Information Security and Computer Fraud, 2015, Vol. 3, No. 1, 1-7
Available online at http://pubs.sciepub.com/iscf/3/1/1
© Science and Education Publishing
DOI:10.12691/iscf-3-1-1

Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey

Chadi RIMAN[*], **Pierre E. ABI-CHAR**[*]

Computer Engineering Department, American University of the Middle East, Egaila, Kuwait
*Corresponding author: chadi.riman@aum.edu.kw, Pierre.abichar@aum.edu.kw

Received June 04, 2015; Revised June 10, 2015; Accepted June 16, 2015

Abstract Nowadays, network security is increasing rapidly and becoming an important and challenging issue. Information and internet security threats and attacks are becoming difficult to be detected. Therefore, encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. In this paper we implemented four encrypt techniques AES, DES, 3DES and E-DES algorithms and compared their performance. A comparative analysis on the above symmetric encryption algorithms has been made. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power. Experiments results are given to analyses the effectiveness of each algorithm. The comparison is made on the basis of these parameters: speed, block size, and key size etc. Educational-DES has better performance than other DES, 3DES, and AES algorithms.

Keywords: *cryptography, DES, 3DES, E-DES, AES, data encryption, decryption*

Cite This Article: Chadi RIMAN, and Pierre E. ABI-CHAR, “Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey.” *Information Security and Computer Fraud*, vol. 3, no. 1 (2015): 1-7. doi: 10.12691/iscf-3-1-1.

1. Introduction

Information security, shortened to InfoSec, is a set of techniques, procedures and policies used to prevent and monitor unauthorized access, misuse, disclosure, disruption, modification of computer network resources. To provide confidentiality, integrity, authentication, privacy and trust is a challenge and requires a lot of effort on how to reinforce the existing techniques against ongoing attempts to breach them, and how to develop new mechanisms that are immune against most types of attacks if not all.

Encryption is one of the most reliable methods used to protect data confidentiality and integrity even since the old days of the Romans. Data encryption is the process of converting data in plain text format into a meaningless cipher text by means of a suitable algorithm. Data decryption is the process of converting the meaningless cipher text into the original information using keys generated by the encryption algorithms. The process of encryption and decryption of information by using a single key is known as secret key cryptography or symmetric key cryptography. In symmetric key cryptography, the same key is used to encrypt as well as decrypt the data. A secure channel is also required between the sender and the receiver to exchange the secret key. Two ciphers modes are adopted by symmetric algorithms: Block ciphers and Stream ciphers. A block cipher is functioning on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. Feistel structure is adopted by many block ciphers. Such a structure consists of a number of identical rounds of processing. In each round, a substitution is performed on one half of the data being processed, followed by a permutation that interchanges the two halves. The original key is expanded so that different key is used for each round.

In Asymmetric key cryptography different keys are used for encryption and decryption. Asymmetric cryptography refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. According to [1], asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique. The classification of major encryption techniques is shown Figure 1.

For the past few decades, the Data Encryption Standard (DES) [2] has been treated as the cipher to breach and to compromise. This was achieved mainly due to weaknesses in the cipher itself. DES was built based on a key of 56 bits. However, only 48 bits where effectively used in the F module of each round. On the other hand, the data block was set at 64 bits. This resulted in relatively easier (when almost exponential increases in computation power are factored in) attacks on the cipher.

