Comparative Study on Various Cryptographic Techniques

K.B. Priya Iyer, Ph.D.
Associate Professor
M.O.P Vaishnav College for Women, Chennai, India

R. Anusha
Under Graduate Student
M.O.P Vaishnav College for Women, Chennai, India

R. Shakthi Priya
Under Graduate Student
M.O.P Vaishnav College for Women, Chennai, India

ABSTRACT
In today's world of internet technology that covers especially communication network security is a challenging issue. Hackers try to gain control over our system and steel data from it. To avoid this providing network security is an important task. Cryptography along with its various methods is used to serve this purpose. Cryptography is a technique to protect message by transforming it into an unreadable format called cipher text. It provides authentication, identification to user data, confidentiality and also provides security and privacy to the data stored. The main objective of this paper is to study the basic terms used in cryptography its purpose and to compare the encryption techniques used in cryptography.

Keywords
Cryptography, Encryption, Decryption

1. INTRODUCTION
The elevated development in the networking technology leads to a common culture for interchanging data among various users very extensively. Hence it causes a major concern for privacy, identity theft, electronic payments, security issue as it is more accessible to reconstruct a copy of data which the malicious user steel from the guided user. Thus the information has to be secured from these people and it must be read or used only by people who are authorized to do it. Sensitive information like ATM cards, banking dealings and public security numbers require more security [1].

The data like texts, images etc are communicated through network. Mobile network communication is growing because people have easy access to internet through mobiles where ever they are. A Mobile Ad-hoc Network (MANET) is comprised of a group of mobile nodes which have the capability of self organization in a decentralized manner and without preset infrastructure [2].

Cryptography is a standard way of securing the electronic documents. Cryptography is the study of data hiding and substantiation [2]. It includes the protocols, algorithms and strategies to refuse the access of illegal users to use the secured data.

Different encryption techniques are used to protect the secret data from unauthorized use. Encryption is a very general method for promoting the data security. This technique converts our data into a format called cipher text and decryption techniques is the vice versa of it. In Cryptography, a block cipher operates on fixed-length groups of bits, termed blocks, with a consistent transformation [3]. When encrypting, a block cipher it takes 128 bit input and output and a secret key. Decryption is similar: the decryption algorithm takes 128 bit input along with secret key and yields 128 bit plain output. To encrypt messages greater than the size of the block, operation called mode is used.

Selective encryption is the technique of encrypting some parts of a condensed data file while leaving other part of plain text unencrypted [3][4]. This type of encryption saves time and cost for data to be encrypted.

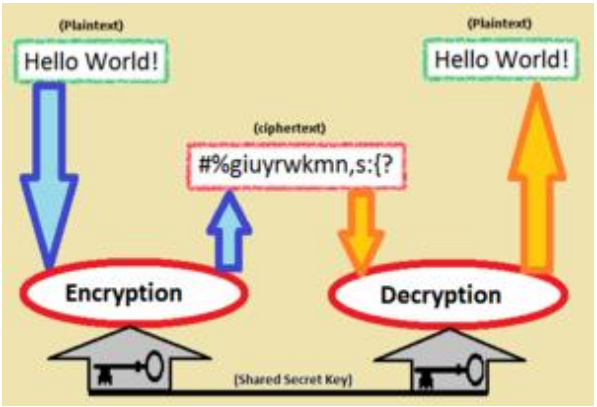
Encryption techniques can be categorized into three namely symmetric, asymmetric and hashing.

Symmetric key cryptography is an algorithm that uses the similar cryptographic keys for both encryption and decryption purpose. The keys may be indistinguishable. In order to maintain a personal information link this algorithms uses a special key that represent a secret that is to be shared between more users [2].

Asymmetric cryptosystems use one key to encrypt a message and another key to decrypt the same message that is transferred to the destination. It is also called as public key cryptosystems. In an asymmetric algorithm secret can be shared between many users who needs the particular data.

Hash functions are algorithms that use no key. They are called as one-way encryption. On a given plain text a fixed size/length hash value is calculated. Because of this content of the plaintext cannot be brought back. Hash functions provide evaluate of the veracity of a file [2].

