ROLE OF CRYPTOGRAPHY IN SECURITY SYSTEM

RAHUL

ABSTRACT

Data is any sort of hold on digital data. Security is concerning the protection of assets. Knowledge security refers to protecting digital privacy measures that square measure applied to stop unauthorized access to computers, personal databases and websites. Cryptography is evergreen and developments. Cryptography protects users by providing practicality for the coding of information and authentication of alternative users. Compression is that the method of reducing the amount of bits or bytes required representing a given set of information.

There square measure several scientific discipline techniques accessible and among them AES is one amongst the foremost powerful techniques. The state of affairs of gift day of data security system includes confidentiality, believability, integrity, non-repudiation. The protection of communication may be a crucial issue on World Wide net. It's concerning confidentiality, integrity, authentication throughout access or piece of writing of confidential internal documents.

Keywords: Data Encryption and Decryption, Compression, Cryptography Concept, Security, Integrity.

I INTRODUCTION

To secure the data, compression is used because it use less disk space (saves money), more data can be transfer via internet. It increase speed of data transfer from disk to memory. Security goals for data security are Confidential, Authentication, Integrity, and Non-repudiation. Data security delivers data protection across enterprise. Information security is a growing issue among IT organizations of all sizes. To tackle this growing concern, more and more IT firms are moving towards cryptography to protect their valuable information. In addition to above concerns over securing stored data, IT organizations are also facing challenges with ever-increasing costs of storage required to make sure that there is enough storage capacity to meet the organization's current and future demands. Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format, called cipher text, using an encryption key. Currently compression and encryption methods are done separately. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around hardness assumptions making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. The growth of cryptographic technology has raised a number of legal

issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

II CRYPTOGRAPHY

The art of cryptography is taken into account to change state at the side of the art of writing. As civilizations evolved, people in general got organized in tribes, groups, and kingdoms. This crystal rectifier to the emergence of concepts like power, battles, supremacy, and politics. These concepts additional burning the natural would like of individuals to speak on the Q.T. with selective recipient that successively ensured the continual evolution of cryptography still. The roots of cryptography area unit found in Roman and Egyptian civilizations. The importance of data and communication systems for society and therefore the world economy is aggravating with the increasing price and amount of knowledge that's transmitted and holds on those systems. At an equivalent time those systems and knowledge also are more and more prone to a spread of threats, like unauthorized access and use, misappropriation, alteration, and destruction.

The activity of data is termed secret writing, and once the knowledge is unhidden, it's known as cryptography. A cipher is employed to accomplish the secret writing and cryptography. Merriam-Webster's dictionary defines cipher as ―a technique of remodeling a text so as to hide it's that means.‖ the knowledge that's being hidden is termed plaintext; once it's been encrypted, it's known as cipher text.

To hide any knowledge 2 techniques area unit principally used one is Cryptography alternative is Steganography. During this paper we have a tendency to use Cryptography. Cryptography is that the science of protective knowledge that provides strategies of changing knowledge into undecipherable kind, so Valid User will access info at the Destination. Cryptography is that the science of victimization arithmetic to encipher and decode knowledge.

III BASIC TERMINOLOGY OF CRYPTOGRAPHY

Computers are employed by several individuals for several functions. like banking, shopping, military, student records, etc.. Privacy could be a essential issue in several of those applications, however are we'd like to create positive that associate unauthorized parties cannot browse or modify messages.

Cryptography is that the transformation of legible and comprehendible information into a kind that can't be understood so as to secure information. Cryptography refers specifically to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", which means hidden, and "graphikos" which suggests writing.

The information that we'd like to cover, is termed plaintext,it's the first text, It may be during a type of characters, numerical information, workable programs, pictures, or the other quite info, The plaintext for instance is that the causing of a message within the sender before cryptography, or it's the text at the receiver when decoding.The data that may be transmitted is termed cipher text, it is a term refers to the string of "meaningless" information, or unclear text that no-one should perceive, except the recipients. it's the

information that   may be   transmitted specifically through   network, several algorithms are wont to rework plaintext into cipher text.

Cipher is the algorithm that is used to transform plaintext to cipher text, this method is called encryption, inother words, it's a mechanism of converting readable and understandable data into "meaningless" data.

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a 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 users at the same time. The example of these tools is the antivirus program.

Network security 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. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks.

Internet Security 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.

3.1 Cryptography Goals

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:

Confidentiality: it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

Authentication: it is the process of proving the identity that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don't have personal knowledge of their identities.

Data Integrity: its ensures that the received message has not been changed in any way from its original form. Thedata may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

International Journal of Advance Research in Science and Engineering

Vol. No.5, Issue No. 12, December 2016

www.ijarse.com

IJARSE

ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

4. Non-Repudiation: it is mechanism used to prove that the sender really sent this message and the message wasreceived by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

5. Access Control: it is the process of preventing an unauthorized use of resources. This goal controls who can haveaccess 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.

3.2 Data Encryption

A 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 two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.

Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

3.3 Data Decryption

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (*plaintext*) into something that appears to be random and meaningless (*ciphertext*). Decryption is the process of converting cipher text back to plaintext.

3.4 Symmetric Key Cryptography

In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.

