A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention

Mohammed Nazeh Abdul Wahid*, Abdulrahman Ali, Babak Esparham and Mohamed Marwan

Limkokwing University of Creative and Technology, Post Graduate Centre, Cyberjaya, Malaysia

Abstract

Encryption is the process of encoding information or data in order to prevent unauthorized access. These days we need to secure the information that is stored in our computer or is transmitted via internet against attacks. There are different types of cryptographic methods that can be used. Basically, the selecting cryptographic method depends on the application demands such as the response time, bandwidth, confidentiality and integrity. However, each of cryptographic algorithms has its own weak and strong points. In this paper, we will present the result of the implementation and analysis that applied on several cryptographic algorithms such as DES, 3DES, AES, RSA and blowfish. Also, we will show the comparisons between the previous cryptographic techniques in terms of performances, weaknesses and strengths.

Keywords: Network security; Data encryption; Secure communication; Attacks; Ciphertext;

Introduction

In recent years, many applications based on internet are developed such as on-line shopping, internet banking and electronic bill payment etc. Such transactions, over wire or wireless public networks demand end-to-end secure connections, should be private, to ensure data authentication, accountability and privacy, integrity and availability, also known as CIA triad [25].

For this reason, the proposed algorithm has utilized Feistel Cipher in safe wifi design (sWiFi). In addition, this system will use Hash-based Message Authentication Code (HMAC) technology for authentication purposes. Experimental tests have provided an evaluation of four encryption algorithms (AES, DES, 3DES, and Blowfish) compared to developed sWiFi systems [26].

Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into ciphertext (scrambled message after encryption). Many encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: Symmetric-key (also called secret-key) and Asymmetric-key (called public-key) encryption [2].

A secure Wi-Fi system for wireless networks: experimental evaluation is a network security system for an application using the proposed algorithm. As for some cryptographic system, it is commonly used to secure communication channels by using public key exchanges based on algorithms such as RSA, DES, AES, Triple DES and Blowfish. From the key exchange, it depends on the key used to encrypt data sent over an unsecured Internet channel. In addition, the existing cryptographic algorithm relies on a data separation model designed by IBM's Horst Feistel [27].

A secure data transmission feature of (CC) cloud computing has plays a very important role in business perspective. For utilizing cloud computing, business trends have to play a lot of money to the cloud service provider. Cloud service provider also has guaranteed either the confidentiality or integrity of the data. This paper proposes an intensive study for the idea of sending already encrypted file through cloud in spite of the original file using RSA and DES algorithm of cryptography [4]. The aim is to provide evidence of which of the encryption methods has more powerful and effectiveness technique when encrypted file is transmitted, so original file is not available even at the network. So even if any intermediate user sees the data, he will not be able to understand the data. That’s why confidentiality and integrity is maintained by this. Hence, security of cloud data will be increased. This work can be enhanced using hybrid approach by integrating multiple cryptography algorithms [28].

Evaluation Metrics

In this paper, the analysis has been done based on the following metrics: [1].

1. Encryption time: The time taken to convert plaintext to ciphertext is encryption time. Encryption time depends upon key size, plaintext block size and mode. In our experiment, we have measured encryption time in milliseconds. Encryption time affects performance of the system [3]. Encryption time must be less making the system fast and responsive.
ii- Decryption time: The time to recover plaintext from ciphertext is called decryption time. The decryption time is desired to be less similar to encryption time to make system responsive and fast. Decryption time affects performance of system. In our experiment, we have measured decryption time is milliseconds.

iii- Memory used: Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm, key size used, initialization vectors used and type of operations. The memory used impacts cost of the system. It is desirable that the memory required should be as small as possible.

