*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 11-18*
*www.iosrjournals.org*

# Survey on Symmetric and Asymmetric Key Cryptosystems

Srinivas Madhira[1], Porika Sammulal[2]
[1](Dept. of Computer Science & Engineering, SBIT, Khammam, Telangana State, India)
[2](Dept. of Computer Science & Engineering, JNTUHCEJ, Karimnagar, Telangana State, India)

***Abstract***: *Cryptography is the collection of techniques used to hide the information securely from the eavesdroppers during its transmission over the network. Cryptography is centuries old, during the course of time a number of techniques have been proposed and developed by the researchers. Some of these techniques have become popular and widely in use today in a varieties of applications. This paper discusses the two most important categories of techniques symmetric and asymmetric cryptosystems.*

***Keywords***: *symmetric cryptosystem, asymmetric cryptosystem, secrete key, private key, public key, authentication, confidentiality, integrity.*

## I. Introduction

Before the era of computer systems, people used to store the valuable information in the cabinet with the locking facility. With the invention and development of the computer systems over the past several decades, organizations started storing the valuable information in the computer systems. The information stored in the computer system is vulnerable to the attacks in the form of unauthorized access to the computer systems and viruses. With the advancements in the technology slowly computers have been connected on to the network which has enabled the sharing of information over the network. The exponential growth in the computer technology enabled the transfer of information over the high speed computer data networks. This has led the organization and individual to transfer the valuable information on the high speed networks. The information transferred on the network is vulnerable to the attacks such as eaves dropping, unauthorized copying or modifications, masquerade, reply, denial of service attacks, etc. Hence, there is a need to protect the transfer of information over the network. A number of techniques have been developed by the researcher over the past several decades to protect the information. The collections of techniques or tools used to protect the information stored in the computer system is called "Computer Security" and the collections of techniques or tools used to protect the information during its transmission is called "Network Security" or "Information Security" or "Internet Security".

## II. Cryptography

Cryptography is the art of science or collection of techniques or tools used to protect the information during its transmission over the network. In order to protect the information to be transmitted, the cryptographic technique converts the plain text message in to some coded form called the cipher text. This cipher text is transmitted to the destination over the public network. The cipher text is not understood or readable by others except source and destination. When destination receives the cipher text, it is converted back to the plain text using same cryptographic technique. Thus, message is secured during the transmission. In addition to securing the message during transmission, a number of other functionalities have been added to the cryptographic techniques over the years, these functions include authentication, confidentiality, integrity, non-repudiation, availability and access control. The cryptographic technique is also called cryptosystem or cryptographic algorithm or encryption/decryption algorithm.

The process of converting plain text into the cipher text is called encryption; converting cipher text back to the plain text is called decryption. Usually encryption is done at source side and decryption is done at the destination side. The algorithm used for encryption is called encryption algorithm and algorithm used for decryption is called decryption algorithm. The encryption and decryption algorithms need not be same. The encryption and decryption process uses secrete information during conversion process known to source or destination or both, this is called key. The algorithm or technique used for conversion is called cryptosystem or cryptographic algorithm or encryption/decryption algorithm. The study of various cryptosystems is called cryptography. The process of obtaining either plain text or key from the cipher text is called cryptanalysis. The person performing cryptanalysis is called cryptanalyst. A number of cryptanalysis techniques have been developed by cryptanalysts over the years. The combination of cryptography and cryptanalysis is called cryptology. The encryption and decryption process is shown in fig. 1.

A number of cryptosystems have been developed by the researchers over the past several decades. Some of them are most popular, have been in use even today and some other have disappeared in the history of cryptography. The cryptosystems have been categorized along many dimensions, one of them is, key, used in

the conversion process. Based on this, cryptosystems have been divided into two categories; symmetric and asymmetric cryptosystems.