Some of the symmetric and asymmetric encryption techniques that are available are DES, 3DES, AES, Blowfish, RSA, Diffie-hellman.



2. BASIC TERMS USED IN CRYPTOGRAPHY

2.1 Plaintext
In computing, plaintext is a readable textual material without much processing. It is an original message not formatted text that a sender wishes to communicate with the receiver. The authentic message that has to be sent to the receiver's end in cryptography is given a unique name called plaintext [4].

2.2 Cipher text

In cryptography, cipher text is a text that comes as a result of encryption performed on plaintext using an algorithm called cipher. This message is a meaningless text and cannot be understood by anyone. Cipher text is also known as encrypted or encoded text as it is a non-readable form of the original text. It cannot be read by human and computer without decryption of cipher text. In cryptography the plaintext is converted to a non-readable text before sending the actual text [3].

2.3 Encryption

Encryption is a process of coding information into a form that is unreadable without a decoding key. Encryption requires two things key and encryption algorithm. It prevents our data and allows only the receiver to read the data with the help of the key. Cryptography uses encryption techniques to send confidential messages .This is a process in which a plaintext is converted to a cipher text. It takes places at the sender's side [5].

2.4 Decryption

Decryption is a reverse process of encryption. It is a process of converting a cipher text back into a plaintext that the user can read and this happens at the receiver's end so that he is able to read the original message from the encrypted message [3]. This also requires two things a key and decryption algorithm.

2.5 Key

A key is a value that is used to encrypt or decrypt a message. It is a numeric or alpha numeric text or may be special symbols also. In cryptography the selection of key is important as security depends on it. It can use symmetric or asymmetric algorithms.

2.6 Symmetric algorithm

Symmetric algorithm is one in which the encryption and decryption key are the same. It can also be a key that is easily calculated from the other. Before sending or communicating with each other the sender and the receiver must agree to the key.

2.7 Asymmetric algorithm

An asymmetric algorithm is an algorithm in which the key used in encryption is different from that of the key used decryption. It is also known as public key cryptography.

2.8 Public key cryptography

Public key cryptography is a technique in which the key used for encryption is made public but only the person who holds the corresponding private key can decrypt the message that is been encrypted and send to him.

2.9 Private key

Private keys are normally known only to the owner. Messages can be encrypted using public key and decrypted using private key.

3. PURPOSE OF CRYPTOGRAPHY

The purpose of cryptography is to protect the data the data that is to be transmitted from hackers (that is person who seeks and exploits the weakness in a computer system and steels data from it). When communicating over any un-trusted medium, which includes any network, particularly the internet in data and telecommunication, cryptography is necessary. Cryptographic technique converts plaintext to a cipher text using encryption technique by which it does not reveal the original message. It can be recovered with the help of decryption technique. Cryptography is a technique that provides a number of security facilities to the data to avoid security issues [1]. It is widely used today because of its security reasons.

3.1 Confidentiality

It ensures that nobody can read the text except the proposed receiver. With this chattel, information is made available only to the authorized persons and is disclosed to unauthorized individuals. When more individuals are drawn in communication, the purpose of cryptography is to give assurance that only those individuals can understand the data/information exchanged. It is done with the help of encryption.

3.2 Authentication

The process of providing one's identity is called authentication. It is used to find whether the information is coming from authorized individual or not.

3.3 Integrity

It is a property that gives assurance that the message that is received has not been changed by any unauthorized individuals or in an accidental manner from the original text. It is enforced by mathematical functions applied to the message being transmitted [1].

3.4 Non-repudiation

A mechanism that proves that sender has really sent that message.

3.5 Access control

Access control is a property in which only authorized individuals can view the message that is sent. They are capable to do it with the help of a key and decryption technique.

4. RELATED WORKS

In this section, the various work and methodologies for cryptographic technique proposed by different authors in various papers are provided.

In [1], Ritu tripathi and sanjay agarwal gives a comparative study on some symmetric and asymmetric techniques based on few criteria's such as effectiveness, flexibility and security.

In [2], MS.Ankita umale and MS.Priyanka Fulare provides a comparative study of symmetric encryption techniques for mobile data caching in WMN. It is done based on the block size, key size and speed of the block ciphers such as AES, DES, RC2 etc.

