A perception of exchange and Transposition Encryption Methods

[1]Amit Joshi, [2]Dr S K Sharma
[1]Research Scholar, Pacific University, Udaipur
[2]Research Supervisor, Pacific University, Udaipur
Email - amitjoshiudr@gmail.com

Abstract: *In the rapid growing word data is one of the prime concern which plays an important in the development. There are lots of issues which are associated with the security of data during the transportation. These are unauthorized and malicious access of data during the data transportation. In the present time data encryption is one of the most important tools or techniques to secure the data from the unauthorized and malicious access of data during the data transportation. It is very much crucial during the data transportation and storage. In the era of cloud computing data security is one of the major term concerns from the data storage and services providing through the data transportation as services. The present paper tries to provide a outlook about the encryptions methods which may utilize for securing data in cloud data transportation and storage.*

Key Words: *Data, Encryption, Security, Access, Cloud, Transportation.*

1. INTRODUCTION:

Nowadays the rapid development in the technology is surrounding the information technology enabled services. The information technology is based on the data, and there are lots of issues which are associated with the security of data during the transportation. As we know that cloud is one of the latest technologies which provide all the facilities via internet. So all the things are based on the data. In the epoch of cloud computing is security of data on internet is one of the major concerns about the data storage and services providing through the data transportation as services. The encryption is most influence loom to achieve data security and privacy. Basically an encryption method is used to conceal the unique content in such a way that the original data is recovered only through decryption process. The encryption be able to be put into operation by using a number of alternate methods, shifting technique, or mathematical operations. By means of apply these methods one can produce a diverse form of data which may be hard to recognize during the transportation. The primary or initial data is known as the plaintext and the encrypted data is called as cipher text. The symmetric key base algorithms are sometimes used for performing encryption activities.

2. CRYPTOGRAPHY:

The encryption and decryption process is accountable under the cryptography, it is the knack of attain security through encoding data to compose them in non-readable form. This is a method that permits one to encode / encrypt the data which can again decrypt exclusive to support of sender. The process of cryptography is not only protects the data but also give s authentication. The communication and network technology is one of the essential part of the cloud technology. As the communication network technology has been is on peak, there is a need to send much data by means of the Internet. Information can be perused and comprehended with no exceptional measures are called plaintext. Cryptography assumes an imperative job uncertain correspondence over the system and it gives a best answer for offer the fundamental assurance against the information interlopers. Cryptography is the study of anchoring information.

Cryptography is method for embedding arithmetic to encode and unscramble information. Cryptography gives you to store touchy data or transmit it over the unreliable systems so that can't be perused by anybody with the exception of the expect beneficiary. Traditional cryptanalysis includes a fascinating blend of expository thinking, utilization of scientific instruments, design discovering, persistence, assurance, and good fortune. Cryptanalysts are additionally called assailants. Cryptology grasps both cryptography and cryptanalysis [3, 4]. Amid correspondence, the sender plays out the encryption with the assistance of a common mystery key and the beneficiary plays out the unscrambling. Cryptographic calculations are comprehensively delegated Symmetric key cryptography and Asymmetric key cryptography. This area explains about administrations and systems of cryptography, processing approaches of plaintext, key distribution and cryptanalysis.

3. CRYPTOGRAPHY SERVICES :

Cryptography gives various security administrations to guarantee the protection of information. That why because of security advantage of cryptography, is broadly utilized now a days. There are following administration of Cryptography talked about beneath:

- Authentication: The data gotten by any framework needs to check the character of the sender that whether the data is touching base from an approved individual.

- Access control: The Prevention of unapproved utilization of an asset i.e. this administration controls who can approach an asset, under what condition access can happen, and what those getting to the asset are permitted to do.

- Confidentiality: Transmitted Information must be gotten to just by the approved party.

- Integrity: Just the approved party is permitted to alter the transmitted data.

- Non-Repudiation: Gives insurance against dissent by one of the elements engaged with a correspondence of having taken an interest in all or part of correspondence.

4. SYMMETRIC ENCRYPTION AND DECRYPTION:

This is one of the fundamental key techniques for encryption, in this technique one of the identical key is utilized for mutually encoding and decoding of messages. The advantages of the symmetric algorithms are that they don't have excessively computing power. Also it is notices that it workings by means of far above the ground speed in encoding. The symmetric key encoding or encryption works in two form either as the block ciphers or as the stream ciphers.

