International Journal of Allied Practice, Research and Review

Website: www.ijaprr.com (ISSN 2350-1294)

Cryptography Encryption and Compression Techniques

Quaiser Bashir Lone[1], Mir Imtiyaz Hussain[2], Ms Monisa[3]
[1]Student, Departmentof Computer Science Engineering & SSM College OF Engg.& Tech., India
[2]Student, Department of Computer Science Engineering & SSM College of Engg.& Tech., India
[3]Guide, Department of Computer Science Engineering & SSM College of Engg.& Tech., India

Abstract- Data communication is an important aspect of our living. Data is defined as any type of digital information stored in the computer. Security is defined as the protection of information. Data security refers to the protection techniques used to prevent the unauthorized access to the computers, personal databases and websites. Data security is the process to protect data and databases, from the accidental and deliberate or malicious modifications and damages of unauthorized accesses. Cryptography is the art and science of hiding the messages to keep the information secure and safe. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data for easy transmission and easy storage of data. There are many cryptographic techniques available and among them AES is one of the most powerful techniques. The information security system of modern technology includes confidentiality, authenticity, integrity, nonrepudiation and access control. The security of communication and communication systems is a very crucial issue on World Wide Web. The main goals of data security are confidentiality, integrity, authentication during access or editing of confidential internal documents.

Keywords: Data Encryption and decryption; Compression; Cryptography Concept; Security; Integrity.

I. INTRODUCTION

Data communication is an important aspect of our living. So, protection of data from the unauthorized access and misuse is essential. The need of security is to ensure that our information remains confidential and only authorized users can access it, and ensuring that no unauthorized user has changed our information, so that it provides full accuracy and efficiency. Compression is used to secure the data because it uses less storage space to store the data, saves money, makes data transmission easy and hence more and more data can be transferred via internet. The primary objectives of data security are to provide data integrity, confidentiality, Authentication and non-repudiation. Data security also delivers protection across business enterprises. Data security is an important issue of all business organisations and IT firms of all sizes. To tackle this growing issue, more and more business and IT firms are moving towards the cryptography to introduce secrecy in the organisations.IT firms are also facing the problems of increasing costs of storage required to meet the organization’s current and future demands. Data compression also involves transformation of data in a given specific format called source code or source message into a format of smaller size called code word. A cryptographydefines a pair of data transformations called encryption and decryption. Encryption is applied to the plain text i.e. the data to be communicated to produce cipher text i.e. encrypted data using encryption key. Decryption uses the decryption key to convert cipher text to plain text i.e. the original data. Now, if the encryption key and the decryption key is the same or one can be derived from the other then it is said to be symmetric cryptography. This type of cryptosystem can be easily broken if the key used to encrypt or decrypt can be found. To improve the protection mechanism Public Key Cryptosystem was introduced in 1976 by Whitfield Diffe and Martin Hellman of Stanford University. It uses a pair of related keys one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one known as public key is disclosed. The message is encrypted with public key and can only be decrypted by using the private key. So, the encrypted message cannot be decrypted by anyone who knows the public key and thus secure communication is possible. 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

Cryptography derived from two Greek words which mean “hidden” or “secret” and “writing” or “study” respectively is the practice and study of techniques for secure communication in the presence of third parties called adversaries. In general, Cryptography is the process of constructing and analysing protocols that prevent unauthorized users and public from reading private messages. The art of cryptography is considered to be born along with art of writing. As civilizations evolved, human beings got organized into tribes, groups and kingdoms. This leads to the emergence of ideas like power, battles, supremacy and politics. These ideas enhanced the need of people to communicate secretly with other specific people which in turn ensured the continuous growth ofcryptography. The art of cryptography was also found in Roman and Egyptian civilizations. The earlier Roman method of cryptography, popularly known as Ceaser Shift Cipher, relies on shifting the letters of the message by an agreed number, the recipient of this message would then shifts the letters of the message back by the same number and obtain the original message.

Cryptography deals with the protection and security of digital data.It refers to the development of techniques based on mathematical algorithms that provide fundamental data security services.

The process of hiding of information is called encryption, and when the information is unhidden, it is called decryption. The encryption and decryption is accomplished by the cipher. Merriam-Webster’s Collegiate Dictionary defines cipher as a method of transforming a text in order to conceal its meaning. The information that is being hidden is called plaintext; and the encrypted information is called ciphertext.

There are two main techniques to hide any data in data security one is called Cryptography and the otheris known as Steganography. In this paper we use Cryptography. Cryptography is the art and science of securing data, which provides techniques of converting data into unreadable form, so that authorized User can access Information at the receiver end.

III. SECURITY SERVICES OR GOALS OF CRYPTOGRAPHY

The techniques of cryptography help us to fulfil many goals of the data security. These goals can be achieved at the same time in an application or one of them at a time. The main aim of using cryptography is to provide the following fundamental information security services.

A. Confidentiality

Confidentiality is the most important and fundamental security service provided by cryptography. Confidentiality means to ensure that the data remains private. It is the process of protecting the transmitted data from passive attacks. It is achieved using encryption.

B. Authentication

Authentication deals with ensuring the communication is authentic. It ensures that the data has been sent only by the identified and authentic sender.

C. Data Integrity

It is the security service that deals with any alteration in the data. We can apply data integrity to the group of messages, a single message or specific fields within a message. It ensures that data is protected from accidental or deliberate (malicious) modification. Data integrity is provided by message authentication codes and hashes.

