International Journal of Computer Applications Technology and Research
Volume 8–Issue 08, 323-326, 2019, ISSN:-2319–8656
DOI:10.7753/IJCATR0808.1006

Performance Comparison of Symmetric Key Crypto System

Thet Naing Htwe
Information Technology Department,
Technological University (Kyaukse)
Mandalay, Myanmar

Nilar Htwe
Faculty of Information Science
University of Computer Studies (Mandalay)
Mandalay, Myanmar

Abstract: Security is the most challenging aspects in the internet and network applications. Internet and networks applications are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Data confidentiality and authentication are normally provided using cryptographic techniques. Cryptography is either based on symmetric keys or asymmetric keys. This paper provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and RC5. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. Based on implementation and study, runtime comparison between the symmetric cryptosystems has been made.

Keywords: Symmetric Key System, AES, DES, RC5,

1. INTRODUCTION

Symmetric Encryption algorithms play a primary role in information security. So this paper has surveyed the most common algorithms and standards available for the encryption of information in the digital form. An encryption algorithm would be useless if it is secure but takes long time in execution. The field of cryptography is becoming very important in today's times as information security is of absolute importance. Contemporarily more and more sensitive data is being stored on computers and transmitted over the Internet. We need to ensure security and safety of information.

Cryptography is used to protect data while it is being communicated between two points. Cryptography is either based on symmetric keys or asymmetric keys [1]. This paper analyzes and studies between the most popular symmetric cryptographic algorithms such as data encryption standard, advanced encryption standard, and RC5. Based on analyze and by doing experiment, runtime comparison between the symmetric cryptosystems have been made.

This paper is organized with five sections. The first section is introduction of the system. Section 2 explains theory of Cryptography. Section 3 explains symmetric algorithms used in this paper such as AES, DES and RC4. Section 4 describes the implementation of the system. Experimental result is explained in section 4 and the next section is conclusion of the system.

2. DOCUMENTS OF CRYPTOGRAPHY

Cryptography provides a number of security goals to avoid a security issue. Due to security advantages of cryptography it is widely used today. Two type of Cryptography: Symmetric and Asymmetric. This paper is concerned with Symmetric cryptography [5, 6].

2.1 Symmetric Algorithms

The Symmetric algorithms use the same key for encryption and decryption while asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key. Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. There are many cryptographic algorithms. This thesis analyzes and studies three of the most common symmetric algorithms DES, AES and RC5. [5]

The field of cryptography include the following items:

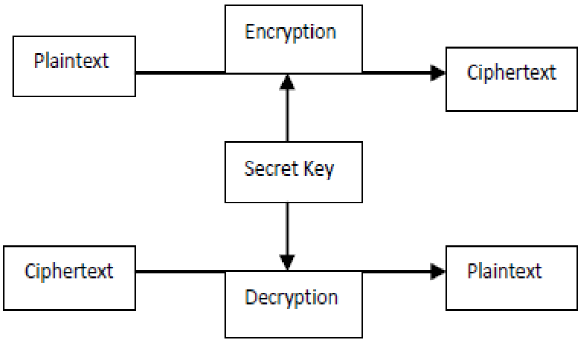

Figure 1 Symmetric Key Cryptography Process

2.1.1 *Plain Text*

The original message that someone wishes to another is defined as Plain Text. In cryptography the real message that has to be sent to the other end is given a special name as Plain Text. Suppose Alice wishes to send the message, *"We shall meet behind the monument in the garden."* to Bob. Here *"We shall meet behind the monument in the garden."* is the plain text.

2.1.2 Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, *"Jr funyy zrrg oruvaq gur zbahzrag va gur tneqra."* is a Cipher Text produced for *"We shall meet behind the monument in the garden."* after applying the Caesar's Cipher with key = 13.

2.1.3 Encryption

A process of converting Plain Text into Cipher Text is called Encryption. Cryptographers use various encryption methods to send confidential messages via an insecure channel. The process of encryption requires two things - an encryption algorithm and a key. An encryption algorithm means the method that has been used in encrypt the data. Encryption happens at the sender's side.

