ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Performance Analysis of Cryptography Algorithms: Blowfish, DES, 3DES, AES, MARS& RC6 with Data Hiding In Images Using Steganography Technique

Shivani Varshney[1], Lalit Mohan Gupta[2], Anuj Gupta[3]

M.Tech. Scholar, Dept. of Computer Science Engineering, ITM, Aligarh, India[1],

Asstt. Professor, Dept. of Computer Science Engineering, VCTM, Aligarh, India[2],

Asstt. Professor, Dept. of Computer Science Engineering, ITM, Aligarh, India[3]

ABSTRACT: Cryptography plays a vital role in securing information in this world of advanced technology it created a virtual world for transferring which is almost or safer world. Cryptography is the process that makes the data impossible to understand for the unauthorized users. Hence provides the feature of confidentiality. Various algorithms are also used for cryptography. Ideally, an optimal algorithm is required for cryptography that has very low cost & provides high performance. But as such there exists no algorithms. Various algorithms have been developed as a compromise to the cost performance. In this, we have combined the two techniques, i.e. cryptography & steganography as they will provide security to the data on both sides of the network, first of all by using encryption algorithm the data gets converted into encrypted form & then through steganography the encrypted from of data is converted into the rough image. Furthermore, steganography also supports data hiding hence, reducing the chances of the tampering or alteration of data.

KEYWORDS: Encryption, decryption, cryptography, steganography. DES, AES, Triple DES, Blowfish, RC6, MARS.

I. INTRODUCTION

In the era of gadgets, processing information storing and retrieving all is done on the basis of computer. Everyone outside from small to big organization, government all prefers computer and internet services. Cryptography and developments are evergreen. Cryptography protects users by providing data encryption functionality and another users authentication. Our whole globe today depends on the internet and its application for every part of their lives. Here comes the requirement for cryptography to secure our data. In a secret writing science, cryptography plays a major role. It is the art of transforming and applying technology to protect information.

Cryptography provides numerous security goals to ensure data privacy, on-alteration of data, and so on. The idea of encryption and encryption algorithm through which we can encode our data in secret code and not be able to read it by hackers or unauthorized persons even if it is hacked.

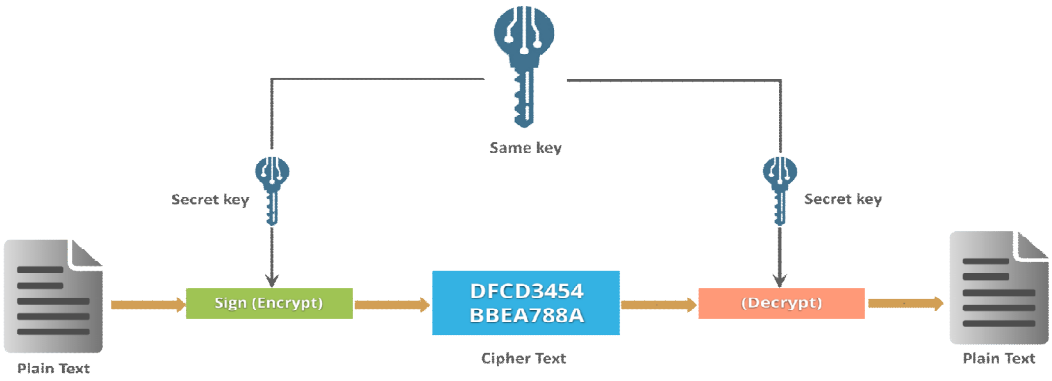
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

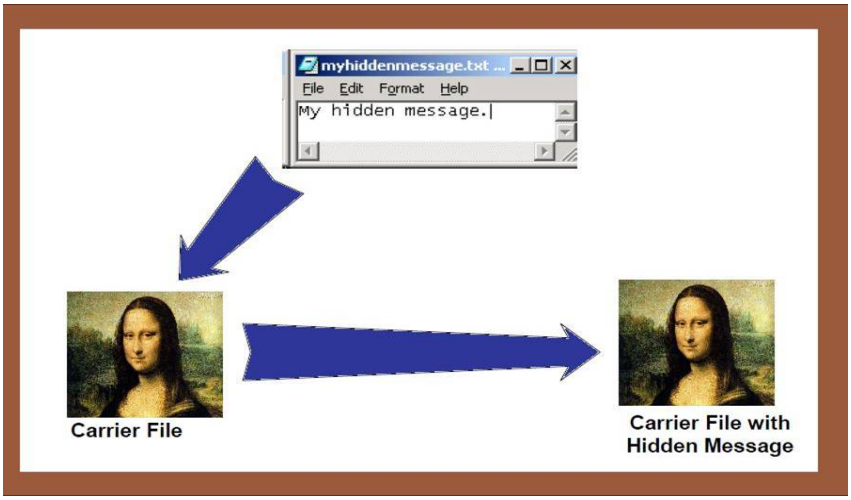
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019



