Analysis of Cryptographic Techniques in Network Security

K.Vanitha, **AP/CSE-Al-Ameen Engineering College, Erode**
K.Anitha, **AP/CSE-CSI College of Engineering, the Nilgiris.**
Dr.A.M.J.Md Zubair Rahaman, **Professor, Al-Ameen Engineering College, Erode**
Dr.M.Mohamed Musthafa, **Professor, Al-Ameen Engineering College, Erode**

Abstract: Cryptography means secret writing. When the data are transferred from sender to receiver over the network through information channel any third parties can intensively read and may modify the data. Here in this paper we elaborate how cryptography will help to secure the data between authorized people. In order to transfer secure data the data will convert to unreadable form before transmitting to the channel. The cryptography applications range have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce. This paper focuses on analysing different types of cryptography, concept of encryption and decryption, a brief introduction to cryptography techniques. If we are taking about security of information then following services come in mind i.e. Confidentiality (privacy of information), Authentication, Integrity (has not been altered) This paper also provides a detailed description of cryptography techniques in Symmetric encryption and a public key cryptography algorithm RSA in Asymmetric encryption.

Key Terms: Cryptography, Security Services, Security Attacks, Symmetric cipher, Asymmetric Cipher, RSA

1. INTRODUCTION

Cryptography means "secret writing" which is the science and art of transforming messages to make them secure and immune to attacks by unauthorized user. The original data/message, before being transformed is called cipher text. An encryption is a process to transform the plain text into cipher text and decryption transforms the cipher text back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure transmission of the message and protect the message from unauthorized users. Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications. Have the top priority such as ecommerce-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information. For example, let us consider a person named Alice a sender who wants to send a data message which has a length of characters to a receiver called Bob. Alice uses an unsecure communication channel. This could be a telephone line, computer network, or any other channel. If the message contains secret data, they could be intercepted and read by hackers. Also they may change or modify the message during its transmission in such a way that Bob would not be able to discover the change. In this survey a various ways of encryption is viewed and have been compared, a lot of examples have been provided.

1.1 CRYPTOGRAPHY SECURITY GOALS

a. ***Confidentiality:*** Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

b. ***Integrity:*** Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

c. ***Availability:*** The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

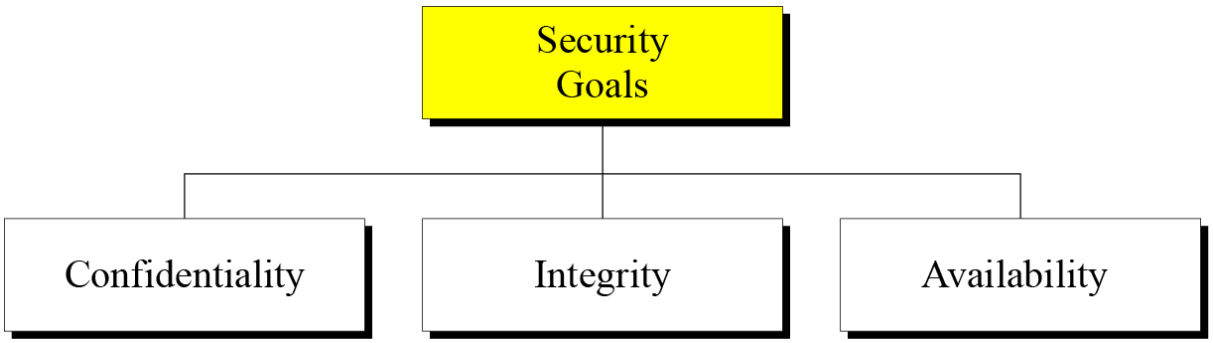

Figure1.1: Security Goals in Cryptography

1.2 SECURITY ATTACKS:

A cyber attack may steal, alter, or destroy a specified target by hacking into a susceptible system. In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an Asset

Types of Attacks

Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in two: "Passive" when a network intruder intercepts data travelling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

1.2.1. Active attack

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. **Spoofing**

When a malicious node miss-present his identity, so that the sender change the topology

b**. Modification**

When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

c. Wormhole

This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network

d. Fabrication

A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices

e. Denial of services

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack.

g. Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

h. Replay attack

It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time, an attacker an intercept the password.