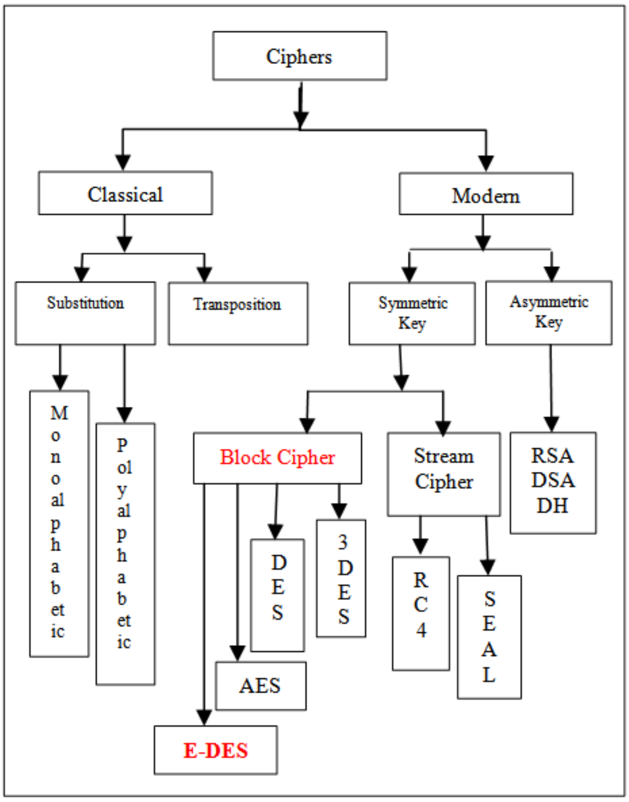

Figure 1. The classification of encryption algorithms

The remainder of this paper is organized as follows. In section 2, a review of literature on encryption algorithm is give. Section 3 presents a detailed description of common block cipher-based encryption algorithms. Section 4 presents a discussion on the efficiency of the simple-DES cipher and its advantages. Section 5 describes the comparative study. Finally, section 6 concludes the paper and presents potential extensions of this work.

2. Review of Literature

Network security and cryptography challenges issues are discussed by various researchers. To give more prospective about the performance of the encryption algorithms, we describe and examine previous work done in field of data encryption. The metrics taken into consideration are processing speed, throughput, power consumption, avalanche effect, and packet size and data types.