Steganography is the communication art and science in a way that hides the communication existence. Steganography plays a major role in the security of information. It is the art of invisible communication by hiding information within other information.
Steganography's main objective is to hide information in the other cover media so that the information is not noticed by another person.
Steganography is derived for covered writing from Greek and essentially means "hiding in plain sight." Steganography is the art of hiding data in data unobtrusively.
Steganography hides a secret message and no one can see in the best case that both parties communicate in secret. This makes steganography suitable for certain tasks that do not involve encryption, such as marking copyright.



Evaluation Parameters: -

Each and every encryption technique has its own pros and cons. For applying an appropriate cryptographic algorithm to a particular application, we should be familiar with performance, durability and debility of the algorithm. Therefore, these algorithms must be studied and analyzed based on various aspects.

Our study is done with following metrics under which the cryptosystems can be compared are illustrated as follows-

1. **Encryption Time –** The time required to transform the original text into the encoded text is known as encryption time. Encryption time is totally dependent on the size of key, plaintext block size and mode. In our

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

project, we estimated encryption time in milliseconds. Performance of the system rely on encryption time. Encryption time is inversely proportional to the system performance.

2. **Decryption Time –** The time required to retransform the cipher text into the plaintext is called decryption time. The decryption time is aspired to be less identical to encryption time to make system susceptible and agile. Performance of the system depends on the decryption time. In our project, we have measured decryption time in milliseconds.
3. **Avalanche Effect-** In cryptography, a phenomenon called diffusion shows cryptographic pros of an algorithm. It there exists a small change in an input then significant amount of change is observed in output. Using hamming distance, we have measured avalanche effect. Hamming distance can be defined as the measure of dissimilarity in information theory. Avalanche effect can be calculated by the following formula:

   Avalanche effect = Hamming distance / file size
4. **Entropy-** The most important property in the process of cryptography is its volatility because it should be random which cannot be imagined or figured out by the traducer or attacker. Entropy can be defined as a degree of randomness present in the information the uncertainty in the information is measured by entropy. For securing the information, we need various data security algorithms to get high randomness in the transformed message, so as to minimize the dependency or make independent relation between key and cipher text. Therefore, makes the relationship between key and cipher text complex. Hence, this property is known as confusion. It is aspired to have high extent of confusion to make it troublesome for the attacker to guess. Entropy emulates the performance of the cryptographic algorithms. How, we use the Shannon's formula for calculating the entropy.

II. LITERATURE REVIEW

[1]Priyadarshini patil, shows in his paper that strong and weak point are clearly seen by encryption techniques. A proper knowledge of strength and weakness of the algorithm must be studied before applying suitable cryptography to an application. Blowfish required smallest memory for implementation as compared to RSA which required largest memory, whereas memories require for DES and AES is of medium size. Blowfish is best suited algorithm.

[2]The algorithm proposed by **Sriram Ramanujam,** has better avalanche effect than any other earlier used algorithms and can be used in the process of encryption. We can see in this paper various classical cipher playfair cipher, vigenere cipher, caesar cipher and many more ciphers have less avalanche effect as comparison to proposed algorithm which cannot be used for encryption for confidential method.

[3]Karthik, research showed that 3DES work more effectively with the block ECB &CBC. He also focusses performance evaluation of particular symmetric encryption algorithms. The particular algorithms are DES, 3DES, blowfish RC2 &RC4. If we change key size the higher key size requires a change in time consumption and in the battery.

