

Implementation of Symmetric Encryption Algorithms

Haider Noori Hussain[*1] Waleed Noori Hussein[*2]
1.Department of Computer science , College of Education for Pure Science, University of Basra, Iraq
2.Department of Mathematics , College of Education for Pure Science, University of Basra, Iraq

Abstract
Cryptography considered being the most vital component in information security because it is responsible for securing all information passed through networked computers. The discussions in this paper include an overview of cryptography and symmetric encryption. This paper also discusses some of the algorithms used in our research. This paper aims to design an application that consist of some symmetric encryption algorithms which allow users to encrypt and decrypt different size of files, also the application can be used as a test field to compare between different symmetric algorithms.
Keywords: Cryptography, symmetric, encryption

1. Introduction

In today's technology, every second data are generated on the internet due to the online transaction. Cryptography is a necessary part of network security which allows the virtual world to be more secure. In many applications of our daily life information security plays a key role (Kumar and Munjal 2011). This applies even stronger for ubiquitous computing applications where a multitude of sensors and actuators observe and control our physical environment (Kumar and Munjal 2011). When developing such applications a software engineer usually relies on well-known cryptographic mechanisms like encryption or hashing. However, due to the multitude of existing cryptographic algorithms, it can be challenging to select an adequate and secure one (Masram, Shahare et al. 2014). A software engineer is not necessarily also an information security expert and, therefore, it is not obvious which one offers enough security. A general method to rank cryptographic algorithms by their strengths would mitigate this problem. With the availability of such a ranking, a software engineer can either look up the current ranking of an algorithm or perform the ranking himself to determine the current strength of such an algorithm (Masram, Shahare et al. 2014). Information may be reached by malicious hacker's .therefore, it is important to provide an effective encoding and decoding method to make sure all data are enhanced and secured. The authorization of accessing data in a network is involved with Network security, which is handled by the network administrator. Clients provide with or are assigned an ID and password or any other authenticating information which provide them access to any data and programs within their authority (Stallings 2006). Network security includes many different types of computer networks, which include public and private, they are used in every network security providing transactions and communications between businesses, government agencies, and individuals. Networks may be private, same as within an enterprise, and others which may be open to public access (Stallings 2006).

The aim of this paper is to investigate and evaluate some of the symmetric encryption algorithms through designing an application using C# programming language. This study evaluates ten symmetric algorithms namely; AES, DES, 3DES, RC6, Blowfish, RC2, Two Fish, Three Fish, Triple DES, and IDEA. The application will be able to encrypt and decrypt different size of files using different symmetric key encryption.

2. Cryptography : An overview

Nowadays, cryptography plays a major role in protecting the information of technology applications. Cryptography actually means secret writing, even the ancient human desire to keep and store secrets (Gupta 2012). In ancient days, cryptography was available only to generals and Emperors, but today it is nearly used by everyone, every day, every time when a credit card transaction is done, a phone call is made, secure website is used; there is a use of cryptography(Menezes, Van Oorschot et al. 1996) . It is nothing unexpected, then, that new types of cryptography came not long after the far-reaching improvement of PC correspondences. In information and telecommunication communications, cryptography is important when importing over any untrusted medium, which incorporates pretty much any system, especially the internet. In cryptography original message is basically encoded in some non-readable format. This process is called encryption. The only person who knows how to decode the message can get the original information (Aleisa 2015).This process is called decryption. Figure 1 shows the process of cryptography.

