A Review on Various Most Common Symmetric Encryptions Algorithms

Sweta K. Parmar[1] Prof. K. C. Dave[2]
[1]PG Student [2]Professor
[1, 2] Department of Instrumentation & Control
[1, 2] L. D. College of Eng. Gujarat, India

Abstract— Security is the most challenging aspects in the internet and network application. Internet and networks applications are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Information security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security system. This paper gives a comparison of various encryption algorithms and then finds best available one algorithm for the network security.

I. INTRODUCTION

Cryptography algorithms play an important role in information security. They can be divided into Symmetric and Asymmetric key cryptography. In Symmetric key encryption only one key is used to encrypt and decrypt data. Symmetric algorithms are of two types: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. .Examples are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm [4].

Asymmetric key algorithm is also known as public key algorithm. In this algorithm, there are two keys public and private used for encryption and decryption. Public key is used to encrypt the message and private key is used to decrypt the message (e.g. Digital signature)[4].

As we are having number of cryptographic algorithm so sometimes it can create little bit confusion to select best one[1]. This paper provides a view to choose the best available one on the basis of their performance parameter. So it provides a great security during data transmission.

II. CRYPTOGRAPHY

Cryptography is the study of Secret (crypto-)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into coded form or unreadable form and that coded form then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances [2].

A. Various Goals [8]

1) Confidentiality
Information in computer is transmitted and has to be a accessed only by the authorized party and not by anyone else.
2) Authentication
The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.
3) Integrity
Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
4) Non Repudiation
Ensure that neither the sender, nor the receiver of message should be able to deny the transmission.
5) Access control
Only the authorized parties are able to access the given information.

A. Basic Terms[8]

6) Plain Text
The original message that the person wishes to communicate with the other is defined as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hellow Friend how are you" is a plain text message.
7) Cipher Text
The message that cannot be understood by any one or a meaningless message is what we call as Cipher text. For Example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".
8) Encryption
A process of converting plain text into cipher text is called as Encryption. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
9) Decryption
A reverse process of encryption is called as Decryption. It is a process of converting Cipher text into Plain text. The process of decryption requires two things- a decryption algorithm and a key. A decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.
10) Key
A key is a numeric or alpha numeric text or may be a special symbol. The key is used at the time of encryption takes place on the plain text and at the time of decryption takes place on the cipher text. For example, if the Alice uses a key of 3 to encrypt the plain text "President" then cipher text produced will be "Suhylghqw".

III. DATA FLOW MODEL OF DATA ENCRYPTION AND DECRYPTION PROCESSES

Data encryption and decryption is the process used in cryptography. Figure 1 given below shows the data encryption and decryption process [1].

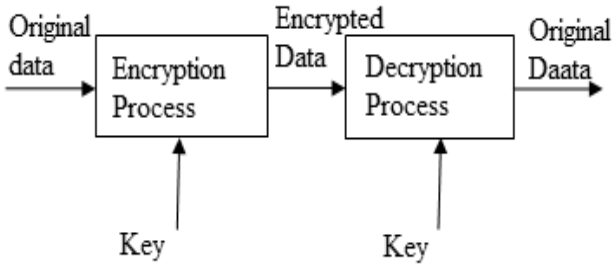

Fig.1: Data Encryption and Decryption Data Flow [1]

As shown in the figure1 when the sender sends a message or some data to the receiver, the data is first encrypted using the encryption algorithm and a key. After that encrypted message or data is decrypted on the receiver side using decryption algorithm and a key. And finally the receiver is receiving the original data. Generally the data encryption and decryption algorithms are same. The sender and receiver use the same algorithm for data encryption and decryption.

IV. ALGORITHM COMPARISION

A. DES (Data Encryption Standard)

DES is a block encryption algorithm. It is a symmetric algorithm, means same key is used for encryption and decryption .It uses one 64-bit key[3]. From 64 bits, 56 bits make independent key, which determine the exact cryptography transformation, 8 bits are used for error detection DES[4].

Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. Many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher[4].