1.2.2 Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring

a. Traffic analysis

In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

b. Eavesdropping

This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

c. Monitoring

In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

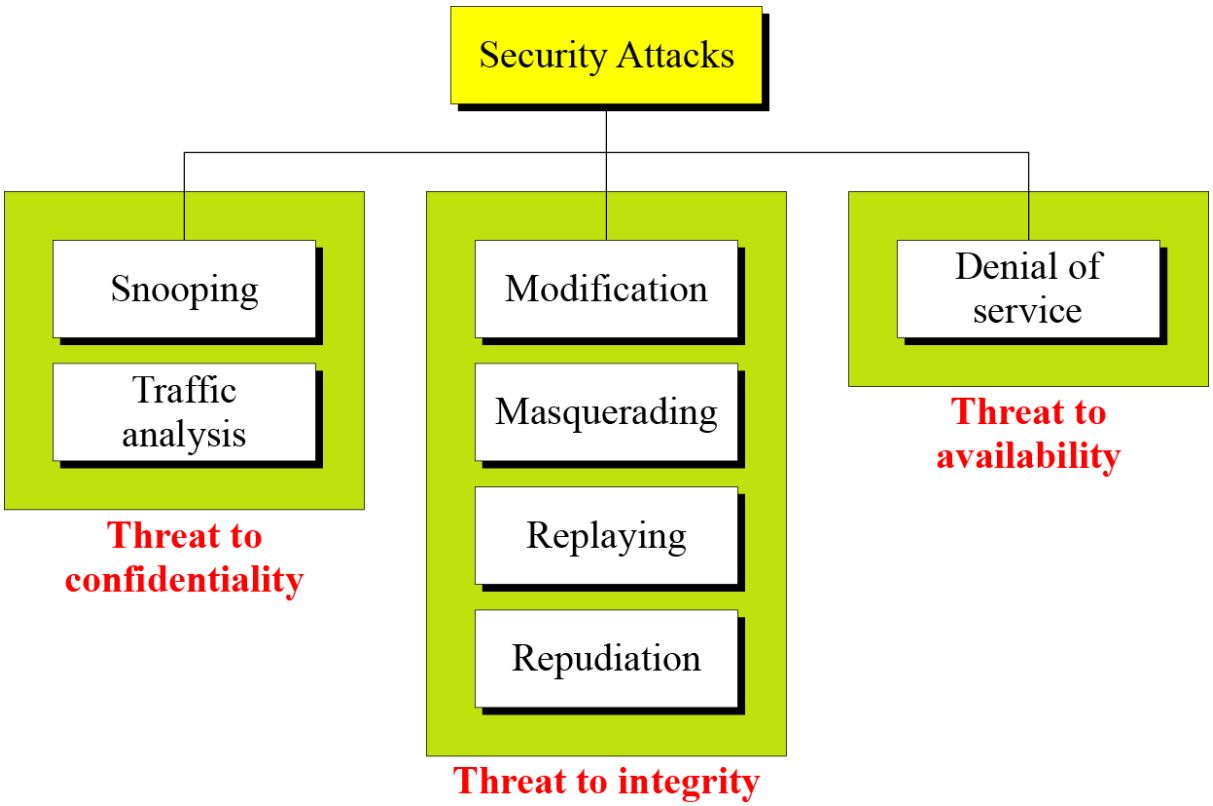

Figure 1.2: Security Attacks in Cryptography

Terminologies Used in Cryptography:

1. Plain text -original message
2. Cipher text- coded message
3. Encrypt -convert plain text into coded text
4. Decrypt - convert coded text into plain text
5. Cryptography-study of encryption principles and methods.

Cryptographic Techniques:

There are two basic techniques for encrypting information:

1. Symmetric encryption (also called secret key encryption)
2. Asymmetric encryption (also called public key encryption).

2. Traditional Symmetric-Key Ciphers

Figure 2.1 shows the general idea behind a symmetric-key cipher. The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the cipher text. To create the cipher text from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from cipher text, Bob uses a decryption algorithm and the same secret key.