[4]Research paper of**Ankit Dhamija,** shows that cryptography and steganography are combinedly used to migrate data on cloud data SCMACS (Secure cloud migration Architecture using Cryptography and steganography) is one of the compliment method which is used to make cryptography as simple yet effective technique as that same key for encryption and decryption are used by both sender and receiver in symmetric key method .symmetric method creates a strengthen approach which lies the affect that private key makes it very safe as no one have private key and can access to it .

[5]Gurpreet Singh,in his paper, we have shown the decryption of the well-liked encryption algorithms such blowfish, DES, 3DES, AES, MARS and RC6. In the world of advanced technology, the use of internet and network is growing on a peak rate. So, it is required to secure the data which is transmitted over different networks. In order to provide security to data over the network, various encryption algorithms are used. In this paper, we have also shown the existing researches in encryption techniques. Each algorithm is unique in its own way, which might be appropriate for various applications and each has its own strong and weak points. According to research done, it is found that AES algorithm is more efficient in concern with throughput, speed, time and avalanche effect. The security provided by these algorithms can be enhanced more if we apply more than one algorithm on our data. In our future research, we will

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

explore this concept and apply the combination of algorithm either sequentially or parallel to make the data storage and retrieval more secure.

[6]Nirmaljeet Kaur,Inthe era of the use of automated information resources there is a need of securing data during transmission. DES is now considered as an insecure mechanism to protect data from unauthorized users.There are found some analytical tests that represent theoretical weakness in the cipher. So, there is a need to augment this algorithm by adding new level of security. In future we can enhance the algorithm by changing the function deployment, S-box design and replacing old XOR by new operations.

[7]Anup,presents Triple DES provides a better-quality encryption process where as we observed that des provide better performance in encryption and decryption process. This becomes a big fault when we are running multiple processes over a network. The time will be increased for triple DES process the future work would also examine the better guarantee of quality and performance for all types of multimedia data.

[8] R. vasantha, Dr.R. Satya Prasad,gave that the algorithms like AES, DES,3 DES and encryption decryption through RSA is not sufficient to secure the data. So according to him these algorithms are not so secure therefore there is a need to enhance the security of these algorithms. He gave his views on cloud computing and preferred standpoint of distributed computing as virtualization. And lateron, also explained the need and importance to make cloud security stronger.

[9] According to **Ako Muhamad Abdullah,** Day by day the use of internet & network is increasing at a peak rate. Digital is being exchange among users on a regular basis. Among the data, few data are such sensitive that it is needed to protect them from attackers. In order to achieve security, encryption algorithms play a vital role to protect the data and avoid it to reach unauthorized access. Different types of algorithm are developed for encrypting the data. One of the most efficient algorithms which are mostly adopted on hardware and software is AES. In this algorithm. It deals with different key sizes like 128, 192 & 256 bits with 128 bits block cipher. In this paper, there are a number of important features of AES to encrypt the data under the various parameters. After the comparison done, researchers show that AES provides much more security in comparison to the other algorithm like DES, 3DES, blowfish etc.

[10] Mohan H.S.,is not considered. The outputs of diffusion analysis indicate that required diffusion level is obtained at the end of 5^{th} round in the MARS encryption algorithm. No major improvement is achieved in the rounds from 6 to 32. Whereas the output of AES indicates that the diffusion level is obtained at the end of 2^{nd} round itself. He also told that MARS good for smart card implementation whereas Rijndael is very good considered for widespread smart card implementation. Therefore, by analyzing various factors he gave that Rijndael is much more secure than MARS.

[11]Abhinandan Aggarwal,presentsImplementation of software leads to small amount of resource requirement but efficient performance and speed can only be achieved by implementing hardware. Effective implementation for AES caused reduced number of slices needed in implementation.

[12] Mardiana,gave that modified RC6 is more efficient for color images because each color image pixel has 24 bits.RC6 has some limitations due to padding problems because it can be used in certain pixel sizes. Therefore modified RC6 solves the padding problem by changing the size of each block. It can also minimize the size or capacity of variables during the process and making it more efficient.

[13] Ramadhan mstafa,showed that another useful technique for protecting information over the internet is steganography. One of the most popular applications in steganography is digital watermarking. In this user can hide the important information inside the image by applying invisible watermark during the transmission of data. Images have some unimportant regions which the human visual system cannot recognize by replacing these regions along with other information. Moreover, Users can also change the least significant bit in each pixel along with the information without compromising with the quality of the image. Even the alterations also do not affect the intensity of the color in the image.