2.1.4 Decryption

The reverse process of encryption is called Decryption. It is the process of converting Cipher Text into Plain Text. Cryptographers use the decryption algorithms at the receiver side to obtain the original message from non readable message i.e. Cipher Text. The process of decryption requires two things - a Decryption algorithm and a key. A Decryption algorithm means the method that has been used in Decryption. Generally the encryption and decryption algorithm are identical but reverse.

2.1.5 Key

A Key is a string of alpha numeric characters, which is used to encrypt & decrypt the message. The Key is used at the time of encryption that works on the Plain Text and at the time of decryption works on the Cipher Text. The selection of key in Cryptography is vital as the security of encryption algorithm depends directly on it. For example, if Alice uses Hill Cipher & a key [11 10 20 09] to encrypt the Plain Text *"Gold is buried under the bush of Red Roses!"* then Cipher Text produced will be *"ymvnikdshwwdmxvsnrnudsihwntmvfwaqi"*.

2.1.6 Encoder

An encoder is the person that wants to send the message & uses encryption to make the message secure.

2.1.7 Decoder

A decoder is the person who decrypts the message. This may be the intended recipient of the message or may be an intruder, trying to get access to the secret message.

3. BACKGROUND STUDY

In this paper symmetric encryption algorithm is used for file transfer system. The security of this symmetric cryptosystem, should not rely on the confidentiality of the algorithm, it depends on the secret of keys [5, 6].

3.1. Data encryption standard (DES)

Data Encryption Standard (DES) DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process [3]. DES algorithm consists of the following steps

For Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will processed by following
   i. The key is split into two 28 halves
   ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
   iv. The rotated key halves from step 2 are used in next round.
   v. The data block is split into two 32-bit halves.
   vi. One half is subject to an expansion permutation to increase its size to 48 bits.
   vii. Output of step 6 is exclusive-OR'ed with the 48-itcompressed key from step 3.
   viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
   ix. Output of step 8 is subject to a P-box to permute the bits.
   x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

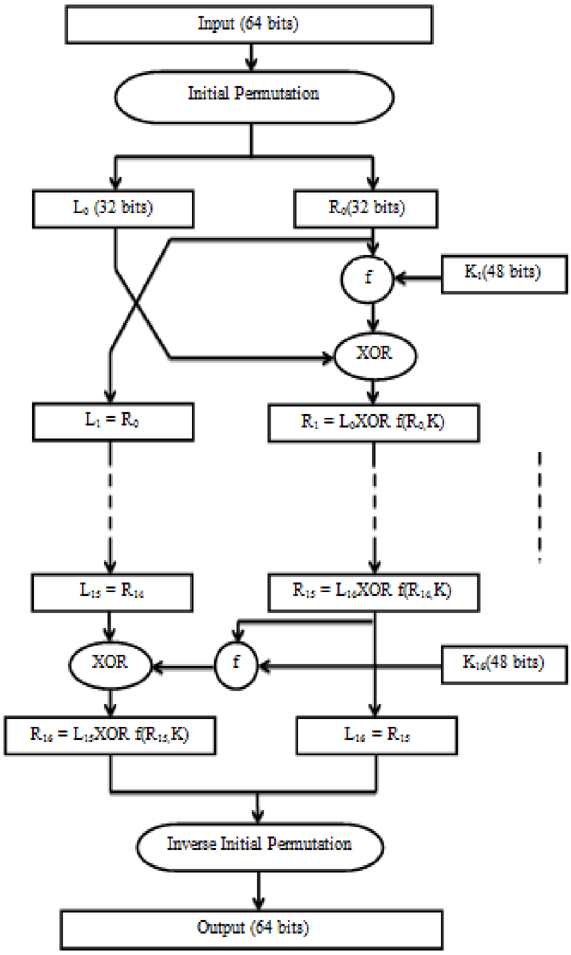

Figure 2 Diagram of DES Algorithm

3.2. Advanced Encryption Standard (AES)

AES algorithm uses a round function that is compared of four different byte-oriented transformation such as Sub byte, Shift row, Mix column ,Add round key. Number of rounds to be used depend on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys.

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm [4]. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the **Inverse Mix** Columns stage. Each of these stages will now be considered in more detail.

