Security System on Data Encryption & Decryption

Mr. Mukul Aggarwal[1], Mr. Deepak Kumar Yadav[2], Dr. Himanshu Arora[3] and Mr. Sudhanshu Vashistha[4]

[1]B. Tech Student, Department of CSE, Arya College of Engineering and Research Center, Jaipur
[2]B. Tech Student, Department of CSE, Arya College of Engineering and Research Center, Jaipur
[3]Professor, Department of CSE, Arya College of Engineering and Research Center, Jaipur
[4]Assistant Professor, Department of CSE, Arya College of Engineering and Research Center,Jaipur

***

Abstract— Now's a day's security is a feature or factor which is most important about any sector which ensures the protection of data. It prevents unauthorized persons, thieves, hackers, etc. In this field, there are three main feature which is essential for data security i.e. confidentiality, integrity, availability, these three main features which prevent from unauthorized any other third person. Confidentiality basically if we send the data from one person to another person then only authorized person can access & integrity if we transfer the information from one to another then no one can change. The availability of the resources should be available 24/7 hour or data should be available on demand. Process of communication using Encryption and Decryption over data. To convert the plain text into ciphertext is Encryption and convert the ciphertext into plain text is Decryption and both methods called as a Cryptology. These processes depend on two types of keys which is public key & private key.

***Keywords*—Encryption, Decryption, Private key & Public key**.

I. INTRODUCTION

In today's generation, data security Most crucial factor which can achieve by information security system. It protects from unauthorized third person. In this information system, there are main two process help to communicate from one person to another person whit security. In earlier before we don't have any security system to protect the data from unauthorized persons or hackers etc. At that time are many possible chances to hack the information. Before this, a user has to put extra effort to transform to information with security because there are many chances to hack or leak that information. In today's generation, we have many algorithms or techniques to prevent the data from unauthorized persons or hackers. In the encryption and decryption process, we can use famous techniques like AES, DES, RSA, etc.

Characteristics of Information Security System

- **Confidentiality:** It has a process two transfer the data from one place to another then only authorized person can access and to prevent the unauthorized person. For example,[1] A credit card or Debit card can only access by authorized persons.
- **Integrity:** When we send data from one place to another then no one can modify then data should be modified.
- **Authentication:** Verification of user identity that means who are sending or who are receiving the data that means after verification both parties are authorized, they can easily sends their data between them.
- **Non-Repudiation:** It is the process to prevent the denial services attack. It is the attack in which third- person directly access the server.
- **Access Control:** It is the process in which only authorized person can only access the data resources

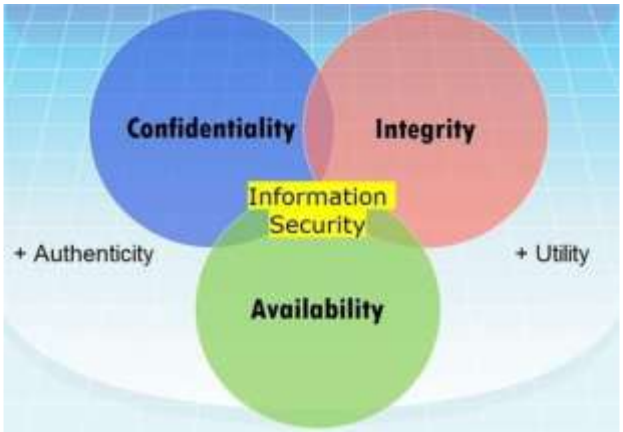

Fig. 1 Characteristics of Information Security System

Security Attacks:

Gaining access to data by unauthorized persons without any authorized any control. Then unauthorized persons can Modify the Data [2], Access the Data and Destroying the Data.

There are two types of attack:

- Passive Attack
- Active Attack

Passive Attack: It is the attacks that only have access to the data but without modifying.

There are two types of techniques in this attack:

- Releasing the Attack: Attackers can only access the data without any modification.
- Traffic Analysis: Attacker observes the data after that getting access to data and increases the traffic flow of the data which cause more traffic and delay produces

Active Attacks: It is the attacks that can have access to the data with modification.

