Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Cryptography Techniques

Vikrant M. Adki, Prof. Shubhanand S. Hatkar
Department of Computer Science and Engineering, SGGSIE&T, Vishnupuri, Nanded, Maharashtra, India

Abstract— In modern world security of the wired and wireless network is an important thing. The cryptography has a major role in providing the security to these networks. The mobile nodes can freely move and join or leave the network at anywhere and anytime. The open architecture and dynamic topology coupled with lack of infrastructure make wireless networks vulnerable to variety of attacks. The various types of attacks can possible on wired and wireless networks such as Ciphertext attacks, Brute force attacks, Known plaintext attacks, Denial of service attacks, Side channel attacks etc. These types of attacks can be prevented by implementing various cryptographic techniques to provide security to user data. This paper includes a comparison of mostly used symmetric algorithms based on performance. In this paper, we observe encryption as well as decryption time of different algorithms with the random size of data packets. These results show that Blowfish method is fast and efficient as compared to other algorithms.

Keywords— Encryption, Decryption, AES, DES, Blowfish, RSA.

I. INTRODUCTION

Cryptography [1][2], is a technique in which storing and transmitting data in a particular form so that only intended user can read and process it. Cryptography is concerned with developing different types of techniques that prevent reading private messages from attackers. As the Internet and different types of electronic devices turn out to be more pervasive, electronic security is turning out to be progressively essential. Cryptography is utilized to secure email messages, MasterCard data, and corporate information. The cryptography is used in various fields like wired networks and wireless networks etc. The important objectives of cryptography are confidentiality, authentication, integrity, non-repudiation, access control and availability. In order to perform encryption and decryption the various cryptographic techniques are used such as AES, DES, 3DES, Blowfish and RSA. These techniques have different key size, block size and number of round and each methods have different execution time and throughput. The cryptography is classified into two types Symmetric Key Systems and Asymmetric Key Systems. In Symmetric Key Systems same keys are used where as in Asymmetric Key Systems various keys are used for encryption and decryption.

II. LITERATURE SURVEY

The different methods used in cryptography explained below.

A. Cryptography

- Plain Text: It is the original form data that a sender wants to send to the receiver. It is an original understandable message that is input to the algorithm.
- Ciphertext: Ciphertext is the scrambled content or message in its coded human unreadable form. The ciphertext is the output of encryption process and input of decryption process If two different keys used for encryption of a message, then two different ciphertexts are produced.
- Encryption Algorithm: It performs different techniques such as substitution and transformation on the plaintext to obtain ciphertext.
- Decryption Algorithm: It is the exactly opposite procedure of encryption technique. To obtain original plaintext it uses ciphertext and secret key.
- Secret Key: The secret key is input to an encryption process. The key value is independent of plaintext and algorithm. Depending on the key being used, the algorithm gives various output. The exact operation performed on that algorithm depend on the key.

B. Need of Cryptography

- Confidentiality: Its main feature is that only sender and receiver should access the contents of message or data. A loss of confidentiality leads to the unauthorized revelation of data.
- Authentication: The authentication is the important feature of being authentic and it is verified and trusted. This method guarantees that the sender of the message should correctly identify.
- Integrity: This property guarantees that the data in the message do not change when it reaches to the receiver. A loss of integrity is an unauthorized modification of message contents.
- Non-repudiation: Gives security against denial by one of the parties required in a communication of having taken an interest in all or part of the correspondence.

- Access Control: Its main function is to prevent illegal use of resources.
- Availability: It guarantees that system will work good and service given to only authorized users.

C. Different Cryptography Techniques

There are two types of cryptography techniques, and they are as follows:

1. *Symmetric Key Cryptography:* To perform operations identical keys are used. It is a conventional system. The Symmetric encryption changes over plaintext into ciphertext utilizing a secret key and encryption algorithm. To obtain plaintext form ciphertext, the decryption algorithm, and same keys should apply to the ciphertext.
2. *Asymmetric Key Cryptography:* In this procedure, two keys are utilized to scramble and decode a message with the goal that it arrives safely at the receiver. Hence also known as Public Key Cryptography. In this method the key is utilized for encryption a message is not quite the same as the key used to decode the message, and each uses two keys, public key and private key for encryption and decryption respectively. When Alice needs to communicate with Bob, then Bob's public key is utilized to encode the message, then by using the private key to Bob decode it.