Singh et al. [3] made the comparison between DES, 3DES, AES and Blowfish symmetric algorithms. The comparison had been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithms encryption/decryption speed. It was concluded that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results as compared to other algorithms, because it required more processing time. Cornwell [4] discussed the design of Bruce Schneier‟s Blowfish encryption algorithm along with a performance analysis and possible attacks. It was concluded about the effectiveness of Blowfish with the other well-known algorithms DES, 3DES, and AES. It was concluded that Blowfish is able to provide long term data security without any known backdoor vulnerability or ability to reduce the key size. For the future scope Blowfish was considered safe and effective design although future reevaluations will be needed. Tamimi [5] compared DES, 3DES, AES and Blowfish symmetric algorithms. The performance of these algorithms under different settings, and different data loads were considered. This study used two modes of operation i.e. ECB and CBC for calculating execution time of each algorithm. This study used C# programming language for simulation. It was concluded that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results as compared to other algorithms, because it required more processing time. CBC mode had added extra time, but it was relatively negligible. Nadeem [6] discussed the popular secret key algorithms DES, 3DES, AES (Rijndael), Blowfish and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in Java programming language, and were tested on different hardware platforms, to present the comparison. The two different machines were: P-II 266 MHz and P-IV 2.4 GHz. It was concluded that Blowfish had an advantage over other algorithms. Also it showed that AES has better performance than DES and 3DES. Also it was concluded that 3DES needs 3 times than DES to process the same amount of data. Dhawan [7] compared the performance of the different encryption algorithms by conducting experiments inside .NET framework. The comparison was performed on the following algorithms: DES, 3DES, RC2, and AES (Rijndael). It was concluded that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations. Singh et al. [8] performed a comparison between the most common four encryption algorithms namely; AES, DES, 3DES and Blowfish in terms of security and power consumption. Experiment results of comparison were carried out over different data types like text, image, audio and video. The simulation results showed that AES has a better performance than other common algorithms. AES is supposed to be better algorithm which was compared to original Blowfish Algorithm. But adding additional key and replacing the old XOR by new operation “#” as a purposed by this study to give more robustness to Blowfish Algorithm and make it stronger against any type of intrusion. This advance Blowfish Algorithm is more efficient in energy consumption and security to reduce the consumption of battery power device. Agrawal et al. [9] made a detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption. It was concluded that the supremacy of Blowfish algorithm over DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data. Also the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms. Seth et al. [10] made a comparative analysis of three algorithms, DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool was used for conducting experiments. It was concluded that RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Based on the text files used and the experimental result it was concluded that DES consume least encryption time and AES has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm. Mandal et al. [11] made the comparison between four most commonly used Symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of parameters: round block size, key size, encryption/decryption time, and CPU process time in the form of throughput and power consumption. It was concluded that blowfish is better than other algorithms. Also AES has advantage over the other 3DES and DES in terms of throughput and decryption time. 3DES has least performance among all mentioned algorithms. Apoorva et al. [12] compared most common symmetric cryptography algorithms: AES, TWOFISH, CAST-256 and BLOWFISH. The comparison took into consideration the behavior and performance of algorithms when different data loads were used. The comparison was made on the basis of these parameters: speed, block size, and key size. It was concluded that blowfish is superior to other algorithm as it takes less time. Although when the data size was very small this difference was not clearly visible. But for file having size greater than 100 KB, it was very clearly visible. Abdul et al. [13] discussed six most common encryption algorithms such as AES (Rijndael), DES, 3DES, RC2, BLOWFISH and RC6. These algorithms were compared and performance was evaluated. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. It was concluded that there is no significant difference when the results are displayed either in Hexadecimal Base encoding or in Base 64 encoding. Secondly in the case of changing packet size, it was concluded that BLOWFISH has better performance than other common encryption algorithms used, followed by RC6. Also in the case of changing data type such as image instead of text, it was found that RC2, RC6 and BLOWFISH has disadvantage over other algorithms in terms of time consumption. Also, it was found that 3DES still has low performance compared to algorithm DES. Finally in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption. Thakur et al. [14] discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings, the presented comparisons takes into consideration the behavior and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size, and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used. Marwaha et al. [15] discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm. Alam et al. [16] discussed performance and efficiency analysis of different block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA and RC2) of symmetric key cryptography. Block cipher algorithms has been compared based on the factors: input size of data(in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block cipher and power consumption. It was concluded that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Saini [17] make a performance analysis of various algorithms-DES, AES, RC2, Blowfish, 3DES and RC6. It was concluded from the simulation outcomes that best algorithm are those that are well known and well documented because they are well tested and well-studied. A good cryptographic system strikes a balance between what is possible and what is acceptable. Alanazi et al. [18] has done the comparative analysis of three Encryption Algorithms (DES, 3DES and AES) within nine factors such as Key Length, Cipher Type, Block Size, Security, Possible Keys, Possible ASCII printable character keys and Time required to check all possible keys at 50 billion keys per second etc. Study shows that AES is better than DES and 3DES. Arora et al. [19] studied about the performance of different security algorithms on a cloud network and also on a single processor for different input sizes. This paper aims to find in quantitative terms like Speed-Up Ratio that benefits of using cloud resources for implementing security algorithms (RSA, MD5 and AES) which are used by businesses to encrypt large volumes of data. Three different kinds of algorithms are used – RSA (an asymmetric encryption algorithm), MD5 (a hashing algorithm) and AES (a symmetric encryption algorithm). The results reported in this paper conclude that the algorithms implemented on cloud environment (i.e. Google App) are more efficient than using them on single system. For both uni-processor (local) as well as cloud (Appengine) environment, RSA is the most time consuming and MD5 is the least. Highest Speed-Up Ratio is obtained in AES for low input file sizes and the Speed-Up Ratio falls sharply as the input file size is increased. For each input size, the Speed-Up Ratio is highest for AES, followed by MD5 and least for RSA algorithm.

3. Detailed Description of Common Encryption Algorithms

The field of cryptography encompasses some of these requirements and has been focus of a growing research effort. The core of this field is the efficient realization of cryptography algorithms in software and/or hardware.

Some commonly used symmetric key encryption algorithms are described as:

A. DES (DATA ENCRYPTION STANDARD)

Introduced in 1977, the Data Encryption Standard (DES) is a symmetric block cipher that is based on the Feistel structure with a block size of 64 bits and a key size of 64 bits. Despite being compromised, DES is s till being used to provide data security by many sectors including the American Bankers Association's and in several security standards like the IP Security Architecture (IPSec) standard [20]. DES uses 16 rounds of a Feistel like encryption method to encrypt plain text. A key schedule is used to derive 16 keys for the successive rounds of encryption from the original key. The block diagram of one round of DES is shown in Figure 2.