B. 3-DES

It uses 64 bit block size with 192 bits of key size. 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. 3DES is slower than other block cipher methods [4].

C. AES:

Advanced Encryption Standard (AES) also known as the Rijndael algorithm is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power[4].

It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. it encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices. AES has been tested for many security applications [4].

D. Blowfish:

Blowfish is a symmetric block cipher that can be effectively used for encryption of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses[5]. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits [5].Now the comparison of symmetric encryption algorithms are based on key size, block size and rounds as shown in table I [4].

Algorithm	Key size	Block size	Rounds
DES	56 bits	64 bits	16
3DES	112 bits or 168 bits	64 bits	48
AES	128 bits, 192 bits, 256 bits	128 bits	10,12 or 14
Blowfish	32-448 bits	64 bits	16

Table (1): Comparison of DES, 3DES, AES and Blowfish algorithms [4]

Now power requirement of Blowfish algorithm can be analysed and compared with other algorithms for same logic to generate the same condition that other algorithm follows in terms of key size [1].

Sr. No.	Algorithms	Key size	Power Consumption(mW)
1	BLOWFISH	128	29.86
2	AES	128	2000
3	IDEA	128	58
4	RIJNDAEL	128	82

Table (2): Power Analysis for algorithms[1]

Power analysis for128 bits key size Blowfish encryption can be compared with other symmetric algorithm which also use 128 bits key size[1].

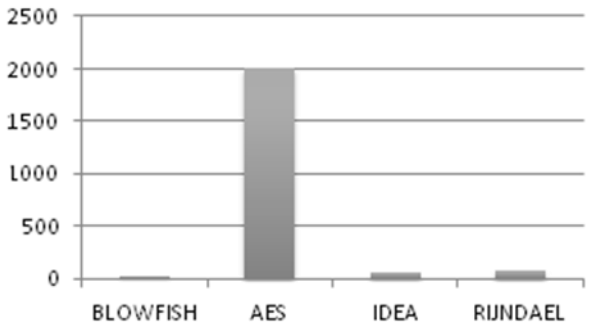

Fig. 2: owner Comparison chart of Blowfish algorithm with AES, IDEA, RIJNDAEL [1]

Figure2 demonstrate the power comparison analysis of Blowfish Algorithm, AES, IDEA and Rijndael Algorithm. From figure it is clear that blowfish consumes negligible amount of power as compared to other algorithm. Among of these AES consumes most amount of power. IDEA And Rijndael consumes more power than blowfish but less than AES [1].

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources. Main purpose here is to calculate the Encryption and Decryption speed of each

algorithm for different packet sizes. Their implementation is tried to optimize the maximum performance for the algorithm. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme. The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value is increased, the power consumption of this encryption technique is decreased [4].

Encryption / decryption algorithms have been tested with different text size files [4].

Input Size(kb)				
	DES	3 DES	ENC	DEC
	ENC	DEC	56	54
50	31	51	48	50
108	35	47	109	75
246	46	71	165	85
320	80	73	227	149
695	145	121	171	153
781	86	121	301	171
900	241	152	307	178
5500	248	166	178	110
7311	1692	954	179	170
22300	1716	119	496	371
Average time	**432**	**295**	**7.52**	**10.0**

Table (3): Throughput of DES and 3DES with different file size (MB/Sec)[4]

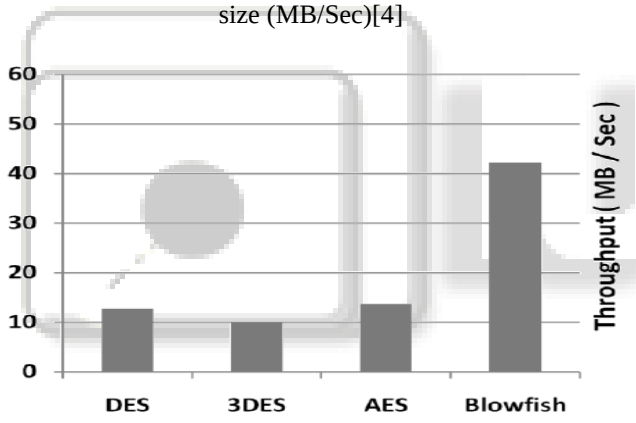

Fig. 4: Throughput of decryption algorithms [4]

All The above results show the superiority of Blowfish algorithm in terms of the throughput, processing time. Again, AES has advantage over the 3DES and DES in terms of throughput and power consumption except Blowfish. 3DES has least performance because of its triple phase encryption characteristics. Finally we can conclude that Blowfish is the best of all[4].