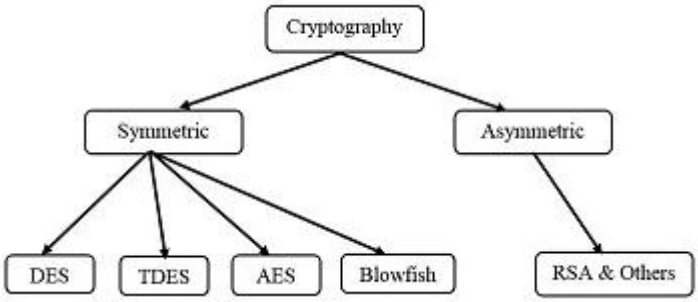

Fig. 1 Classification of Cryptography

III. RELATED WORK

In this section, we describe existing work done on algorithms.

A. DES

The Data Encryption Standard (DES) is popular encryption technique and used by a large number of persons. The DES is block cipher technique in which it uses the same key for to encode and decode. The Block size and Key size DES is 64-bits and 56-bits respectively. It consists of 16 identical stages (Rounds), Initial Permutation (IP) and Final Permutation (FP). The DES consist of following steps:

1. In the first step 64-bit, the plaintext is given as input to the IP and IP is performed on plaintext and to obtain the Permuted Input it rearranges the bits.
2. The second step includes of 16-rounds of the same function, and it also contains permutation and substitution methods.
3. The last round (sixteenth) output contains 64-bits, and they are a function of input plaintext and key
4. By swapping the output of left and right side, the preout is produced.
5. At that point preout is gone through IP i.e. opposite of IP to create 64-bit ciphertext.

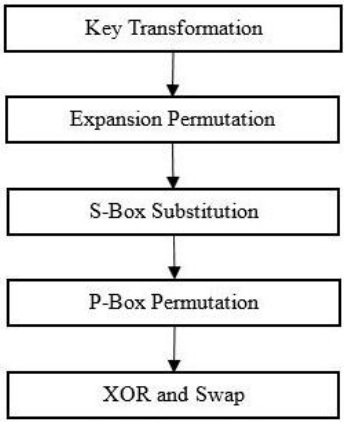

Fig. 2 Single Round DES

B. 3DES

Triple-DES is Triple Data Encryption (TDES) with 56,112 or 168-bits key size. The TDES has an Encrypt-Decrypt-Encrypt pattern for Encryption and Decrypt-Encrypt-Decrypt pattern for Decryption. The TDES Encryption has following steps:

1. The First key is for encryption of plaintext
2. The Second key is for decryption of encrypted message produced by Step 1.
3. The Third key is for encryption of decrypted message produced by Step 2.

$$ciphertext = E_{k3}(D_{k2}(E_{k1}(plaintext)))$$

Where C(t)= Ciphertext produced when encryption performed on plaintext.
E_{k1} and E_{k3} = DES Encryption using key k1 and key k3 respectively
D_{k2} = DES Decryption using key k2
The TDES Encryption has following steps:

1. The First key is for decryption of ciphertext.
2. The Second key is for encryption of decrypted message produced by Step 1.
3. The Third key is for decryption of encrypted message produced by Step 2.

$$plaintext = D_{k1}(E_{k2}(D_{k3}(ciphertext)))$$

D_{k1} = DES Decryption using key k1
E_{k2} = DES Encryption using key k2
D_{k3} = DES Decryption using key k3

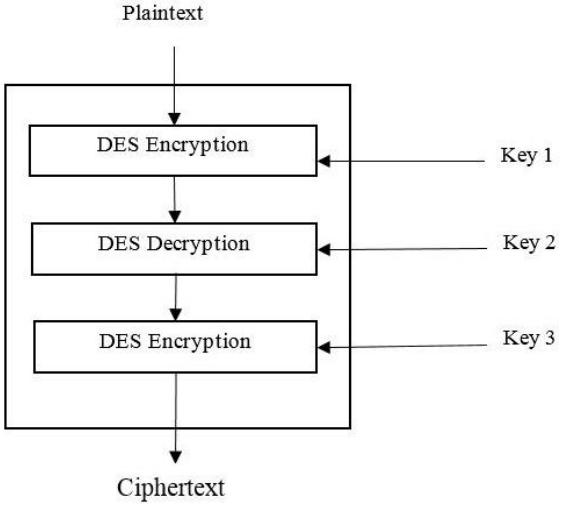

Fig. 3 TDES Encryption

This three-step technique is called triple-DES. Its block size is 64-bits. Initially, TDES calculation by three keys needs 2^{168} conceivable mixes and with two keys needs 2^{112} conceivable mixes. It is impractical to attempt such a major mix, so TDES is the strongest encryption algorithm and gives an application in the banking sector. The major disadvantage is time-consuming.