iv- Avalanche effect: In cryptography, a property called diffusion reflects cryptographic strength of an algorithm. If there is a small change in an input, the output changes significantly. This is also called avalanche effect. We have measured Avalanche effect using hamming distance. Hamming distance in information theory is measure of dissimilarity. We find hamming distance as sum of bit-by-bit xor considering ASCII value, as it becomes easy to implement programmatically. A high degree of diffusion i.e. high avalanche effect is desired. Avalanche effect reflects performance of cryptographic algorithm.

v- Entropy: is the randomness collected by an application for use in cryptography that requires random data. A lack of entropy can have a negative impact on performance and security.

vi- Number of bits required for encoding optimally: the number of bits required to encode an encrypted character should be less. Since, the encrypted bit will be transmitted over a network after encoding; this metric tells us the bandwidth required for transmission. If an encrypted bit is encoded with fewer bits, it will consume lesser bandwidth and lesser storage as well. Hence, this impacts cost.

**Methods**

As we have mentioned that Encryption is the process of encoding information or data in order to prevent unauthorized access. There are different types of cryptographic methods that can be used. Each one of them serving different topology and all provide secure transmitted data through network links and ensure authentication and confidentiality. All these end to end encryption and decryption algorithms have to be applied in the physical layer and security layer of the computer application. At the same time a specific IP configurations are need to be considered as well as the protocol that will be used to transmit the traffics. The diagram below showing us the cipher security classes which are subdivided into 2 models: classical and modern class. The most common and used is the modern class due to the dynamic and static cryptography techniques that this technique was deployed with. It is known also by its types;

i. Secret Key (Symmetric Key) in a symmetric cryptosystem, the same key is used for encryption and decryption [5,11].

ii. Public Key (Asymmetric Key) in an asymmetric, the encryption and decryption keys are different but related. The encryption key is known as the public key and the decryption key is known as the private key. The public and private keys are known as a key pair [5].

So, our focus point in this paper is on these two types with their classes to show the significance for each one of them through our literature and to prove which one is the best with what environment. (Figure 1)
Advanced Encryption Standard (AES)

Advance Encryption Standard (AES) algorithm was developed in 1998 by Joan Daemen and Vincent Rijmen, which is a symmetric key block cipher [7]. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is refered to as AES-128, AES-192, or AES-256, depending on the key length. During encryption decryption process, AES system goes through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with adding Round Key stage [30]. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; 1- Sub-Bytes, 2- Shift rows, 3- Mix-columns, 4- Add round Key. In the final (10th) round, there is no Mix-column transformation. Figure shows the overall process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns. Each round of AES is governed by the following transformations [12]:

3.4.1 Substitute Byte transformation AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box, which is known as Rijndael Sbox [13]. (Figure 2)

Figure 2: AES (Advanced Encryption Standard) process
Data Encryption Standard (DES)

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST). The algorithm submitted to the National Bureau of Standards (NBS) to propose a candidate for the protection of sensitive unclassified electronic government data. It is now taken as unsecured cause of its small size and a brute force attack is possible in it. The key length is 56 bits and block size is 64 bit length. It is vulnerable to key attack when a weak key is used. It began with a 64 bit key and then the NSA put a restriction to use of DES with a 56-bit key length, hence DES discards 8 bits of the 64-bit key and then uses the compressed 56 bit key derived from 64 bits key to encrypt data in block size of 64bits. DES can operate in different modes - CBC, ECB, CFB and OFB, making it flexible. It is vulnerable to key attack when a weak key is used. In January 1999 distributed net and the Electronic Frontier Foundation (EFF) collaborated to publicly break a DES key in 22 hours and 15 minutes. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES) [14-16].

