www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 11 Nov 2015, Page No. 15083-15090

A Survey of Commonly Used Cryptographic Algorithms in Information Security

***Manjula G.*[1] *and Dr. Mohan H.S.*[2]**

[1]Research Scholar, VTU, Belgaum, Karnataka, India

[2] Professor& HOD, Dept of Information Science & Engineering
SJB Institute of Technology, Bangalore, India

ABSTRACT

Progression in computing powers and parallelism technology are creating obstruction for credible security especially in electronic information transactions under cryptosystems. An enormous set of cryptographic schemes persist in which each has its own affirmative and feeble characteristics. Some schemes carry the use of long bits key and some support the use of small key. Practical cryptosystems are either symmetric or asymmetric in nature. With the fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form by using Encryption and Decryption Techniques. This survey compares trendy encryption techniques for convinced selection of both key and cryptographic scheme.

General Terms
Information Security, Encryption
Keywords
Encryption, RSA, DES, 3DES, AES, BLOW FISH

I Introduction

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-distribution 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. Any transaction on a network should be confidential, to ensure data authentication, accountability and confidentiality, integrity and availability, also known as CIA triad [1].

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. The NIST Computer Security Handbook [NIST95] defines the term computer security as, “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources”. Security in networking is based on Cryptography (a word with Greek origins, means “secret writing”), the science and art of transforming messages to make them secure and immune to attack [2]. Cryptography converts the message into a non readable format and sends the message over an unsecure channel. “Encryption is a process of transferring plaintext information to a form called cipher text using an algorithm called cipher which is readable only by whom who has special knowledge called encryption key”. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

II. Cryptography Goals

Cryptography is used to achieve many goals and some of the goals are as follows:

1. Authentication: it is a process of giving identity to someone to access particular resource using the keys.

2. Confidentiality: It is most important goal of cryptography, which ensure that nobody understand the message except the one who has the cipher key.

3. Data Integrity: It is the process of ensuring that nobody is allowed to alter the transmitted message except the party who is allowed to do so.

4. Non-Repudiation: Ensure that neither the sender nor the receiver of the message should be allowed to deny the transmission of the message.

5. Access Control: Ensure that only the authorized parties are able to access the transmitted message.

III Basic Terminologies used in Cryptography

Computers are used by millions of people for many purposes such as banking, shopping, military, student records etc Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing [3]. The information that we need to hide, is called plaintext , It's the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the first draft of a message in the sender before encryption, or it is the text at the receiver after decryption. The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. Many algorithms are used to transform plaintext into cipher text [4]. Cipher is the algorithm that is used to transform plaintext to cipher text, The opposite of cipher mechanism is called decipher (decode) that is the algorithm which recovers the cipher text, this method is called decryption The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key. Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks while information security is about how to prevent attacks, and to detect attacks on information-based systems [2]. Cryptanalysis (code breaking) is the study of principles and methods of deciphering cipher text without knowing the key, typically this includes finding and guessing the secrete key, The field of both cryptography and cryptanalysis is called cryptology [4,15]. Symmetric encryption refers to the process of converting plaintext into cipher text at the sender with the same key that will be used to retrieve plaintext from cipher text at the recipient. while asymmetric encryption refers to the process of converting plaintext into cipher text at the sender with different key that will be used to retrieve plaintext from cipher text at the recipient.The attackers are not just monitoring on the traffic, but they also attempt to breach or shut down the service [3,5]. Authentication is the process of determining whether someone is the same person who really is, such as login and password in login pages while authorization is the process of ensuring that this person has the ability to do something [3, 4, 5]. Brute force is the attacker who is trying all of the possible keys that

DOI: 10.18535/Ijecs/v4i11.37

may be used in either decrypt or encrypt information [5].

IV Classification of Cryptography algorithms

Cryptography Algorithms can be classified into two parts:

- **Symmetric cryptography**

This type of cryptography practices only one key for both encryption and decryption, and it is also called secret key cryptography [6]. This technique works by the following
principles:
1. The plaintext is encrypted with the key to produce cipher text and it is sent to the receiver.
2. The receiver uses the same key to decrypt the cipher text and finds the original plaintext.

In Symmetric key cryptography both the sender and the receiver must know the same key in order to use the technique. In decryption, same secret key is used by applying the reverse transformation of the cipher text block and original plain text is produced[7].

- Asymmetric Cryptography (PKC)

This technique requires two types of keys: one to encrypt the plaintext and one to decrypt the cipher text, and it doesn't work without one or another. It is called asymmetric cryptography because it is used a pair of keys: one is the public key that can be advertised by the owner to whoever he wants, and the other one is the private key and it is known only by the owner. Two prime numbers are generated by a special set of rules, and the product of these numbers is a very large number, from which it derives the key-set [8].

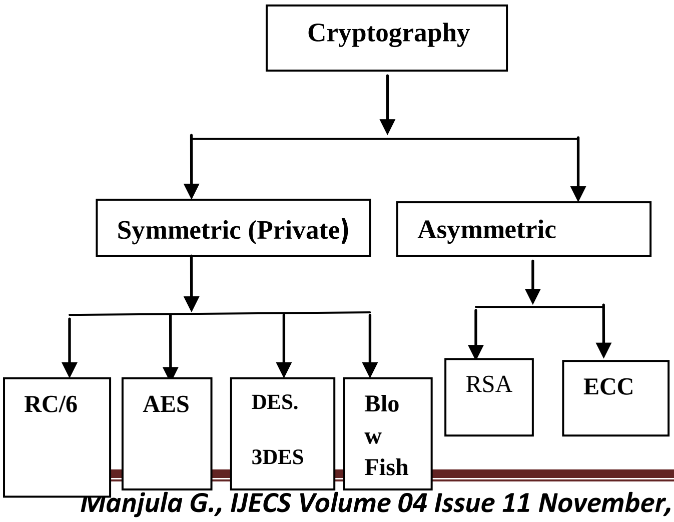

Fig 1: Different Cryptographic Techniques

V Related works

This subsection describes and examines previous work done in field of data encryption. The metrics taken into consideration are processing speed, throughput, power consumption, avalanche effect, packet size and data types.

Arora et al. [9] studied about the performance of different security algorithms on a cloud network and also on a single processor for different input sizes. This paper aims to find in quantitative terms like Speed-Up Ratio that benefits of using cloud resources for implementing security algorithms (RSA, MD5 and AES) which are used by businesses to encrypt large volumes of data. Three different kinds of algorithms are used – RSA (an asymmetric encryption algorithm), MD5 (a hashing algorithm) and AES (a symmetric encryption algorithm). RSA is the most time consuming and MD5 is the least.

Seth et al. [10] have done the comparative analysis of three algorithms; RSA, DES and AES while considering certain parameters such as computation time, memory usage and output byte. Experimental results show that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Mandal et al. [11] compared two most widely used symmetric encryption techniques i.e. data encryption standard (DES) and advanced encryption standard (AES) on the basis of avalanche effect due to one bit variation in plaintext keeping the key constant memory required for implementation and simulation time required for encryption. Avalanche effect is the property of any encryption algorithm in which a small change in either the key or the plaintext should produce a significant change in the cipher text. Avalanche effect is very high for AES as compared to DES which shows AES is better than DES. AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that involve monetary transactions.

VI Cryptanalysis

There are two general approaches for attacking a conventional encryption algorithm [18]:

Cryptanalysis: This is used for deciphering a message without any knowledge of the enciphering details. Cryptanalysis is the science of recovering the plaintext of a message without the access to the key. Successful cryptanalysis may recover the plaintext or the key. It also finds weakness in the cryptosystem.