C. AES

It is a symmetric block cipher developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen in 1998.The AES stands for Advanced Encryption Standard and based on design method called as a substitution-permutation network. The AES-128, AES-192, and AES-256 block ciphers are included in it. Every cipher encodes and decodes information in the block of 128-bits utilizing cryptographic keys of 128-bits, 192-bits, and 256-bits respectively. The AES is a symmetric cipher and it uses the identical key to perform encryption and decryption on message. For 10 rounds, 12 rounds and 14 rounds AES use 128-bits, 192-bits and 256-bits keys are used respectively.

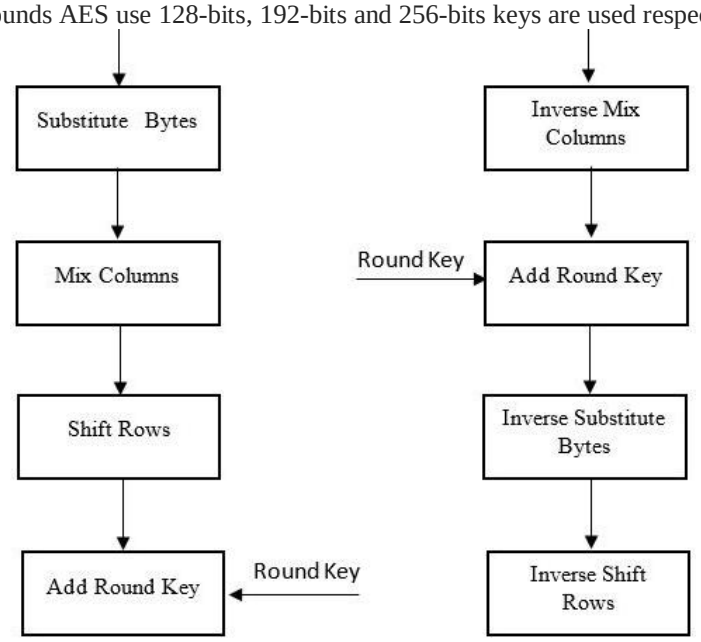

Fig. 4 AES process for Single Round

The AES Encryption, Decryption, and processing round have following 4-stages:

1. Substitute byte: To carry out a byte-by-byte substitution of the block it uses an S-box.
2. Shift rows: A simple permutation.
3. Mix column: A substitution that makes use of arithmetic over GF(2^8).
4. Add round key: A simple bitwise XOR of the current block with a portion of expanded key.

D. Blowfish

It is a designed by Bruce Schneier in 1993. It is symmetric block cipher technique. Its block size is 64-bit, and key length is variable. Its variable key length ranges from 32-bits to 448-bits. It is one of the fastest technique which has developed up to date [4]. This algorithm is unpatented and placed in the public domain due to which it can be used freely by anyone. Blowfish algorithm contains two parts Key Expansion and Data Encryption. The key of the Blowfish calculation is 448 bits, so it requires 2^{448} mixes to look at all keys.