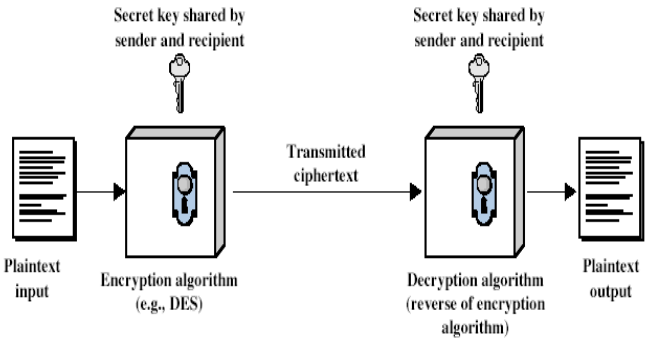


**Fig.1.** Encryption and Decryption Process

## III. Symmetric Cryptosystems

If the message to be transmitted is encrypted with a key before the transmission and decrypted with the same key after the transmission then it is called symmetric cryptosystem. In this, the key used for encryption and decryption is known only to the sender and the receiver of the information. Since, same key is used at both sides they are called symmetric key cryptosystems; only one key is used at both sides they are called single key or one key cryptosystems; these techniques have been in use from the early days of the computers so they are called conventional cryptosystems. The security of these systems depends on the secrecy of the key. The person who knows the key can easily decrypt the cipher text. Hence, key must be maintained secretly because of this they are called private key or secrete key cryptosystems. The cryptosystem is secure as long as the key is secrete.

A number of symmetric key cryptosystems have been developed over the past several decades by the researchers. DES, Triple-DES, RC2, RC4, AES, CAST-128, Blowfish and RC5 are few examples of symmetric key cryptosystems. Most of these cryptosystems follow a basic structure developed by the Horst Feistel of IBM in 1971. This structure is called Feistel Structure. The feistel structure generates product cipher with alternate stages of substitutions and permutations. It has been proved that the symmetric key cryptosystems which use feistel structure are strong against cryptanalysis attacks. The feistel structure is shown in fig. 2.

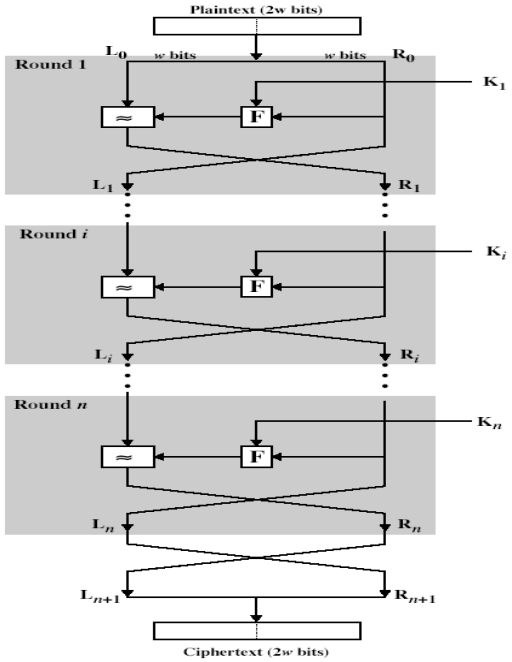


**Fig 2.** Feistel Structure

The advantage of using feistel structure for the cryptosystem is that, we need not have separate encryption and decryption algorithms. The decryption algorithm is same as encryption algorithm except that the

keys are used in the reverse order in decryption algorithm. The encryption and decryption process of feistel structure is shown in fig.3.

