International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 6, November- December 2017 ISSN 2278-6856

Analytical Study on Encryption Techniques and Challenges in Network Security

Anuraj C.K[1], Dr.Shelbi Joseph[2]

[1]Research Scholar, Division of Information Technology, School of Engineering, Cochin University of Science & Technology, Cochin, India

[2]Assistant Professor, Division of Information Technology, School of Engineering, Cochin University of Science & Technology, Cochin, India

Abstract

Importance of data security and network security is increasing day by day for various hardware and software applications in human life. Now many of the human activities are automated and in future more areas will come as part of network system. So most of the devices will come to the internet and it is important to ensure security of data being transmitted. The encryption algorithms play a huge role to ensure security of data during transmission. This paper presents the various ways to classify and compare different symmetric encryption algorithms based on the process, structure and modes used for encryption and decryption. Also the performance of the widely used symmetric algorithms such as DES, 3DES, AES, and Blowfish are compared in this paper to evaluate the efficiency. The encryption algorithms are used by many application areas, but most of them are not free from attacks. The analysis of block cipher encryption algorithms based on the application areas and vulnerability to various attacks are listed in this paper. These comparisons and analyses will be useful to identify most suitable algorithm for different application areas like cloud, Bigdata, IOT, WSN and MANET. The analysis of encryption algorithms based on the performance and vulnerabilities to various attacks gives the significance of the existing security algorithms in future computing trends and the need of more secure encryption techniques.

Keywords: Encryption algorithm, Network security, Security Attack, Symmetric Encryption, Block Cipher, Cryptography

1. INTRODUCTION

The analysis of various encryption algorithms with large number of applications such as DES [1], 3DES [2], AES [3], Blowfish [4] , Twofish [5], Serpent [6], RC2 [7], RC5 [8], RC6 [9] and IDEA [10] are performed based on the structure used, input block size, key size, applications and attacks happened to them. This is helpful to identify the pros and cons of each algorithm in different platforms or application areas. The performance evaluation of DES, 3DES, AES and Blowfish algorithms based on the encryption speed, decryption speed, throughput and security level is used to identify the suitability of these algorithms in various computing applications. The various attacks possible against different symmetric block cipher algorithms gives the security level of each algorithm. To overcome the limitations of existing algorithms and also to enhance the security against various attacks, new encryption algorithms or modification of algorithms are required periodically.

The communication and networking is important in most of the business applications. Most of the business and military application areas are dealing with sensitive information's. So it is important to protect data transmitted through various networks [11]. Recently WannaCryransomware [12] attacked computers of more than 99 countries in the world. Computer security and network security is always needed to be updated. Cryptography [13] is an important technique to provide security to the data during transmission. Confidentiality, integrity, authentication, availability, access control and non-repudiation are the key security concepts or heart of data security. There are lots of security attacks are trying to break the security concepts to access or modify the information being transmitted. There are lots of encryption algorithms are available to protect the information during transmission by maintaining the key security concepts. The security is an important aspect in the areas of Cloud Computing [14], Internet of things (IOT) [15], Big Data [16], Wireless Sensor Network (WSN) [17], mobile ad hoc network (MANET) [18] and many other application areas.

Most of the encryption algorithms are vulnerable to various security attacks which occur during the transmission of information through the network. Mainly two types of security attacks occur against cryptographic algorithms such as crypt analysis attack and brute-force attack [19]. It is important to understand the algorithms which are resistant against various crypt analytic attacks and brute force attacks for providing better security to various real life computing applications. The main aim of most of the attacks is to get key used for encryption. The key exchange and authentication protocols are important for providing the security to the information transmitted through the network. The studies shows that the expected number of IOT devices in 2020 will be more than 50 billion [20]. The report of International data corporation (IDC) shows that the big data and business analytics market will grow to $203 billion by 2020.The emerging areas like IOT and Bigdata are dealing with large number of real time information's and exchange of those information requires good level of security.

This paper discussed the background of cryptography and different encryption techniques in section II. The section III shows different ways to classify symmetric encryption

techniques. The widely used block cipher encryption structures are compared in section IV. Next section analyze the block cipher modes based on various parameters. Then section VI explains various security concepts and classification of security attacks possible against various symmetric encryption techniques. The section VII analyze major block cipher algorithms with different parameters. Section VIII evaluate the performance of the four most useful algorithms. Final section gives conclusion and relevance of new encryption algorithms.

2. BACKGROUND STUDY

Cryptography has evolved [21] into this fast growing world as an essential technique to provide network security, operating system security, data base security and many other hardware and software security. Cryptography is a procedure used to convert our original data (plain text) into an unreadable format (cipher text) at the time of sending and at the receiver end the cipher text is converted back to the original plain text for secure transmission of data. Cryptographic techniques are classified into substitution ciphers, transposition ciphers [22] and concealment based on how plain text is converted into cipher text. Based on how the keys are used there are mainly two types of cryptographic techniques, symmetric key cryptography (Conventional encryption) [23] and asymmetric key cryptography (Public key encryption) [24] and based on how plain text is processed there are mainly two types of encryption algorithms, block ciphers [25] and stream ciphers [26]. Another way of classifying cryptographic algorithm are mono alphabetic cipher and poly alphabetic cipher [22] based on the mapping of plain text alphabet to cipher text alphabet.

2.1 Substitution Techniques

This is one of the classical encryption technique which involve the substitution of a cipher text symbol for a plain text symbol [22].This method replaces the plain text bit patterns with cipher text bit patterns or plain text letters with other letters, numbers or symbols based on the key values. Examples of this method are Caesar cipher, Playfair cipher and Hill cipher.

2.2 Transposition Techniques

The process of mapping plain text letters to cipher text letters is achieved by performing some permutation on the original plain text letters [22]. This method can be made more secure by performing more than one transposition operation. Examples of transposition ciphers are Rail fence technique and Columnar transposition.