Key

Plain text   Cipher text   Plain text

Encryption ⟶ Decryption

Symmetric Cryptosystem
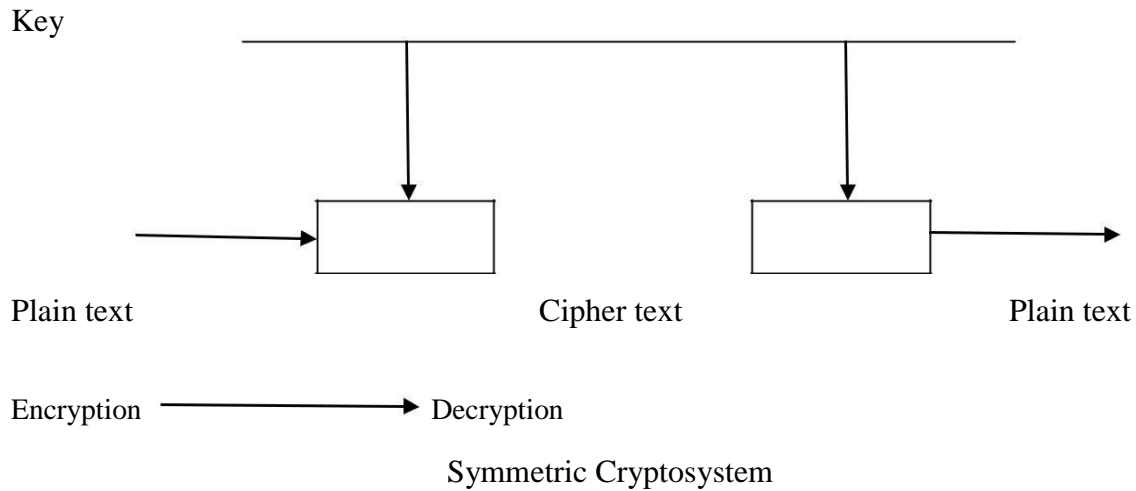
3.5 Asymmetric Key Cryptography

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key.

Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.

Plain text   Cipher text   Plain text

Encryption ⟶ Decryption

Asymmetric Cryptosystem
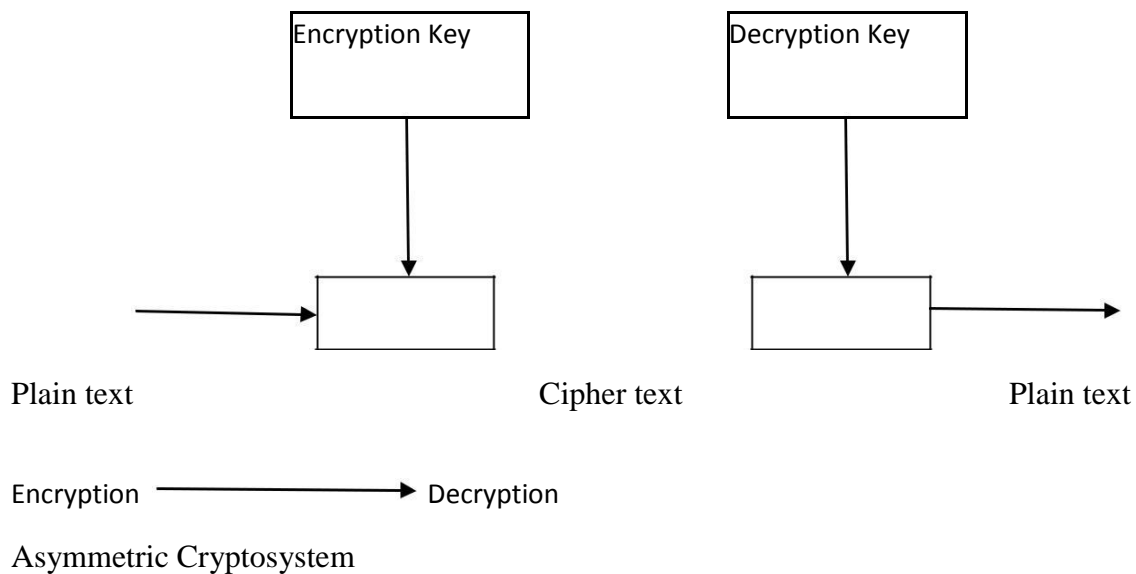
3.6 Compression

Data compression offers an attractive approach for reducing communication costs by using available bandwidth effectively. Compression algorithms reduce the redundancy in data representation to decrease the storage required for that data. Over the last decade there has been an unprecedented explosion in the amount of digital data transmitted via the Internet, representing text, images, video, sound, computer programs etc.

Data compression implies sending or storing a smaller number of bits. Compression is the reduction in size of data in order to save space or transmission time. Many methods are used for this purpose; in general these methods can be divided into two broad categories: Lossy and Lossless methods. Lossy Compression generally used for compress images. In this original data is not identical to compressed data that means there is some loss e.g. Block Truncation Coding, Transform Coding, etc. Lossless Compression used for compress any textual data.

IV SUMMARY

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 the decipher key, and "data cannot be changed" means the original information would not be changed or modified.

REFERENCES

[1]SwarnalataBollavarapu and Ruchita Sharma-‖ Data Security using Compression and Cryptography Techniques‖

[2] ManojPatil, Prof. VinaySahu——‖ A Survey of Compression and Encryption Techniques for SMS‖

[3] Bobby Jasuja and AbhishekPandya –—‖ Crypto-Compression System: An Integrated Approach using Stream Cipher.Cryptography and Entropy Encoding‖

[4] https://msdn.microsoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx.

[5] https://www.techopedia.com/definition/1773/decryption.

[6]www.computerhope.com/jargon/d/decrypti.htm.

[7] https://en.wikipedia.org/wiki/Cryptography.

[8] https://www.techopedia.com/definition/25403/encryption-key

[9] http://searchsecurity.techtarget.com/definition/private-key

[10]https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf