International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 11, November 2016)

Cryptograpy for Secure Communication: An Overview

M. Amuthavalli[1], V. Vanitha[2], G. V. Vijey Kaarthik[3]
[1,2]*MCA, Er. Perumal Manimekalai College of Engineering*
[3]*Asst. Prof, Er. Perumal Manimekalai College of Engineering*

***Abstract*-- Online communication is one of the common means of globalized communication .people being related to online communication system with various devices such as mobile phones, computer or other e-communication tools increases the need to secure communication network from third parties between the sender & receivers. There are many aspects to secure approach in online communication environment. Cryptography is the art & science of secret writing communication.**

***Keywords*-- Encryption, Decryption, Symmetric key cryptography, Asymmetric key cryptography, AES, DES, RSA algorithm.**

I. Introduction

Online communication (e-communication) refers to reading, writing, and communication via networked computers. It may be synchronous computer-mediated communication (whereby people communicate in real time via chat or discussion software, with all participants at their computers at the same time), or *asynchronous c*omputer mediated communication (where by people communicate in a delayed fashion by computer, using programs such as email) and threading and writing of online documents via the World Wide Web[1].Online communication is one of the common means of communication in this era of globe village. As the number of people being connected to online communication system.Through their mobile phone, computer or any other electronic communication tools increases, there is need to secure the communication networks from adversaries (third parties) between the sender and receivers. One of the best approaches to securing data or information between sender and receivers from third parties is cryptography. Cryptography is the study of information hiding & retrieval. Cryptography is derived from the Greek words: krypton, "hidden" & graph in, "to write"(or) "hidden writing".it is the art of protecting the information by transformation it in to an meaningless format in which a message can be hidden from readers only the intended recipient will be able to convert in to original message.

We need to security & safety of your message using cryptography techniques is becoming very important in today's period as information security is fixed importance.

II. Literater Review

There has been a lot of research in the field of symmetric key, online communications cryptography. Some are related to the development in the field whereas some are a part of increasing its effectiveness on the present scenario: Cryptography System for Online Communication Using Poly Alphabetic Substitution Method [1] Cryptography, Cryptosystem, Decrypt data, e-communication, Encrypted data, online communication, and encoder/decoder algorithm. Network security with cryptography [2] proposed a principle which allows general purpose processors to operate with secret keys in a highly secure way. It is a base on the formation of split processor, cipher and key zones. Symmetric key cryptography [3] proposed the instruction set extensions for improving the software implementations of symmetric key algorithms. The instructions had a significant positive effect on the execution time.

III. Design Methodology

- Public/Private
- Encryption/Decryption
- Keys
- Encoder
- Decoder

3.1 Public/Private

This is a pair of keys that have been selected so that if one is used for encryption ,the other is used for decryption .the exact transaction performed by the encryption algorithm depend on the public key (or) private key is provided as input.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 11, November 2016)

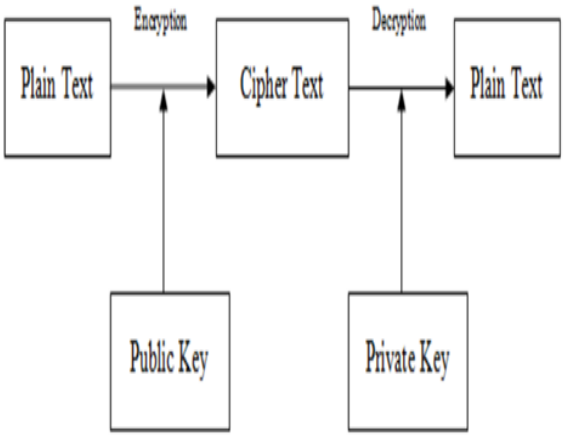

Figure 1 Public/Private [7]

3.2 Encryption/Decryption

The encryption algorithm performs various transformations on the plaintext. This decryption algorithm accepts the cipher text &the matching key and produces the original plaintext.

Example[1]

A B C D E F G H I J K L M N O P Q R S T U V W X Z
A A B C D E F G H I J K L M N O P Q R S T U V W X Z
B B C D E F G H I J K L M N O P Q R S T U V W X Y A
C C D E F G H I J K L M N O P Q R S T U V W X Y Z A
D D E F G H I J K L M N O P Q R S T U V W Y Z A B C
E E F G H I J K L M N O P Q R S T U V W Y Z A B C D
F F G H I J K L M N O P Q R S T U V W Y Z A B C D E
G G H I J K L M N O P Q R S T U V W X Y Z A B C D E
H H I J K L M N O P Q R S T U V W X Y Z A B C D E F
I I J K L M N O P Q R S T U V W X Y Z A B C D E F G
J J K L M N O P Q R S T U V W X Y Z A B C D E F G
K K L M N O P Q R S T U V W X Y Z A B C D E F G H
L L M N O P Q R S T U V W X Y Z A B C D E F G H I J
M M N O P Q R S T U V W X Y Z A B C D E F G H I J
N N O P Q R S T U V W X Y Z A B C D E F G H I J K L
O O P Q R S T U V W X Y Z A B C D E F G H I J K L M
P PQ R S T U V W X Y Z A B C D E F G H I J K L M N
Q Q R S T U V W X Y Z A B C D E F G H I J K L M N
R R S T U V W X Y Z A B C D E F G H I J K L M N O P
S S T U V W X Y Z A B C D E F G H I J K L M N O P Q
T T U V W X Y Z A B C D E F G H I J K L M N O P Q
U U V W X Y Z A B C D E F G H I J K L M N O P Q R
V V W X Y Z A B C D E F G H I J K L M N O P Q R S
W W X Y Z A B C D E F G H I J K L M N O P Q R S T
X X Y Z A B C D E F G H I J K L M N O P Q R S T U
Y Y Z A B C D E F G H I J K L M N O P Q R S T U V
Z Z A B C D E F G H I J K L M N O P Q R S T U V W

3.3 Key

A Key is a string of alpha numeric characters, which is used to encrypt & decrypt the message[2]. The Key is used at the time of encryption that works on the Plain Text and at the time of decryption works on the Cipher Text[3].

3.4 Encoder

An encoder is the person that wants to send the message & uses encryption to make the message secure.

3.5 Decoder

A decoder is the person who decrypts the message. This may be the intended recipient of the message or may be an intruder, trying to get access to the secret message[6].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 11, November 2016)

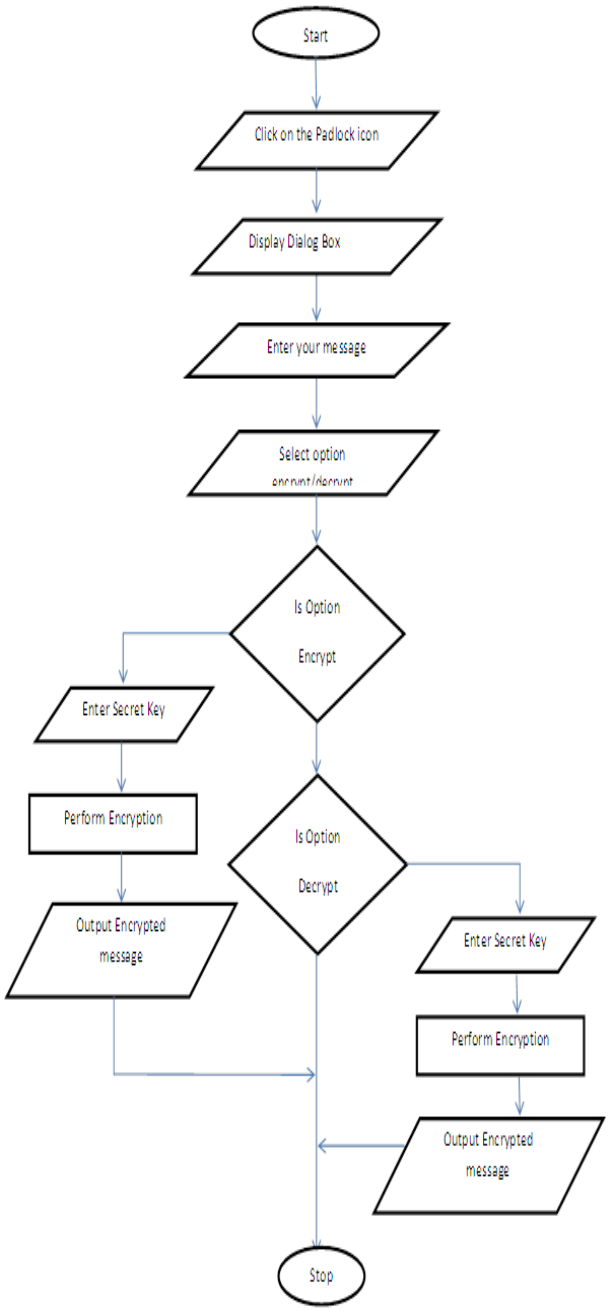

Figure2 Flowcharts For The Cryptography [1]

3.5.1 *Asymmetric cryptosystem*

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was suggested by "Daffier and Hellman in 1976".

A type of cipher was proposed which uses two different keys :(1) one key used for enciphering can be made public(2) other used for deciphering, is kept secret.

3.5.2 Symmetric cryptosystem

In symmetric cryptosystems (also called conventional, secret-key or one-key cryptosystems), the enciphering and deciphering keys are either identical or simply related, Both keys must be kept secret, and if either is compromised further secure communication is impossible. Keys need to be exchanged between users, often over a slow secure communication[5].

IV. Model Of New System Keys

- There are two types of algorithm using
- AES algorithm
- DES algorithm

4.1 Advanced Encryption Standard (AES) Algorithm

AES is a symmetric key algorithm which operates on two dimensional arrays of bytes known as state and the state consists of four rows of each bytes. AES has key size of 128,192 OR 256 Bits which protect against certain current and future attacks. Hardware and software both implementation are faster and can be implemented on various platforms. which protect against certain current and future attacks[3].

4.2 Data Encryption Standard (DES) Algorithm

DES is a symmetric block cipher having 64-bits long input key but uses only 56-bits in length. The decryption is performed by same password as encryption only the stages are carried out in reversed manner.DES has 16 rounds so to produce cipher text the main algorithm is repeated 16 times. Des is more vulnerable to brute force attack because as the number of round increases the algorithm of security exponentially increases[4].

V. Conclusion

The need for security of information/data from sender to receivers in an online communication cannot be over emphasized. Although the ultimate goal of cryptography, and the mechanisms that makes it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources[6]. So a more realistic goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker.

This research work developed stand-alone software that implements Crypto grapy for secure communication using various keys like Encryption Decryption keys, AES, DES, RSA algorithm[1].

REFERENCES

[1] Yemini. Safe Aigbokhan, E. Edwin Okapi F. Mercy, "Cryptography System For Online Communication Using Poly", International Journal Advanced Networking And Applications,vol 06,issue 1(2014),pp.2151-2157

[2] Prof.Mukund R.Joshi, Renukaavnash Kakas, "Network Security With Cryptography", International Journal Of Computer Science And Mobile Computing, vol 04,issue 1(2015), pp.201-204

[3] Pretty Singh1, Praveen Shende2,"Symmertickey Cryptography: Current Trends ",International Journal of Computer Science And Mobile Computing, vol 03,issue 12 (2014), pp.410-415

[4] Harsh Ad, J.Tawari Agoutis Swan Hade, "Network Security: Attack And Component", International Journal Of Research In Science And Engineering vol 01,issue 1(2014),pp.401-405

[5] Nehagarg, Paraiba Yadhv, Pratibha Yadav,Inscience "Comparison Of Asymmetric Algorithm In Cryptography", International Journal Of Computer Science And Mobile Computing, Vol.03,issue 4(2014),pp.1190-1196

[6] Prof.V.P.Narkheede,Ms.P.S.Ajabe2,Mr.S.M.Dandage, Ms.P.B.Zoë,"A Review Of Public Key Cryptography For Secure Communication Using RSA", International Journal Of Advent Research In Computer And Electronics.vol 02,issue3(2015)pp.1-4