Input Size(kb)	AES		Blowfish	
	ENC	DEC	ENC	DEC
50	56	64	38	38
108	40	57	45	29
246	110	75	43	64
320	162	147	44	90
695	212	144	47	91
781	165	152	66	96
900	260	172	66	103
5500	258	170	118	100
7311	1365	880	105	139
22300	1366	883	152	137
Average time	399.4	274	72	88.7
Throughput	9.35	13.6	51	42.11

Table (4): Throughput of AES and blowfish with different file size (MB/Sec)[4]

In the previous section the comparison is based on speed, power consumption and throughput of encryption and decryption algorithms. Now the comparison of two best algorithm AES and Blowfish Will be done for other data type such as images[6].

Image(JPEG)	Time (millisecond)	
	Blowfish	Rijindael
Img 1	87	102
Img 2	99	123
Img 3	134	234
Img 4	156	267
Img 5	198	278
Img 6	345	456
Average Time	169.8	243.3
throughput	15.9	10.8

Table (5):Average time and throughput for encryption based ondifferent images[6]

Fig 5: Throughput of Encryption algorithms [6]

From these result shows that blowfish has a better performance than the AES.

Image(JPEG)	Time (millisecond)	
	Blowfish	Rijindael
Img 1	76	92
Img 2	95	111
Img 3	120	136
Img 4	146	162
Img 5	168	184
Img 6	267	283
Average Time	145.3	161.3
throughput	18.2	16.4

Table 4:Average time and throughput for decryption based on Different images[6]

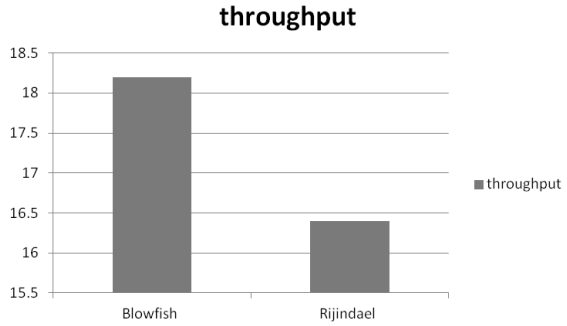

Fig. 6. Throughput of Encryption algorithms[6]

V. CONCLUSION

This paper represents the performance evaluation of symmetric algorithm from the other reviewed papers. So by reviewing the papers we finally conclude that the blowfish algorithm has a better performance than the other symmetric algorithms in all most all parameters.

ACKNOWLEDGEMENTS

Author thanks Prof. K. C. Dave for his valuable guidance for this paper. Author is also thankful to her staff and colleagues for their co-operation.

REFERENCES

[1] Deepak Kumar Dakate, Pawan Dubey, "Performance Comparison of Symmetric Data Encryption Techniques", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.
[2] Amogh Mahapatra and Rajballav Dash, thesis on, "Data Encryption & Decryption by using Hill Cipher Technique and Self Repetitive Matrix", National Institute of Technology Rourkela 2007.
[3] S. Pavithra and Mrs. E. Ramadevi, " Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.
[4] Pratap Chandra Mandal, " Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.
[5] http://pocketbrief.net/related/BlowfishEncryption.pdf
[6] M. Anand Kumar and Dr.S.Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithm", I. J. Computer Network and Information Security, 2012, 2, 22-28, Published Online March 2012 in MECS.
[7] Schneier, applied cryptography, John Wiley & Sons, New York, 1994
[8] Thambiraja, G Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques", International journal of advanced research in computer science and software engineering, volume 2, issue 7, july 2012.
[9] www.wikipidia.com