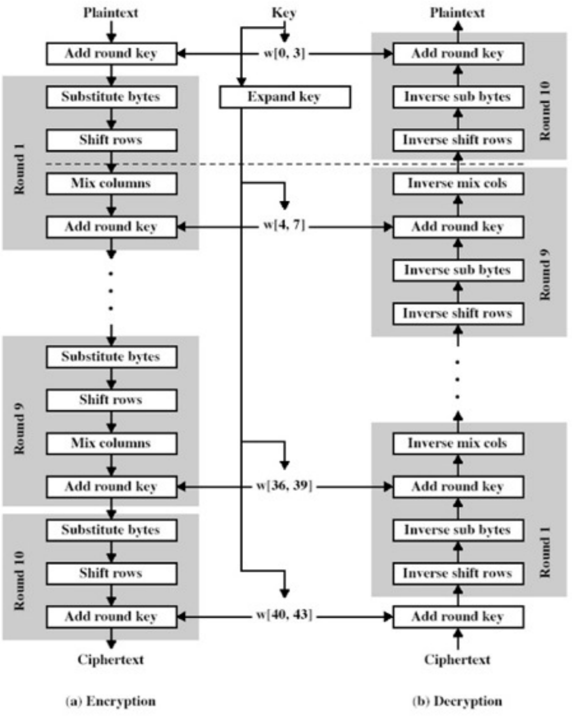

Figure 3. AES encryption and decryption

Figure 3 shows the overall structure of AES. The input to the encryption and decryption algorithms is a single 128-bit block. In FIPS PUB 197, this block is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix. These operations are depicted in Figure 3a. Similarly, the 128-bit key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words; each word is four bytes and the total key schedule is 44 words for the 128-bit key Figure 3b. Note that the ordering of bytes within a matrix is by column. So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the in matrix, the second four bytes occupy the second column, and so on.

3.3. RC5 symmetric algorithm

The RC5 encryption algorithm is a block cipher that converts plain text data blocks of 16, 32, and 64 bits into cipher text blocks of the same length. It uses a key of selectable length b (0, 1, 2, ..., 255) byte. The algorithm is organized as a set of iterations called rounds r that takes values in the range (0, 1, 2, ..., 255) as illustrated in figure 4.

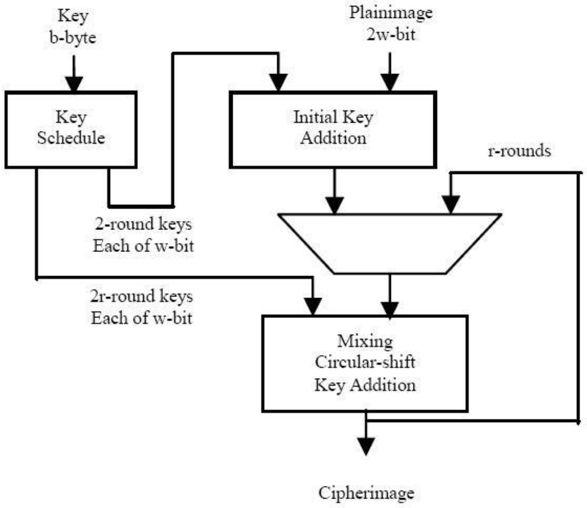

Figure 4 RC5 Encryption Algorithm

3.3.1 Operation of RC5

The operations used in RC5 are defined as followings.

1. A+B integer addition modulo 2w
2. A-B integer subtraction modulo 2w
3. A⊕B bitwise exclusive-or of w-bit words
4. A<<<B rotation of the w-bit word A to the left by the amount given by the least significant lg w bits of B
5. A>>>B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B

There are three routines in RC5: key expansion, encryption, and decryption [2, 5]. We discus each of them in next sections, Key-Expansion algorithm is used to generate the round sub keys that will be use in both encryption and decryption algorithms. RC5 has different algorithms for encryption and decryption, in encryption it uses integer addition modulo 2w but in decryption it uses integer subtraction modulo 2w. RC5 is a symmetric key encryption

4. IMPLEMENTATION OF THE SYSTEM

This paper describes the comparison of encryption time and decryption time of three popular symmetric key algorithms. In processing of three algorithms, it compares encryption and decryption time of various file sizes using DES, AES, and RC5 symmetric algorithms and then shows comparison results in table and in graph.