In [3], E.Thambiraja, G.Ramesh and Dr.R.Umarani gives us a survey on various most common encryption techniques. A consolidation of various papers is done as a survey and has been provided in the literature review. It also focuses on image and information encryption techniques.

In [4][5], Authors provide a comparative study on different encryption techniques based on security, performance and behavior.

In [6][8], Authors gives a comparative study on various security algorithms like AES,DES,3DES,RC2etc for cache consistency.

In [7], The paper provides an assessment of six most commonly used algorithms conducted at different settings for each algorithm.

In[9][10], Authors provide a comparative study and performance analysis of few common block ciphers based on nine factors and resource utilization.

5. ASSESSMENT ON DIFFERENT CRYPTOGRAPHIC ALGORITHMS

This section describes the recent and most secured cryptographic algorithms that are proposed enable network security are compared and a conclusion is made out of it.

With the rapid growth of the internet both the wired and the wireless networks must and should provide security to the data's that is being transmitted. There are different types of cryptographic algorithms found to accomplish this task. A few algorithms amongst them are taken for comparison. Each algorithm has its own pros and cons. The following are the algorithms that are compared for network security [5].

5.1 DES

Data encryption standard (DES) is a symmetric key algorithm which was found by IBM in the year 1977. This algorithm uses a key size of 56bits and a block size of 64bits. This algorithm is a block cipher and it uses feistel network to transfer messages [8]. It takes about 16 rounds to convert messages and its network security can be broken by brute force attack. Benefit of this algorithm is that DES has been around a long time, even now no real weakness has been found, the most efficient attack is still found to be brute force attack. It is actually fast in hardware and relatively fast in software [6]. Drawback of the algorithm is as technology is improving there is a possibility to break the encrypted code in DES and as we use private key for cryptography if it is lost we cannot get the readable data at the receiving end [10].

5.2 RSA

Rivest-Shamir-Adleman(RSA) is asymmetric algorithm developed by Ron Rivest, Adi Shamir and Leonard adleman in the year 1977. This algorithm uses a key size greater than 1024bits and its block size depend on the key size that is being used. Block size is often calculated with a formula i.e 1+floor((x-1)/8)' where x is the key size. It is a block cipher and common networks are used to transfer messages. It takes 1 round to convert one message and its security is broken by timing attack [9]. Benefit of this algorithm is that it uses public key to transfer messages and also provides security to digital signatures that cannot be repudiated. Drawback of the algorithm is that even though the public key is safe its speed is comparatively low.

5.3 AES

Rijndael was selected as the (AES) Advanced Encryption Standard in Oct-2000 Designed by Vincent Rijmen and Joan Daemen in Belgium NIST. This algorithm uses a key size of 128, 192 or 256bits and a block size of 128, 192 or 256bits. It is a rajndael cipher and uses feistel networks to transfer messages. It takes 10, 12 or 14 rounds to convert messages and its security is broken by chosen plain attack. Benefit of this algorithm is that it is more secure and faster in both hardware and software [8]. Drawback of the algorithm is that it needs more processing and requires more rounds of communication when compared to DES.

5.4 Diffie-hellman

Diffie-hellman was found by whitfield diffie and martin hellman in the year 1976. This algorithm doesn't have specified key size because it uses key exchange management and has a block size of 64bits. It is a symmetric key cipher and uses common network to transfer messages. It takes nearly 14 round to convert a message and its security is broken by eaves dropping. Benefits of this algorithm is that security factors with respect to the fact that solving the discrete algorithm is very challenging, and that the shared key is never itself transmitted over the channel. Drawback of it is the lack of authentication [1].

5.5 Aria

Aria algorithm was found by South Korean researchers in the year 2003. This algorithm has a key size of 128, 192 or 256bits and a block size of 128bits. It is a block cipher and uses substitution permutation network to transfer messages. It takes 12, 14 or 16 rounds to convert a message and its security is broken by man in the middle attack. Benefit of this algorithm is that data and indexes are crash safe and it can replay almost everything from the log. Therefore, you make a backup of aria by just copying the log. Drawback of the algorithm is that the storage of very small rows are not efficient for page format and merge tables don't support aria.

