Applying & Evaluation Cryptography Files Using Symmetric Cryptography Algorithms of Block Cipher Type

Haifaa Abd Al-Zahra Atee
Foundation of Technical Education

Received: 15/03/2011
Accepted: 29/05/2011

ABSTRACT

The process of transfer and exchange of important data files from one place to another or over the Internet requires high protection and confidentiality to keep it away from theft and tampering. Therefore, there are many algorithms that are designed to encrypt files and provide a safe environment for better transfer of data from one place to another or over the network. In this research, implementation and evaluation of a symmetric cryptography algorithms of block cipher type is used to encrypt and decrypt files with different sizes, four algorithms of symmetric encryption block cipher type are used. It was found that there are differences in the time takes to encrypt and decrypt same files which using different encryption algorithms. So found that the AES algorithm is the fastest in the encryption and decryption, either 3-DES algorithm was the slowest. Also found that the time takes to encrypt the files was less...
Applying & Evaluation Cryptography Files Using Symmetric Cryptography Algorithms Of Block Cipher Type

Haifa

than the time it takes to decode the files in all algorithms used in this research. Four algorithms are used to encryption and decryption files, these are: AES (Rijndeal), Triple DES, Towfish, and Blowfish.

INTRODUCTION

Nowadays when more and more sensitive information is stored on computers and transmitted over the internet, we need to ensure information security and safety.

One of the most uses of encryption is encrypting files to provide secret transition from location to another or over the internet. It doesn't depend on if the files send via public or private networks. Files may be opened by anyone along the way – so anybody, ISP, boss, etc. Even if computer connected to server and send files via secret FTP protocols, it only means that the files can't be seen while transmitting between the computer and server. When the files reaches to server, it can be seen by FTP server provider. Then the server usually sends the files to the recipient in an unsecured way and files can also be easily seen by anyone.

According to all the above, really, there is only one sure way to protect the files security and privacy – using cryptography.

In this research, different sizes of files are used to implement and evaluate the encryption and decryption operation. Four symmetric cryptography algorithms of block cipher type are used, these are: Towfish, AES (Rijndeal), Triple DES, and Blowfish. It was found that there are differences in time that takes to encrypt and decrypt same files which using different encryption algorithms. Also found that the time it takes to encrypt the files was less than the time it takes to decode the encryption in all algorithms used in this research.

The experimental part of all selected block cipher algorithms has been implemented using Visual Basic programming language. Visual Basic is a high-performance language for technical computing(1). AES and Towfish has block size of 128 bits, but 3-DES and Blowfish has 64 bits as a block size.

What is Cryptography?

Cryptography is the science of using mathematics to encrypt and decrypt data, or more exactly is the art of achieving security by encoding information to make them non-readable (2).
In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography enables to store sensitive information or transmit it across insecure networks (like the internet) so that it can't be read by anyone except the intended recipient (2). The origin of the word cryptography comes from Greek, where "crypto" meant "hidden" and "grafik" meant "writing" (1).

There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. A single key is used for both encryption and decryption(2).

There are two types of symmetric algorithms: Stream ciphers and Block ciphers. A stream cipher operates on a stream of plaintext bit by bit, while a block cipher operates on a stream of plaintext block by block. That is a stream cipher encrypts plaintext individually, and an encryption key is used for one bit only in a stream cipher. A block cipher divided a stream of plaintext into blocks, and an encryption key is used for all bits in one block in a block cipher. figure(1) illustrate the cryptography techniques (2).

![Fig.-1: Cryptography Techniques](image-url)
Symmetric & Asymmetric Key Cryptography

Symmetric Key Cryptography

In symmetric key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext (2,3).

They are usually related and it is easy to derive the decryption key once one knows the encryption key. In most cases, they are identical. A Secret key should be shared (or agreed) both the communicating parties (4).

Symmetric key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing (5).

A block cipher is a scheme to encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher (2,6).