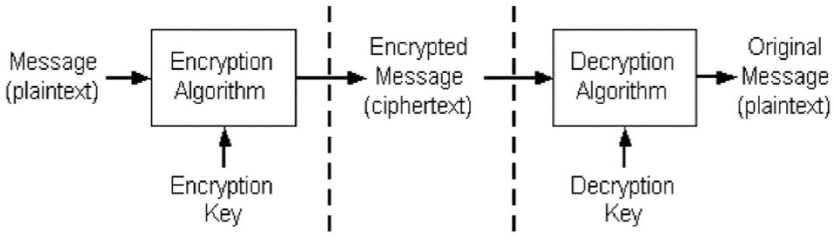

Figure 1: Cryptography process

There are main services provided by symmetric cryptography (Menezes, Van Oorschot et al. 1996, Dworkin 2001). All these services deal with storing or transmitting of data. These services are as follows:

- *Confidentiality:* keeping the data secret.
- *Integrity:* keeping the data unaltered.
- *Authentication:* to be certain where the data came from.

On the basis of key used, cipher algorithms are classified as (Surya and Diviya 2012):

- Asymmetric key algorithms (Public-key cryptography), where two different keys are used for encryption and decryption.
- Symmetric key algorithms (Private-key cryptography), where the same key is used for encryption and decryption.

On the basis of input data, ciphers are classified as (Surya and Diviya 2012):

- Block ciphers is used to encrypt data with a fixed size, and
- Stream ciphers, which encrypt continuous streams of data.

Classical ciphers used substitution and transposition for encryption and decryption (Dworkin 2001). The rotor machine is a device that is used to encrypt and decrypt secret messages. It is a stream cipher device and electro-mechanical in nature Performance of any encryption algorithms depends upon the mainly two things that are security and time required for encryption. Following are some of the parameters that can have effect on encryption time of the ciphers algorithms(Singh and Maini 2011):

a. Data type: There are various data types' files. Data type represents the encoding of the files. Common examples are as follows:
- Text: ANSI, UNICODE (16 & 32 bit little and Big Endian), UTF-8.
- Audio: WAV, AIFF, M4A, MP3, WMA, MP4.
- Video: AVI, MOV, MP4, MPEG, WMV, GIF.
- Images: JPEG, TIFF, GIF, BMP, PNG.
- Others: Medical Informatics Standard i.e. DICOM (Images/Binary + Text), HL7 etc.

b. Data size: is the space occupied by a file on a disk. Audio and video files take more space on disk than textual files as they contain multimedia information.

c. Data Density: Density of data represents the amount of different information present in the data. The more the information, the dense is the data and lesser the information, sparse is the data. For example if there are two files, X and Y, both contain 2000 words and having size 50kb and 200kb respectively, then file X is denser. The more the information, the dense is the data and lesser the information, sparse is the data. Sparse file is a file that contains most of the empty spaces and attempts to use the computer space more effectively(Singh and Maini 2011).

d. Key size of cipher algorithm: key size is the size of the key measured in bits and will depend on algorithm. For example AES is having key sizes 128, 192 and 256 bits.

e. Cipher block modes: In cryptography, block cipher mode for a block cipher algorithm indicates how ciphertext blocks are encrypted from plaintext blocks and vice versa. Commonly used block cipher modes are ECB, CBC, CFB, OFB, PCBC and CTR etc(Singh and Maini 2011).

3. Symmetric Encryption

Symmetric key cryptographic ciphers come in two types, stream and block ciphers. Stream ciphers work on bits stream or bytes stream. Stream ciphers are used for securing data of terminal and wireless applications. Block ciphers perform encryption or decryption on fixed size block of data (Curtmola, Garay et al. 2011). The plaintext is not always in multiple of the block size, therefore padding bits are needed to compensate partially filled block. The padding scheme defines how the plaintext is filled with data for the last block. In network applications block ciphers are used for transmission of files of huge sizes which require high security. Deciphering ciphertext without knowing the key is called cryptanalysis. Cryptanalysis of block ciphers is difficult compared to stream ciphers (Stallings 2006). Hence in most of the applications, block ciphers are used for providing better security than stream ciphers. The structure of the cipher algorithms describes the construction of blocks for the ciphers.