2.3 Asymmetric Key Encryption

Asymmetric key algorithms use two keys, a public key (PU) and a private key (PR) for encryption and decryption as shown in Figure 1. Each user have their own private key and public key. In this algorithm the sender (John) encrypt the plain text message (M) input into cipher text (C) by using the public key PUa of the receiver (Alex), which is known to the parties involved in the transmission. At the receiver end the cipher text is converted back into the original plain text by applying the receiver's private key (PRa) because the receiver's private key and public key are related. So only the authorised person at the receiver end can decrypt the encrypted message. In public key algorithms key exchange is easier but encryption and decryption are complex and time consuming. Also public key algorithms are vulnerable against chosen plain text attack. The main examples of Public key algorithms are RSA, ECC and Diffie-Hellman key exchange algorithm.

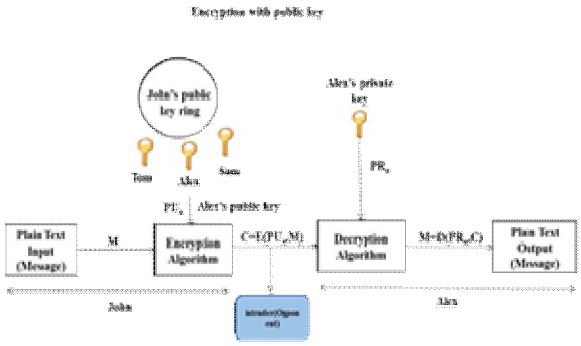

Figure 1 Public key Encryption

The encryption operation at the sender side produce a transmitted Cipher Text, C = E (PUa, M) and decryption at the receiver end gives original plain text, M = D (PRa, C).Public key encryption can be represented as a six tuple, {Plain Text, Encryption Algorithm, Public Key, Private Key, Cipher Text, Decryption Algorithm}.Plain text is the original message or data that is fed in to the algorithm as input. Encryption algorithm performs various transformations on the plain text. Public key and private key are the two keys related to each other and one key is used for encryption and other key is used for decryption. Cipher text is the scrambled message produced as output and it depends on the plain text and the Key. Decryption algorithm produces the original plain text by matching the key on the cipher text.

2.4 Symmetric Key Encryption

The symmetric key encryption algorithms are fast and simple encryption techniques. Here same key (K) and algorithm is used for encryption and decryption as shown in Figure 2. In this method of encryption, the plain text (M) is converted into cipher text (C) using the plain text and secret key which are fed into the encryption algorithm as input. Then at the receiver end the cipher text is converted back to the original plain text by supplying the cipher text and the secret key into the decryption algorithm as input. In conventional encryption algorithms key exchange is an overhead but encryption and decryption operations are fast as compared to public key encryption techniques. Symmetric key encryption algorithms are vulnerable against various cryptanalysis and brute-force attacks. The widely used conventional encryption algorithms are AES and Blowfish.

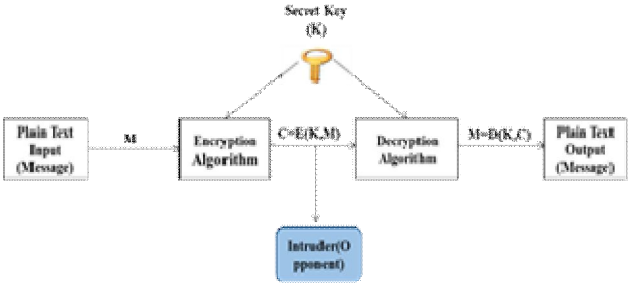

Figure 2 Symmetric key Encryption

The encryption operation at the sender side produces a transmitted Cipher text, C = E (K, M) and decryption at the receiver end gives original plain text, M = D (K, C). Symmetric key encryption can be represented as a 5 tuple, {Plain Text, Encryption Algorithm, Secret Key, Cipher Text, Decryption Algorithm}.Plain text is the original message or data that is fed in to the algorithm as input. Encryption algorithm performs various substitutions and transformations on the plain text. Secret key is an input to the algorithm which is independent of plain text and of the algorithm. Cipher text is the scrambled message produced as output and it depends on the plain text and secret Key. Decryption algorithm is the reverse of encryption algorithm which takes the cipher text and the secret key as input and produces the original plain text.
Symmetric encryption is used to provide privacy to the data or to protect information. Asymmetric encryption is used to authenticate a user, verify a message is authentic and distribute symmetric keys. The Table 1 shows the comparison of symmetric and asymmetric encryption schemes.

Table 1: Comparison of Symmetric and Asymmetric Key Encryption

Symmetric Key Encryption	Asymmetric Key Encryption
Same algorithm and same key is used for encryption and decryption	One algorithm is used for encryption and a related algorithm is used for decryption with two keys, Public key for encryption and its private key pair for decryption
The sender and receiver share the algorithm and key	The sender and receiver have matched pair of keys, no need to exchange keys
The key is kept as secret	Only one key(private key) is kept as secret
Fast encryption and decryption	Slower than conventional encryption
Less complex algorithm for encryption and decryption compared to public key encryption	More complex algorithm for encryption and decryption compared to conventional encryption
Key exchange is an overhead	No Need to exchange keys
Knowledge about the algorithm and sample of cipher text is insufficient to determine the key	Knowledge about the algorithm , one of the keys and sample of cipher text is insufficient to determine the other key

2.5 Stream Ciphers

Stream ciphers perform encryption and decryption on stream of plain text and cipher text, usually one bit or byte at a time. Sometimes stream ciphers operates on one 32-bit word [27]. Stream ciphers are more suitable for real time applications such as multimedia. The example of stream ciphers are A5 and RC4.

2.6 Block Ciphers

Block ciphers perform encryption and decryption on blocks of plain text and cipher text, usually a block size of 64 bits. Sometimes block size is more than 64 bits [27]. Linear cryptanalysis is one of the widely used attacks on block ciphers. The examples of block ciphers are DES, AES and Blowfish.