[14] Dhara rana,presented the various steganography techniques with the use of various cover media like text, image, audio or video files. Different image file formats have various techniques of hiding data. Audio and video files are also used for secure data interchange. In recent times the images are the not widely used as their cover media to secure the data. It is necessary to exchange the confidential or private data between two entities on a regular basis so research is being made for strong steganography is a continuous ongoing process.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

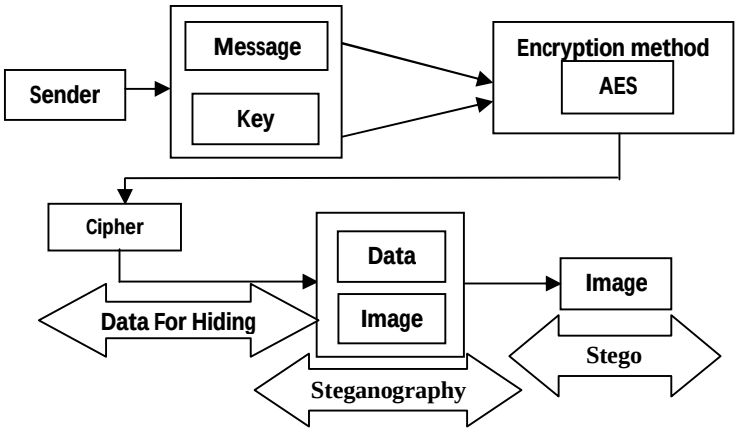
Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

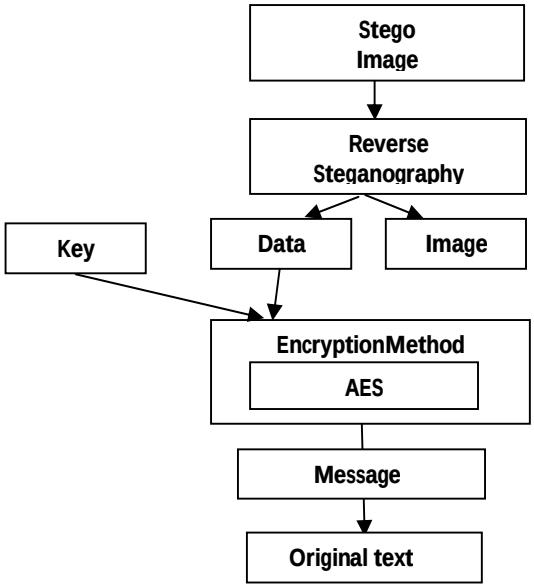
III. PROPOSED METHOD

In this paper, we implemented all algorithms in JAVA and run on various file size to compare the performance of all algorithms. As an input, we take same input file of various size throughout the testing process. We used the same system so that the memory and processor conditions remain same. After the comparison of algorithms on various parameter, we found AES the most ambitious and used it to encrypt the data. In this paper, we have also defined a secure method to send data from one computer to another computer using a combined approach of cryptography and steganography. The user encrypt the original data then hide the encrypted data behind an image. This is the most secure way to send a confidential message from one computer to another. The receiver receives the image and extract the data hidden in the image and with the key decrypt the data.

