Performance Comparison with Symmetric key Cryptography

Kyaw San Win, Khin Kyu Kyu
Computer University, Kalay
kyawsanwincu@gmail.com, khinkyu28@gmail.com

Abstract

Today Cryptanalysis is used to secure dada for transmission over open networks such as the internet. The symmetric key is encouraging the use of larger key sizes and complex algorithms to achieve an unbreakable state. Symmetric key cryptography, also called secret key cryptography is a method that uses the same key for encryption of plaintext to generate the cipher text and decryption of the cipher text to get the original plaintext. In this system, performance of comparison with symmetric key cryptography is presented along the algorithm of AES (Advance Encryption Standard) and RC4 (Ron's Code4). AES and RC4 used the block, stream cipher method for encryption and decryption of file such as text file, word file, image file and media file. This paper compares the performance of stream cipher and block cipher with variable keys length and time.

1. Introduction

Since ancient times, encryption has been applied to protect information. In today's internet, the focus is on securing applications like e-commerce transitions, electronic mail, and file transfers. Cryptographic methods are the most popular methods for securing the messages. Cryptography is central to digital rights management (DRM), a group of techniques for technologically controlling use of copyrighted material, being widely implemented and deployed at the behest of some copyright holders. The application of cryptography security method for data is used in this system. There are two methods that are used in symmetric key cryptography: block and stream. The block method divides a large data set into blocks based on predefined size or the key size, encrypts each block separately and finally combines blocks to produce encrypted data. The stream method encrypts the data as a stream of bits without separating the data into blocks. Then the system analyzes the processing time of these algorithms.

2. Cryptography

Cryptography is the art of secret writing [4, Page 47]. It is also known as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it.

Person capable of unscrambling it. With the shear volume of sensitive internet transactions that occur daily, the benefit of securing information using cryptographic processes becomes a major goal for many organizations. Essentially, it becomes an issue of deterrence. Generally, all cryptographic processes have four basic parts:

Plaintext -Unscrambled information to be transmitted. It could be a simple text document, a credit card number, a password, a bank account number, or sensitive information such as payroll data, personnel information, or a secret formula being transmitted between organizations.

Cipher text - Represents plain text rendered unintelligible by the application of a mathematical algorithm. Cipher text is the encrypted plain text that is transmitted to the receiver.

Cryptographic Algorithm - A mathematical formula used to scramble the plaintext to yield cipher text. Converting plain text to cipher text using the cryptographic algorithm is called encryption, and converting cipher text back to plain text using the same cryptographic algorithm is called decryption.

Key - A mathematical value, formula, or process that determines how a plaintext message is encrypted or decrypted. The key is the only way to decipher the scrambled information.

2.1. Type of Cryptographic Functions

There are three kinds of cryptographic function: secret key functions, public key functions, and hash functions [3].

- Secret key cryptography involves the use of one key.
- Public key cryptography involves the use of two keys.
- Hash functions involve the use of zero key.

Secret Key Cryptography
In secret key cryptography also called symmetric-key cryptography, the encryption key can be calculated from the decryption key and vice versa. Most symmetric algorithms use the same key for both encryption and decryption, as shown below (figure 1).

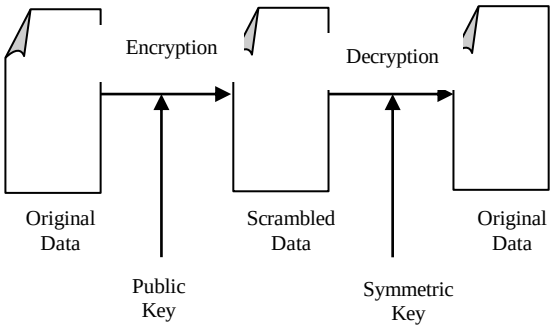

Figure 1. Secret Key Cryptography

The development of the public-key cryptography is the greatest and the only true revolution in the entire history of cryptography. From its earliest beginnings to modern times, virtually all cryptographic systems have been based on the elementary tools of substitution and permutation.

Public-key cryptography
Public-key cryptography also called asymmetric cryptography involves a pair of keys: a public key and a private key, associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret.) Data encrypted with your public key can be decrypted only with your private key.

Hash Function
Another special type of encryption is a hash (also known as a message digest or one-way function), which is a method where the enciphering the process is irreversible. The plaintext can never be recovered from the ciphertext. This may seem pointless but it is probably the form of encryption that is the most familiar to computer users.

A cryptographic hash function is a mathematical transformation that takes a message of arbitrary length (transformed into a string of bits) and computes from it a fixed-length number.

2.2. Method of Encryption

There are a variety of different types of encryption methods, they can be classified according to the way in which the plaintext to processed (which can be either stream cipher or block cipher), according to the type of operations used for transforming plaintext to ciphertext. The second class can be one of two styles, substitution and transposition.