2.7 Monoalphabetic Cipher

This is one of the substitution technique. This method map the plain text alphabet to cipher text alphabet, that is a single cipher alphabet is used per message [22]. Example of this method is DES.

2.8 Polyalphabetic Cipher

This method is also a substitution technique. This technique uses a set of related monoalphabetic substitution rules based on the key value and the key determines the rule chosen for a given transformation [22]. The examples of this method are Vigenere cipher and Vernam cipher.

3.CLASSIFICATION OF SYMMETRIC ENCRYPTION TECHNIQUES

The symmetric cipher algorithms can be classified into substitution techniques and transposition techniques based on how plain text is converted into cipher. The examples of substitution and transposition techniques are shown inFigure 3.

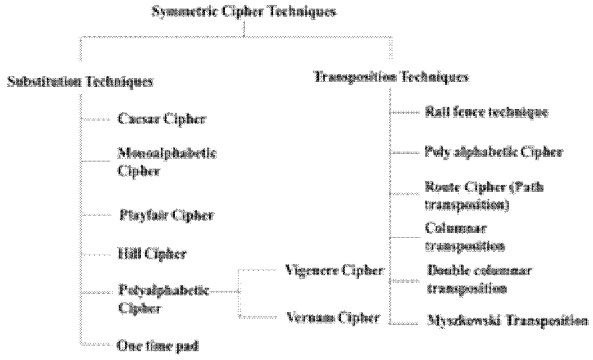

Figure 3 Classification of symmetric ciphers based on how plain text is converted into cipher

The symmetric cipher techniques are also classified into block ciphers and stream ciphers based on how the plain text is processed. The examples of block cipher algorithms are shown in Figure 4.

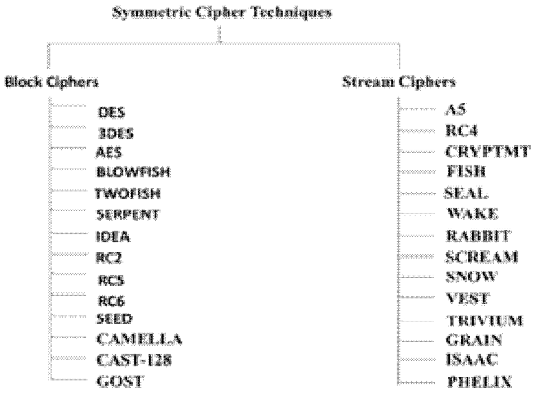

Figure 4 Classification of symmetric cipher algorithms based on how plain text is processed

The block cipher encryption algorithms have wide range of applications in the field of data security. The comparison of the structure used for encryption and decryption and cryptographic modes used for encryption and decryption helps to understand the pros and cons of different block cipher encryption structures and block cipher encryption modes. This study will be useful to understand the working of a block cipher encryption algorithms.

4. COMPARISON OF BLOCK CIPHER ENCRYPTION STRUCTURES

The analysis of block cipher encryption algorithms based on the structures used by them are helpful for understanding the complexity of operations and security level that the algorithms possesses. The common structures used by the block cipher encryption algorithms are Feistel Network structure [28] and Substitution- Permutation Network structure (SPN).

4.1 Feistel Network

The Feistel proposed [28] a symmetric structure which is used for the construction of block ciphers. It is commonly known as Feistel network. Most of the block ciphers are using Feistel network including DES, 3DES, Blowfish, Twofish, RC5 and RC6. The Feistel structure has an advantage as compared to Substitution- Permutation Network structure, that is the encryption and decryption operations are very similar and no need to invert the round function.

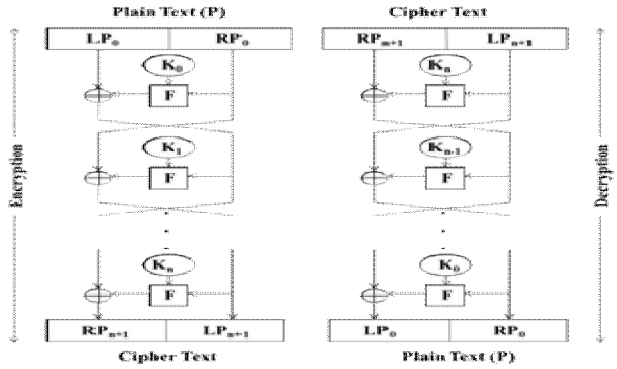

Figure 5 Feistel Encryption and Decryption

The Figure 5 shows the structure of a Feistel network, Where F be the round function and K_0 ,K1, ……, $K_n$are the keys for round 0,1, …....,n. The plain text P is split into two halves $LP_0$and RP_0. For each round i=0, 1, 2,……, n, compute

$LP_{i+1} = RP_i$

$RP_{i+1} = LP_i \oplus F(RP_i, K_i)$

Then the cipher text produced is (RP_{n+1}, LP_{n+1}). Decryption can be performed on the cipher text by computing for i=n, n-1, ……, 0. Then,

$RP_i = LP_{i+1}$

$LP_i = RP_{i+1} \oplus F(LP_{i+1}, K_i)$, It produces the plain text blocks (LP_0,RP_0)

4.2 Substitution –Permutation Network (SPN)

The Substitution-Permutation Network or an SP-network is used for the construction of block ciphers where a series of linked mathematical operations used in block cipher algorithms. The plain text block and key (round keys) is fed into the SPN as input and performs several rounds of substitution and permutation operations alternatively to produce cipher text blocks. Then we reverse the process by inversing the S-boxes and P-boxes and applying the round keys in reversed order for decryption. The SPN network is used by many block cipher algorithms such as AES, Serpent,SAFER, SHARK, and Square.The Figure 6 shows a substitution–permutation network with n rounds, encrypting a plaintext block of 16 bits into a ciphertext block of 16 bits. The S-boxes are the S_i's, the P-boxes are the same P, and the round keys are the K_i's.