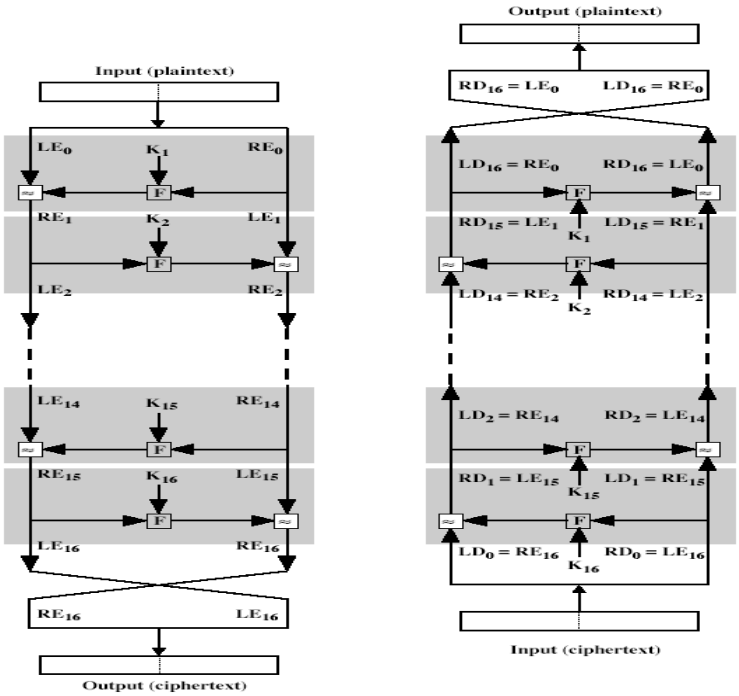


**Fig.3.** Encryption and Decryption Process of Feistel structure

### 3.1 Data Encryption Standard(DES)

Data Encryption Standard (DES) algorithm is a symmetric key cryptosystem. It is a modified version of LUCIFER symmetric key cryptosystem developed by Horst Feistel of IBM in 1971 as a part of cryptographic project. LUCIFER is a 64 bit block cipher with a key length of 128 bits. It has been modified by Walter Tuchman and Carl Meyer, the modification is the reduction in its key size from 128 bits to 56 bits. This algorithm is adopted as a standard encryption algorithm by National Bureau of Standards (NBS), now National Institute of Standards and Technology (NIST) in 1973. It process the data in 64 bit blocks hence, it is called block cipher. DES is a block cipher and generates product cipher. It converts the 64-bit plain text block into 64-bit cipher text block through a series of permutations and substitutions. DES has total 19 rounds of processing; first round is initial permutation which is followed by 16 identical rounds of processing, followed by a 32bit swap round and Inverse to initial permutation round. Each of 16 identical rounds uses a unique 48 bit key generated from 56 bit key input of DES. The encryption and decryption process of DES is shown in fig.4.

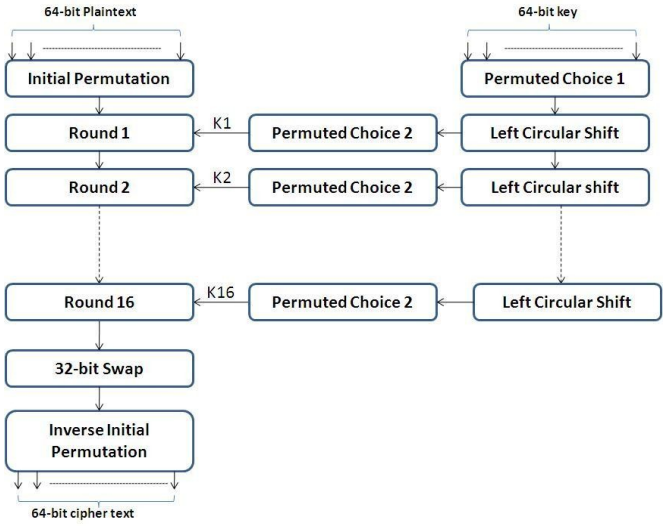


**Fig.4.** DES Encryption Process

DES follows feistel structure hence, the decryption process is same as encryption process except that the keys in 16 identical rounds are to be used in the reverse order. DES has strong internal structure hence, it is strong against statistical cryptanalysis attacks, linear cryptanalysis attacks, differential cryptanalysis attacks and timing attacks. When this algorithm was adopted as standard in 1973 by NBS, it was strong even against brute force attack but because of exponential growth in the computing power during last several decades, now it is not secure. In 1996 NBS announced to go for Triple DES instead of DES. Today DES cracker machines are available to break DES ciphers.

### 3.2 Triple DES

Triple DES (TDES) is same as DES except that DES is repeated three times. It was proposed by NIST and adopted as a standard in 1996. The TDES uses effectively 168 bit key i.e. each DES stage uses a unique 56 bit key hence effective key length is 168 bits. Hence, it has been made strong against brute force attack. The encryption and decryption process of TDES is shown in fig.5.