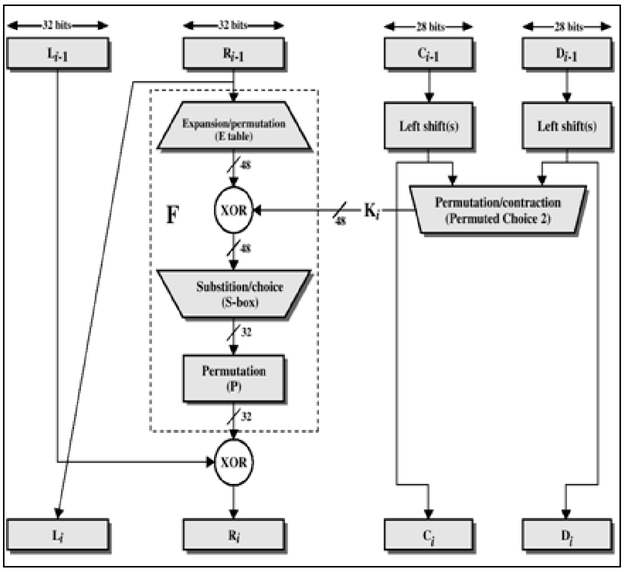

Figure 2. Depiction of one round of DES

Although DES uses a 64-bit key; 8 of these bits are only used for odd parity and do not count in the key length. The effective key length of DES is 56 bits which means 2^{56} possible different keys. A full 64-bit key has 256 times as many key combinations. In addition to the short key, the DES key schedule does not guarantee random keys for the 16 encryption rounds (The generated keys can be all-ones, all-zeros, or distinguishable patterns of ones and zeros [21]).

This made it possible for techniques based on differential and linear cryptanalysis [2] to attack the DES. Moreover, using a brute force key search seems not so difficult with the computation power levels in recent computer systems. Consequently, the Triple DES (3DES) was introduced to solve the key problems of DES. In a typical implementation of the 3DES cipher, the plaintext is encrypted with one key. The resulting cipher text is decrypted with another key, and, finally, the resulting text is encrypted again with the initial key (first key used). To implement the 3DES algorithm, two different keys are needed. However, implementations with three different keys are also possible. Compared to DES, 3DES offers a key length of 112 bits. This is an improvement of 2^{56} combinations over the 56 bit key. Although the problem of short key is solved with 3DES, the problem with of (relatively) non-random key generation remained in 3DES but with a reduced effect. In addition, 3DES is almost one third as fast as DES.

B. 3DES (TRIPLE DATA ENCRYPTION STANDARD)

Triple DES was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques such as those used by the EFF DES Cracker. Triple DES has always been regarded with some suspicion, since the original algorithm was never designed to be used in this way, but no serious flaws have been uncovered in its design, and it is today available cryptosystem used in a number of Internet protocols [20,21].

C. AES (ADVANCED ENCRYPTION STANDARD)

The Advanced Encryption Standard (AES), also known as the Rijndael cipher, was introduced in 2000. It uses 128, 192, or 256 bit key for encryption. This provides improvements of 2^{72}, 2^{136}, and 2^{200} over the 56 bit DES key, respectively. With longer keys, it became much harder to break the AES. In addition, AES compensated another shortcoming of the DES, the block size. AES encrypts blocks of 128 bits, which means it is more resilient against information leak (caused by repetitive blocks). Using DES, one can encrypt up to 32GB with a single key [22]. On the other hand, AES allows 256 billion gigabytes to be processed with the same key before any leak can occur. Moreover, while DES uses the Feistel network, where the text block is divided into two halves before going through the encryption steps, AES applies a series of substitution and permutation steps to create the encrypted block. The block diagram of AES is shown in Figure 3.