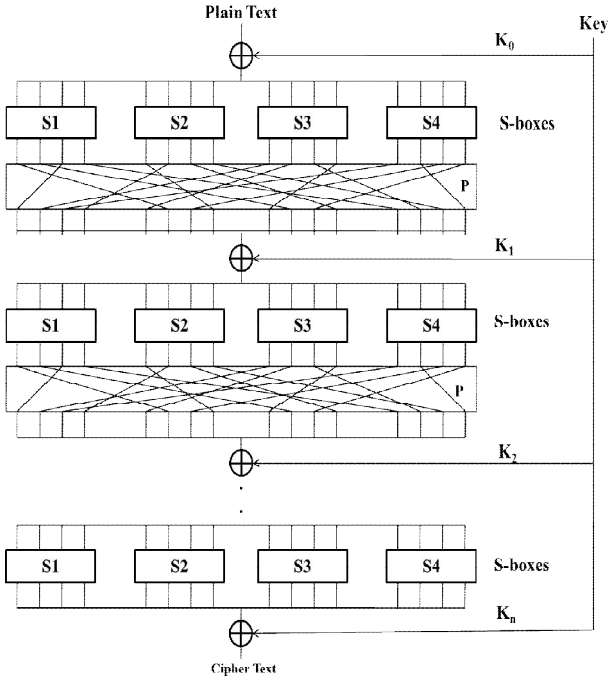

Figure 6 Substitution- Permutation Network

The block cipher encryption algorithms have wide range of applications and most of the block ciphers algorithms are using Feistel and SPN networks. The analysis of these two structures based on their encryption and decryption style,

use of key and round function, complexity of structure and security level is shown in Table 2.

Table 2: Comparison of Feistel and SPN Network

Feistel Network	Substitution-Permutation Network (SPN)
Encryption and decryption oper ations are similar	Encryption and decryption operations are not similar
Each round consisting of a substitution step followed by a permutation step	Alternating rounds of S-boxes and P-boxes to produce the ciphertext block
Decryption is done by applying the key in reverse order	Decryption is done by using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order
Round function does not have to be invertible for decryption	Applying the round keys in reversed order for decryption
Less complex as compared to SPN	More complex operations as compared to Feistel Network
Less Secure as compared to SPN	More Secure and resistant against attacks
Slower than SPN	Faster than a Feistel network
Examples: DES, 3DES, Blowfish, Twofish, RC5 and RC6	Examples: AES, Serpent, SAFER, SHARK, and Square

5. ANALYSIS OF BLOCK CIPHER MODES

Cryptographic modes combines the basic cipher and it consist of simple operations as well as some feedback operations [27]. Cryptographic modes are classified into two based on the way in which plain text is processed, block cipher modes and stream cipher modes. Block ciphers have more applications in the field of data security and network security. The commonly used block cipher modes are Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC) and Propagating Cipher Block Chaining Mode (PCBC), Cipher-Feedback Mode (CFB), Output-feedback (OFB) and Counter (CTR). Some of the block cipher modes can also be implemented as stream cipher, such as CFB, OFB and CTR. The ECB and CBC modes are the commonly used block cipher modes and also they are having large number of applications.

5.1 ECB Mode

ECB mode is the simplest and most common way to use a block cipher where the plain text is divided into blocks and each block encrypted into cipher text blocks separately. In this method the identical plaintext blocks are encrypted into identical ciphertext blocks. Thus the intruder can predict the patterns. So it doesn't provide confidentiality of information, and it is not recommended for use in all cryptographic protocols. The ECB mode encryption and decryption in block cipher mode is shown in Figure 7.

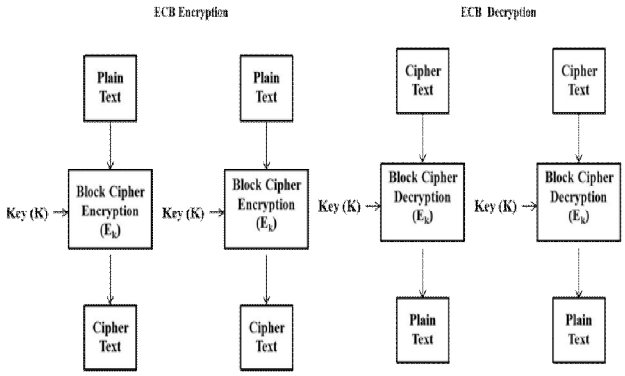

Figure 7 Electronic Codebook Mode

5.2 CBC Mode

This is one of the most commonly used block cipher mode of operation. In CBC mode the encryption is sequential, that is the plain text is XORed with the previous cipher text blocks before encryption. Then the cipher text blocks are decrypted and XORed with the feedback register and this process continues until the end of the message as shown in Figure 8.The mathematical representation shown below. The Main drawback of this method is that a change of one bit in a plaintext or initialization vector affects all the successive ciphertext blocks.

In CBC Encryption, $C_i = E_k(P_i \oplus C_{i-1})$

In CBC Decryption, $P_i = D_k(C_i) \oplus_1$

C_o=Initialization Vector

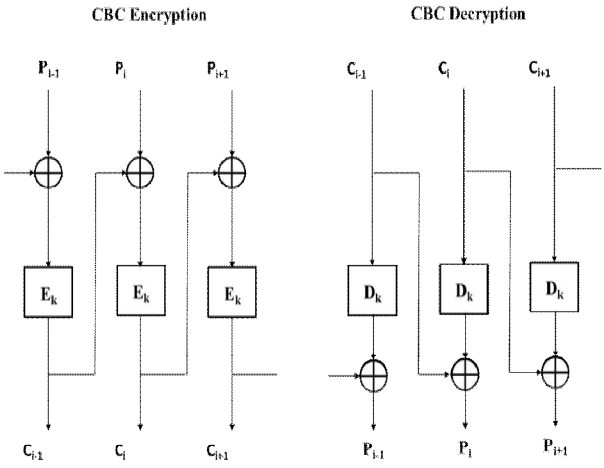

Figure 8 Cipher Block Chaining Mode

The analysis of ECB and CBC block cipher encryption modes are shown in Table 3. This comparison shows that CBC mode is more suitable to encrypt block ciphers if security is the primary concern. The CBC mode of block cipher encryption produces complex ciphertexts as compared to ECB mode. Other encryption modes are more or less similar to CBC mode. So CBC mode of block cipher encryption is more complex and secure among cryptographic modes.

