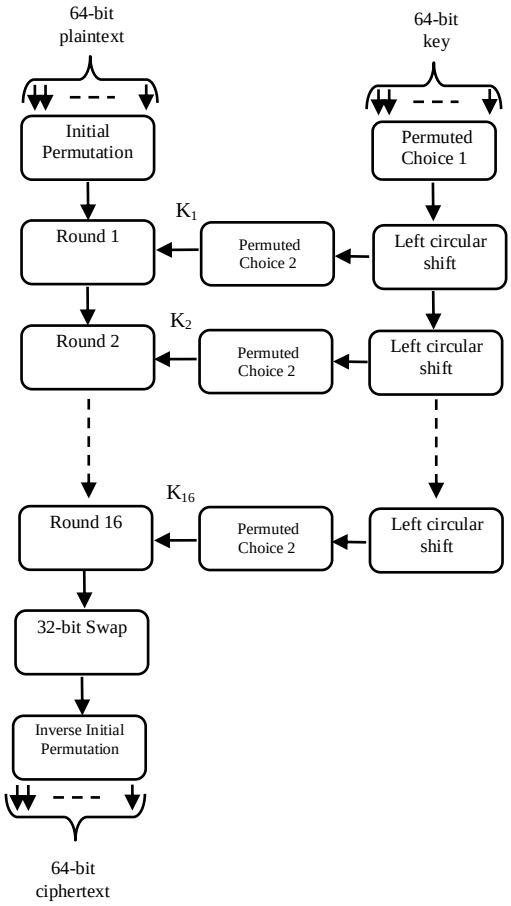

Figure 4: DES Encryption Algorithm

4. System Design

The fundamental design of the system is shown in figure 5.The system consists of file or folder to be processed and key, can choice DES or RC5 to encrypt and decrypt. Then using DES and RC5, can coding encrypt or decrypt. And then compare time for DES and RC5 display the result with table.

First, the user1 can choose any file and key to encrypt and then will send the encryped file to the user2. And then user2 accept encrypted file from the user1. The user 2 can decrypt using the same key and it shows the decryption time. Encrypted the any files are transferred from user 1 to user 2. Second, user1 can receive the encrypted file from the user2. Then, user1 can decrypt using the same key and it show the decryption time. So, user1 and user2 are same authentication.

The any files are encrypt/decrypt with secret key by using DES algorithm and it stores the encryption and decryption time. This file is encrypt/decrypt with secret key by using RC5 algorithm and it stores the encryption and decryption time. The any files are transferring between the network computers by using DES and RC5 algorithm. The most important transformation is the one that includes the secret key. The implementation can study the processing time for each encryption algorithm. Various file sizes are using any key for encrypt and decrypt. Each of file size is using any key for encrypt and decrypt.

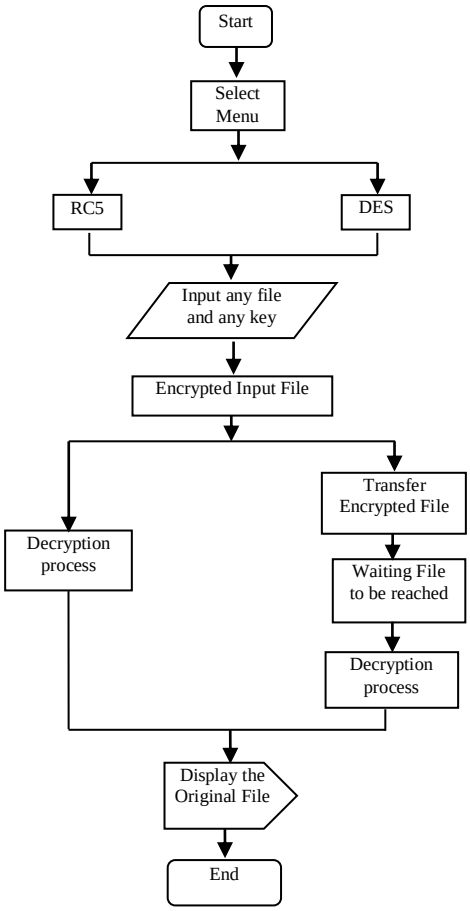

Figure 5: System Design

4.1 Using Input and Select DES or RC5

The input files are many file types such as Microsoft Word, Excel, MP3 and PDF and so on. Using inputs files, can select for encryption and decryption by using DES and RC5 algorithms.

4.2 File Transfer

This page is file transfer page. If the user1 want to transfer the encrypted data file to the user2. Click 'Browse' button and user1 can be chosen the encrypted file. User1 wants to type the user2's IP address then click the 'Send File' button. Then "Connected to sever" box is display.

Figure 6: File Transfer Box

Click the 'Send File' button if user1 and user2 are connected. Then click 'OK'.

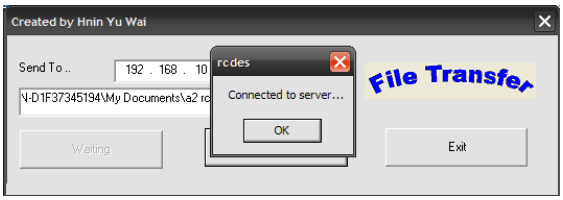

Figure 7: Connect to sever

Display the File Send box then click 'OK'. User1 can be send file.