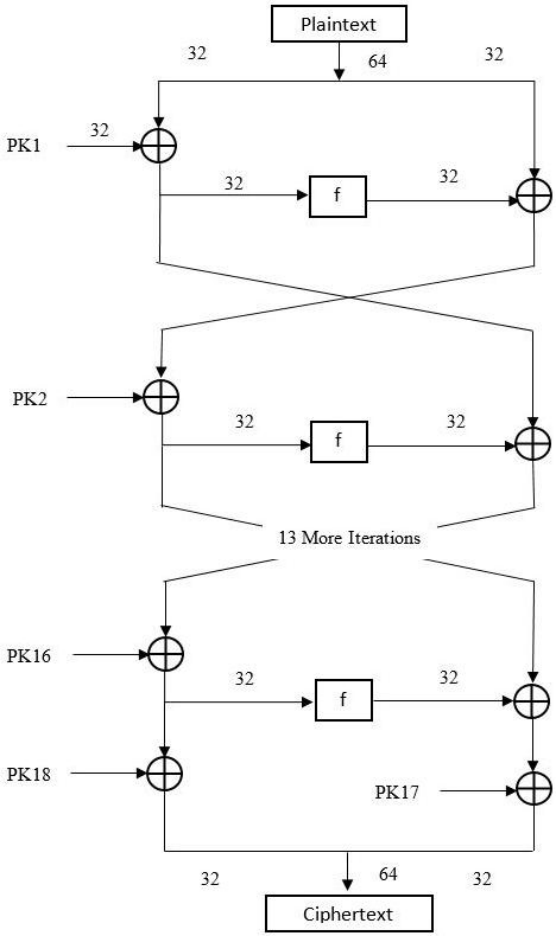

Fig. 5 Blowfish Encryption

E. RSA

This algorithm was developed at MIT in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA). It is public-key cryptosystem used for secure data transmission. This algorithm uses two keys, first to encrypt second to decrypt. The public key used for encryption of messages and decrypted by using the private key. In this method, any one key is kept secret. The following steps are performed to obtain the keys for RSA algorithm:

1. Select two large prime numbers a and b.
2. Calculate n=a*b; where n is modulus for both keys.
3. Select e (public key) such that it is not a factor of (a-1) (b-1).
4. Calculate d (private key) such that:
   d*e mod (a-1) (b-1)=1.
5. For encryption, calculate the ciphertext C from plaintext M as $C= M^e \bmod n$.
6. For decryption, calculate the plaintext M from the ciphertext C as $M= C^d \bmod n$

F. Comparision

Table I Comparision of Different algorithms

Algorithm	Developed By	Algorithm Pattern	Size of key (bits)	Size of Block (Bits)	Number Of Round	Attack
DES	IBM in 1975	Feistel Network	56	64	16	Brute Force Attack

3DES	IBM in 1998	Feistel Network	56, 112 or 168	64	48	Theoretically Possible
AES	Joan Daemen and Vincent Rijmen in 1998	Substitution-Permutation Network	128, 192 or 256	128	10, 12 or 14	Side Channel Attacks
Blowfish	Bruce Schneier in 1993	Feistel Network	32-448	64	16	Not Yet

IV. ADVANTAGES AND DISADVANTAGES

A. DES

1) Advantages:

a) DES was introduced long time ago in 1977, so no real weakness was found.

b) A DES is likewise an ANSI and ISO standard so anybody can learn and execute it.

2) Disadvantages:

a) It's key size.

b) It is fast in Hardware implementation as compared to software implementation.

B. 3DES

1) Advantages:

a) TDES is a technique to reuse DES executions, by falling three examples of DES (with particular keys).

b) TDES is secure up to no less than 2^{112} security, so it is unbreakable with today's innovation.

2) Disadvantages:

a) It is moderate, particularly in programming.

b) It has low performance.

C. AES

1) Advantages:

a) This method is more secure as compared to other techniques.

b) It supports larger key size than DES and TDES.

2) Disadvantages:

a) It has low performance.

D. Blowfish

1) Advantages:

a) It is symmetric block cipher and used as an option for DES.

b) As it uses variable length key from 32-bits to 448-bits making it suitable for both residential and exportable use.

c) Since it released in 1993 so the Blowfish code is not cracked up till now.

d) It has faster performance than other encryption algorithms.

2) Disadvantages:

a) It requires more space for the cipher text because of difference between key size and block size.

E. RSA

1) Advantages:

a) The Public Key encryption and increased security is major advantage of RSA algorithm.

b) As it uses two keys, then public key is used for encryption and private key for decryption.

c) In RSA algorithm, the private keys are never transmitted nor revealed.

d) It provides a method for digital signature and that cannot repudiate.

2) Disadvantages:

a) The speed is a major disadvantage of the public key system.

b) The Public Key Cryptography might be defenseless against mimic, regardless of the fact that client's private keys are not accessible.