There are three types of techniques in this attack:

- Masquerade attack: In this attack, third-person modifies the data at the time of transmission by accessing the control and sends the modified data which confuses to the receiver end.
- Replay Attack: In this attack third person get access to the data and modifies it and then sends the modified data to the receiver and the receiver gets the wrong data again and again.
- Denial of Services: In this attack third person directly attacks on the server and get access to the data and modifies, when the sender accesses the server then the sender gets modified data at the beginning.

II. ENCRYPTION & DECRYPTION METHOD

The system which is discussed in this paper is the Information Security System for maintain the security at the time of data transmission [3]. To transmit the data of text which is of two types:

1. Plain Text: The text is in a readable format by users.
2. Cipher Text: The text is not in a readable format by users. Users have to convert Plain Text to Ciphertext if the user wants to secure the information.

The way of transforming plain text into cipher text is known as Encryption and the way of transforming cipher text into plain text is known as Decryption process.

The study of encryption is called Cryptography, the study of decryption is called Cryptoanalysis and both the study of both encryption and decryption is called Cryptology.

Keys: It is a group of bits that plays a major role in the encryption and decryption process.

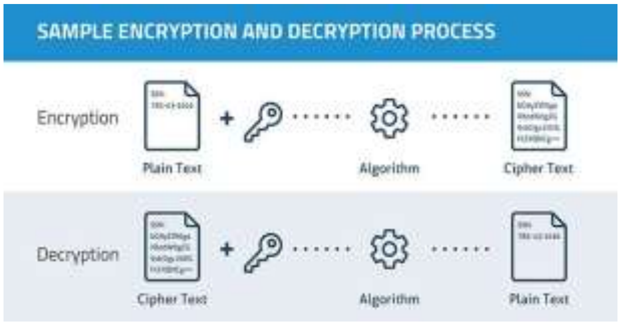

Fig 2: Encryption and Decryption

Process Encryption can be done in Two way:

1. Stream Cipher: In this, the encryption process is converting bit by bit.
2. Block Cipher: In this encryption process is converted into a group of bits.

There are two types of Encryption Process:

1. Symmetric Encryption Process: The conversion of plain text into ciphertext with the help of Public Key. In this process at the sender & receiver side, users use Public key.
2. Asymmetric Encryption Process: The conversion of plain text into ciphertext at the sender side uses Public Key and at after passing the information at the receiver side uses the decryption process by using its own Private Key.

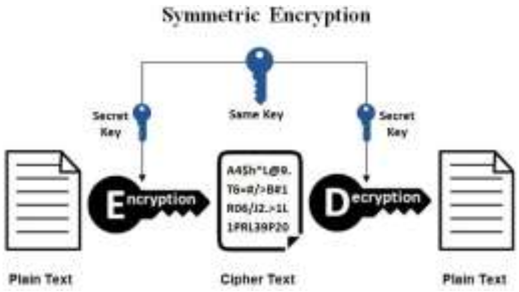

Fig 3: Symmetric Encryption

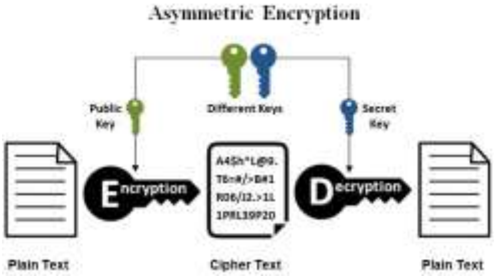

Fig 4: Asymmetric

Encryption Techniques:

1. Substitution Technique: In this technique, it replaces the plain text character with alpha text character.

   There are two types of substitution techniques:

   - Caesar Cipher: In this technique with the help of a given key to find out the Mod from all twenty-six alphabet to predict the ciphertext.
   - Play Fair: To find out the ciphertext we will divide the plain text into a pair of letters, differentiate repeat letters in the pair with dummy letters [4]. In pair of lain text letters should be in the same row replace then with rightmost letter.