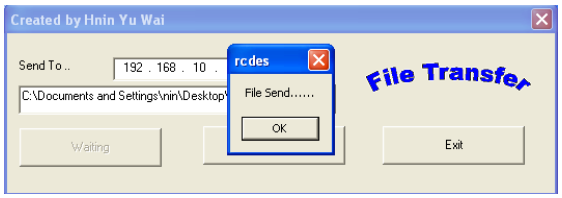

Figure 8: File Send Box

4.3 File Receiver

Figure 9 shows the file received. After the transferred from the user1 click "Waiting" button.

Then display the Server Started box. Click " OK '' button.

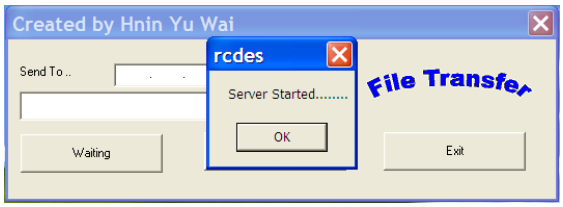

Figure 9: Server Started

In user2, shows File Received box. Click 'OK'. User2 can be received file from the user1.

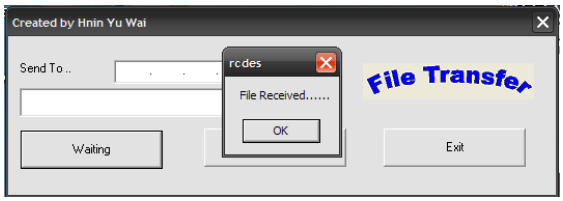

Figure 10: File Receive

4.4 Comparison Time for DES and RC5

In tables, show the compare time for DES and RC5 algorithm.

In this system, any file types can be encrypted the performance of using RC5 and DES algorithm. And then shows the performance of RC5 quick better than DES for encryption time and decryption time. Finally, it is found that DES has low performance when compared with RC5 algorithm encrypt large file size used.

Table 1 Compare time for DES and RC5 of excel file

File Type	File Size(byte)	Encrypt		Decrypt	
		DES (ms)	RC5 (ms)	DES (ms)	RC5 (ms)
Excel	16384	93	78	93	78
Excel	16896	94	94	110	94
Excel	20480	125	78	109	94
Excel	23040	141	109	109	78
Excel	27136	125	94	110	79
Excel	29184	125	94	125	93
Excel	29696	125	94	125	94
Excel	27648	125	94	125	93
Excel	36864	141	94	140	94
Excel	53760	172	125	188	125

Table 2 Compare time for DES and RC5 of PDF file

File Type	File Size(byte)	Encrypt		Decrypt	
		DES (ms)	RC5 (ms)	DES (ms)	RC5 (ms)
PDF	30395	125	78	140	78
PDF	102225	297	140	297	141
PDF	173117	453	203	468	187
PDF	238283	610	250	609	250
PDF	309115	765	297	766	266
PDF	384234	937	328	953	312
PDF	551751	1328	437	1312	438
PDF	809282	1922	609	1937	625
PDF	823163	1984	657	1969	609
PDF	4003349	9125	2796	9172	2750

Table 3 Compare time for DES and RC5 of Word file

File Type	File Size(byte)	Encrypt		Decrypt	
		DES (ms)	RC5 (ms)	DES (ms)	RC5 (ms)
Word	21504	125	78	110	62
Word	24576	109	78	125	62
Word	25088	109	79	110	62
Word	26112	109	78	109	62
Word	27648	109	63	125	78
Word	30720	125	28	125	79
Word	71168	218	109	235	109
Word	93696	266	125	266	125
Word	138752	391	172	375	141
Word	462848	1141	359	1125	375

5. Conclusion

The performance of symmetric key cryptography that is implemented using only blocks cipher algorithms. Symmetric algorithms are faster and easier to be implemented than the asymmetric key algorithms but need to manage two or more keys for every different communications. If user is typing to read a secret message that was not intended for user and don't know the encoding method, it is called "cracking" the code. The more cipher text user has, the easier it is to crack the code. The implementation is limited by few keys for time delay. Use of high performance networks to transfer data can enhance performance.

5.1 Limitation

In software implementation, the algorithm of RC5 round just only 16. To get better the performance of RC5 encryption, it can be used more than 16 time. Any files can be encrypted in this system.

5.2 Further Extension

One of the approaches to increase the performance of symmetric key cryptography is focused on the algorithm and hardware. Another related effort adds instruction set support for fast substitutions, permutations, rotates, and modular arithmetic. Choosing a larger number of rounds presumably provides and increased level of security.

References

[1] Bengt Beckman, Codebreakers: Arne Beurling and the Swedish Crypto Program during World War II., ISBN 0-8218-2889-4

[2] Bruce Schneier**,** .Applied Cryptography - Second Edition., p 210-211, John Wiley & Sons, 1996, ISBN 0-471-11709-9

[3]Http://en.wikipedia.org/wiki/Public key_cryptography

[4]http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf

[5] National Bureau of Standards,Data Encryption Standard, FIPS-Pub.46. National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[6] www.cryptographyworld.com/concepts.htm

[7] www.cryptographyworld.com/DES.ht

[8] William Stallings,Cryptography and Network Security Principles and Practices, Third Edition.