Brute – Force attack: The attack tries every possible key on a piece of cipher text until an intelligible translation into plain text is obtained. This is tedious and may not be feasible if key length is relatively long.

VII Description of Common Encryption Algorithms

There are many cryptographic algorithms available in the market to encrypt the data. The strength of encryption algorithm heavily relies on the computer system used for the generation of keys. Some important encryption algorithms are discussed here***:

A.Rivest-Shamir-Adleman (RSA)

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key [12, 13]. RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES. Following illustrates the sequence of events followed by RSA algorithm for the encryption of multiple blocks.

- ***Key Generation Procedure***

1. Choose two distinct large random prime numbers p & q such that p ≠ q.
2. Compute n= p × q.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that 1<e<phi(n)
5. Compute d to satisfy the congruence relation d × e = 1 mod phi (n); d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

- ***Encryption***

Plaintext: P < n
Cipher text: C= P^{e} mod n.

- ***Decryption***

Cipher text: C
Plaintext: P=C^{d} mod n.

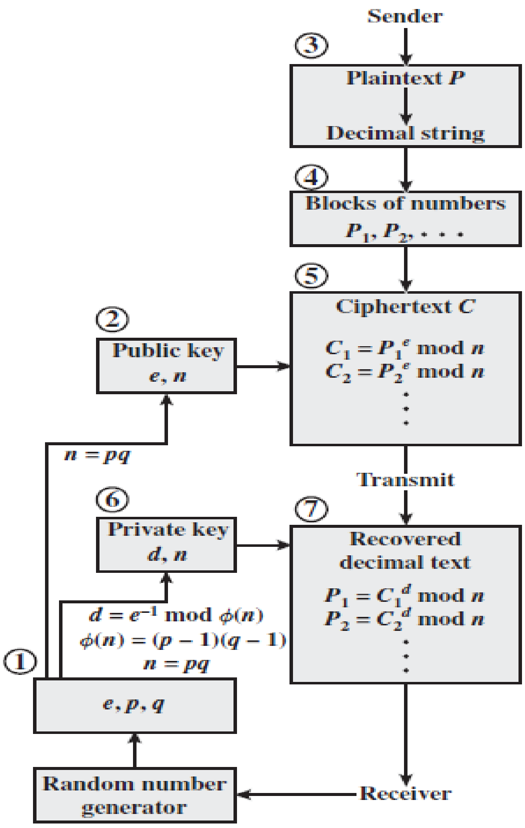

Fig 2: RSA processing of Multiple Blocks

B. Data Encryption Standard (DES)

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key [14].

Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications [15].

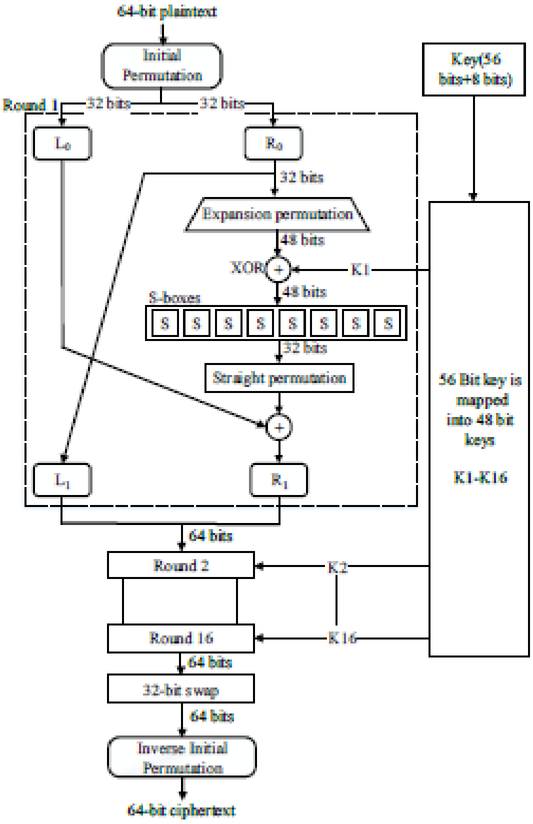

Fig 3: General Depiction of DES

C. Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [17]. The standards define three keying options

Option 1, the preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives keyspace of 3 × 56 = 168 bits.

Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives keyspace of 2 × 56= 112 bits.

Option 3 is a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm.
In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods [16]

D. Advanced Encryption Standard (AES)

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text [19]. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching the final round, this output goes though nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation [3, 20]. Figure 4 shows the overall process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.
Each round of AES is governed by the following transformations [10]:

- ***Substitute Byte transformation***

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael Sbox.

- ***Shift Rows transformation***

It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, is cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

- ***Mixcolumns transformation***

This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

- ***Addroundkey transformation***

It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse.

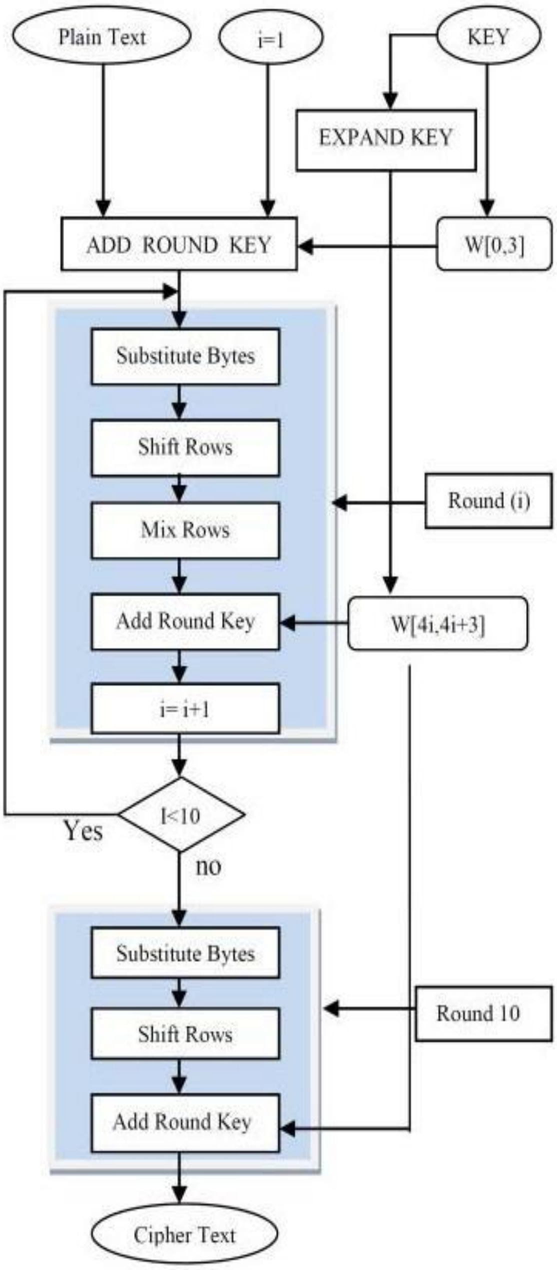

Fig 4: AES (Advanced Encryption Standard) process

E. Blowfish Algorithm

Bruce Schneier designed Blowfish algorithm in 1993. The algorithm description is defined in the Bruce Schneier URL [17]. Blowfish is a 64 bit block cipher with variable length key from 32 bit (4 bytes) to 448 bits (56 bytes). The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is suitable and efficient for hardware implementation. The algorithm has two parts- Key expansion and Data Encryption. The key expansion step converts 448 bit key into 4168 bytes. A P-array of size 18 and four S-boxes whose size is 256 each of which are initialized to hexadecimal digits of π. XOR each entry in P array and S boxes with 32 bits of the key. There are total 16 rounds of data encryption. In each round a 32 bit subkey is XORed with leftmost 32 bits of plaintext and the result is then passed to the F function of Blowfish. This result becomes rightmost 32 bits for the next round and the output of F function is XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for the next round and so on.