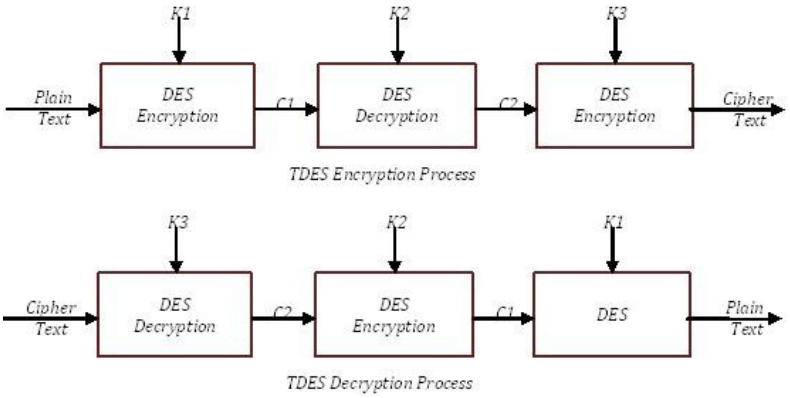


**Fig.5.** TDES Encryption and Decryption Process

### 3.3 DESX

DESX is a DES variant from RSA Data Security, Inc. DESX uses a technique called whitening to obscure the inputs and outputs to DES. In addition to a 56-bit DES key, DESX has an additional 64-bit whitening key. These 64 bits are XORed to the plaintext before the first round of DES. An additional 64 bits, computed as a one-way function of the entire 120-bit DES key, is XORed to the cipher text after the last round. Whitening makes DESX much stronger than DES against a brute-force attack; the attack requires (2120)/n operations with n known plaintexts. It also improves security against differential and linear cryptanalysis; the attacks require 261 chosen plaintexts and 260 known plaintexts, respectively.

### 3.4 CRYPT(3)

CRYPT(3) is a DES variant found on UNIX systems. It is primarily used as a one-way function for passwords, but sometimes can also be used for encryption. The difference between CRYPT(3) and DES is that CRYPT(3) has a key-dependent expansion permutation with 212 possible permutations. This was done primarily so that off-the-shelf DES chips could not be used to construct a hardware password-cracker.

### 3.5 Generalized DES

Generalized DES (GDES) was designed both to speed up DES and to strengthen the algorithm. The overall block size increases while the amount of computation remains constant.

### 3.6 Madryga

In 1984, W. E. Madryga developed an algorithm and named it as madryga algorithm. It is symmetric block cipher and efficient for software. It has no irritating permutations and all its operations work on bytes. Researchers at Queensland University of Technology examined Madryga, along with several other block ciphers. They observed that the algorithm didn't exhibit the plain text-cipher text avalanche effect. Additionally, many cipher texts had a higher percentage of ones than zeros.

### 3.7 New DES

NewDES was designed in 1985 by Robert Scott as a possible DES replacement. The algorithm is not a DES variant, as its name might imply. It operates on 64-bit blocks of plaintext, but it has a 120-bit key. NewDES is simpler than DES, with no initial or final permutations. All operations are on entire bytes. Scott

showed that every bit of the plaintext block affects every bit of the cipher text block after only 7 rounds. NewDES has the same complementation property that DES has.

### 3.8 Other Symmetric Cryptosystems

Few more symmetric cryptosystems are FEAL, REDOC, LOKI, Khufu and Khafre, RC2, RC5, IDEA, MMB, Skipjack, GOST, CAST, Blowfish, SAFER, Crab, 3-way, SAFER, AES, etc.

### 3.9 Disadvantages of Symmetric Key Cryptosystems

There are some problems with symmetric key cryptosystems. The key used in the encryption/decryption process must be maintained securely by the two participants. The key distribution becomes a problem when the participants are at large distance from each other. The key distribution is also a problem when many people are involved in communication such as in distributed environment. However, because of their fastness they are being used in combination with public key cryptosystems in a number of applications.

## IV. Asymmetric Cryptosystems

If the message to be transmitted is encrypted with one key before the transmission and decrypted with a different key after the transmission then it is called asymmetric cryptosystem. These cryptosystems use two keys one for encryption and other for decryption. The two keys are different but mathematically related. It is very difficult to generate one key with the knowledge of other key. Since, different keys are used at each side they are called asymmetric key cryptosystems or double key or two key cryptosystems. Out of two keys one key is distributed to the public and other key is kept securely with the owner. The key distributed to the public is called public key and the key kept with the owner is called private key. Any key can be used for encryption with other key is used for decryption. Since it uses the concept of public keys they are called public key cryptosystems. The security of these systems depends on the secrecy of private the key and the computational time required to break the cipher. The person who knows private key can easily decrypt the cipher text. Hence, private key must be maintained secretly by the owner of the keys. In public key cryptosystems each participant generates a pair of keys, distributes one of the keys to the public and keeps other key secretly with him. Any user 'A', who desires to send a message to the participant 'B', encrypts the message with the public key of B and sends it to B. The encrypted message only decrypted by the private key of B, since only B has his private key nobody else can decrypt it hence; message is secure during the transmission.