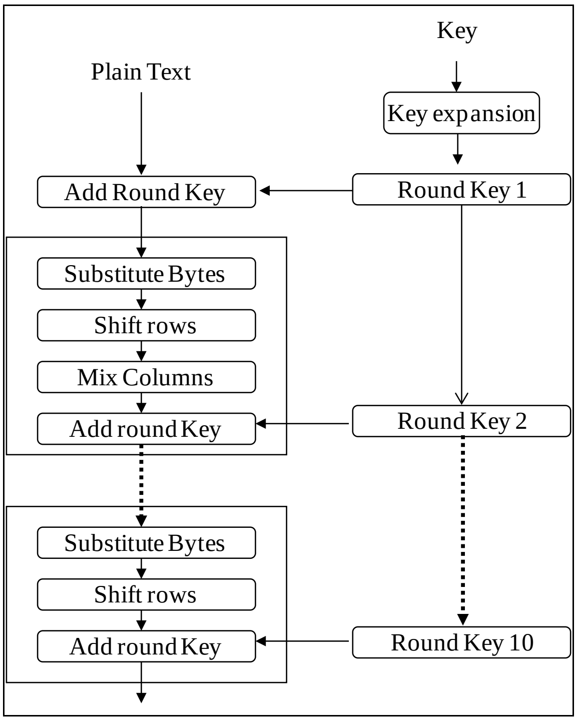

Figure 3. AES Block Diagram

D. E-DES (Educational DATA ENCRYPTION STANDARD)

Riman et al [23] introduced E-DES, the Educational Data Encryption Standard as an enhancement of DES. The main changes proposed to implement E-DES include a larger key and block size, an improved F function in each round, an improved key schedule, and more complex permutation functions. In addition, the proposed cipher uses one of the components from AES, the substitution box; thus the name E-DES.

In this section, we describe E-DES and detail its components.

Similar to DES, E-DES relies mainly on the Feistel Network with 16 rounds, where the first operation is application of the initial permutation of the plaintext. Then, each round consists of the sequence:

1. The permuted plaintext is split into two halves, left and right.
2. Right half text moves to the left without any manipulation, and left half is XORed with the output of a function F that takes round key and right half as inputs.

Finally, after 16 rounds are completed, the inverse initial permutation is applied to the produced text yielding the ciphered text block. This structure is illustrated in Figure 4.

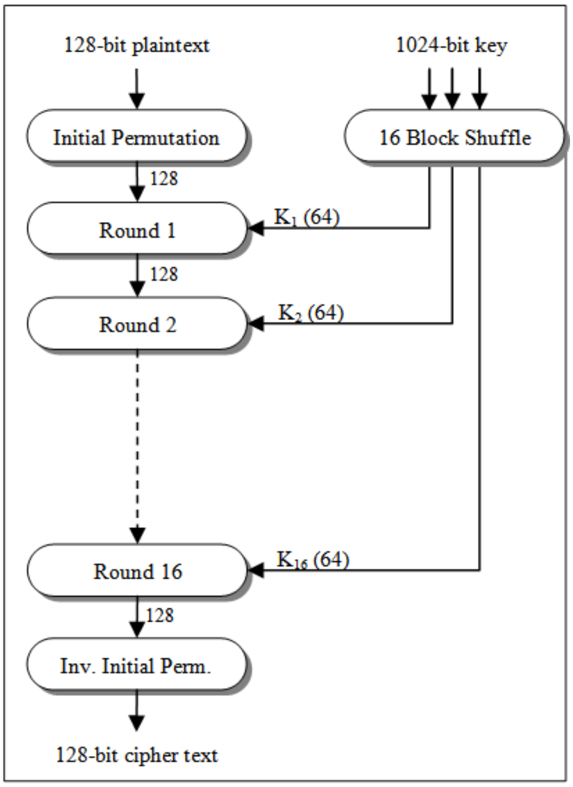

Figure 4. General Encryption Structure

As mentioned earlier, E-DES uses a larger plain text block and initial key sizes. The plaintext block in E-DES is 128 bits and the initial key size is 1024 bits.