2. Transportation Technique: Changing the bit position of the plain text to get the security.

   There are two types of transportation techniques:

   - Rail Fence Cipher: To generate the ciphertext by jumbling the plain text for providing good security but it can be easily accessed by the third person.
   - Row Transportation Cipher: To generate the ciphertext by this technique first we have to consider a unique key number from range 0 to 9 then we will arrange the plain text according to the unique key number then arrange the ciphertext according to the ascending key value.

III. Algorithms of Information Security

The famous algorithm for encryption and decryption process to transmit the information of data by using

A. DES (Data Encryption Standard):

It is the block cipher algorithm that follows the Feistel structure. It works on 64-bit block size which has 16 numbers of round and with key size 64-bit, so it will produce 64-bit ciphertext with 16 number of subkeys and with the size of 48-bit.

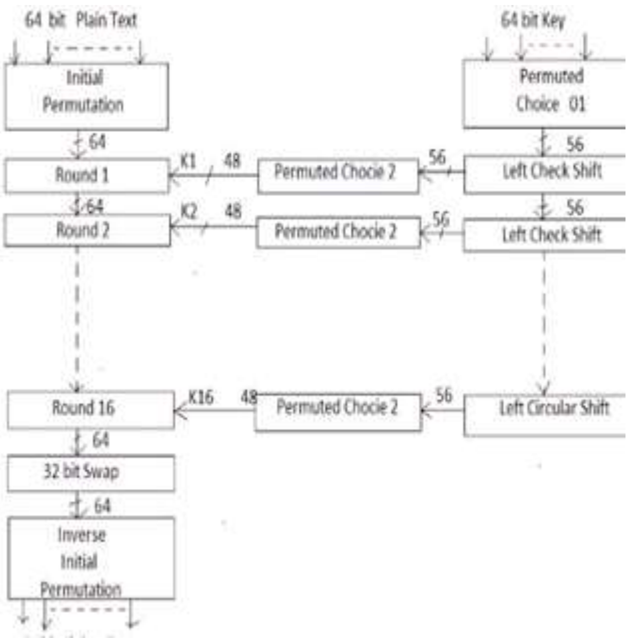

Fig. 5 Working of DES Algorithm

B. AES (Advanced Encryption Standard):

It is the block cipher algorithm. It works on 128-bit block size which has 10, 12, 14 number of round and with key size varies between 128, 192, 256bits so it will produce 128-bit ciphertext with size of 128-bit.

C. RSA (Rivest-Shamir-Adleman):

It belongs to the asymmetric key algorithm which uses the public key cryptosystem.[5] To generate the ciphertext, we have to follow some steps:

For the encryption process to find out the ciphertext C= P^e Mod N

For the decryption process to find out the plain text P= C^d Mod N

Where,

e and d are Public key and we will calculate the e, d, and N.
Suppose take two prime number P and Q
Step 1. We will calculate the N by-product of P and Q N= P x Q
Step 2. We will find out the Φ,
Φ= (P-1) (Q-1)
Step 3. Find out thee it belongs between 1<e<Φ or should be coprime or should not belongs in the factor of P and Q or not divisible by N.
Step 4. To find out the d by the equation of d * e Mod Φ = 1 we will use Extended Euclidean Algorithm Equation
ax + by = gcd (a, b) where,
a= Φ, b= e
Step 5. After finding then d we will check the condition to Predict the d

- If d >Φ then d = d Mod Φ
- If d is -ve then d= d + Φ

Step 6. After finding d and e put the value in eq of encryption and decryption and here is the result.