Mathematically linked series of operations are used in Substitution-permutation network in cryptography to construct the block of the Symmetric key cryptographic block cipher. Plain text is taken as an input and number of alternating rounds of S-Box substitution and permutation are applied to get a single ciphertext block. The reverse process is done for decryption of the blocks(Canright 2005). Symmetric key cryptographic ciphers have different structures that are used to construct the block of the different Symmetric key block ciphers. There are symmetric key structures like Feistel network, Substitution-permutation network etc (Curtmola, Garay et al. 2011).

In the case of feistel network, the encryption and decryption process of the block are almost similar to each other, except it requires the reversal of key schedule. Iteration is a characteristic feature of fiestel network cipher as an internal function knows as round function. Block ciphers come in various block modes. Block mode for cipher algorithm determines how ciphertext blocks are created by encryption from plaintext blocks and vice versa. ECB, CBC, CFB, OFB, PCBC and CTR etc. are commonly used block modes (Elminaam, Abdual-Kader et al. 2010). ECB has poor security properties since encryption of a block with a fixed size always yields the same result; hence susceptible to dictionary attacks, replay attacks etc. All other modes require an initialization vector while encrypting the first block and are considered to be more secure. If we are not using a random initialization vector, then CBC is also susceptible to dictionary attacks. Parallelization in encryption cannot be achieved with CBC mode(Kim, Lim et al. 2006). PCBC mode is similar to CBC mode with a little variation. In case of CBC first plaintext block is XORed with IV and remaining all plaintext blocks are XORed with previous ciphertext blocks; while in case of PCBC operation on first plaintext block is similar to CBC but remaining all plaintext blocks are XORed with previous plaintext as well as previous ciphertext block (Elminaam, Abdual-Kader et al. 2010). CTR acts as stream cipher and does not require additional padding bits. CTR provides better security with a 128-bit block, but its security is inadequate if 64-bit block is used without random nonce (initialization vector). Parallelization in encryption can be achieved with CTR mode. CFB and OFB are also streaming modes like CTR. In OFB mode, the last block of keystream is continually encrypted to produce key stream; while in CFB mode, the last block of ciphertext is always encrypted to produce key stream to encrypt next plaintext block. Streaming models are more prone to bit-flipping attacks (Curtmola, Garay et al. 2011). Table 1 shows the advantage and disadvantage of using symmetric encryption (Backes and Pfitzmann 2004, Agrawal and Mishra 2012).

Table 1: Advantage and disadvantage of symmetric encryption

Advantage	Disadvantage
Simpilisity:All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.	Need for secure channel for secret key exchange: Sharing the secret key in the beginning is a problem in symmetric key encryption.
Encrypt and decrypt your own files: There is no need to create different keys. Single-key encryption is best for this.	Too many keys: A new shared key has to be generated for communication with every different party.
Fast: Symmetric key encryption is much faster than asymmetric key encryption.	Origin and authenticity of message cannot be guaranteed: Since both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.
Uses less computer resources: Single-key encryption does not require a lot of computer resources when compared to public key encryption.	-
Prevents widespread message security compromise: A different secret key is used for communication with every different party.	-

There are different symmetric cryptographic algorithms in the literature (Masram, Shahare et al. 2014). Some of them are described below:

a. AES

Advance Encryption Standard (AES) algorithm was developed in 1998 by Joan Daemen and Vincent Rijmen, which is a symmetric key block cipher. AES algorithm, supports any combination of data and key length of 128, 192, and 256 bits. AES allows a 128 bit data length that can be split into four basic operational blocks. These blocks are considered as array of bytes and organized as a matrix of the order of 4×4 which is also called as state and subject to rounds where various transformations are done. For full encryption, the number of rounds used is variable N = 10, 12, 14 for key length of 128,192 and 256 respectively. Each round of AES uses permutation and substitution network and is suitable for both hardware and software implementation (Biham 1997).

b. Blowfish

Blowfish was first published in 1993.It is symmetric key block cipher with key length variable from 32 to 448

bits and block size of 64 bits. Its structure is a fetal network. Blowfish is symmetric block cipher that can be used as an informal replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and commercial use. Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. From then it has been analyzed considerably, and it is slowly gaining popularity as a robust encryption algorithm. Blowfish is not patented, has a free license and is freely available for all uses (Thakur and Kumar 2011).

c. DES

Data Encryption Standard (DES) is symmetric key block cipher. The key length is 56 bits and block size is a 64-bit length. It is vulnerable to key attack when a weak key is used. DES was found in 1972 by IBM using the data encryption algorithm (Thakur and Kumar 2011).