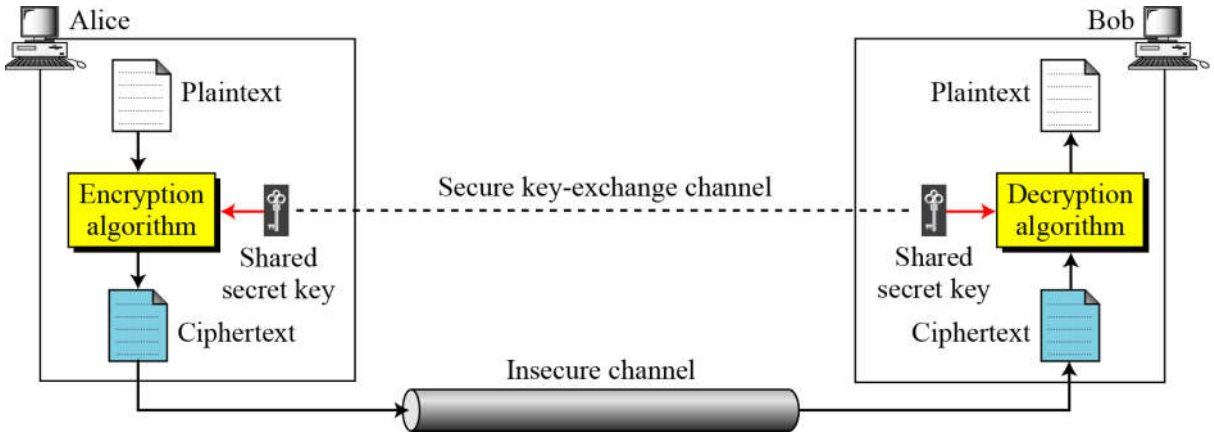

Figure 2.1 Symmetric Cipher Model

If P is the plaintext, C is the ciphertext, and K is the key,

$$\text{Encryption: } C = E_k(P) \qquad \text{Decryption: } P = D_k(C)$$

$$\text{In which, } D_k(E_k(x)) = E_k(D_k(x)) = x$$

2.1 SUBSTITUTION TECHNIQUE:

A substitution cipher replaces one symbol with another.

2.1.1 Monoalphabetic Cipher:

In monoalphabetic substitution, the relationship between symbols in the plaintext to a symbol in the cipher text is always one-to-one.

Exemple : Additive Cipher

The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature.

Exemple :

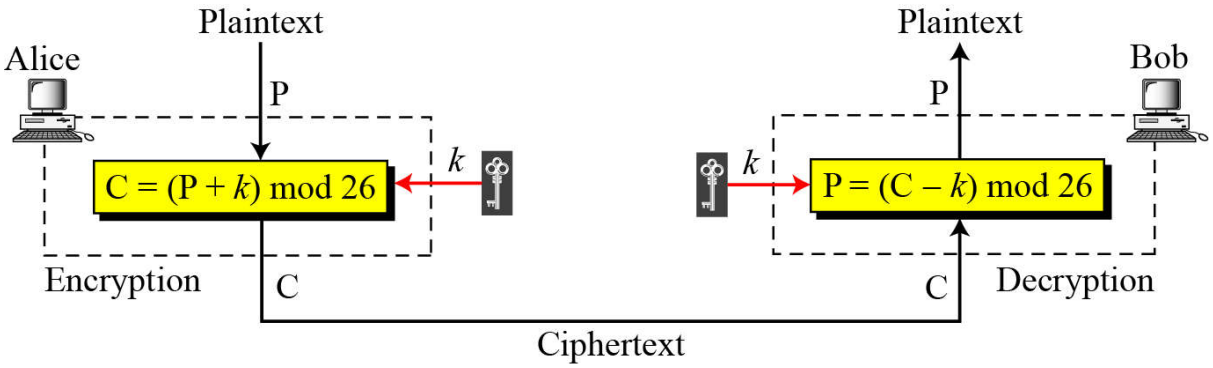

Figure 2.2 Additive Cipher Model

Key=15

Plain Text=HELLO

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Encryption :

Decryption :

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

2.1.2 Polyalphabetic Ciphers

In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between characters in the plaintext to a character in the cipher text is one-to-many.

Example:Vigenere Cipher

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3 \ldots$ $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$

Let us see how we can encrypt the message "She is listening" using the 6-character keyword "PASCAL". The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

2.2 TRANSPOSITION CIPHERS

A transposition cipher does not substitute one symbol for another; instead it changes the location of the symbols.

A good example of a keyless cipher using the first method is the rail fence cipher. The ciphertext is created reading the pattern row by row. For example, to send the message "Meet me at the park" to Bob, Alice writes

She then creates the ciphertext "MEMATEAKETETHPR".

3. Asymmetric key cipher Or Public Key Cipher

Figure 3.1 shows the general idea behind a symmetric-key cipher Asymmetric key cryptography uses two separate keys: one private and one public.