Method/File Size (KB)	150	192	306	852	1120
DES	2.9	3.1	3.3	4.1	5.4
AES	1.6	1.7	1.8	2.1	2.2
RC5	3.0	4.8	5.9	6.7	9.0

4.1 Experimental result

The experimental results of encryption and decryption time on various text files using DES, AES, and RC5 algorithms are shown in Table 1, Table 2 and Figure 5 and 6. Table 1 shows the results of comparing encryption time (s) on each various file sizes (KB) using three methods. Table 2 shows decryption time (s) for each various file size (KB). Figure 5 and Figure 6 show results by charts.

Table 1. Comparison of Encryption Time (s)

Method/ File Size (KB)	150	192	306	852	1120
DES	1.1	1.2	1.3	1.4	1.5
AES	1	1.4	1.6	1.8	2.1
RC5	3.1	3.7	4.1	4.7	5.1

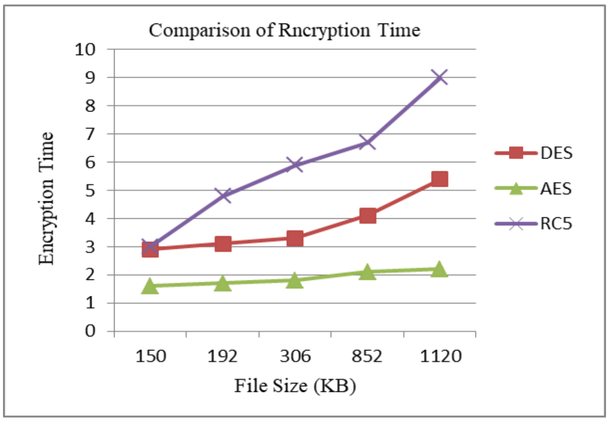

Figure 5. Comparison of Encryption Time

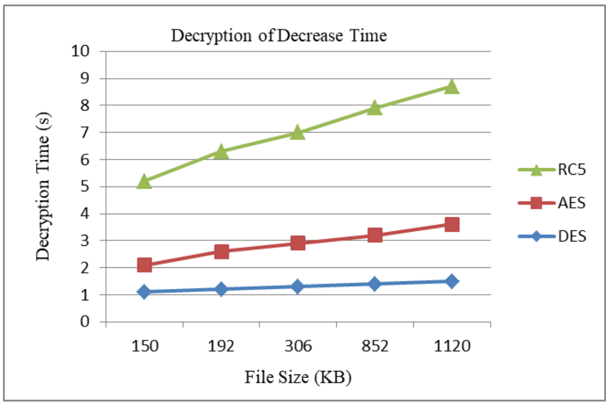

Figure. 6 Comparison of Decryption Time

5. CONCLUSION

This paper has investigated the comparison among the most popular symmetric algorithms. Among several algorithms, this paper describes the comparison of encryption and decryption time of DES, AES, and RC5 methods. After making several testing and comparing three techniques, encryption time is distinctly different but decryption time is not very different.

Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RC5 consume longest encryption time. We also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RC5 algorithm.

It can be used to learn cryptography and popular symmetric key algorithms, to learn comparing encryption and decryption time of these algorithms. It can be used for only text files format. So, it can be extended for audio file and image file formats and also compare for security point of view of three symmetric algorithms. the information has to be secured though transmit it, Sensitive information like ATM cards, banking dealings and public security numbers require to be secured. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very general method for promoting the information security. The development of encryption is moving towards a prospect of endless possibilities.

REFERENCES

[1] Ritu Tripathi, Sanjay Agrawal, Comparative Study of Symmetric and Asymmetric Cryptography Techniques, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

[2] Dr. Prerna Mahajan & Abhishek Sachdeva, A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA), Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[3] Abdel-Karim Al Tamimi, “Performance Analysis of Data Encryption Algorithms”.

[4] Andreas Sterbenz, Peter Lipp, “Performance of the AES Candidate Algorithms in Java”.

[5] William Stallings, *Cryptography and Network Security Principles and Practicle*, Fourth Edition

[6] *http://www.abo.fi/~ipetre/crypto/*