SENDER SIDE



RECEIVER SIDE



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

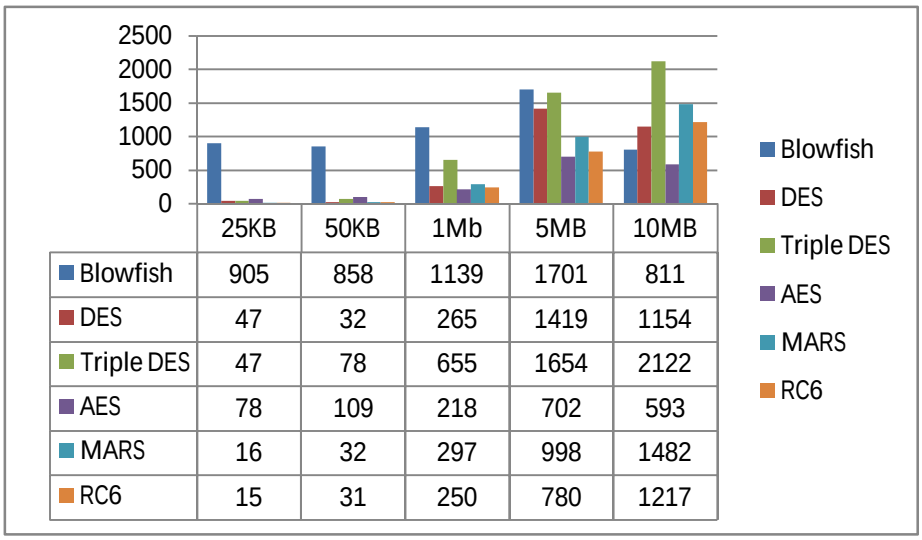
IV. RESEARCH OBJECTIVE

1- Using a combined approach of cryptography & steganography to securely transfer messages from one site to another.
2- It also provides security in two ways (cryptography and steganography).
3- To find an optimum algorithm for the process of cryptography to ensure the most secure way of communication.

OBJECTIVE AND SCOPE: We have provided a secure and secure method of transmitting data to the cloud servers in the proposed technique. In this technique, we used the technique of steganography and cryptography that provided important data for the users with multilayered protection. Symmetric approach is used in cryptography, which is much more expensive than the asymmetric approach. Every time calculations take dynamic values, which is even better. It uses LSB method for embedding bits in the pixel elements of the image in the case of steganography.

V. RESULTS AND DISCUSSIONS

ENCRYPTION TIME:



	25KB	50KB	1Mb	5MB	10MB
Blowfish	905	858	1139	1701	811
DES	47	32	265	1419	1154
Triple DES	47	78	655	1654	2122
AES	78	109	218	702	593
MARS	16	32	297	998	1482
RC6	15	31	250	780	1217

Fig.1 Encryption time vs. File Size analysis

As the results show, Blowfish algorithm take more encryption time in compare to others algorithm, while AES take less encryption time in compare to others algorithm. Triple DES is enhanced version of DES implementation uses three instances of DES with distinct key. Triple DES is more secure in compare to DES but inefficient in software. AES take less time among all algorithms. AES is efficient in some software platform.

DECRYPTION TIME: This has been observed from the obtained results that all algorithms take less decryption time in compare to encryption time.

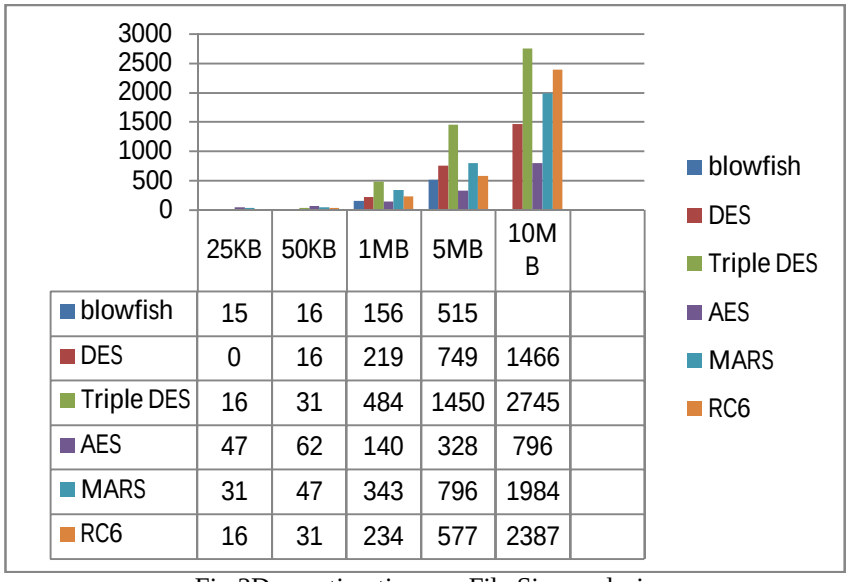
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