In detail, the initial plaintext is divided into two 64 bit blocks, and each block is encoded separately. The cipher consists of 16 rounds: the first round is preceded with an initial permutation (IP) and last round is followed by an inverse initial permutation (IP^{-1}). The 1024 bit key is divided into 16 separate sub-keys for the 16 rounds, yielding sub-keys is of 64 bits each. The 16 keys, which are completely independent, are shuffled using a key permutation function before being distributed to rounds, which adds to the randomness of the sub key generation, thus making the recognition of round keys more difficult.

Then, each round *i* consists of:

1. Dividing text P_i into two halves right R_i and left L_i
2. Swapping right half input to left half output ($L_{i+1} = R_i$),
3. Performing XOR on the left half input with the function F, and sending result to right half output ($R_{i+1} = L_i \oplus F(R_i, K_i)$).

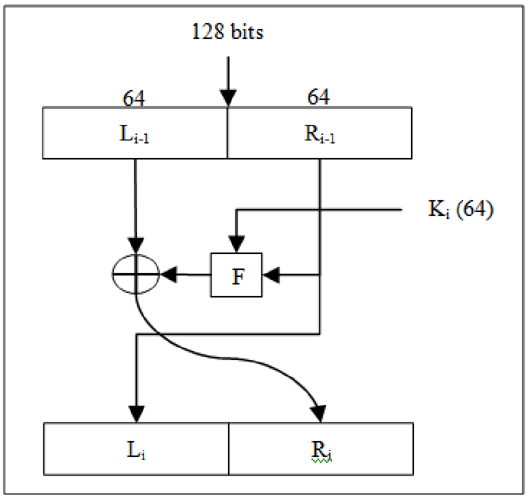

Figure 5. One Round Encryption Structure

Figure 5 shows the general structure of each round in E-DES. As to the function F, it takes two inputs: the right half input of the text and the round key. F consists of a first permutation P1 on the text (right hand 64 bits of the text). The result is XORed with the Round Key (also kept at 64 bits). The output is treated as 8 blocks of 1 byte each. The 8 blocks are then shuffled and passed through 8 different AES like substitution boxes (S1 to S8). The results of the 8 Substitution boxes are merged again to 64 bits, and then passed to a second permutation P2, which leads to the final output of the F function. Figure 6 shows the complete structure of function F.

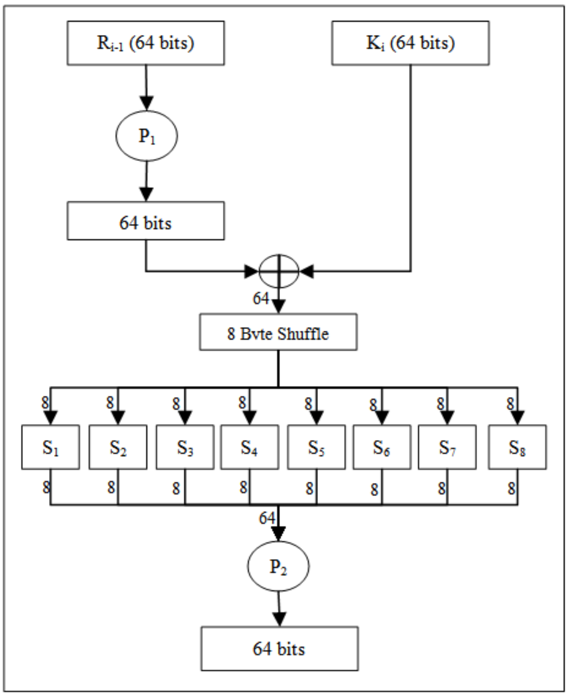

Figure 6. Function F Structure

The main difference between the proposed S-boxes in E-DES from the use of the S-box in AES is the independence between the different S-boxes proposed here for each 8 bit blocks.

Each substitution box, which takes 8 bits input and gives 8 bits output, consists of 16 rows and 16 column bytes. The left 4 bits of the input determine one row, and the right 4 bits determine one column. The byte intersection of the selected row and column is the output of the substitution.