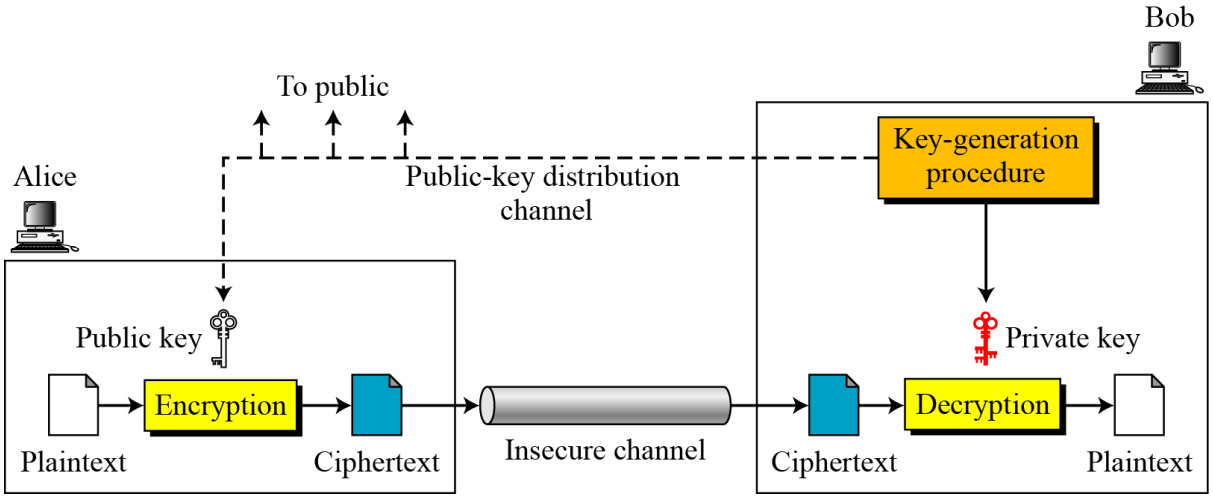

Figure 3.1 Asymmetric Cipher Model

Encryption/Decryption Process:

$C=f(K_{public}, P)$

$P=g(K_{private}, C)$

3.1 RSA Algorithm

RSA stands for Rivest Shamir and Adleman name of three inventors. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

```
RSA_Key_Generation
{
    Select two large primes p and q such that p ≠ q.
    n ← p × q
    φ(n) ← (p − 1) × (q − 1)
    Select e such that 1 < e < φ(n) and e is coprime to φ(n)
    d ← e^−1 mod φ(n)                    // d is inverse of e modulo φ(n)
    Public_key ← (e, n)                  // To be announced publicly
    Private_key ← d                      // To be kept secret
    return Public_key and Private_key
}
```

```
RSA_Encryption (P, e, n)                 // P is the plaintext in Z_n and P < n
{
    C ← Fast_Exponentiation (P, e, n)    // Calculation of (P^e mod n)
    return C
}
```

```
RSA_Decryption (C, d, n)                 //C is the ciphertext in Z_n
{
    P ← Fast_Exponentiation (C, d, n)    // Calculation of (C^d mod n)
    return P
}
```

Example:

Bob chooses 7 and 11 as p and q and calculates $n = 77$. The value of f(n) = (7 − 1)(11 − 1) or 60. Now he chooses two exponents, e and d, from Z_{60}*. If he chooses e to be 13, then d is 37. Note that $e \times d \bmod 60 = 1$ (they are inverses of each Now imagine that Alice wants to send the plaintext 5 to Bob. She uses the public exponent 13 to encrypt 5.

Plaintext: 5	$C = 5^{13} = 26 \bmod 77$	Ciphertext: 26

Bob receives the ciphertext 26 and uses the private key 37 to decipher the ciphertext:

Ciphertext: 26	$P = 26^{37} = 5 \bmod 77$	Plaintext: 5

4. CONCLUSION

Cryptography is a very interesting field in computer science area because the amount of work done is only kept secret. There are various techniques and algorithm studied and different types of research have been done. The best algorithms are those which are well documented and well known because the algorithms are well tested and well studied. This paper further studied that symmetric key cryptography are faster than asymmetric systems.

But asymmetric key cryptography are more scalable and provide more authentication and non- repudiation easily. But there we still need to develop such an algorithm that makes the encryption decryption process easier than RSA, DES and many more algorithms

REFERENCES

[1]. Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, "An Overview Of security Problems in MANET".

[2] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2,P-239-244.

[4]. Anupam Joshi and Wenjia Li. "Security Issues in Mobile Ad Hoc Networks- A Survey".

[5]. Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks".

[6] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[7] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[8] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[7] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[8] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.

[9] Swati Kashyap, Er.Neeraj Madan "A Review on: Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2015.

[10] B.Nithya, Dr.P.Sripriya, "A Review of Cryptographic Algorithms in Network Security" International Journal of Engineering and Technology (IJET) Vol 8 No 1 Feb-Mar 2016.