International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

A Survey on Various Cryptography Techniques

Mitali[1], Vijay Kumar[2] and Arvind Sharma[3]

[1,2,3]Swami Devi Dyal Group of Professional Institutions, Barwala,
Distt. Panchkula, Haryana, India

Abstract

In modern era, evaluation of networking and wireless networks has come forward to grant communication anywhere at any time. Security of wireless networks is main aspect and the process of cryptography plays an important role to provide the security to the wireless networks. There are various cryptography techniques both symmetric and asymmetric. The survey is done on some of the more popular and interesting cryptography algorithms currently in use and their advantages and disadvantages are also discussed. This paper provides a fair performance comparison between the various cryptography algorithms on different settings of data packets. In this paper we analyze the encryption and decryption time of various algorithms on different settings of data.

Keywords: Encryption, DES, AES, Blowfish, RSA

1. INTRODUCTION

Cryptography [1, 2] is the art and science of achieving security by encoding messages to make them readable. The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more vulnerable of duplicating of data and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of wireless communication, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the wireless. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their comparison.

2. LITERATURE SURVEY

Some of the concepts used in cryptography are described here [1]:

2.1 Cryptography

- Plain Text: Any communication in the language that we speak- that is the human language, takes the form of plain text. It is understood by the sender, the recipient and also by anyone who gets an access to that message.
- Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.
- Encryption: The process of encoding plain text messages into cipher text messages is called encryption.
- Decryption: The reverse process of transforming cipher text messages back to plain text is called as decryption.
- Key: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

2.2 Purpose of Cryptography

Cryptography serves following purposes:

- Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.
- Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.
- Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.
- Non- repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.
- Access Control: Access Control specifies and controls who can access what.
- Availability: The principle of availability states that resources should be available to authorized parties all the times.

2.3 Types of Cryptography

Two types of cryptography is studied:

- Symmetric Key Cryptography: When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography.
- Asymmetric Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is

known as asymmetric key cryptography.

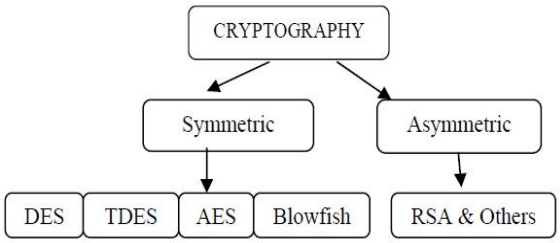

Figure 3.1: Classification of Cryptography

3. RELATED WORKS

This subsection describes and examines previous work on most common algorithm.

3.1 DES

DES is a block cipher that uses shared secret key for encryption and decryption. DES algorithm as described by Davis R. [3] takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length. In the case of DES, each block size is 64 bits. DES also uses a key of 56 bits to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt the message. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). The Broad level steps in DES are as follows [1]:

1. In the first step, the 64-bit plain text message is handed over to an Initial permutation (IP) function.
2. The initial permutation is performed on plain text.
3. The IP produces two halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now, each of LPT and RPT go through 16 rounds of encryption process.
5. In the end, LPT and RPT are rejoined and a final permutation (FP) is performed on the combined block.
6. The result of this process produces 64-bit cipher text.

Rounds: Each of the 16 rounds, in turn, consists of the broad level steps and shown in Figure 3.1.

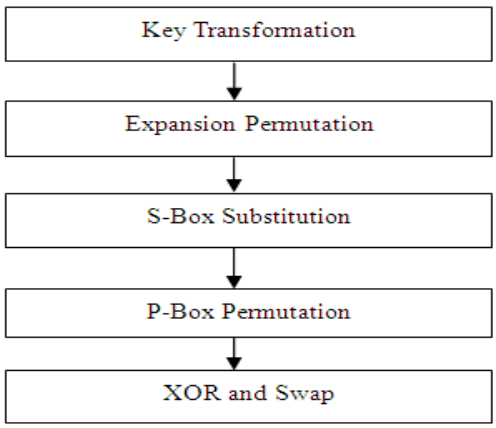

Figure 3.1: Details of One Round in DES

3.2DES

3DES (Triple DES) is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt-Encrypt (EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plain text message, t.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t))) \quad (1)$$