5.6 Clefia

Clefia algorithm was found by sony in the year 2007. This algorithm has a key size of 128, 192 or 256bits and a block size of 128bits. It is a block cipher and use feistel network to transfer messages. It takes 18, 22 or 26 rounds to convert a message and its security is broken by cache attack. Benefit of this algorithm is its enhanced implementation efficiency in terms of both hardware and software (that is maximum throughput of 1.424 gbps) and high speed operation. Drawback this algorithm is that the last feature of 4 branch structure because of diffusion speed of smallest F-functions is slower.

5.7 Threefish

Threefish algorithm was found by Bruce schneir, Neils ferguson, Stefan lucks, Doug whiting, Mihir bellare, Tadayoshi kohno, Jon callas and jessewalker in the year 2008. This algorithm has a key size of 256, 512 or 1024bits and a block size of 256, 512 or 1024bits. It is a block cipher and uses feistel network to transfer messages. It takes 72 rounds to convert a message and its security is broken by boomerang attack. Benefit of this algorithm is that it provides a good and secured class of keys. Drawback of this algorithm is that it consumes a lot of memory.

5.8 Speck

Speck was found by Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers in NSA in the year 2013. This algorithm has a key size of 64, 72, 96, 128, 144, 192 or 256bits and a block size of 32, 48, 64, 96, or 128bits. It is a block cipher and uses ARX network to transfer messages. It takes 22, 23, 26, 27, 28, 29, 32, 33 or 34 rounds to convert a message and its security is broken by rectangle attack. Benefit of this algorithm is that image coding utilizing scalar quantization on hierarchical structures of transformed images has been a very effective and computationally simple technique. Drawback of this algorithm is that in speck the blocks are recursively and adaptively partitioned such that high energy area are grouped together into smaller sets and low energy areas are grouped together as larger sets.

5.9 Simon

Simon was found by Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers in NSA in the year 2013. This algorithm has a key size of 64, 72, 96, 128, 144, 192 or 256bits and a block size of 32, 48, 64, 96, or 128bits. It is a block cipher and uses feistel network to transfer messages. It takes 32, 36, 42, 44, 52, 54, 68, 69 or 72 rounds to convert a message and its security is broken by chosen cipher text attack. Benefit of this algorithm is that it solves black box problem and takes advantage of quantum effect. Drawback of this algorithm is that it examines an oracle problem which takes polynomial time on quantum computes but exponential times on a classical compute.

5.10 Chiasmus

Chiasmus was found by BSI in the year 2013. This algorithm has a key size of 160bits and a block size of 64bits. It is a block cipher and uses substitution permutation network to transfer messages. It takes 12 rounds to convert a message and its security is broken by man in the middle attack. Benefit of this algorithm is that it is easy to install and the drawback is that its hardware product is subjected to greater risks than a hardware solution.

Table 1 [6][8][11]. Illustrating comparisons between different types of cryptographic algorithm

PARAMETERS	CHIASMUS	SIMON	SPECK
DEVELOPER	BSI	Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers	Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers
YEAR	2013	2013	2013
KEY SIZE	160bits	64, 72, 96, 128, 144, 192 or 256bits	64, 72, 96, 128, 144, 192 or 256bits
BLOCK SIZE	64bits	32, 48, 64, 96, or 128bits	32, 48, 64, 96, or 128bits
ROUNDS	12	32, 36, 42, 44, 52, 54, 68, 69 or 72	22, 23, 26, 27, 28, 29, 32, 33 or 34
CIPHER TYPE	block cipher	Block cipher	Block cipher
NETWORK TYPE	substitution permutation network	Feistel network	ARX network
SECURITY ATTACKS	man in the middle attack	chosen cipher text attack	rectangle attack
MERITS	Easy to install	It solves black box problem, takes advantage of quantum effect	Image coding has been a very effective and computationally simple technique
DEMERITS	Hardware product is subjected to greater risks	Examines an oracle problem	Recursively and adaptively partitioned

Table 2 [6][8][11]. Illustrating comparisons between different types of cryptographic algorithms