Rivest-Shamir-Adleman (RSA)

RSA is founded in 1977 is a public key cryptosystem. RSA is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir & Adelman [9,29]. It is one of the best-known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys size is 1024 to 4096 bits. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it by using his own private key [20,21]. RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand, if large p & q lengths are selected then it consumes more time and the performance is degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p & q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases in increases the system’s overheads by taking more processing time. Figure illustrates the sequence of events followed by RSA algorithm for the encryption of multiple blocks. Decrypt blocks of data consisting of 64 bits by using a 64-bit key [22]. (Figure 3)
Blowfish

Blowfish was first published in 1993 [6]. It is a symmetric key block cipher with key length variable from 32 to 448 bits and block size of 64 bits. Its structure is fiestal network. Blowfish is a 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 [8]. 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. It suffers from weak keys' problem; no attack is known to be successful against. Blowfish is not patented, has free license and is freely available for all uses [24].

Results and Discussions

In this paper, the results are analyzed based on the implementation that performed in [1,27].

i- Figure 4 shows that the blowfish algorithm records the fastest encryption time, and RSA algorithm records the slowest encryption time. Based on the encryption time we will select the blowfish technique for further evaluation.

ii- Figure 5 shows that the decryption time for all algorithms is faster than the encryption time. Also, blowfish algorithm records the fastest decryption time and RSA algorithm records the slowest decryption time. Based on the decryption time feature we will select the blowfish technique to be considered at the next evaluation level.

iii- Up next in the table 1 presents that memory used for unit operations for all cryptographic techniques that we studied. Blowfish consumed less memory storage than other types, while RSA uses the highest memory.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Memory used (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>18.2</td>
</tr>
<tr>
<td>3DES</td>
<td>20.7</td>
</tr>
<tr>
<td>AES</td>
<td>14.7</td>
</tr>
<tr>
<td>Blowfish</td>
<td>9.38</td>
</tr>
<tr>
<td>RSA</td>
<td>31.5</td>
</tr>
</tbody>
</table>

iv- Figure 6 displays that AES manifests the highest avalanche effect, whereas RSA manifests the least avalanche effect. This has turned the attention back to AES for further analysis and improvements.

v- As the entropy test and final experiment. Table 2 shows that blowfish records the highest average entropy per byte of encryption. That should highlight the blowfish algorithm achievements for consideration of a new security aspect.
A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention

Guessing Attacks Prevention

We can consider that blowfish and AES algorithms are used to prevent the application from guessing attacks and it can be applied on top of all the internet protocols that are based on IPv4 and IPv6 and the examinations recoded in this paper showing that all the algorithms and the classes are functioned well with different execution time and memory consumption.

References

Table 2: Average entropy values

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Average entropy per byte of encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>2.9477</td>
</tr>
<tr>
<td>3DES</td>
<td>2.9477</td>
</tr>
<tr>
<td>AES</td>
<td>3.84024</td>
</tr>
<tr>
<td>Blowfish</td>
<td>3.93891</td>
</tr>
<tr>
<td>RSA</td>
<td>3.0958</td>
</tr>
</tbody>
</table>

Table 3: Optimal encoding length

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Average number of bits demanded to optimally encode a byte of encrypted data</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>27</td>
</tr>
<tr>
<td>3DES</td>
<td>40</td>
</tr>
<tr>
<td>AES</td>
<td>256</td>
</tr>
<tr>
<td>Blowfish</td>
<td>128</td>
</tr>
<tr>
<td>RSA</td>
<td>44</td>
</tr>
</tbody>
</table>

Conclusion

Each of cryptographic algorithms has weakness points and strength points. We select the cryptographic algorithm based on the demands of the application that will be used. From the experiment results and the comparison, the blowfish algorithm is the perfect choice in case of time and memory according to the criteria of guessing attacks and the required features, since it records the shortest time among all algorithms. Also, it consumes the minimum memory storage. If confidentiality and integrity are major factors, AES algorithm can be selected. If the demand of the application is the network bandwidth, the DES is the best option. We can consider that blowfish and AES algorithms are used to prevent the application from guessing attacks and it can be applied on top of all the internet protocols that are based on IPv4 and IPv6.

17. 3DES. Available from: http://www.cryptosys.net/3des.html
19. 3DES. Available from: http://en.wikipedia.org/wiki/Triple_DES