Table 3: Comparison of ECBand CBC Modes

ECB Mode	CBC Mode
Basic form of block cipher encryption	Advanced form of block cipher encryption
Each block encrypted independently	Each ciphertext block is dependent on all plaintext blocks processed up to that point
No Chaining	Chaining occurs
No error propagation	Error propagation
Identical plaintexts encrypted similarly	Identical plaintext block results in different ciphertext by changing IV or the first plaintext
Less Complex	Add Complexity to the encrypted data
Less secure and not widely used	More secure and widely used
Susceptible to replay attacks	Susceptible to Man-in-the-Middle attack

The comparison between different block cipher modes based on various parameters such as encryption is parallelizable, decryption is parallelizable, random read access, chaining occurs and error propagation is shown in Table 4. This analysis gives a clear idea about the structure and various features of different block cipher modes of operations.

Table 4: Comparison of Block Cipher Modes

Cryptographic Mode	Encryption parallelizable	Decryption parallelizable	Random read access	Chaining	Error Propagation
ECB	✓	✓	✓	×	×
CBC	×	✓	✓	✓	✓
PCBC	×	×	×	✓	✓
CFB	×	✓	✓	✓	✓
OFB	×	×	×	×	✓
CTR	✓	✓	✓	×	×

6. ANALYSIS OF SECURITY ATTACKS

The symmetric encryption algorithms are widely used to provide security for many application areas such as Cloud computing, IOT, WSN and MANET and other real life products. These symmetric encryption algorithms are protecting data in the system and also the information's transmitted through the network by ensuring the key security concepts. The attackers are trying to decrypt the scrambled messages by breaking the security concepts.

6.1 Security Concepts

The aim of every security mechanism is to maintain key security concepts during the transmission of information. The system or data in the network is said to be secure only if the security concepts such as Confidentiality, integrity, authentication, availability, Access control and non-repudiation is maintained. Confidentiality preserves authorized access to information and ensures data confidentiality and privacy. Confidentiality is ensured by preventing unauthorized access to data in the system and also data transmitted through the network. The integrity of data and system is ensured by preventing unauthorized modification or destruction of information. Authenticity verifies the parties involved in the transmission. Authenticity is the property of being genuine. The validity of a message, message originator and transmission is being verified and trusted. Availability is the reliable access to data for all authorized users at all time. In non-repudiation, the authorship of the transmitted message can be verified successfully. This service prevent the authors from denying the authorship of a message. Access Control is the ability to limit and control access to host systems and applications via communication link.

6.2 Security Attacks

The intruders or attackers are trying to get information's or messages stored in a system or data transmitted through the network through different attacks. The attacks which are successful against different security mechanisms shows the weakness of the security system used to detect and prevent from various attacks. The different security attacks are generally classified as Passive attack and active attack as shown in Figure 9.

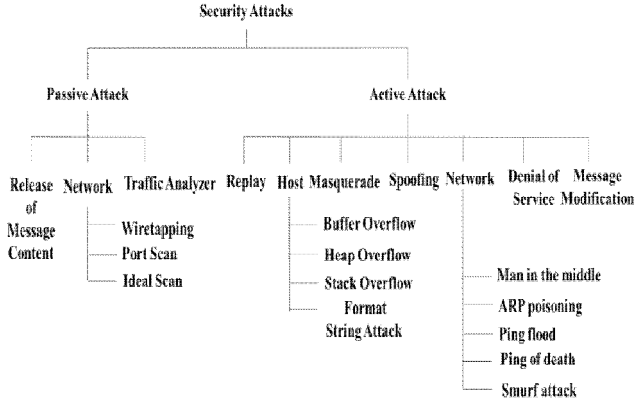

Figure 9 Classification of security Attack

Many of the conventional encryption algorithms are not successful against various security attacks. The attacks possible against different symmetric encryption algorithms are shown in Figure 10. There are mainly two types of approach to attack a symmetric encryption scheme, Cryptanalysis attacks and Brute –force attacks. The main objective of attacking an encryption scheme is to recover the key used for encryption.

6.2.1Cryptanalysis

The cryptanalysis attacks are trying to find the weakness of the code, cipher, cryptographic protocol or key management schemes. The examples of crypt analysis attack include Chosen plain text attack, Cipher text only attack, Known plain text attack, Chosen Text attack, Chosen Cipher Text attack, Meet-in-the-Middle attack,

XSL attack, Side Chanel attack and many other attacks as shown in Figure 10.

6.2.2 Brute-force attack

In brute-force attack, attackers try every possible key on the cipher text blocks until the successful translation of cipher text into plain text is obtained. Examples are shown in the Figure 10.

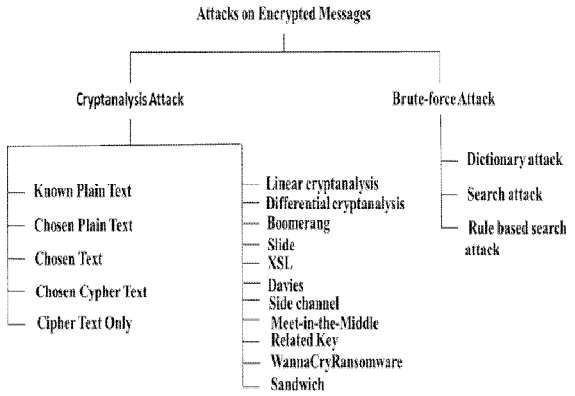

Figure 10 Attacks on Encrypted messages

The cryptanalysis attacks occur against various block cipher algorithms are shown in Table 5. The cryptanalysis attacks are classified based on the amount of information known to cryptanalyst. This analysis shows various information's used by the cryptanalyst to attack an encrypted message.

