IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 60-63

Discussing Security Aspect In Cryptography

[1.]S.Uma Mageshwari, [2.]Dr. R.Santhi
Research Scholar, R& D Centre, Bharathiar University , Coimbatore.
Research Supervisor, Bharathiar University, Coimbatore.

Abstract: *Cryptography is a science of writing secret messages. The various cryptographic algorithms do this process with different methodology. Each algorithm differs on the basis of key size and the number of steps invloved to produce ciphertext.. The key plays a vital role for Encryption (plaintext to Ciphertext) and Decryption(Ciphertext to Plaintext) process. This paper emphasizes terminology used in Cryptography, various algorithms, key illustration of each algorithm and shown implementation of Encryption/Decryption process with sample data by using different approaches.*

Keywords: *Encryption, Decryption, Algorithms, Key.*

I. Introduction

A.Attacks

The network security attacks are of two types namely:

- Active attacks : Modifying the information.
- Passive attacks : Obtaining the information but not to modify the contents.

B.Services

- The different security services are listed below:
- Confidentiality : Protecting the information from an intruder.
- Data Integrity : Receiving data must be same as the data sent.
- Data Availability : Providing data available to the authorized users.
- Non – Repudiation : The message cannot be denied by the communicaties parties.
- Authentication : Ensuring the sender and receiver.

C. Techniques

In Cryptography there are two techniques available. They are:

- Symmetric Cryptography : Encryption and Decrytion process uses same key.
- Asymmetric Cryptography : Different keys used for Encryption and Decryption process.

D. Cryptography Algorithms

AES(Advanced Encryption Standard) : It is a Symmetric Block cipher algorithm.
DES(Data Encryption Standard) : Identifies 64 –bit blocks and Symmetric algorithm
BLOWFISH : This is Symmetric Crptography with with Block size about 64 bits.
HMAC(Hash Message Authentication Code): It sends message with MAC (hash fucntion and Key) code.
DIGITAL SIGNATURE : Adopts asymmetric cryptography and tie person identity with the message.

DIFFIE HELLMAN KEY EXCHANGE : Exchanges key between Sender & Receiver.
RSA(Rivest-Shamir-Adleman) : Implements aymmetric key cryptography.
SHA(Secure Hash Algorithm) : It is One way and keyless Hash function.

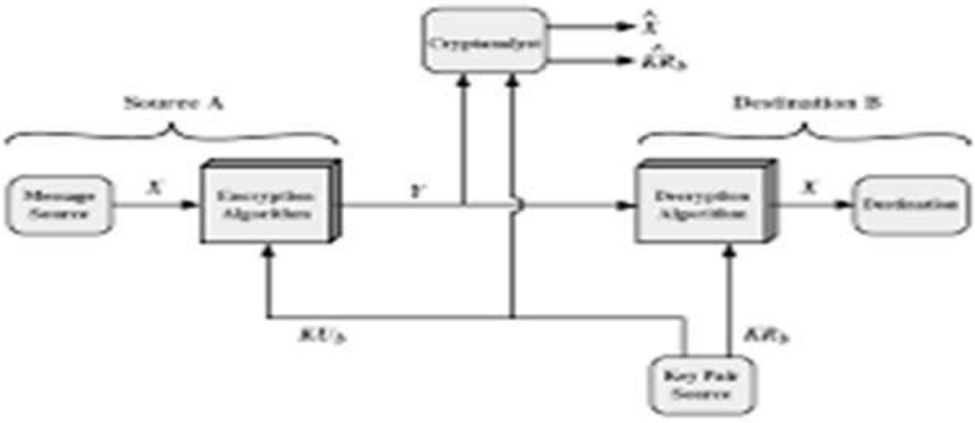

Figure 9.2 Public-Key Cryptosystem: Secrecy

II. Key Length

The few Cryptographic algorithms are listed below with key length illustration:

- AES(Advanced Encryption Standard) : The key sizes can be 128, 192 and 256 bits.
- DES(Data Encryption Standard) : It uses 56 bits for key represenatation.
- ECC(Elliptic Curve Cryptography) : Key size is determined based on elliptic curve over finite fields.
- Diffie – Hellman Key Exchange : The key can be from 1024 bits to 2048 bits.
- MD5(Message Digest): It supports key of 128 bits.
- SHA(Secure Hash Algorithm): Size of the key is upto 512 bits.
- HMAC(Hash Message authentication code): Key is upto 512 bits.
- Two Fish : The length of the key size is upto 256 bits.
- Blow Fish : Key length from 32 bits to 448 bits.
- RSA (Rivest-Shamir-Adleman) : Upto 2048 bit keys.