Where C(t) is cipher text produced from plain text t,

E_{k1} is the encryption method using key k1

D_{k2} is the decryption method using key k2

E_{k3} is the encryption method using key k3

Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t))) \quad (2)$$

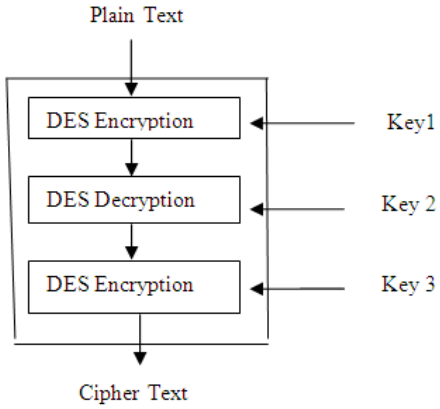

Figure 3.2: Encryption in 3DES

TDES algorithm with three keys requires 2^168 possible combinations and with two keys requires 2^112 combinations. It is practically not possible to try such a huge combination so TDES is a strongest encryption algorithm. The disadvantage of this algorithm it is too time consuming.

3.3 AES

The AES cipher [6] is almost identical to the block cipher Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128-bit key is 10. Unlike its predecessor DES, AES does not use a Feistel network. Feistel networks do not encrypt an entire block per iteration, e.g., in DES, 64/2 = 32 bits are encrypted in one round. AES, on the other hand, encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds.

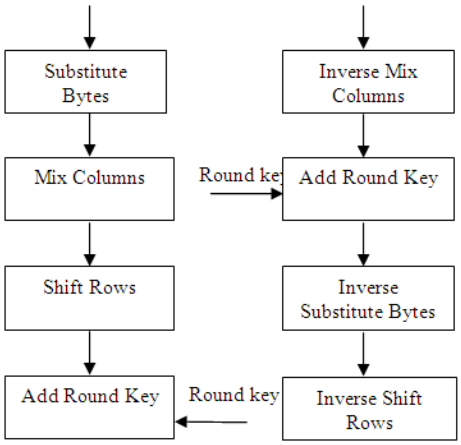

Figure 3.3: One Round of encryption and Decryption in AES

Encryption Round Decryption Round Each processing round involves four steps:-

- Substitute byte: a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift rows: a transposition step where each row of the state is shifted cyclically a certain number of steps.
- Mixcoloumn: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add round key: each byte of the state is combined with the round key using bitwise XOR.

AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

AES Encryption:

The encryption process in AES involves following steps:

(i) Do the one-time initialization process:
  (a) Expand the 16-byte key to get the actual Key Block to be used.
  (b) Do one time initialization of the 16-byte plain text block (called State).
  (c) XOR the state with the key block

(ii) For each round do the following:
  (a) Apply S-Box to each of the plain text bytes.
  (b) Rotate row k of the plain text block (i.e. state) by k bytes.
  (c) Perform mix columns operation.
  (d) XOR the state with the key block.

3.4 Blowfish

Blowfish [5] is one of the most common public domain encryption algorithms provided by Bruce Schneier - one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. The Blowfish algorithm was first introduced in 1993. The blowfish encryption is shown in figure below:

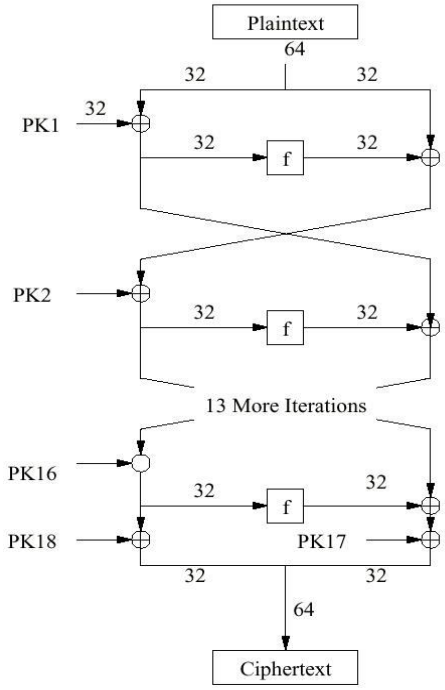

Figure 3.4: Blowfish Encryption

Operation of Blowfish:

Blowfish encrypts 64-bit block cipher with variable length key. It contains two parts

- Subkey Generation: This process converts the key upto 448 bits long to subkeys to totaling 4168 bits.
- Data Encryption: This process involves the iteration of a simple function 16 times. Each round contains a key dependent permutation and key- and data dependent substitution.