As in the case of DES, decryption of E-DES is similar to encryption starting with cipher text. After Initial Permutation (IP), last round of encryption is applied to cipher text with the last round key. Rounds are visited in reverse order until the first round. Finally, inverse initial permutation is applied, and plaintext is completely retrieved.

4. E-DES: Efficiency and Advantages

In this section, we discuss the main advantages of E-DES and its enhancement compared to DES. The first strong aspect of E-DES is the text block size which is 128 bits (64 bits on DES). Second, the initial key is 1024 bits (56 bits for DES), and the round keys are 64 bits (48 bits effective in DES). Third, round keys are derived independently from the original key, which is divided into 16 sub keys. The sub-keys are then permuted before being used for the respective rounds. The run down independence of sub-keys is an important aspect not found in DES or AES.

On the other hand, the function F itself features 8 independent one byte substitution boxes similar to AES compared to the 8, 6 to 4 bit, DES S-boxes. In addition, 8 byte shuffle (permutation) is performed in F before entering into the S-boxes.

In terms of implementation of E-DES, the algorithm via software is fairly simple, even simpler than DES, especially for the round key generation, which is fairly direct and simple since all sub-keys are independent. As is the case in AES implementation, the byte substitution in the S-boxes is fairly simple too. Finally the decryption algorithm is almost identical to the encryption, thus it is of the same complexity of the encryption algorithm.

A. Avalanche effect

Avalanche effect is a desirable property of cryptographic algorithms. When an input or key is slightly changed by a single bit, the output changes by almost half the bits. We already know that DES and AES have strong avalanche effect.

E-DES was tested with a sample input 128 bit block containing zero bits and 1024 bit key of zero bits. The input was changed to 127 zero bits and 1 one-bit. The result difference with respect to first scenario was of 73 bits. On the other hand, if the input stays zero and key becomes all zero bits except 1 one-bit, and then output is changed by 68 bits.

Another test was performed on E-DES, but now with random key and random plain text. Again, 1 bit was changed in the plain text. The result changed from previous result in 67 bits. Again, the test repeated with same plain text, but with a change in 1 bit of the key. The result changed from previous one in 57 bits.

B. Speed

A C++ software was built to test E-DES algorithm's speed in comparison to DES and AES.

A standard text of 128 bit size with a simple key (all zero bits), and then with randomly generated key was run for 3000 iterations, with a total of 48KB message size. It took around 7 seconds to run on DES, 21 seconds on 3DES, 13 seconds on AES, and only 2 seconds on E-DES.

C. Brute Force Attack

Brute force attack is trying to find the key using all possible combinations using a fast guessing tool. We considered a guessing rate of one thousand billions keys per second (10^{12} keys/sec). For DES that has a key size of 56 bits, we have 2^{56}possible keys. If we try the brute force attack, we divide 2^{56} by 10^{12}, we get the maximum number of seconds needed to get the right key. In this case it is 72058 seconds. If we divide this number by 3600 to get number of hours, we get 20 hours which is less than 1 day. If we do the same for the other encryption methods diving by 24 to get number of days, and then by 365.25 to get number of years, we calculated the following: $1.6\text{x}10^{14}$ years for 3DES (2^{112} keys), 10^{19} years for AES (2^{128} keys), and 10^{152} years for E-DES (2^{1024} keys).

D. Cryptanalysis

Cryptanalysis is hard to achieve for several reasons. First the large key of 1024 bits and independence of the sub-keys make it really hard for exhaustive key search.

On the other hand, differential cryptanalysis which tries to test the difference of inputs' effect on the outputs, is also hard to do given the strong round function F. The strength of F is mainly of using 8 different S-Box functions similar in concept to the single substitution box in AES.

5. The Detailed Comparative Analysis

Based on literature review by various researchers a theoretical analysis was made on the selected algorithms. Encryption algorithms play an important role in communication security where memory usages, output byte and battery power are the major issue of concern.

The selected algorithms DES, 3DES, AES and E-DES are used for performance evaluation.