III. Security & Confidentiality

The information transmitted over the network can be secured with the following steps:

- Plaintext is given as an Input.
- Using any Cryptographic algorithm , Plaintext is converted into Ciphertext using key.
- The Ciphertext is decrypted using same or different key.
- Output will be the same as Plaintext.
- The encrytion/decryption process uses same key, then it is called Symmetric algorithm.

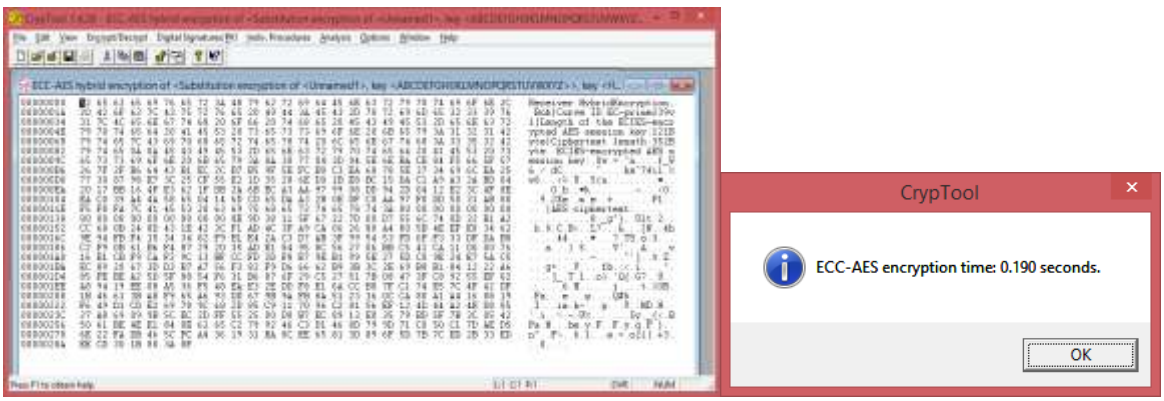

Figure 1: Sample output after Encryption process

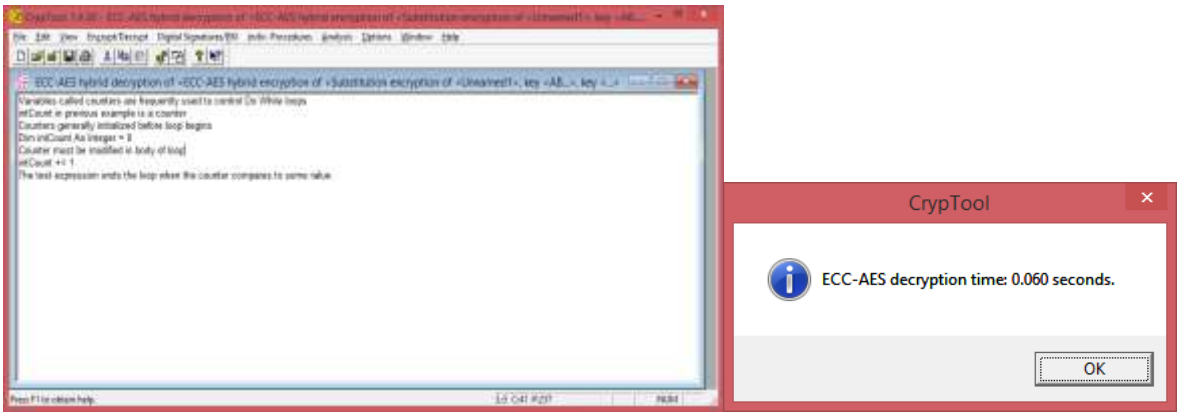

Figure 2: Sample text after Decryption process

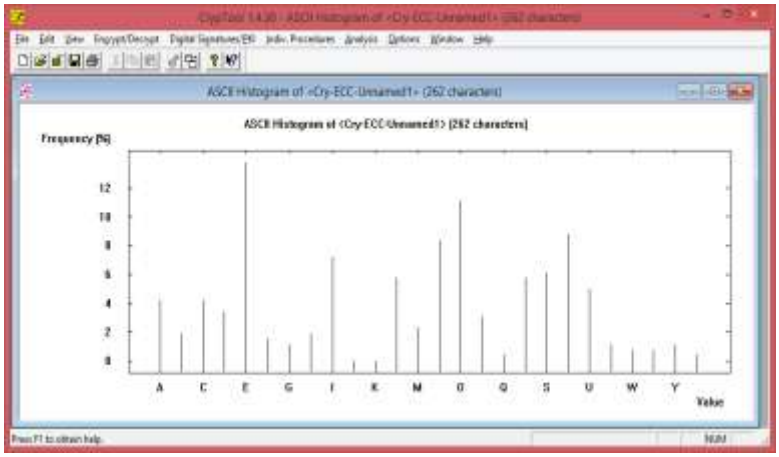

Figure 3: Histogram Analysis for the Sample text