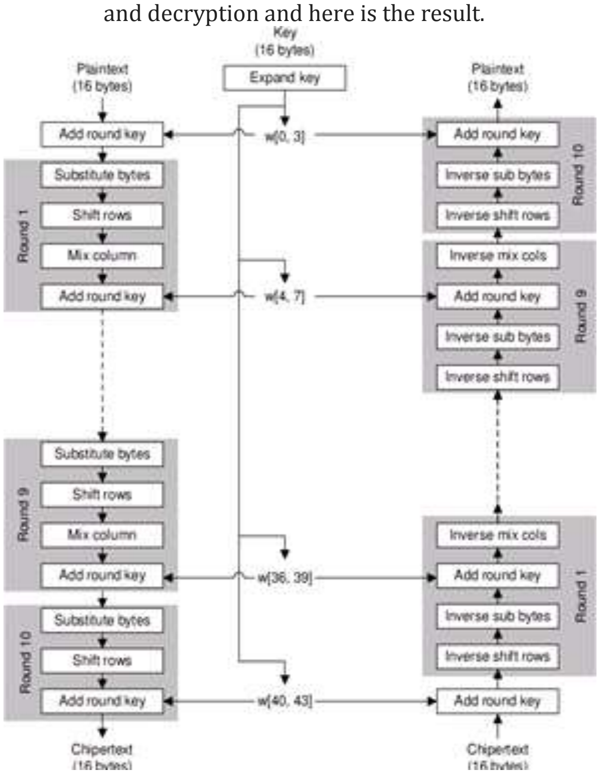

Fig.6 Working of AES Algorithm

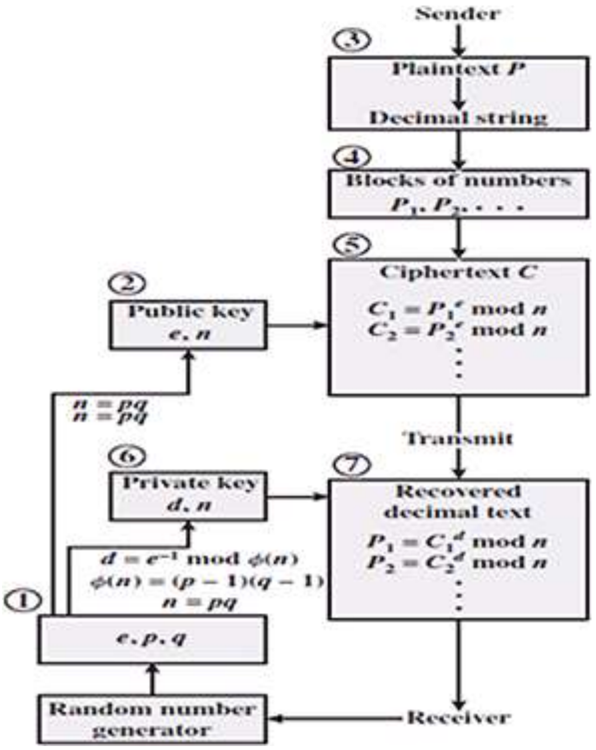

Fig.7 Working of RSA Algorithm

IV. CONCLUSIONS

Information Security System is most important for data protection which prevents all the illegal uses or any data losses. It provides the best solution to protect the information data by using some special technique or mechanism so users don't worry about any information leakage or losses. If they use a security system there will be no chance of data losses.

V. REFERENCES

[1] K. Kiili, "Digital game-based learning: Towards an experiential gaming model," The Internet and Higher Education, vol. 8, no. 1, pp. 13-24, 2005.

[2] M. Olivier, "A LAYERED SECURITY ARCHITECTURE: DESIGN ISSUES," South African Computer Journal, vol. 2003, no. 31, pp. 53-61, 2003.

[3] J. Chapin, "Key Considerations in Choosing a Zero Client Environment for View Virtual Desktops in VMware Horizon," 2014. [Online]. Available:

[4] J. H. Lala, "IT Monoculture Security Risks and Defenses," IEEE Security and Privacy, vol. 7, no. 1, pp. 12-13, 2009.

[5] P. Zenezia, "InfoWorld," 22 12 2014. [Online]. Available

[6] Sattarova Feruza Y. and Prof.Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 2, April, 2007

[7] Manas Paul and Jyotsna Kumar Mandal, "A Universal Session Based Bit Level Symmetric Key Cryptographic Technique to Enhance the Information Security", (IJNSA), Vol.4, No.4, July 2012

[8] Information Security: Principles and Practice, Mark Stamp Second Editionvol. 9, no. 2, pp. 14-21, 2005.