Public key cryptosystems overcome the draw backs of symmetric key cryptosystems. The key distribution in public key cryptosystem is easy. The private key is known only to the owner hence, cryptosystem is strong as long as owner keeps the private key secretly. The public key cryptosystem concept was first proposed by Diffie and Hellman. A number of public key cryptosystems have been developed over the years by the researchers. RSA, Diffie-Hellman, Elgamal, etc. are best examples of public key cryptosystems.

### 4.1 RSA Public Key Cryptosystem

RSA is popular public key cryptosystem widely in use in a number of applications today. It was developed by Ron Rivest, Shamir and Adleman in 1973. RSA stands for first letter in the names of these three researchers. In RSA the message M to be considered as an integer between 0 and (n-1), where n is a large prime number, $M < n$. Now, encrypt the message M by raising it to the $e^{th}$ power modulo n where e is an integer, $e < \phi(n)$, $\phi$ is the Euler's totient function. The result is the cipher text C which is also an integer, $C < n$.

$$C \equiv E(M) \equiv M^e \pmod{n}, \text{ for a message M, } M<n.$$

To decrypt the cipher text C, raise it to another power d, again modulo n where d is an integer, $d < \phi(n)$, $\phi$ is the Euler's totient function.

$$M \equiv D(C) \equiv C^d \pmod{n}, \text{ for a cipher text C, } C<n.$$

The encryption key is the pair of positive integers (e, n). Similarly, the decryption key is the pair of positive integers (d, n). Each user makes encryption key public and keeps the corresponding decryption key private. To get the values of n, e, and d follow the steps below

- First select two large prime numbers p and q, $p \neq q$, Keep p and q values private
- Compute n as the product of p and q, $n = p \times q$, n is public
- Calculate $\phi(n)$, using p and q, $\phi(n) = (p-1) \times (q-1)$, where $\phi(n)$ is the Euler's totient function, keep $\phi(n)$ value private
- Pick the integer e to be a large, random integer which is relatively prime to $\phi(n)$ such that d satisfies: $\gcd(e, \phi(n)) = 1$, e is public, $e < \phi(n)$
- The integer d is computed from $\phi(n)$ and e, to be the multiplicative inverse of e modulo $\phi(n)$, thus we have,

$$e \times d \equiv 1 \pmod{\phi(n)}, \text{ d is private}$$

- Hence, Public Key={e, n} and Private Key = {d, n}

In hardware, RSA is about 1000 times slower than DES. In software, DES is about 100 times faster than RSA. These numbers may change slightly as technology changes, but RSA will never approach the speed of symmetric algorithms. However, RSA encryption speed can be increased by selectively about choosing a value of e. The three most common choices for e value are 3, 17, and 65537 ($2^{16} + 1$).

**4.2 Knapsack Cryptosystem**

The first algorithm for generalized public-key encryption was the knapsack algorithm developed by Ralph Merkle and Martin Hellman. It could only be used for encryption, although Adi Shamir later adapted the system for digital signatures. Knapsack algorithms get their security from the knapsack problem, an NP-complete problem. This algorithm was found to be insecure in the applications but, it is used for knowing how an NP-complete problem can be used for public-key cryptography.

**4.3 Pohlig-Hellman Cryptosystem**

The Pohlig-Hellman cryptosystem is similar to RSA but, it is not an asymmetric cryptosystem, because the keys are easily derivable from each other; both the encryption and decryption keys must be kept secret.