Basically the two methods of producing ciphertext are stream cipher and block cipher. The two methods are similar except for the amount of data each encrypts on each pass.

3. Steam Cipher

Stream cipher is called synchronous if key stream does not depend on the plaintext. It depends on the key alone.

A typical stream cipher encrypts one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time. In Stream cipher structure, a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. A pseudorandom stream is one that is unpredictable without knowledge of the input key. The output of the generator, called a keystream, is combined one byte at a time with the plaintext, it stream using the bitwise exclusive-OR (XOR) operation. For example if the next byte generated by the generator is 01101100 and the next plaintext byte is 11001100, then the resulting cipher text byte is:

```
  11001100    plaintext
⊕ 01101100    key stream
  10100000    cipher text
```

Decryption requires the use of the same pseudorandom sequence:

```
  10100000    cipher text
⊕ 01101100    keystream
  11001100    plaintext
```

The stream cipher is similar to the one-time pad. The different is that a one-time pad uses a genuine random number stream, whereas a stream cipher uses a pseudorandom number stream. [9, Page 192]

3.1. RC4 Algorithm

RC4 is a stream cipher designed in 1987 by Rom Rivest for RSA Security. It is a variable key size stream cipher with byte- oriented operation. The

algorithm is based on the use of a random permutation.

RC4 is the most widely used stream cipher. It is used in the SSL/TLS (Secure Sockets Layer/Transport Layer Security) standards that have been defined for communication between Web browsers and servers. It is also used in the WEP (Wired Equivalent Privacy) protocol that is part of the IEEE 802.11 wireless LAN standard.

RC4 Initialization

1. j = 0
2. $s_0 = 0$, $s_1 = 1$, …, $s_{255} = 255$
3. Let the key be k_0, …,k_{255} (repeating bits if necessary)
4. For i= 0 to 255
   J = (j + S_i + k_i) mod 256
   Swap S_i and S_j

RC4 Key stream Generation

Generate an output byte B by:

1. i = (i + 1) mod 256
2. j = (j+ S_i) mod 256
3. Swap S_i and S_j
4. t = (S_i + S_j) mod 256
5. B = S_i

B is XOR with next plaintext byte

RC4 Steps

The steps for RC4 encryption algorithm is as follows:

1. Get the data to be encrypted and the selected key.
2. Create two string arrays
3. Initiate one array with the numbers from 0 to 255
4. Fill the other array with the selected key
5. Randomize the first array depending on the array of the key.
6. Randomize the first array within itself to generate the final key stream
7. XOR the final key stream with the data to be encrypted to give cipher text.

4. Block Cipher

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used[1]. Examples of block ciphers are DES, IDEA, Blowfish, AES - Advanced Encryption Standard etc.

4.1. AES

AES is based on a design principle known as a Substitution permutation network, it is fast in both software and hardware, is relatively easy to implement, and requires little memory. Unlike its predecessor DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits.

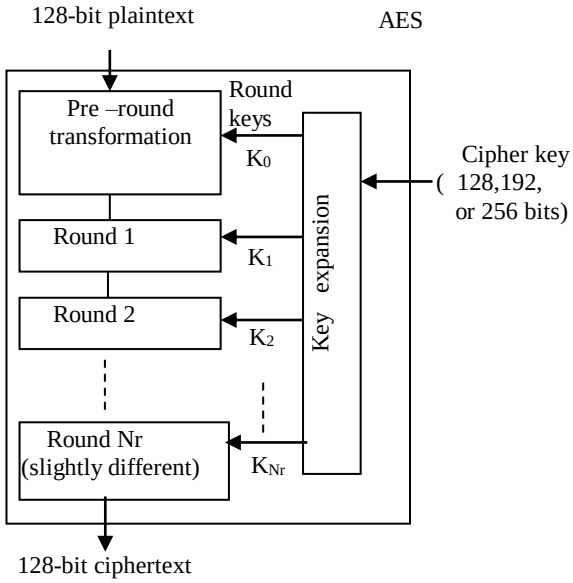

Figure 2. General Design of AES Encryption Cipher

Rijndael Pseudo-code

Rijndael with 10 rounds is described by the following code:

AddRoundKey(S,K[0]);
SubBytes(S);
ShiftRows(S);
MixColumns(S);
AddRoundKey (S,K[i]);
}
Sub Bytes(S);
Shift Rows(S);
Add Round Key(S,K[10]);
Nigel Smart - Frederik Vercauteren

`SubBytes` - a non-linear substitution step where each byte is replaced with another according to a lookup table.

`ShiftRows` - a transposition step where each row of the state is shifted cyclically a certain number of steps.