From the above discussion, Blowfish algorithm is better than other algorithms regarding processing time. Gurjeevan Singh, Ashwani Kumar Singla and K.S. Sandha [3] have provided analysis of the algorithm. The following encryption algorithms AES, DES, 3DES, and Blowfish are executed with a various text file with different size. The experiment results shown below: The Table 2 consist of a comparison of encryption and the Table 3 consist of decryption time. The both tables contain execution time of encryption algorithm and decryption algorithm in a various text file with different size.

Table II Comparison Of Encryption Time (In Milliseconds) Of All Four Methods With Variable Size Of Packets

Text File Size in Kbytes	**AES**	**3DES**	**Blowfish**	**DES**
20	42	34	25	20
48	55	55	37	30

108	40	48	45	35
241	91	82	46	51
322	115	115	48	47
780	165	170	65	85
910	213	230	68	145
5501	260	310	120	250
7200	210	286	109	260
7838	1240	1470	122	1280
22335	1370	1800	155	1720
42000	1530	2300	165	2100
99000	1720	2750	190	2600
Average Time	542.38	742.30	91.92	663.30

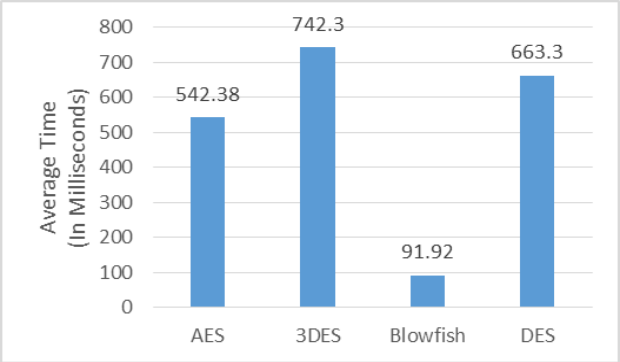

Fig. 6 Encryption Time (In Milliseconds)

Table III Comparison of Decryption time (in milliseconds) of all four methods with variable size of packets

Text File Size in Kbytes	**AES**	**3DES**	**Blowfish**	**DES**
20	45	40	28	34
48	63	53	37	50
108	57	50	29	47
241	61	78	53	72
322	77	88	67	75
780	150	151	95	122
910	144	173	90	160
5501	172	180	102	168
7200	165	1108	85	988
7838	660	1507	150	1052
22335	885	1708	140	1200
42000	998	2030	190	1800
99000	1208	2730	210	2200
Average Time	360.38	761.23	98.15	612.92

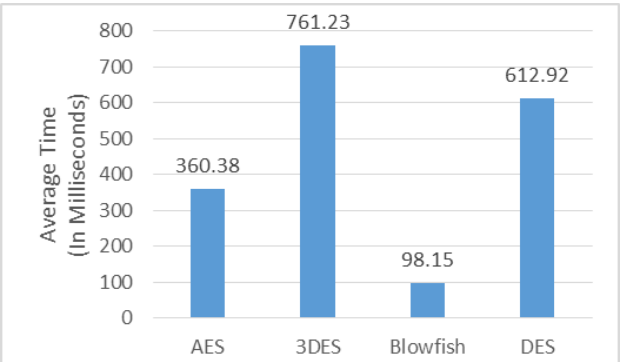

Fig. 7 Decryption Time (In Milliseconds)

V. CONCLUSIONS

In this wireless world nowadays the security of information is a more critical viewpoint. This paper shows the performance analysis of DES, 3DES, AES and Blowfish algorithms and above results demonstrate that Blowfish algorithm has higher performance regarding encryption time and decryption time and 3DES is less efficient as compared to other algorithms. In Future, we improve throughput and speed by using encryption and decryption methods. It can take low processing time and low power consumption. In future, we concentrate on the picture, sound and video for creating more grounded encryption algorithm with rapid, throughput, and less energy & less power consumption.

REFERENCES

[1] A William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.
[3] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha "Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.7
[4] Pratap Chandra Mandal "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
[5] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Technique", International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 4, July-August 2014
[6] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[7] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.
[8] E. Thambiraja, G.Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques," International Journal of Advanced Research in ComputerScience and Software Engineering, Vol 2, Issue 7, July 2012.
[9] Monika Agrawal, Pradeep Mishra," A Comparative Survey of Symmetric Key Encryption Techniques," International Journal of Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