PARAMETERS	THREEFISH	CLEFIA	ARIA
DEVELOPER	Bruce schneir, Neils ferguson, Stefan lucks, Doug whiting, Mihir bellare, Tadayoshi kohno, Jon callas and jessewalker	Sony	South Korean researchers
YEAR	2008	2007	2003
KEY SIZE	256, 512 or 1024bits	128, 192 or 256bits	128, 192 or 256bits
BLOCK SIZE	256, 512 or 1024bits	128bits	128bits
ROUNDS	72	18, 22 or 26	12, 14 or 16
CIPHER TYPE	Block cipher	Block cipher	Block cipher

NETWORK TYPE	Feistel network	Feistel network	substitution permutation network
SECURITY ATTACKS	Boomerang attack	Cache poisoning attack	man in the middle attack
MERITS	Provides a good and secured class of keys	Enhanced implementation efficiency in terms of both hardware and software, high speed operation	data and indexes are crash safe
DEMERITS	consumes a lot of memory	last feature of 4 structure diffusion speed of smallest F-functions is slower	merge tables don't support aria

Table 3 [6][8][11].Illustrating comparisons between different types of cryptographic algorithms

PARAMETERS	**AES**	**DES**	**RSA**	**DIFFIE-HELLMAN**
DEVELOPER	Vincent Rijmen and Joan Daemen in Belgium NIST	IBM	Rivest, Adi Shamir and Leonard adleman	whitfield diffie and martin hellman
YEAR	2000	1977	1977	1976
KEY SIZE	128, 192 or 256bits	56bits	>1024bits	uses key exchange management
BLOCK SIZE	128, 192 or 256bits	64bits	Depends on key size	64bits
ROUNDS	10,12 or 14	16	1 round for each message	14
CIPHER TYPE	Rijndael cipher	Block cipher	Block cipher	symmetric key cipher
NETWORK TYPE	Feistel network	Feistel network	Common network	Common network
SECURITY ATTACKS	Chosen plain attack	Brute force attack	Timing attack	Eaves dropping
MERITS	more secure and faster in both hardware and software	no real weakness has been found	uses public key, provides security to digital signatures that cannot be repudiated	security factors in solving discrete algorithm is very challenging, the shared key is never itself transmitted over the channel
DEMERITS	needs more processing	possibility to break the encrypted code in DES	speed is comparatively low	Lack of authentication

On comparing different types of algorithms there is no algorithm that is considered to be fully secured, all algorithms has its own pros and cons. Till today AES and DES algorithms are used in almost all system. AES is a rijndael cipher and it is fast too [12]. In DES even now there is no real weakness has been found and the most efficient attack is still brute force attack. But some feel that as technology is improving day by day there is a possibility to break the encrypted code in DES. AES is considered to be more secure and it is faster in both hardware and software. By design AES is faster in highlight their differences in terms each of 16 rounds. But AES actually needs more processing. Three fish algorithm provides good and secured class of keys but the problem it has is it consumes a lot of memory. [7] For banks and credit cards RSA algorithms are more preferred as they provide security to digital signatures that can be repudiated by the hackers. Because of this reason RSA is still used in banks. As mentioned earlier every algorithm has its own merits and demerits, the user must decide to choose appropriate algorithms that will best suite his needs.

Cryptanalysis is a common name given to various attacks that occurs in cryptographic algorithms. It works by breaking the encrypted code created to send message to a receiver safely by applying some algorithm. The different cryptanalysis attacks are classified as follows.

6. CRYPTANALYSIS ATTACKS

6.1 Known-plaintext attack

The Known-plaintext attack is an attack in which the criminal has both the plain text and its encrypted version of cipher text with him [3]. These details will help him to know the secret keys and code books that are being used by the user.

6.2 Chosen- plaintext attack

In a chosen plaintext attack it has the potential to decide on a random plaintext to be encrypted and it acquires the corresponding cipher text.

6.3 Rectangle attack

Rectangle attack increases the probability of using multiple differentials in each sub-cipher. It is easy to recover the key as it reduces data complexity by considering all quarters.

6.4 Brute-force attack

It is a passive and slow attack [3]. In this type of attack the hacker tries all possibilities of the key until he succeeds and the message is not broken.