Blowfish suits the applications where the key remain constant for a long time (e.g. communication link encryption) but not where the key changes frequently (e.g. packet switching).

3.5 RSA

RSA is a public key algorithm invented by Rivest, Shamir and Adleman [7]. The key used for encryption is different from (but related to) the key used for decryption. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct large prime numbers p and q.
2. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.
3. Compute n = pq; n is used as the modulus for both the public and private keys
4. Select the public key (i.e. the encryption key) E such that it is not a factor of $(p - 1)$ and $(q - 1)$.

5. Select the private key (i.e. the decryption key) D such that the following equation is true:
   (D*E) mod (p-1)*(q-1) = 1
6. For encryption, calculate the cipher text CT from the plain text PT as follows:
   CT = PT^E mod N (3.1)
7. Select CT as the cipher text to the receiver.
8. For decryption, calculate the plain text PT from the cipher text CT as follows:
   PT = CT^D mod N (3.2)

3.6 Comparison

Comparative study of the cryptographic algorithms both symmetric as well as asymmetric has been done.

Table 1: Comparison of Cryptography Algorithms

ALGORITHM	CREATED BY	KEY SIZE (BITS)	BLOCK SIZE (BITS)
DES	IBM in 1975	56	64
3DES	IBM in 1978	112 or 168	64
AES	JOAN DAEMEN & VINCENT RIJMEN IN 1998	256	128
BLOWFISH	BRUCE SCHNEIER IN 1993	32 - 448	64

E. Thambiraja, G.Ramesh and Dr. R. Umarani in [8] have done survey on most common encryption techniques. Monika Agrawal and Pradeep Mishra in [9] have also done a comparative survey on Symmetric Key Encryption Techniques. Gurjeevan Singh, Ashwani Kumar Singla and K.S.Sandha in [4] have provided comparison of various cryptographic algorithms.

DES

Advantages and Disadvantages of DES are Advantages

1) DES algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications.
2) Although introduced in 1976, it has proved resistant to all forms of cryptanalysis.

Disadvantages

1) Its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours.
2) It was recognized that DES was not secure because of advancement in computer processing power

3DES:

Advantages

1) It uses 64 bit block size with 192 bits of key size. It is simple like DES because the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time.
2) 3DES is easy to implement (and accelerate) in both hardware and software.

Disadvantages

1) 3DES is slower than other block cipher methods.
2) It has poor performance.

AES

Advantages

1) The purpose of the AES algorithm is to replace the older and less reliable algorithms, such as Data Encryption Standard (DES).
2) AES encryption is fast and flexible.
3) The AES has also been employed in other areas such as to secure information in smart cards and online transactions.
4) Until May 2009, the only successful published attacks against the full AES were side-channel attacks on some specific implementations.
5) In June 2003, the U.S. Government announced that AES could be used to protect classified information.
6) The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths.

Disadvantages

1) AES in Galois/Counter Mode (GCM) is challenging to implement in software.
2) The size of key length is too long that makes it complex sometimes.

Blowfish

1) Blowfish is block cipher 64-bit which can also be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits.
2) Blowfish is fast as its encryption rate on 32-bit microprocessor is 26 clock cycles per byte.
3) It is compact as it can execute in less than 5 kb memory.
4) It is simple because it uses only primitive operations like addition, XOR and table lookup, making its design and implementation simple.
5) It has a variable key length upto a maximum of 448 bits long making it both flexible and secure.
6) No attack is known to be successful against this. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less.
7) Blowfish is considered to be the best out of all encryption algorithms.