Table 1. Comparative Analysis of Symmetric Encryption Algorithms

Factors	DES	3DES	AES	E-DES	References
Key length (bits)	56	112, 168	128, 192 or 256	1024	Stallings[2]; Riman [23]; Agrawal et al. [9]
Cipher Type	Sym.	Sym.	Sym.	Sym.	Stallings[2]; Riman [23]
Block (bits)	64	64	128	128	Stallings[2]; Riman [23]
Rounds	16	48	10,12,14	16	Stallings[2]; Riman [23]
Developed	1975	1978	1998	2013	Stallings[2]; Riman [23]
Security	Not good	Passing	Secure	Secure	Hamdan[18]
Possible Key	2^{56}	2^{112}	2^{128}	2^{1024}	Hamdan[18] Riman [23]
Time for Brute Force key attack (10^{12} keys/sec)	<1 day	$1.6\text{x}10^{14}$ years	10^{19} years	10^{152} years	Calculated in Section 4 part C.
Avalanche effect	Resists	Resists	Resists	Resists	Singh et al. [15]
Encryption Software	Fast	Slow	Medium	Very fast	Calculated in Section 4 part B
Time to encrypt 48KB	7s	21s	13s	2s	Calculated in Section 4 part B

6. Conclusion and Future Work

In this paper a new comparative study between DES, 3DES, E-DES and AES is presented. With the theoretical comparisons, experimental analysis and comparison is done for the above algorithms. Based on the text files used and the experimental result it was concluded that the new E-DES algorithm consumes least encryption time as compared to the other mentioned algorithms.

The E-DES cipher shows an improvement over DES in two main areas: implementation is more straightforward and security is enforced with larger key and data block sizes.

Currently, a software implementation of the encryption algorithm has been completed and will be made available after the implementation of the decryption part is finalized. Next, we are planning to produce a hardware implementation of the E-DES algorithm that can be useful to make it available in embedded and mobile systems. The implementation is to be done using the microcontroller board PIC16F877.

References

[1] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

[2] W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.

[3] Singh S Preet, Mani Raman, “Comparison of Data Encryption Algorithms”, International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.

[4] Cornwell Jason W, “Blowfish Survey”, Department of Computer science, Columbus State university, Columbus, GA, 2010.

[5] Tamimi A. Al., “Performance Analysis of Data Encryption Algorithms”, Oct 2008.

[6] Nadeem Aamer, “Performance Comparison of Data Encryption Algorithms”, Oct 2008.

[7] Dhawan Priya, “Performance Comparison: Security Design Choices”, Microsoft Developer Network October 2002.

[8] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. “A Study of New Trends in Blowfish Algorithm” International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.

[9] Agrawal Monika, Mishra Pradeep, “A Comparative Survey on Symmetric Key Encryption Techniques”, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[10] Seth Shashi Mehrotra, Mishra Rajan, “Comparative analysis of Encryption algorithm for data communication”, International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[11] Mandal Pratap Chandra, “Superiority of Blowfish Algorithm” IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

[12] Apoorva, Kumar Yogesh, “Comparative Study of Different Symmetric Key Cryptography”, IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206.

[13] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., “Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA, Volume 8, 2009, pp. 58-64

[14] Thakur Jawahar, Kumar Nagesh. “DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis”, IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[15] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, “Comparative Analysis of Cryptographic Algorithms”, International Journal of Advanced Engineering Technology/IV/III/July-Sep, 2013/16-18.

[16] Alam Md Imran, Khan Mohammad Rafeek. “Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.

[17] Saini Bahar, “Survey On Performance Analysis of Various Cryptographic Algorithms”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014, pp. 1-4.

[18] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, Volume 2, ISSUE 3, pp. 152-157, March 2010.

[19] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012.

[20] W. Tuchman, A Brief History of the Data Encryption Standard, Internet besieged: countering cyberspace scofflaws. ACM Press/Addison-Wesley Publishing Co. New York, NY, USA, 1998, pp. 275-280.

[21] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-2/goodbye_des.html.

[22] http://www.differencebetween.net/technology/difference-between-des-and-aes/.

[23] C. Riman and H. Hallal. “DES Based Educational Data Encryption System”, *International Conference on Security and Management SAM 2013 (WORLDCOMP’13)*, Las Vegas, USA, July 2013.