6.5 Timing attack

As we know each operation in a computer takes some time to perform, the timing attack compromises a cryptosystem to find the time taken by the computer to execute that particular algorithm.

6.6 Chosen-cipher text attack

In this attack the cryptologist gathers data, minimum of partially, by selecting a cipher text and it gets back the decipherment beneath and unknown key [1].

6.7 Boomerang attack

In a boomerang attack the block cipher is got by choosing differential cryptanalysis. It was published in 1999.

6.8 Man-in-the-middle attack

In this attack the hacker is place in the middle of the two parties through communication channels who wish exchange their keys for secure communication. Man-in-the-middle attack is an active attack.

6.9 Cache poisoning attack

It is basically the hacking/corruption of internet server's table which is the system table which replaces other address with that of the system address. It is also called as domain name system (DNS) attack or DNS cache poisoning attack.

7. CONCLUSION

Based on the comparisons made on different cryptographic algorithms such as AES, DES, clefia, speck and RSA etc, we found that in this internet world nowadays, security of data play a major role as data and communications are passed and are done over open networks very often. From our evaluation, we found that in cryptographic algorithms symmetric encryption technique and asymmetric encryption techniques both have a higher ratio for encryption. [1][2]The key size is higher in asymmetric algorithm because of which in case of changing key size, it is viewed that higher key size leads to clear change in the battery and time consumption. In an asymmetric encryption technique the RSA algorithm is more secure as the code is complex because of its key size, tunability and also because of its use of factoring of high prime number for key generation.RSA is considered to be the efficient in storing digital signatures that cannot be repudiated. [2]Hence, RSA is found to be the best algorithm in this technique. Many findings say that if throughput is increased, power consumption is decreased. In symmetric encryption technique throughput is increased, power is decreased and because of which the speed is fast and is viewed as a good technique.[4][5] In symmetric techniques DES is considered to be the most secured because the most efficient attack on it is still now brute force attack and AES is proven to be fast in both hardware and software. But if we see the overall performance of all symmetric algorithms AES is viewed as a better solution. Threefish a derived algorithm from blowfish consumes less power and it is also fast. We would like to conclude by saying that all algorithms either symmetric or asymmetric algorithm all have their own pros and cons.[6] Each algorithm is unique in its own way and they are useful in real time encryptions. Each one is suitable in different applications, so it depends on the user to select the most appropriate algorithm that is best suited to his needs. Through our analysis on different cryptographic algorithms we wish to provide a pathway for future researchers to promote the performance and security of cryptographic algorithms.

8. REFERENCES

[1] Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC),volume 1,issue 6,june 2014, ISSN 2348 – 4853.

[2] Ms. Ankita Umale, Ms. Priyanka Fulare, " Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", The International Journal Of Engineering And Science (IJES) ,volume 3,issue 3,page 7-12,2014, ISSN (p): 2319 – 1805.

[3] E.Thambiraja, G.Ramesh and 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,ISSN: 2277 128X.

[4] Apoorva, Yogesh Kumar," Comparative Study of Different Symmetric Key Cryptography Algorithms", International Journal of Application or Innovation in Engineering & Management (IJAIEM),volume 2,issue 7,july 2013, ISSN 2319 – 4847.

[5] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram," Comparative analysis of performance efficiency and security measures of some encryption algorithms", International Journal of Engineering Research and Applications (IJERA),volume 2,issue 3,may-jun 2012 ISSN: 2248-9622.

[6] S. Abdul. Elminaam, H. M. Abdul Kader, M.M.Hadhoud, ,"Performance Evaluation of Symmetric Encryption Algorithms" , International Business Information Management Association (IBIMA),2009.

[7] M. Abolhasan, T. Wysocki and E. Dutkiewicz," A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks, Vol. 2, pp.1-22, 2004.

[8] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[9] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.

[10] Harsh Kumar Verma , Ravindra Kumar Singh "Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", International Journal of Computer Applications, ISSN: 0975-8887.

[11] 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.

[12] Shashi Mehrotra Seth, Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST, Vol. 2, Issue 2, June 2011 pp.192-192.