`MixColumns` - a mixing operation which operates on the columns of the state, combining the four bytes in each column

`AddRoundKey` - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

Final Round (no `MixColumns`)
`SubBytes`
`-ShiftRows`
`-AddRoundKey`

5. Proposed System

There are two main parts in this system; Comparison of Encrypt and Decrypt Time with single file with key. .

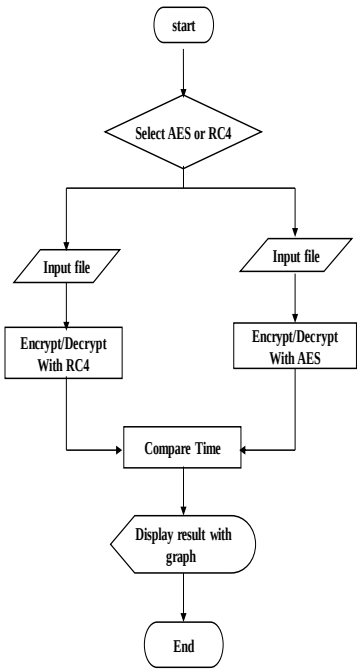

Figure 3. System Design

In this system, the input file is encrypted or decrypted with the symmetric key by using RC4 or AES two algorithms, This system implements only file encryption/decryption processes. By using this system is implemented for security and knowing about the cryptography and comparison between encryption and decryption time. The graph show with the result of the compare time.

5.1. Experimental Results

In this system, same key must be used for both encryption and decryption. This system is implemented over the single processor version. AES block cipher and RC4 stream cipher algorithms are used in this system.

The same file is encrypted and decrypted with two algorithms. Encrypt time and decrypt time of AES and RC4are nearly equal. As show in figure, execution time of RC4 is faster than AES.

Table 1.Time Comparison Result of System

File size (kb)	AES Encrypt/Decrypt (sec)		RC4 Encrypt/Decrypt (sec)	
24	94	125	47	47
54	125	266	94	94
9	47	47	31	16
1888	4359	9188	2766	2797
40956	91250	196828	59703	60094

The final result of the system is shown in figure 4 and figure 5. This figure is encryption and decryption time comparison by using AES and RC4 algorithms. In figures, show the stream cipher is faster than block cipher.

Figure 4. Encryption Time Comparison with AES and RC4

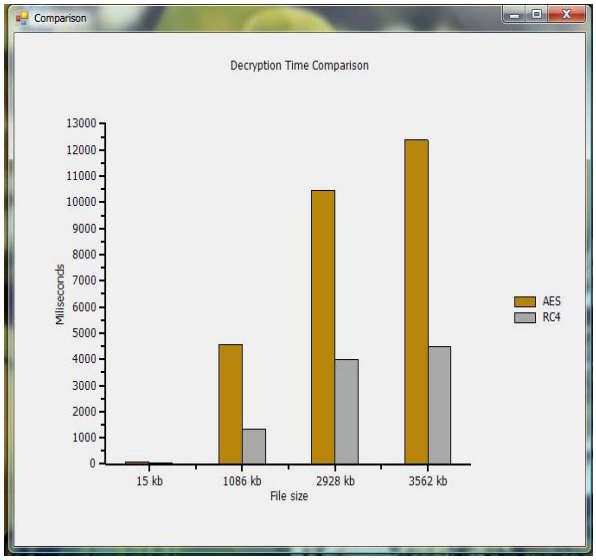

Figure 5. Decryption Time Comparison with AES and RC4

6. CONCLUSION

The goal of cryptography is to make it possible for people to exchange a message in such away that other people cannot understand the message. The performance of symmetric key cryptography is implemented using block cipher and stream cipher algorithms. The system is implemented over the single processor version of the symmetric key cryptography. The security analysis is limited by few keys for time delay. 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, general permutations, rotates, and modular arithmetic. The performance can be enhanced by using high performance networks to transfer data.

7. References

[1] Allam Mousa and Ahmad Hamad **"EVALUATI-ON OF RC4 ALGORITHM FOR DATA ENCRYPTION"** .

[2] Charlie Kaufman, Radia Perlman, Mike Speciner **"NETWORK SECURITY PRIVATE COMMUNICATION IN A PUBLIC WORLD" Second Edition**

[3] Martin Steinebach, Sascha Zmudzinski, Torsten Bölke, **"Audio Watermarking and partial encryption**", Fraunhofer IPSI, 64293 Darmstadt, Germany, University of Magdeburg, 39104Magdeburg, Germany

[4] William Stallings, **"Cryptography and Network Security"**, Second Edition

[5]AndrewnS.Tanenbaum,"COMPUTER NETWORKS" Fourth Edition, Prentice Hall, 2003.