Asymmetric Key Cryptography

Asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. Public key cryptography intends for public keys to be accessible to all users (2,6).

Block Ciphers

Block cipher is a symmetric cipher which encrypts information by breaking it down into blocks and encrypting data in each block. A block cipher encrypts data in fixed blocks (commonly of 64 bits). Some example of a symmetric encryption algorithms of block cipher type are: AES(Rijndeal), Blowfish, CAST5, DES, Triple DES, IDEA, RC2, RC5, RC6, Gost, Serpent, and Twofish (7,8). Figure (2) illustrates the encryption and decryption operation for block cipher.
In this research, randomly selected four symmetric cryptography algorithms of block cipher type, all selected algorithms are explained in below section.

**AES Block Cipher (Rijndael Block Cipher)**

Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen as a candidate algorithm for the AES. AES stands for Advanced Encryption Standard. AES is a symmetric key encryption technique which will replace the commonly used Data Encryption Standard (DES). The Advanced Encryption Standard algorithm approved by NIST in December 2001 uses 128-bit blocks.

The block cipher currently supports key lengths of 128, 192, and 256 bits. Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which can scramble the data, but also increase the complexity of the cipher algorithm.

**Triple DES**

Triple DES is a variation of Data Encryption Standard (DES). It uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. The size of the block for Triple-DES is 64 bit. The idea behind Triple DES is to improve the security of DES by applying DES encryption three times.
Applying & Evaluation Cryptography Files Using Symmetric Cryptography Algorithms Of Block Cipher Type

using three different keys. Triple DES algorithm is very secure (major banks use it to protect valuable transactions), but it is also very slow(7,10).

**Blowfish Block Cipher**

Blowfish is a symmetric encryption algorithm designed in 1993 by Bruce Schneier as an alternative to existing encryption algorithms. Blowfish has a 64-bit block size and a variable key length - from 32 bits to 448 bits. It is a 6-round Feistel cipher and uses large key-dependent S-boxes.

Blowfish is similar in structure to CAST-128, which uses fixed S-boxes(7,10).

**Twofish Block Cipher**

Twofish is a symmetric block cipher. Twofish has a block size of 128 bits and accepts keys of any length up to 256 bits. Twofish has key dependent S-boxes like Blowfish(11).

Twofish encryption algorithm was designed by Bruce Schneier, John Kelsey, Chris Hall, Niels Ferguson, David Wagner and Doug Whiting. The National Institute of Standards and Technology (NIST) investigated Twofish as one of the candidates for the replacement of the DES encryption algorithm(12).

**Related Works**


In this research, four different cryptography algorithms used to measure the efficiency of cryptograph in terms of time it takes to encrypt and decrypt different sizes files using symmetric encryption algorithms of block cipher type.

**Hardware & Software Specification**

One of the most important performance criteria of the encryption algorithms is execution time. Execution time related to many parameters such as structure of the algorithm, number of round, size of file, and the selected target device.[101]

The encryption and decryption algorithms were implemented by the following hardware and software specifications:

1- Intel(R) Celeron(R) D CPU 3.06 GHZ.
2- 1 GB RAM.
3- Asrock 945GCM-S Mother Board.
4- Windows XP professional ver.2002, service pack 2.
5- Hard disk 320 GB with 80GB free in C partition (C partition used as a target device).
6- All selected algorithm are tested with 16 round except AES, it tested with 12 round.
7- 128 bit data block used for AES & Twofish, the Blowfish & 3-DES used 64bit as a data block.
8- 128 bit used as a key size in both AES, Blowfish, and Twofish, but 56 bit used in 3DES.
Applying & Evaluation Cryptography Files Using Symmetric Cryptography Algorithms Of Block Cipher Type

Haifa

The main steps used to encrypt and decrypt the files is represent in figure(3) as show below:

```
Original file (plaintext) → Encryption Algorithm → Encrypted file (Ciphertext) → Decryption Algorithm → Original file (plaintext)
```