3.1 Diffie –Hellman Algorithm

i).This algorithm receives two inputs prime modulo and generator.

ii). Sender (Alice) and receiver (Bob) fix up the secret number.

iii).Generate secret key by means of two inputs and secret number.

iv). Exchange the generated key between the persons.

v). Calculate the key with exchanged values between Alice and Bob.

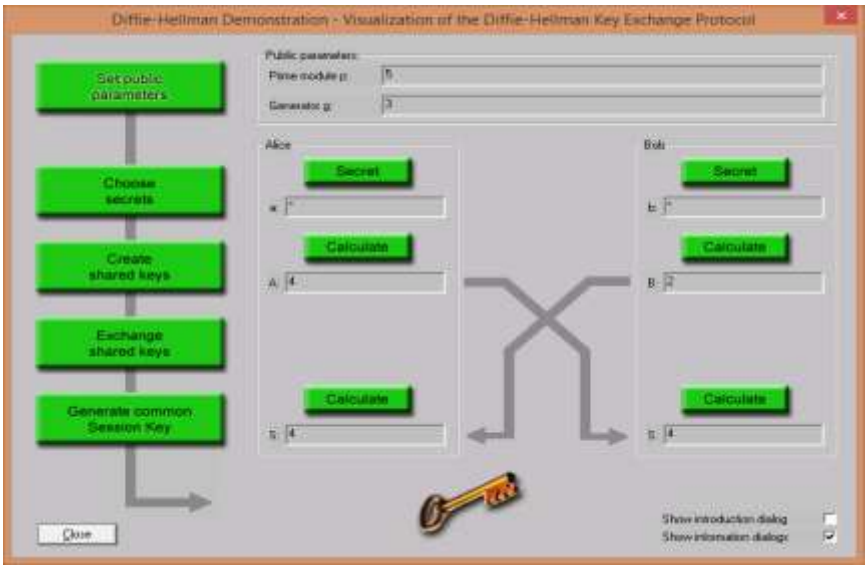

Figure 4: Diffie – Hellman Key Exchange with A & B

3.2 AES(Advanced Encryption Algorithm)

This is Symmetric Cryptographic algorithm in which pliantext is given as a parameter to AES encrypt algorithm to convert plaintext into ciphertext. With the same key it is decrypted by using AES decrypt algorithm.