Like RSA, $C = M^e \bmod n$

$M = C^d \bmod n$

where e x d Ξ 1 (mod some complicated number)

Unlike RSA, n is not defined in terms of two large primes, it must remain part of the secret key. If someone had e and n, they could calculate d. Without knowledge of e or d, an adversary would be forced to calculate

$e = \log_M (C) \bmod$ , which is difficult because e is the discrete logarithm of C base M

**4.4 ElGamalCcryptosystem**

The ElGamal is a public key cryptosystem. It can be used for both digital signatures and encryption; it gets its security from the difficulty of calculating discrete logarithms in a finite field. To generate a key pair, first choose a prime, p, and two random numbers, g and x, such that both g and x are less than p. Then calculate

$y = g^x \bmod p$

The public key is y, g, and p. Both g and p can be shared among a group of users. The private key is x. To encrypt message M, first choose a random k, such that k is relatively prime to p - 1. Then compute

$a = g^k \bmod p$

$b = y^k M \bmod p$

The pair, a and b, is the ciphertext. Note that the ciphertext is twice the size of the plaintext. To decrypt a and b, compute

$M = b/a^x \bmod p$

Since $a^x$ Ξ $g^{kx}$ (mod p), and $b/ax$ Ξ $y^k M/a^x$ Ξ $g^{xk} M/g^{xk}$ Ξ M (mod p), this all works well. This is same as Diffie-Hellman key exchange except that y is part of the key, and the encryption is multiplied by $y^k$.

**4.5 Diffie-Hellman Cryptosystem**

Diffie-Hellman is the first public-key algorithm ever invented. It gets its security from the difficulty of calculating discrete logarithms in a finite field, as compared with the ease of calculating exponentiation in the same field. Diffie-Hellman can be used for key exchange or distribution applications. With this Alice and Bob can use this algorithm to generate a secret key but, it cannot be used to encrypt and decrypt messages. The math is simple. First, Alice and Bob agree on a large prime, q and g, such that g is primitive root of q, mod n. These two integers don't have to be secret. Alice and Bob can agree to them over some insecure channel. They can even be common among a group of users. It doesn't matter.Then, the protocol goes as follows:

- Alice chooses a random large integer A and sends to Bob
  $X = g^A \bmod q$
- Bob chooses a random large integer B and sends to Alice
  $Y = g^B \bmod q$
- Alice computes
  $K = Y^A \bmod q$
- Bob computes
  $K' = X^B \bmod q$

Both K and K ′ are equal to $g^{AB} \bmod q$. No one listening on the channel can compute that value; they only know q, g, X and Y. Unless, they can compute the discrete logarithm and recover A or B, they do not solve the problem. So, K is the secret key that both Alice and Bob computed independently.

### 4.6 Other Public Key Cryptosystems

Few more public key cryptosystems are Rabin's public key cryptosystem, Williams public key cryptosystem, McEliece public key cryptosystem, Elliptic Curve public key cryptosystem, LUC public key cryptosystem, Finite Automaton Public-Key Cryptosystem, etc. Out of all these public key cryptosystems Elliptic Curve public key cryptosystem is now becoming popular because it uses small length keys and provides an equivalent level of security as that of RSA.

### 4.7 Disadvantages of Asymmetric Key Cryptosystems

Public key cryptosystems uses large keys containing more than 1024 bits because of this their encryption and decryption speed at the hardware and software level is slow compared with symmetric encryption algorithms. Hence, hybrid cryptosystems are being used to improve the speed.

## V. Differences between symmetric and asymmetric key cryptosystems

Public key cryptosystems are different from symmetric key cryptosystems. Symmetric key cryptosystems use Boolean logics for manipulating the bits whereas public key cryptosystems uses exponential mathematical equations. Symmetric key cryptosystems use simple operations such as OR, AND, EXOR, etc. whereas public key cryptosystems use complex mathematical equations. Symmetric key cryptosystems are fast whereas public key cryptosystems are slow because of complex mathematical operations. The key length in symmetric key cryptosystems is relatively small when compared with that of public key cryptosystems. Keys distribution in symmetric key cryptosystems is difficult where as in public key cryptosystems it is relatively easy. Both types of cryptosystems have their own advantages and disadvantages and both are secured. No one is superior to other. The security of any cryptosystem depends on the length of the key and computational time required to break the cipher.

## VI. Conclusions

In this paper, various types of symmetric and asymmetric key cryptosystems have been discussed. Each type of cryptosystem has its own advantages and disadvantages. It is found that symmetric key cryptosystems are faster than the asymmetric key cryptosystems. If the combinations of these two cryptosystems are used, it increases the speed and security of the communication. Hence, asymmetric key cryptosystems are used for distributing the secret key of the symmetric key cryptosystems. Once key is distributed between the participants all communication is encrypted and decrypted using symmetric key cryptosystem.