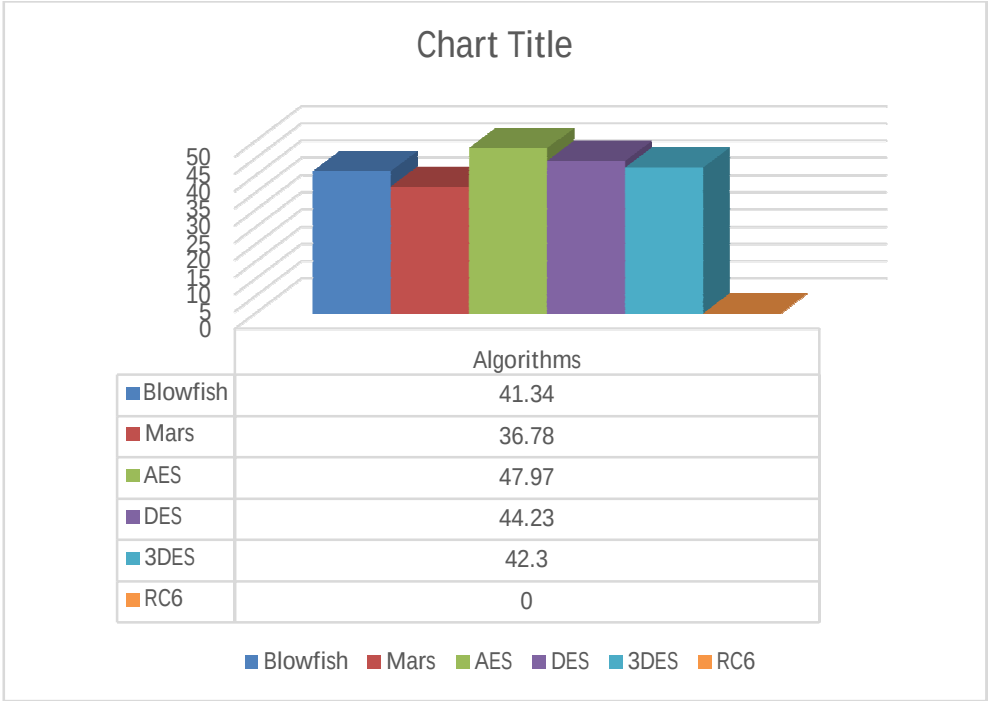
Vol. 8, Issue 5, May 2019



	25KB	50KB	1MB	5MB	10MB	
blowfish	15	16	156	515		
DES	0	16	219	749	1466	
Triple DES	16	31	484	1450	2745	
AES	47	62	140	328	796	
MARS	31	47	343	796	1984	
RC6	16	31	234	577	2387	

Fig.2Decryption time vs. File Size analysis

AVALANCHE EFFECT:



	Algorithms
Blowfish	41.34
Mars	36.78
AES	47.97
DES	44.23
3DES	42.3
RC6	0

Fig. 3 Avalanche effect analysis for Blowfish, MARS, AES, DES, Triple DES and RC6

Results demonstrate that AES show highest avalanche effect whereas RC6 shows least Avalanche effect. Avalanche effect is the degree of diffusion of information i.e. changes in any bit of the input give major changes in bits of output

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

information. AES is based on a substitution permutation network using multiplicative inverse and allowing for transformation over GF extends to high mixing of information leading to high diffusion in output.

ENTROPY:

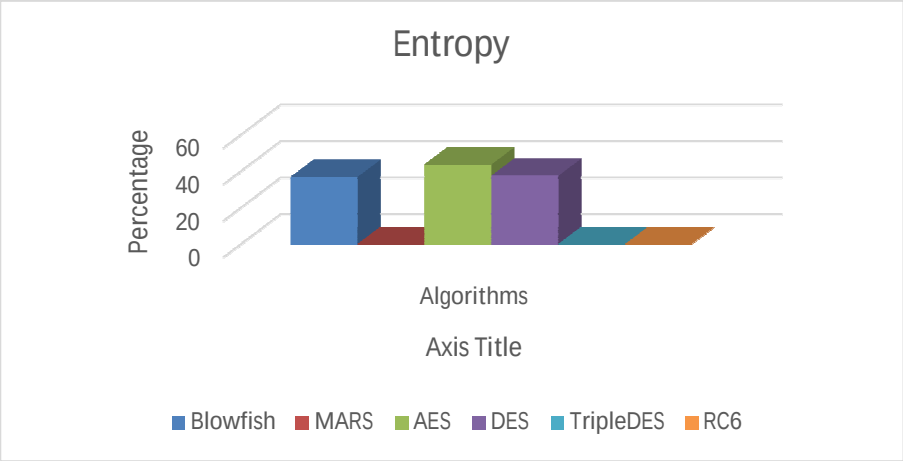


Fig. 4 Entropy effect analysis for Blowfish, MARS, AES, DES, Triple DES and RC6

Entropy is the process of measurement of randomness in the information. High percentage in entropy give more security to data because information can not be guess easily by the intruders and lead to difficulty to obtain the original message. This measure uncertainty of the information. In cryptographic process, we require randomness of the ciphertext, lead less dependent between key and cipher text. Results shows in Fig.4 that AES algorithm achieve high percentage in entropy so it is more secure in compare to all.

VI. CONCLUSION

This paper presented a descripted study of the most liked encryption algorithms such as Blowfish, DES, 3DES, AES, MARS and RC6. Day by day the use of network and internet is increasing rapidly. Therefore, there is a need to secure the data during transmission over various networks and different services. In order to achieve the security of data various encryption methods are used. Each method used is unique in its own manner which may be suitable for different factors and each has its own strengths and weak point.
An innovative approach to migrating data through the combination of cryptography and steganography on cloud servers. In this, we found AES the most ambitious and used it to encrypt the data. This is the best way to secure an authenticated information during its transmission over insecure channel.

REFERENCES

[1]priyadarshinipatil**, "**Acomprehensive evaluation of cryptographic algorithms; DES,3DES, RSA& Blowfish**",**International conference on information security & privacy (ICISP2018),11-12 December 2015, Nagpur, INDIA.
[2]Sriram Ramanujam&MarimuthuKaruppiah**,** "designing an algorithm with high avalanche effect**",**IJCSNS International Journal of computer science & Network Security, VOL. 11 No.1, January 2011.
[3]Karthik,**"**Data encryption & decryption by using triple DES & performance analysis of crypto system**",**International Journal of scientific engineering & Research (IJSER) VOL.2 issue 11, November 2014.
[4]Ankit Dhamija, **"**A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration**",**IEEE paper April 2016.
[5]Gurpreet Singh, **"**A study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security**",**International Journal of computer Applications (0975-8887) volume 67-No.19, April 2013.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

[6]Nirmaljeet Kaur, **"**Data Encryption Standard Algorithm (DES) for Secure Data Transmission**",** International Journal of Computer Applications (0975-8887).
International Conference on Advances in Emerging Technology (ICAET 2016).
[7]Anup**, "**Image Encryption using Triple DES Algorithm**",**Imperial Journal of interdisciplinary Research (IJIR) vol-3, issue-5,2017ISSN:2454-1362.
[8]R. vasantha, Dr.R. Satya Prasad**,"**An Advanced Security Analysis by using Blowfish Algorithm**",** International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2017IJSRCSEIT, volume 2 issue 6 ISSN: 2456-3307.
[9]Ako Muhamad Abdullah**,"**Advanced Encryption Standard(AES) Algorithm to Encrypt and Decrypt Dat**",** June 16,2017.
[10] Mohan H.S**,"**Performance Analysis of AES and MARS Encryption Algorithms**",**IJCSI International Journal of Computer Science Issues, VOL.8, Issue 4,1 July 2011.
[11]Abhinandan Aggarwal**,"**Implementation of AES Algorithm**",**International Journal of Engineering Research & Science (IJOER) ISSN [2395-6992]
[vol-2, issue-4 April-2016].
[12]Mardiana**,"**Modification of RC6 Block Cypher Algorithm on Digital Image**",**International Conference on Information and Communication Technology (IconICT).
[13]Ramadhan mstafa**,"**Information Hiding in Images Using Steganography Techniques**",** conference paper: March 2013.
[14]Dhararana**,"**A Review paper on Steganography Techniques**",** International Journal of Modern Trends in Engineering and Research e-ISSN: 2349-9745,p-ISSN:2393-8161.
[15]Mohammad Shirali-Shahreza, "A new method for real time steganography", ICSP 2006 Proceedings of IEEE.
[16]HarshavardhanKayarkar, "A Survey on Various Data Hiding Techniques and their Comparative Analysis".