Table 5: Attacks on Encrypted Messages

Security Attacks	Information Known to Cryptanalyst
Known Plaintext	Encryption Algorithm Cipher text One or more Plain text and Cipher text Pairs formed with secret key
Side Channel	Timing information Power consumption Electromagnetic leaks or sound Technical knowledge of the internal operation of the system
Chosen Plaintext	Encryption Algorithm Cipher text Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Chosen Text	Encryption Algorithm Cipher text Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key Cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key
Cipher Text Only or Known Cipher Text	Encryption Algorithm Cipher text
Chosen Cipher Text	Encryption Algorithm Cipher text Cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key
Linear Crypt analysis	Encryption Algorithm Cipher text Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Boomerang attack	Encryption Algorithm Cipher text Plain text
Differential Crypt analysis	Encryption Algorithm Cipher text Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Davies attack	Encryption Algorithm Cipher text One or more Plain text and Cipher text Pairs formed with secret key

7. ANALYSIS OF BLOCK CIPHER ALGORITHMS

The block cipher algorithms are widely used in many applications. The analysis of the commonly used block cipher algorithms with their application areas and vulnerability to various attacks are shown in Table 6.This analysis is helpful to understand the structure used by different block cipher algorithms for encryption and decryption, their block sizes, key sizes and number of rounds of operations. The vulnerabilities of various algorithms still gives some scope to improve existing symmetric encryption algorithms.

Table 6: Comparison of Block Cipher Encryption Algorithms

Algorithm	Block Size (bits)	Key Size (bits)	Structure	Rounds	Applications	Attacks Possible
DES	64	56	Feistel Network	16	Educational Purpose	Brute force attack, Differential Cryptanalysis(DC), linear cryptanalysis (LC), and Davie's attack
3DES	64	56,112,168	Feistel Network	48	Smart Payment Cards, ATM	Meet-in-the-middle attack, Chosen-plaintext or known plaintext attack
AES	128	128,192,256	Substitution-Permutation network	10,12,14	Hardwares, Smart Cards, High performance computers, Cloud	Cryptanalysis, side channel attack, XSL attack
Blowfish	64	32-448	Feistel Network	16	Image encryption and decryption, ATM	Birthday attack, Known-Plaintext attacks
Twofish	128	128,192,256	Feistel Network	16	File, Folder and e-mail encryption	Differential cryptanalysis attack
Serpent	128	128,192,256	Substitution-Permutation network	32	File, and Folder encryption	Meet-in-the-middle attack, amplified-boomerang attack, linear cryptanalysis, XSL attack

RC2	64	8–1024	Source-heavy unbalanced F eistel network	16 of type MIXING, 2 of type MASHING	System Security	Related-key attack, Chosen-plaintext attack
RC5	32, 64 or 128	0 to 2040	Feistel – like Network	1-255	Cluster Computing	Differential attack, Brute force
RC6	128	128,192,256	Feistel Network	20	Network Communication	Plaintext attack, X2 -attack
IDEA	64	128	Lai-massey scheme	8.5	PGP	Differential attack, Meet-in-the-middle attack, Narrow-bicliques attack

8. PERFORMANCE ANALYSIS OF SYMMETRIC BLOCK CIPHER ALGORITHMS

The performance of the DES, 3DES, AES and Blowfish algorithms are analyzed based on the encryption time and decryption time. The data (Text file) with different packet size is used for calculating the average encryption time and average decryption time. Then throughput is calculated from the encryption time and decryption time.

8.1 Experimental Setup

The performance of the encryption algorithms are evaluated using Java programming language with javax.cryptoand Java.security packages available in Java Cryptography Extension (JCE) which is an extension to java platform and part of Java Cryptography Architecture (JCA). The experiments are conducted using Intel(R) Core(TM) i-5-3470 CPU @ 3.20 GHz 3.20 GHz processor with 4GB of RAM on Windows 7 64 Bit Enterprise SOE v1.7 operating system. The development kit used for the compilation of simulation program is Jdk 1.8.0_102. The encoding scheme used is Base64 Encoding. The experiments are conducted many times to ensure consistency of results.

8.2 Result Analysis

The simulation results of encryption time and decryption time for various encryption algorithms in milliseconds with different packet size used is given in Table 7 and Table 8. The encryption time and decryption time is used to calculate the throughput of encryption and decryption. The throughputs gives the speed of different encryption and decryption algorithms. It is calculated by dividing the total size of packets used in Kilobytes with total time for encryption or decryption in seconds for each algorithm.

Table 7: Execution Time for Encryption (milliseconds)

Size on Disk	DES	3DES	AES	Blowfish
16	4	4	3	2
44	6	9	4	3
100	9	16	6	5
208	13	25	8	8
520	28	51	17	22
892	32	75	17	28
1040	38	87	18	32
Throughput (Kb/sec)	21692.31	10561.8	38630.14	28200

Table 8: Execution Time for Decryption (milliseconds)

Size on Disk	DES	3DES	AES	Blowfish
16	1	2	3	2
44	4	7	6	3
100	8	11	8	5
208	12	19	9	8
520	26	41	14	14
892	39	67	15	22
1040	42	81	16	25
Throughput (Kb/sec)	21363.64	12368.42	39718.31	35696.2

The comparison of execution time (milliseconds) of different symmetric block cipher algorithms for encryption and decryption is shown in Figure 11 and Figure 12. It shows that on an average AES is taking less time for encryption and decryption as compared to other algorithms. But for small sized packets Blowfish algorithm taking less time for encryption and decryption.