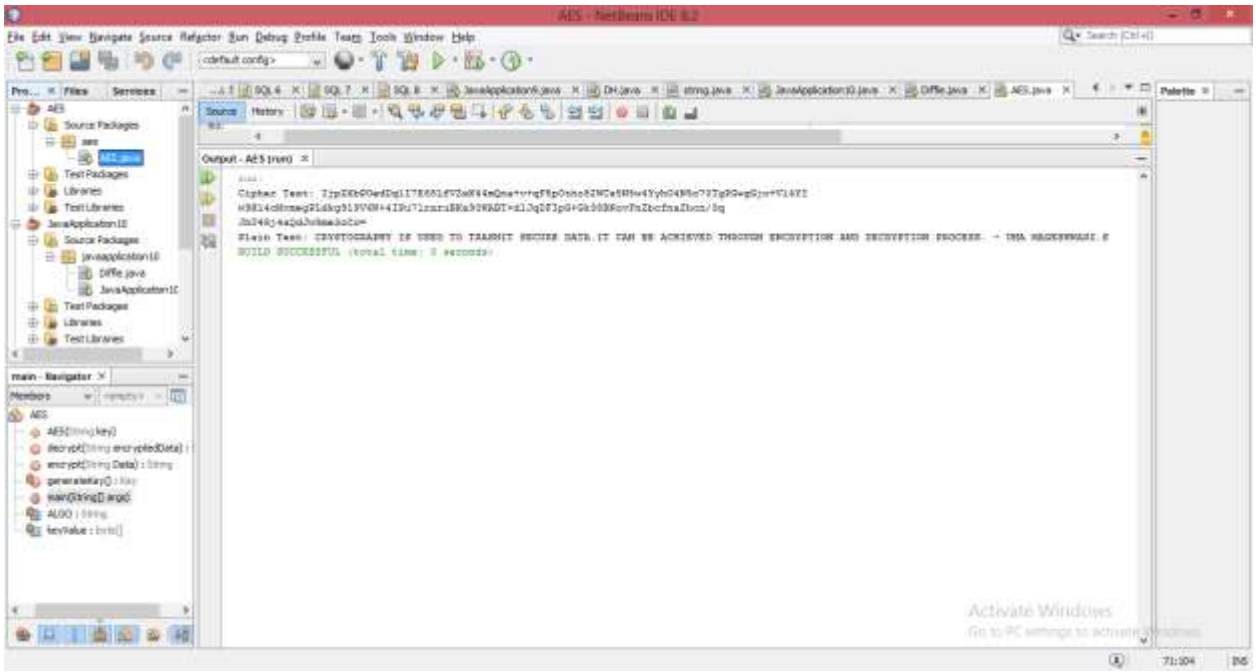

Figure 5: Encryption and Decryption Process with AES Algorithm

IV. Conclusion

Data transmission over the insecure network causes malicious attacks from an intruder. This can be resolved by using any cryptographic algorithms to tranmit the data securely. Before sending the message over the communication channel the data must be protected with Encryption and Decryption process by using the key. The key size may vary depends on the chosen algorithm. Hence the attcker not able to identify the original message send by the sender. The Receiver decrypts the same to get the original text. Thus the information can be protected with various cryptographic algorithms.

References

[1]. Cryptography and Network Security – William Stallings, Fourth Edition, PHI,2006.

[2]. D.Lohit Kumar,Dr.A.R.Reddy, Dr.S.A.K.Jilani,'Implementation of 128 – bit AES algorithm MATLAB', International Journal of Engineering Trends and Technology(IJETT), Vol.33, Issue No.3,March 2016,ISSN: 2331-5381.

[3]. HimjaAgrawal, Prof.P.R.Badadpure,'A Survey Paper on Elliptic Curve Cryptography', International Research Journal of Engineering and Technology(IRJET),Vol.3, Issue No.4,April 2016. e-ISSN: 2395- 0056.

[4]. https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties.

[5]. D.Stinson, Cryptography : theory and practice, CRC Press Inc.,Boca raton,(1995).

[6]. Atul kahate " Cryprography and Network Security", Tata McGraw –Hill Companies, 2008.

[7]. 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.

[8]. Lavisha Sharma , Anuj Gupta, 'International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)', Vol. 2, Issue No. 5, 2016, ISSN: 2454-132X.

[9]. SoramRanbir Singh, ajoy kumar khan, TakhellambamSonamanisingh, 'A Critical Review on Elliptic Curve Cryptography',2016 International Conference on Automatic Control and Dynamic Optimization Trechniques (ICACDOT), IEEE 978-1-5090-2080-5, 2016.

[10]. P.Muthu Kannan, Anupriya Asthana International Journal of Latest Research in Science and Technology ISSN (Online): 2278-5299.