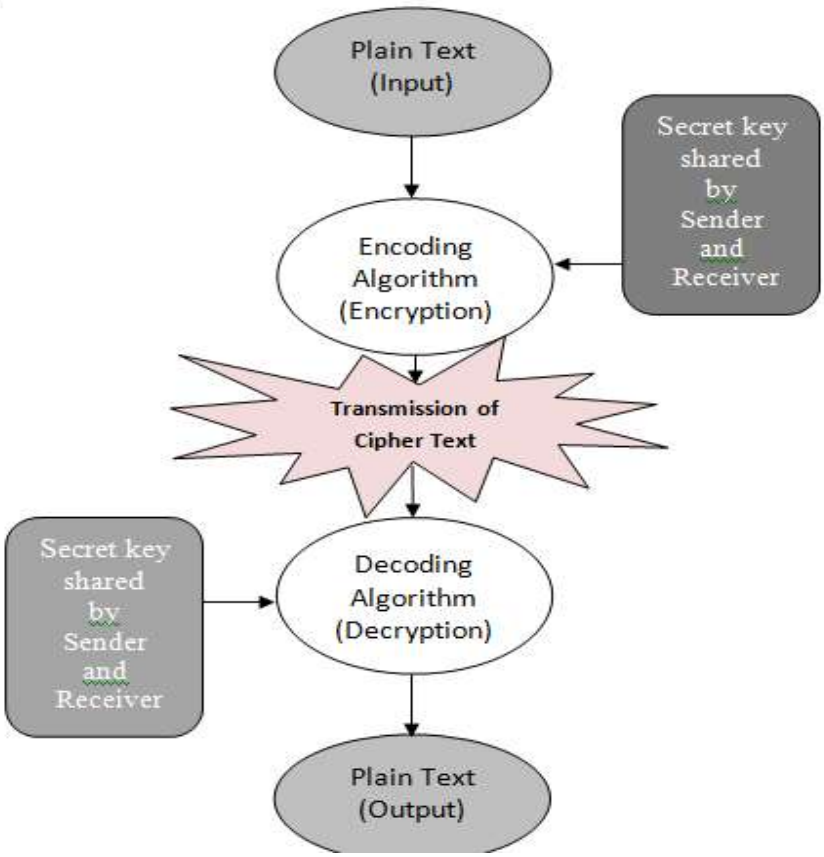

Figure-1: A Fundamental process of Cryptography

In general mode the block cipher form gives; entire data is separated into quantity of blocks. It is found on the size of the block the key is given for encryption. In the context of the stream ciphers method data is separated in the little bits sets and randomized form of the dataset will works for encryption. The symmetric key is one of the faster form for cryptography and also secure and easy for the system operating. There are 2 prerequisites for secure utilization of regular encryption:

We require a solid encryption algorithm – the rival ought to be notable decode cipher text or to find the key regardless of whether s/he is in the ownership of various cipher texts together with the plaintext that created each cipher text.

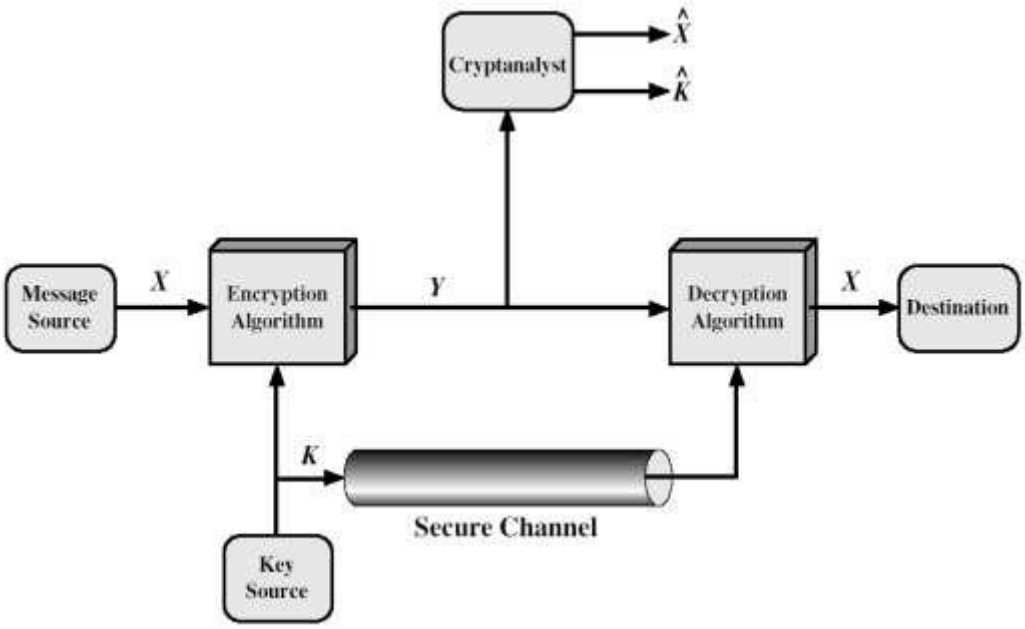

Figure-2 – Algorithm for Encryption

Sender and receiver more likely than not got duplicates of the secret key in a secure manner and must keep the key secure. On the off chance that somebody can find the key and knows the algorithm, all correspondence utilizing this key is coherent

We expect that it is illogical to unscramble a message based on the cipher text in addition to learning of the encryption/decoding algorithm, i.e. we don't have to keep the algorithm secret; we have to keep just the key secret.

5. CONCLUSION :

This paper tries to give a perception of cryptography and significance of the cryptography in the network and data security. The process if cipher text is described here. The role and importance of cipher text in the cloud computing is also described here in the brief. The b

Lock diagram for the encryption and decryption is given here with the extension of algorithmic view of the process. The algorithm for encryption is able to encode the type of data being communicated and kind of conduit throughout which data is being communicated. The chief aspiration of this very basic article is to give primary facts about the cryptographic algorithms and symmetric key encryption techniques.

REFERENCES:

1. Ayushi, “A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010.
2. Mohammad ShahnawazNasir, Prakash Kuppuswamy “Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm “International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013.
3. Preeti poonia and Praveen Kantha, “ Comparative Study of Various Substitution and Transposition Encryption Techniques”, International Journal of Computer Applications (0975 – 8887) Volume 145 – No.10, July 2016
4. Satish Kumar Garg” Modified Encryption and Decryption Using Symmetric Keys at Two Stages: Algorithm SKG 1.2” International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6, June 2014 ISSN: 2277 128X.
5. Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. DubeyASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile ComputingIJCSMC, Vol. 4, Issue. 8, August 2015.
6. Senthil, K., K. Prasanthi, and R. Rajaram . "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research(ICCIC), 2013 IEEE International Conference on. IEEE,2013.
7. SomdipDey “An Integrated Symmetric Key Cryptographic Method Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm” I.J.Modern Education and Computer Science, 2012, 5, 1-9 Published Online June 2012 in MECS.
8. William Stallings “Cryptography and Network Security: Principles and Practices”, PHI Learning Private Limited, Forth Edition, 2009, pp 64 - 86.