The F function is the distinguishing feature of Blowfish and is applied as follows .First Divide XL (32 Bits) into four 8-bit quarters: a, b, c, and d. Then apply the formula. F (XL) = {(S1 [a] + S2 [b]) S3 [c]} + S4 [d])}
Where + means addition modulo 2^32, and means exclusive OR and S1, S2, S3, S4 are four substitution boxes.

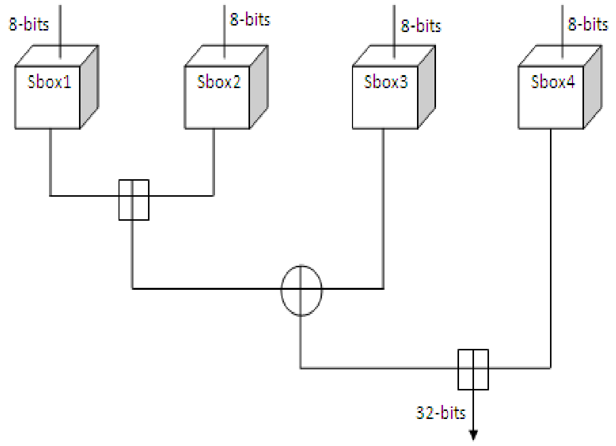

Fig 5: F Function diagram of Blowfish

- Divide 64-bits into two 32-bit halves: XL, XR
  For i = 1 to 16
- XL = XL XOR Pi
- XR=F(XL) XOR XR
- Swap XL and XR
- Swap XL and XR (Undo the last swap)
- XR=XR XOR P17
- XL = XL XOR P18
- Concatenate XL and XR

VII Conclusion

Data security is one of the import aspects of communication. Security of data can be achieved using the art of cryptography. There are many algorithms available for cryptography but the selection of one of the best algorithm is also very important. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. In this paper, it has been surveyed on the existing cryptographic techniques. These cryptographic techniques are studied and analyzed well to ensure the security proceedings.

References

[1] Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010.

[2] Behrouz A Forouzan, “Data Communications and networking”, McGraw-Hill, 4th Edition.

[3] D.Delfs., and K. Helmut.,: " Introduction To Cryptography: Principles and applications ", Second Edition. Springer Science & Business Media, (2007), Germany.

[4] H.Kenneth, " Elementary Number Theory and Its Applications " Third Edition. Addison-Wesley, (1992): Germany

[5] D.Salomon" Data Privacy and Security " First Edition. Springer-Verlag New York, ., (2003):, Inc. USA.

[6] Gary C. Kessler, An overview of Cryptography, 28April2013 http://www.garykessler.ne/library/crypto.html

[7] RSA Laboratories- Cryptographic tools; section 2.1.5. Unpublished: http://www.rsa.com/rsalabs/node.asp?id=217

[8] Ing. Cristian MARINESCU, prof.dr.ing. Nicolae ŢĂPUŞ ; "An Overview of the Attack Methods Directed Against the RSA Algorithm"; Revista Informatica Economica, nr. 2(30)/2004

[9] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012.

[10] Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

[11] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[12] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[13] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011

[14] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, pp. 106-111, January 2011.

[15]"DES",http://www.tropsoft.com/strongenc/des.htm

[16]"3DES",http://en.wikipedia.org/wiki/Triple_DES

[17] Bruce Schneier (2008,October) The Blow Fish Encryption Algorithm.[online] http://www.schneier.com/blowfish.html

[18] Mohan H.S and A. Raji Reddy "Performance Analysis of AES and Mars Encryption Algorithms",IJCSI International Journal of Computer Science Issues,Vol.8,Issue 4,No 1.July 2011.