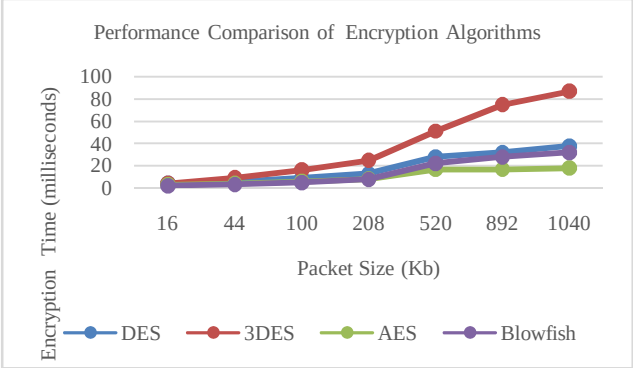

Figure 11 Comparison of Encryption Time of Block Cipher Algorithms

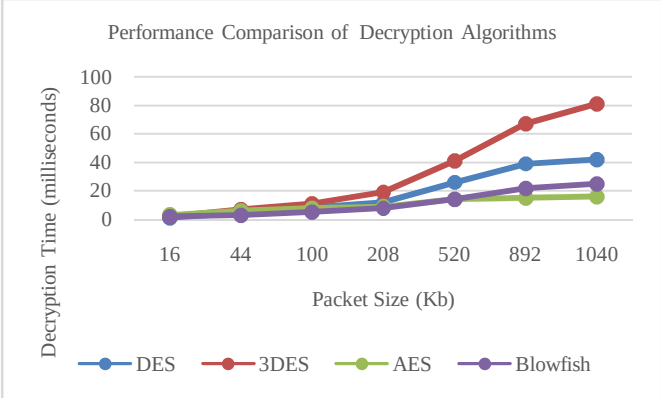

Figure 12 Comparison of Decryption Time of Block Cipher Algorithms

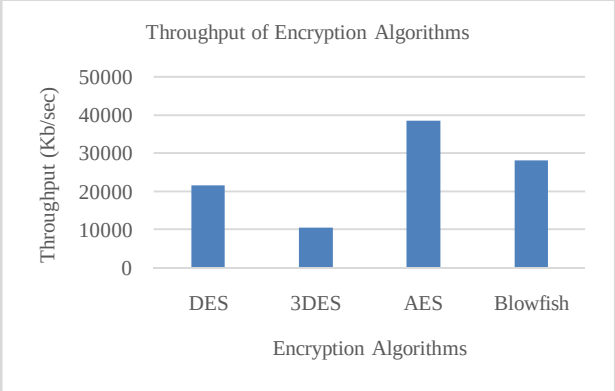

Figure 13 Comparison of Average Throughput of Encryption Algorithms

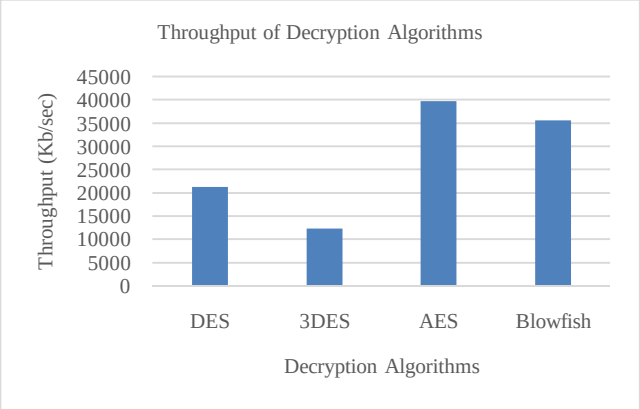

Figure 14 Comparison of Average Throughput of Decryption Algorithms

The comparison of throughput of encryption in block ciphers is shown in Figure 13 and throughput of decryption is shown in Figure 14. The performance analysis of block cipher algorithms based on average throughput is shown in Figure 15. The analysis of time taken by block cipher algorithms for encryption and decryption and average throughput values shows that AES is the faster algorithm than Blowfish, DES and 3DES. The throughput of Blowfish algorithm is better for small sized packets as compared to AES. So Blowfish is more suitable for applications dealing with small sized packets such as IOT applications.

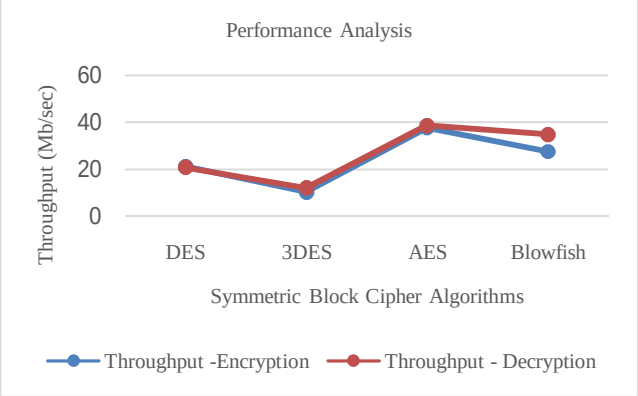

Figure 15 Performance Analysis of Block cipher Algorithms based on Average Throughput

9. CONCLUSION

This paper presents different ways toclassify symmetric encryption algorithms. This analytical study gives a fair review on cryptographic techniques and pros and cons of various symmetric key encryption algorithms. This paper also shows the importance of block ciphers and block cipher modes of encryption and decryption to enhance security. This paper performed an analysis of various security attacks possible againstblock cipher encryption algorithms. Then different block cipher algorithms are compared based on their block size, key size, number of rounds, cryptographic structure, application areas and vulnerability against various security attacks. The performance evaluation of DES, 3DES, AES and Blowfish algorithms has done based on the throughputs of encryption and decryption. This analysis shows that AES is the better algorithm for Cloud, Bigdata, WSN and MANET applications as far as security and overall performance is considered. AES does not have any well known weak points so far. The AES algorithm with complex rounds, larger key size and larger number of rounds considered as more secure and resistant against all types of existing security attacks. Blowfish is considered as faster algorithm for small sized packets and it is suitable for IOT applications. This study shows the limitations of existing encryption algorithms in different perspective and relevance to modify it or to develop new algorithms to face challenges in a fast growing technological world.