RSA

Advantages

1) The primary advantage of RSA is increased security: as the private keys do not ever need to be transmitted or revealed to anyone. Whereas in a secret-key system, there is always a chance that an enemy could discover the secret key while it is being transmitted.
2) Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well.
3) Digitally signed messages can be proved authentic to a third party, such as a judge, thus allowing such messages to be legally binding.

Disadvantages

1) A disadvantage of using public-key cryptography for encryption is speed: they are very slow in processing.

For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. The study so far shows the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. Gurjeevan Singh, Ashwani Kumar Singla and K.S.Sandha have provided comparative analysis of encryption algorithms. The four encryption algorithms (AES. 3DES, Blowfish and DES) have been tested with different text file sizes. The experiment results are shown below: Comparison of encryption time has been explained in the Table 2 and also the execution time of various encryption algorithms on different text file size.

Table 2: Comparative Encryption Times (In ms) of various algorithms with different packet size

Text File Size (in Kbytes)	AES	3DES	Blowfish	DES
20	42	34	25	20
48	55	55	37	30
108	40	48	45	35
242	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	742.31	91.92	663.31

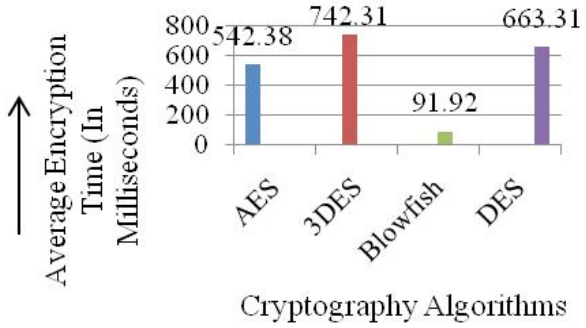

Figure 2: Encryption Time of Each Algorithm (In ms)

The results for the comparison described in Figure 2 shows the superiority of Blowfish algorithm over the other algorithms in terms of the processing encryption time. Because less the time; less will be the power consumption and more the speed of the algorithm. Second point can be noticed here that AES has advantage over the other 3DES and DES in terms of processing encryption time except Blowfish. In third point we say can that DES has better performance than 3DES. Fourth point which has been concluded that 3DES has least performance than all.

4. CONCLUSION

In this wireless world nowadays, the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. In this paper, it has been surveyed about the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. This paper presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. The presented simulation results show the numerous points. Firstly it was concluded that Blowfish has better performance than other algorithms followed by AES.
3DES has least efficient of all the studied algorithms. In future we can use Encryption techniques in such a way that it can consume less time and power furthermore; we try to develop stronger Encryption Algorithm with high speed and minimum energy consumption..

References

[1.] Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill Companies, 2008.
[2.] William Stallings “Network Security Essentials (Applications and Standards)”, Pearson Education, 2004.
[3.] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Society

magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.
[4.] 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.
[5.] Pratap Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
[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 on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

AUTHOR

Mitali[1] received the B.Tech. degree in Computer Engineering from Haryana College of Technology & Management, Kaithal, Haryana, India in 2010 and pursuing M.Tech in Computers Engineering from year 2012 from Swami Devi Dyal Group of Professional Institutions, Barwala, Haryana, India. She has worked as a lecturer in CSE Department in T.R. Abhilashi Memorial Institute of Engineering and Technology, Distt. Mandi, H.P., India for more than 1 year i.e. 1st Aug, 2010 – 31st Aug, 2011.

Vijay Kumar[2] received the B.Tech. degree in Computer Engineering from CITM, Faridabad, Haryana in 2010 and M.Tech. degree in Computer Engineering from Deenbandhu Chhotu Ram University, Murthal, Haryana, India in 2013. He has qualified GATE in 2011-2012. He is now working as an Assistant Professor in Computers Department in Swami Devi Dyal Group of Professional Institutions, Barwala, Haryana, India.

Arvind Sharma[3] received the B.Tech. and M.Tech. degrees in Computer Engineering from Maharishi Markandeshwar University, Muulana, Haryana, India in 2012 and 2014, respectively. He is now working as an Assistant Professor in Computers Department in Swami Devi Dyal Group of Professional Institutions, Barwala, Haryana, India.