In this paper, ten symmetric algorithms have been evaluated to test their encryption and decryption through an application implemented in C# on Visual Studio. The application is able to encrypt and decrypt any type of file with different sizes. The application shows information such as time of encryption, time of decryption, memory used and speed.

4. Implementation

The encryption and decryption of AES, DES, 3DES, RC6, Blowfish, RC2, Two Fish, Three Fish, Triple-DES and IDEA algorithms were implemented in C# on Visual Studio based on different parameters such as Time complexity, speed memory encryption and decryption were measured on Intel(R) Core(TM) i7-4510U CPU @2.00GHz 64 bit system with 8 GB of RAM running Windows 10. The obtained results in the application will help us to study and analyse the efficiency of the symmetric encryption algorithm for the above-mentioned parameters. The implementation of symmetric algorithms involves following steps:

- Key Generation
- Encryption
- Decryption

Encryption and decryption can be done using any computer. The idea of an encryption is basically to secure the data held within a message or file and to ensure that the data is unreadable to others. The unencrypted message or file is often referred to as plaintext, and the encrypted message or file is referred as ciphertext. The encryption process contains a key length in a number of bits this key is used by ten encryption algorithms. In our implementation, the System.security.cryptography namespace was used to provide cryptographic services, which include secure encoding and decoding of data, as well as many other operations, such as hashing, random number generation, and message authentication. Many classes were included such as AesCryptoServiceProvider and AesCng. The encryption of different file types and size are implemented. The main screen of the application is shown in Figure 2 which include two option for encryption: file encryption and text encryption.

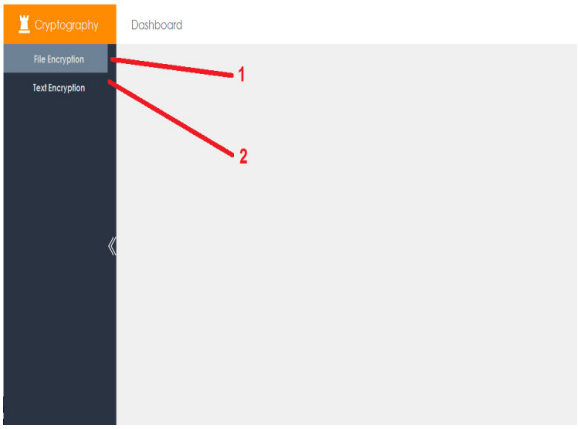

Figure 2: Main Screen

After selecting file encryption or text encryption the second screen will show up as shown in Figure 3, which allow the use to choose any symmetric algorithm to proceed with the encryption or decryption process.

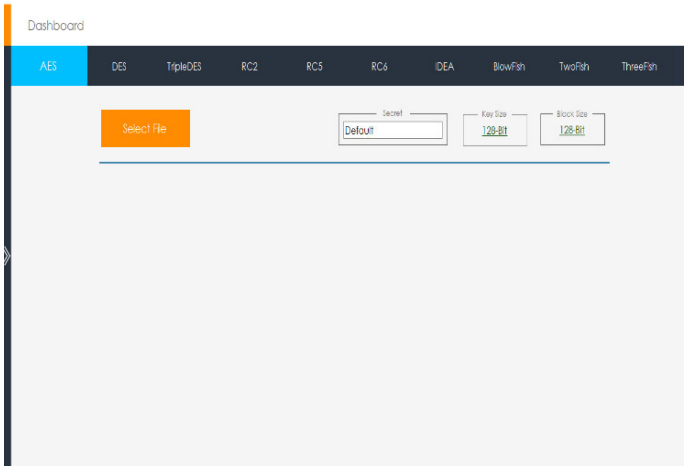

Figure 3: Algorithms screen

The encryption and decryption screen is displayed as follow in Figure 4:

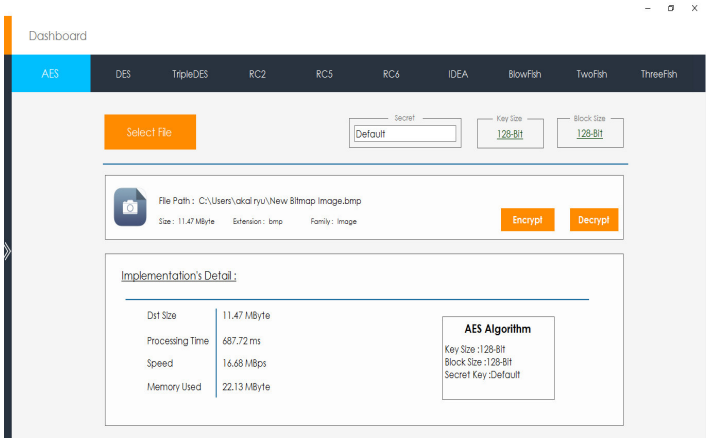

Figure 4: Encryption and decryption screen

Encryption and decryption screen contains result information of the file or text after been encrypted or decrypted such as file name, file path, processing time speed, memory used, key and the block size. This application can be used to compare between different symmetric algorithms to measure their performance, most of the symmetric algorithm has been implemented and can be used for future studies.

5. Conclusion

In this research paper, we have discussed the concept of cryptography with symmetric encryption. Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength, and weakness of the algorithms. Cryptography is the most vital component in information security because it is responsible for securing all information passed through networked computers. In this paper an application has been designed to encrypt and decrypt any type of file with any size , the application consist of ten symmetric encryption algorithm namely; AES, DES, 3DES, RC6, Blowfish, RC2, Two Fish, Three Fish, Triple DES and IDEA, the application can be used to test the performance of symmetric algorithm using different types of format.

References

Agrawal, M. and P. Mishra (2012). "A comparative survey on symmetric key encryption techniques." International Journal on Computer Science and Engineering **4**(5): 877.

Aleisa, N. (2015). "A Comparison of the 3DES and AES Encryption Standards." International Journal of Security and Its Applications **9**(7): 241-246.

Backes, M. and B. Pfitzmann (2004). Symmetric encryption in a simulatable Dolev-Yao style cryptographic library. Computer Security Foundations Workshop, 2004. Proceedings. 17th IEEE, IEEE.

Canright, D. (2005). A very compact S-box for AES. International Workshop on Cryptographic Hardware and Embedded Systems, Springer.

Dworkin, M. (2001). Nist Special Publication 800-38A, 2001 Edition, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Dec.

Gupta, P. (2012). "Cryptography based digital image watermarking algorithm to increase security of watermark data." International Journal of Scientific & Engineering Research **3**(9): 1-4.

Kim, H.-W., S.-Y. Lim and H.-J. Lee (2006). Symmetric encryption in RFID authentication protocol for strong location privacy and forward-security. Hybrid Information Technology, 2006. ICHIT'06. International Conference on, IEEE.

Menezes, A. J., P. C. Van Oorschot and S. A. Vanstone (1996). Handbook of applied cryptography, CRC press.

Singh, S. P. and R. Maini (2011). "Comparison of data encryption algorithms." International Journal of Computer Science and Communication **2**(1): 125-127.

Surya, E. and C. Diviya (2012). "A Survey on Symmetric Key Encryption Algorithms." International Journal of Computer Science & Communication Networks **2**(4): 475-477.