References

[1]. National Bureau ofStandards – Data Encryption Standard, FIPS Publication 46, 1977.
[2]. Wayne G. Barker, “Introductiontotheanalysis of the Data Encryption Standard (DES)”, A cryptographicseries, Vol. 55, p. viii + 190, Aegean Park Press, 1991.
[3]. J. Daemen and V. Rijmen, “AES Proposal: Rijndael”, Original AES submissiontoNIST, 1999. AES Processing Standards Publications, http://www.csrc. nist.gov/publications/fips/fips197/fips-197.pdf
[4]. BruceSchneier, “TheBlowfishencryption algorithm”, Dr. Dobb’sJournalof Software Tools, 19(4), p. 38, 40, 98, 99, April 1994.
[5]. Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson (1999-03-22). TheTwofishEncryptionAlgorithm: A 128-Bit Block Cipher. New York City: JohnWiley&Sons. ISBN 0-471-35381-7.
[6]. RossJ. Anderson (2006-10-23). "Serpent:ACandidate BlockCipherfortheAdvanced EncryptionStandard". Universityof Cambridge Computer Laboratory. Retrieved 2013-01-14.
[7]. Lars R. Knudsen, VincentRijmen, Ronald L. Rivest, Matthew J. B. Robshaw: OntheDesign and Security of RC2. Fast Software Encryption 1998: 206–221.
[8]. Ronald L. Rivest, “RC5Encryption Algorithm”, Dr DobbsJournal, Vol.226, PP. 146-148, Jan 1995.

[9]. Ronald L. Rivest, M. J. B. Robshaw, R.Sidneyand Y. L. Yin, "TheRC6 Block Cipher", M. I. T. LaboratoryforComputerScience, 545 Technology Square, Cambridge, MA 02139, Version 1.1-August 20, 1998.
[10]. Nick Hoffman, "A SimplifiedIDEA Algorithm", Cryptologia, Taylor & Francis, Inc. Bristol, PA, USA , doi:10.1080/01611190701215640.
[11]. Schneier B.Secretand Lies: Digital Security in a NetworkedWorld. Wiley; 2000.
[12]. Young, A.; M. Yung(1996). Cryptovirology: Extortion-basedsecuritythreatsand countermeasures. IEEE Symposiumon Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.
[13]. Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbookof TheoreticalComputer Science. 1. Elsevier.
[14]. Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, MatsNaslund, MakanPourzandi"A quantitativeanalysis of current securityconcerns and solutionsforcloud computing", Springer 2012.
[15]. M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards ananalysis of securityissues, challenges, and open problemsin theinternet ofthings", in services (SERVICES), 2015 IEEE WorldCongresson, June 2015, pp.21-28.
[16]. Couch N and Robins B, Big Data forDefenceand Security, report, RoyalUnitedServicesInstitute (RUSI), 2013; pp. 2 -36.
[17]. Chris Karl of, David Wagner, "SecureRouting in WirelessSensor Networks: Attacksand Countermeasures", AdHocNetworks (elsevier) Page: 299-302, year 2003.
[18]. Stajano F, Anderson RJ. There surrecting duckling: security issues for ad-hoc wireless networks. In: Proceedings of the seventh international workshop On security protocols; 1999. p. 172–94.
[19]. [19] Muhammad IrfanAziz, SaleemAkbar, "Introduction
[20]. tocryptography", ISBN 0-7803-9262-0/05 IEEE, 2005.
[21]. Verizon (January, 2015).Createintelligent, more meaningfulbusinessconnections. Retrievedfrom http:// www.Verizonenterprise .com/solutions/connected-machines/
[22]. Van Tilborg, HenkC. A.;Jajodia, Sushil, eds. Encyclopedia ofCryptographyand Security. Springer. ISBN 978-1-4419-5905-8., p. 455, 2011.
[23]. William Stallings, "Cryptographyand Network Security Principles and Practice" , Pearson Education Inc., 2014.
[24]. Delfs, Hans &Knebl, Helmut ,"Symmetric-key encryption". Introductiontocryptography: principles
[25]. andapplications. Springer. ISBN 9783540492436, 2007.
[26]. NinghuiLi,"AsymmetricEncryption",Springer,DOI: https://doi.org/10.1007/978-0-387-39940-9_1485.
[27]. M. J. B.Robshaw, "Block Ciphers", TechnicalReport, RSALaboratories,Number TR – 601, July 1994.
[28]. M. J. B. Robshaw, "StreamCiphers", Technical Report, RSA Data Security, Inc., Number TR – 701, p. 46, July 1995.
[29]. BruiceSchneier, "AppliedCryptographyProtocols, algorithms, and SourceCode in C", Wiley Inc., 2015.
[30]. Feistel. H, "Cryptography and Computerprivacy", Scientific American, May 1973.

AUTHORS

Anuraj C.K received the B.Techdegree in Computer Science and Engineering from M.G. University, Kottayam in 2011 and M.E. degree in Computer Science and Engineering from Anna University, Chennai in 2014. He now with Division of Information Technology, School of Engineering , Cochin University of Science and Technology for doing research in the field of networks and security. His area of interests include Cryptography, Network Security, Cloud Computing and IOT security.

Dr. Shelbi Josephreceived theBE. Degree from University of Madrasin 1992 in Computer Science and M.Tech degree in Computer Sciencefrom Department of Computer Science, National Institute ofTechnology, Tiruchirappalli in 2006. He spent seven years in softwareindustry, and currently working as Assistant professor, Division ofInformation Technology, School of Engineering, Cochin University ofScience and Technology.He carried out his research work leading to Ph.D at School ofEngineering, Cochin University of Science and Technology in SoftwareReliability. His areas of interest are Software Engineering, SoftwareReliability, Open Source Software and Data Mining.