## Acknowledgment

I would like to express my sincere gratitude to the Management, Directors and Principal of Swarna Bharathi Institute of Technology (SBIT), Khammam for their strong support and encouraging us to publish the papers. I would also like to thank Mrs. S. Neelima, Assoc. Prof., Department of Computer Science & Engineering, SBIT and Mrs. Y. Laxmi Prasanna, Assoc. Prof., Department of Computer Science & Engineering, SBIT for giving their valuable suggestions during preparation this technical paper.

## References

[1] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.

[2] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques", presented at National Computer Conference, New York, June 7–10, 1976.

[3] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", This research was supported by National Science Foundation grant MCS76-14294, and the Officee of Naval Research grant number N00014-67-A-0204-0063.

[4] William Stallings, "Cryptography and Network Security", Principles and Practices, Pearson Education, 3rd Edition, 2003.

[5] William Stallings, "Network Security Essentials", Applications and Standards, Pearson Education, 3rd Edition, 2008.

[6] Bruce Schneier, "Applied Cryptography", Protocols, Algorithms, and Source Code in C, Second edition, John Wiley and Sons.

[7] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw Hill Publishers, New Delhi, 2007.Matt Blumenthal, "Encryption: Strengths and Weaknesses of Public-key Cryptography ", submitted to Department of Computing Sciences, Villanova University, Villanova, PA 19085.

[8] Ikshwansu Nautiyal and Madhu Sharma, "Encryption using Elliptic Curve Cryptography using Java as Implementation tool", IJARCSSE, Vol.4, Issue.1, pp. 620-625, Jan.2014.

[9] Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Pubic Key Cryptosystem Using Short Range Natural Number Algorithm", IJARCSSE, Vol.2, Issue. 8, pp. 134-138, Aug. 2012.

[10] Preeti, Bandana Sharma, "Review Paper on Security in Diffie-Hellman Algorithm", IJARCSSE, Vol.4, Issue. 3, pp. 264-266, March 2014.

[11] Saranya K, et al., "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014, pp.539-544.

[12] Mini Malhotra, Aman Singh, "Study of Various Cryptographic Algorithms", International Journal of Scientific Engineering and Research (IJSER), Volume 1 Issue 3, November 2013, pp.77-88.

[13] Alese, B. K., Philemon E. D., Falaki, S. O, "Comparative Analysis of Public-Key Encryption Schemes", International Journal of Engineering and Technology Volume 2 No. 9, September, 2012, pp.1552-1568.
[14] Douglas R.Stinson, "Cryptography: Theory and Practice", CRC Press, Inc., Boca Raton,FL, USA, 1995.
[15] Martin E. Hellman, "An Overview of Public Key Cryptography", IEEE Communication Magazine, Nov. 1978, Vol.16, Issue no.6.
[16] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithm", IEEE Trans. Inform, Theory, IT-31, no.4, pp469-472, July 1985.
[17] TAHER ELGAMAL, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Algorithms", In Proceedings of CRYPTO84 on Advances in cryptology, pages 10{18. Springer-Verlag New York, Inc., 1985.
[18] Kuna Siva Sankar, "Public Key Cryptosystems (Rsa & Elgamal)", A dissertation submitted to National Institute Of Science Technology, Odisha, India, NIST, Summer research Fellowship.

**Madhira Srinivas,** working as an Associate Professor in the Department of Computer Science and Engineering(CSE), Swarna Bharathi Institute of Science & Technology(SBIT), Khammam. He obtained his B.Tech degree from REC, Warangal and M.Tech degree from JNTUH, Hyderabad. Now, he is pursuing Ph.D. in Computer Science and Engineering from JNTUH, Hyderabad. His research areas include Cryptography & Network Security, Computer Networks, Unix Internals, Computer Graphics and Operating Systems.

**Dr. Porika Sammulal,** working as an Assistant Professor in the Department of Computer Science & Engineering(CSE) of JNTUH College of Engineering, Jagityal. His areas of specialization include Cryptography & Network Security, Data Mining and Warehousing, Grid Computing, Cluster Computing, Cloud Computing and UnixInternals.