Fig. - 3: Main Steps for Encryption & Decryption the Files

**EXPERIMENTAL RESULTS**

**Performance Comparison Of The Selected Block Cipher**

Two parameters are used as a factors to measuring the efficiency of four selected algorithms that are: size of files and the time required for encryption and decryption the files. The size of files is related with the time consuming to encrypt or decrypt the file. AES and Towfish has block size of 128 bits, but 3-DES and Blowfish has 64 bits as a block size. Among all the selected block cipher algorithms the AES algorithm was the fastest because it can perform the encryption and decryption process within shorter time than the others, but the 3-DES algorithm was the slowest (because it used 3 round of encryption (each round have 16 subround) with different key to improve the security), it takes longest time than the other algorithms. While the Twofish and Blowfish comes sequentially after AES and before 3-DES in terms of speed and efficiency.

Encryption and decryption time for AES, Twofish, Blowfish, and 3-DES algorithms with size 50Mb, 100Mb, 150Mb, 200Mb, and 250 Mb are illustrated in table(1).
Table-1 : The experimental results for selected algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>AES</th>
<th>Towfish</th>
<th>Blowfish</th>
<th>3-DES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>2:30</td>
<td>3:10</td>
<td>2:70</td>
<td>4:17</td>
</tr>
</tbody>
</table>

T.Enc. : Encryption time ; T.Dec. : Decryption time
The time is measured by second and millisecond

The execution time for the each one of selected block cipher algorithms are shown in the figure(4), figure(5), figure(6), and figure(7).

![AES Algorithm](image1)

**Fig.- 4: Execution Time for the AES Algorithm**

![Twofish Algorithm](image2)

**Fig.- 5: Execution Time for The Twofish Algorithm**
Applying & Evaluation Cryptography Files Using Symmetric Cryptography Algorithms Of Block Cipher Type

**Fig. - 6: Execution Time for The Blowfish Algorithm**

**Fig. - 7: Execution Time for the 3-DES Algorithm**

Figure(8), figure(9), figure(10), and figure(11) show the execution time of encryption and decryption operation for all selected block cipher algorithms.

**Fig.-8: Execution Time of Encryption operation for all selected algorithm**
Fig.-9: Execution Time of Decryption operation for all selected algorithm

Fig.-10 : Execution Time of Encryption operation for all selected algorithm

Fig.-11: Execution Time of Decryption operation for all selected algorithm
Figure(12) show the encryption & decryption time for all selected algorithms. With all the above figures, it is clear that the AES algorithm have the best performance to encrypt and decrypt the files ,the Towfish and Blowfish below the AES, the 3-Des algorithm is the slowest one among all the selected algorithm, it takes the longest time to encrypt and decrypt the same size of files.

**Fig.-12: Encryption & Decryption Time For All Selected Algorithms**

- **T.Enc.AES**: Time Encryption for AES algorithm.
- **T.Dec. AES**: Time Decryption for AES algorithm.
- **T.Enc. Twofish**: Time Encryption for Twofish algorithm.
- **T.Enc. 3-DES**: Time Encryption for 3-DES algorithm.
- **T.Dec. 3-DES**: Time Decryption for 3-DES algorithm.

Cryptography is used to achieve many goals like confidentiality, data integrity, authentication, safety transfer of date etc. In order to achieve these goals various cryptographic algorithm are designed.
Randomly selected four cryptography algorithms, these are AES, Twofish, Blowfish, and 3-DES, in term of specification parameters, it found that:

1. When increase the file's size, the time taken to encrypt or decrypt the files also increase.
2. In general, the time taken to encrypt files less than the time taken to decrypt the files.
3. AES algorithm is the fastest between all selected algorithm, twofish and Blowfish below the AES, the 3-DES is the slowest one among all the selected algorithms (it takes longest execution time to encrypt or decrypt same file).

REFERENCES

Applying & Evaluation Cryptography Files Using Symmetric Cryptography Algorithms Of Block Cipher Type


