UGC Approved Journal
Research Link
Since March 2002
An International, Registered & Refereed Monthly Journal : Computer Science
Research Link - 169, Vol - XVII (2), April - 2018, Page No. 27-28
ISSN - 0973-1628 ■ RNI - MPHIN-2002-7041 ■ Impact Factor - 2015 - 2.782

Cryptography Techniques

Data is collection of raw facts and figures or any type of stored digital information. Security is about the protection of assets. In modern era evaluation of networking and wireless network has come in information and communication technology, there are so many things that gives the facility to deal with these technology using internet. To make secure data transmission over networks cryptography is used. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. The algorithm selected for cryptography should fulfill the conditions of integrity protection, conventional message authentication and digital signatures. A number of cryptography techniques are developed for achieving secure communication. ***Key Words : Encryption, Decryption, Cryptography, Private key, Public Key, Symmetric Key algorithm, Hash Function.***

MRS. POOJA

Introduction :

Today's our entire globe is depending on internet and its application for their every part of life. Here comes the requirement of securing our data by ways of cryptography.

Cryptography is the practice of secure data communication in the presence of third party. Cryptography encrypt the data at the transmitter end to protect it from stolen and from errors. The Word "cryptography" comes from the Greek words for "Secret Writing".Cryptography is the art of secret writing. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it.

The importance of information and communication systems for society and the globe economy is intensifying with the increasing value and quantity of data that is transmitted and stored on these system. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access, and use, misappropriation, alteration and destruction.

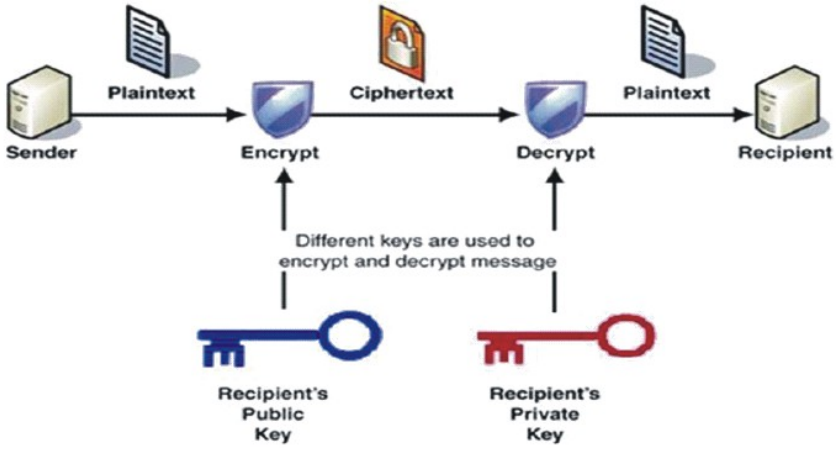
The message to be encrypted, known as plain text, are transformed by a function that is parameterizes by a key. The output of encryption process, known as cipher text, is then transmitted, often by messengers or radio. We assume that the enemy, or intruder, hears and accurately copies down the complete cipher text. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the cipher text easily.

Basic Terminology of Cryptography :

Cryptography : It is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word Cryptography comes from the Greek word "kryptos" that means hidden, & "graphikos" which means writing.

Plain Text : The information that we need to fide, is called plain text. It is the original text. It could be in the form of characters, numerical data, executable programs, pictures, or any other kind of information.

Cipher Text : The data that will be transmitted into coded form is called cipher text. It is the term refers to the string of "meaningless: data or unclear text that nobody must understand, except the recipients. It is the data that will be



Assistant Professor (Department of Computer Science), S.D. College, Hoshiarpur (Punjab)

transmitted exactly through network. Many algorithms are used to transform plain text into cipher text.

Key : It is an input to the encryption algorithms and this value must be independent of plain text. This input is used to transform the plain text into cipher text, so different keys will yield different cipher text. On the receiver side, the inverse of the key will be used inside the algorithm instead of key.

Computer Security :

It is generic term for a collection of tools designed to protect any data from hackers,theft,corruption, or natural disaster. While allowing these data to be available to the user at the same time. The example of these tool is the antivirus program.

Network Security :

It refers to any activity designed to protect the usability, integrity, reliability and safety of data during their transmission on a network. Network security deals with hardware and software.

Internet Security : It is measures and procedures used to protect data during their transmission over a collection of interconnected networks, while information security is about how to prevent attacks and to detect attacks on information based systems.

Purpose of Cryptography :

By using Cryptography many goals can be achieved. These goals can be either all achieved at the same time in one application, or only one of them.

These goals are :

Authentication : It is the process of providing the identity that assures the communication entity is the one that is claimed to be. This process ensures that the origin of the message is correctly identified.

Confidentiality : The principle of confidentiality specifies that only the sender and intended recipient should be able to process the contents of messages.

Data Integrity : It ensures that the received message has not been changed in any way from its original form.

Access Control : It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources. If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

Non Repudiation : it is the mechanism used to prove that the sender really sent this message, and the message was received by the specific party, so the recipient cannot claim that the message was sent.

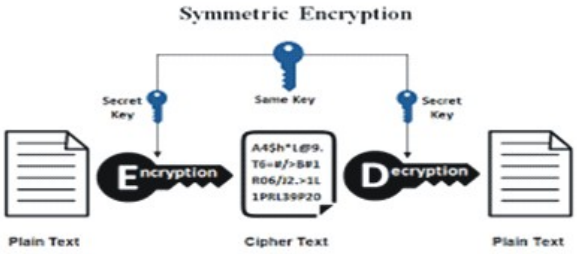
Data Encryption / Decreyption :

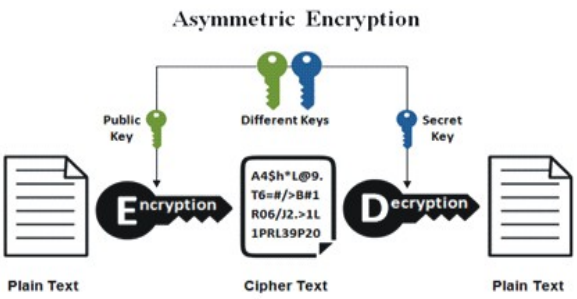
Data Encryption : is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Cryptography uses 2 types of keys :

(i) Symmetric key **(ii)** Asymmetric key

Symmetric key has been around the longest, they





utilize a single key for both encryption & decryption of the cipher text. This type of the key is called Secret Key. Most cryptographic processes user symmetric encryption to encrypt data transmissions, but use asymmetric encryption to encrypt and exchange data.

Data Decryption :

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the WWW, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or decoded text or other data, and converting back into text that user or the computer can read and understand.

Encryption is the process of translating plain text data into something that appears to be random and meaningless(cipher text). Decryption is the process of converting cipher text into plain text.

Conclusion :

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has decipher key, and "data cannot be altered" means the original information would not be changed or modified. Cryptography has been emerged as essential tool for data transmission.

References :

(1) http://en.wikipedia.org/wiki/cryptograhy (2) B.A. Forouzan, Cryptography and Network Security, India: Tata McGraw Hill publishing company. (3) Singh, Gurjeevan ; Singla, Ashwani Kumar and Sandha, K.S. : "Performance evaluation of Symmetric Cryptograhy Algorithms", International Journal of Electronics and Communication Technology, vol 2, issue 3, Sept 2011. (4) http://www.tutorialpoint.com/cryptography/cryptography_tutorial.pdf (5) http://www.techopedia.com/definition/1773/decryption