D. Non-Repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data has no right to deny the creation or transmission of the data created by him to a recipient.

E. Access Control

It is the process of protecting the resources from the unauthorized access. It controls who can have access to the resources and also defines the restrictions and conditions under which one can access the resources.

IV. DATA ENCRYPTION

Data encryption is a security method in which the information is encoded in such a manner that only the authorized user can read it. It is a random string of bits created explicitly for scrambling and unscrambling data.Data security is designed with objectives to ensure that every key is unique and unpredictable.

Generally, there are two types of keys used in Cryptography- Symmetric and Asymmetric keys. Symmetric keys are the type of keys that utilize a single key for both encryption and decryption processes. These are also known as secret keys and have been used from the long time. Secret key ciphers are of two types-Stream ciphers and Block Ciphers. Stream ciphers are the type of ciphers that process one bit at a time i.e. it applies key and algorithm to a single bit at a time. Whereas, Block ciphers are the type of ciphers that processes a block of bits simultaneously i.e. it applies private key and algorithm to a block of bits simultaneously.

Symmetric encryption is mostly used by cryptographic processes for encrypting data transmissions while as asymmetric encryption is used for encrypting and exchanging secret key. The one of the drawbacks of this system is that if either sender or receiver loses the secret key or the key is intercepted, then the system is broken and the communication cannot take place securely.

V. DATA DECRYPTION

The main objective of implementing encryption-decryption system is security and privacy. When the information is transferred via internet, it can be accessed by various unauthorized users or organizations.

Decryption is defined as the process of converting the encoded and encrypted data or text into the text that can be read and understood by you and the computer. It can also be used to describe the method of un-encrypting the data manually or using the proper codes and keys. The process of translating plain text data (plaintext) into the random and meaningless data (ciphertext) is known as Encryption. While as,the process of converting the ciphertext back to plaintext is called Decryption.

VI. TYPES OF CRYPTOGRAPHY

A. Symmetric Key Cryptography

Symmetric key cryptography isthe type of cryptography which consists of encryption methods in which both the sender and the receiver have the same secret key or the same secret key is exchanged between the sender and the receiver. Thus when private key cryptography is used for communication between two parties, then both the sender and the receiver must have the secret key. It is also known as private key cryptography.

Symmetric ciphers can be either stream ciphers or block ciphers. Stream ciphers are the type of ciphers that apply key and algorithm to a single bit at a time. Block ciphers are the type of symmetric ciphers that apply key and algorithm to a block of bits simultaneously. Data encryption standard (DES) and advanced encryption standard (AES) are the two most important block ciphers designated by the US government.

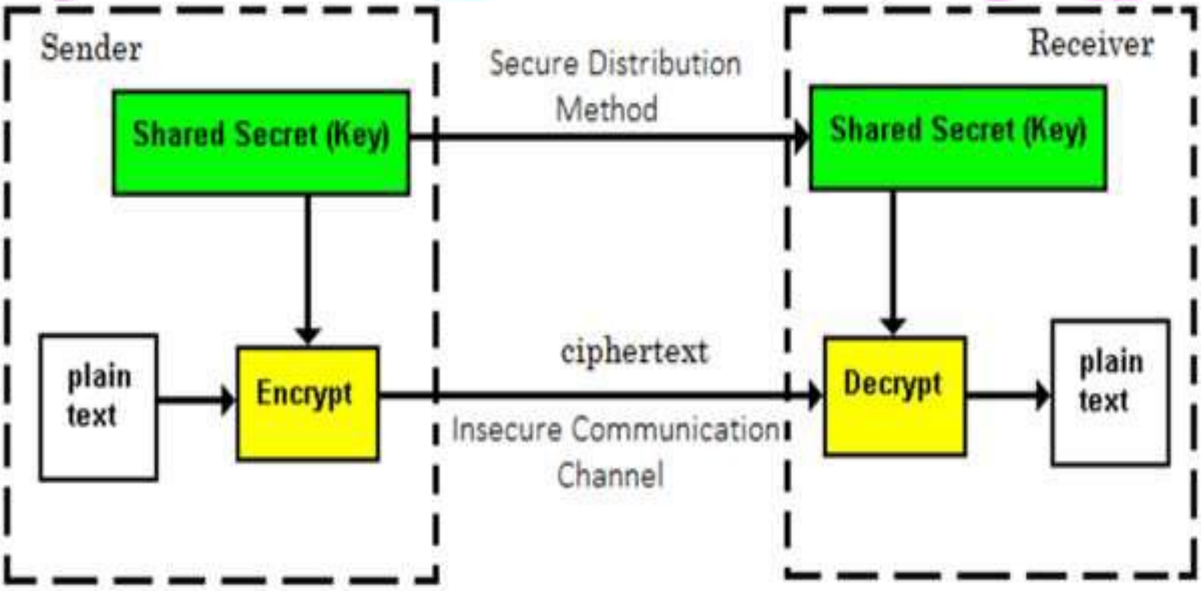

Fig.1 Symmetric key Cryptography

B. Asymmetric Key Cryptography

Asymmetric key cryptography is a two key system and is also known as Public Key Cryptography. It is a type of Cryptography which consists of two separate keys, one secret key and one public key. One key is used to encrypt the information and another key is used to decrypt the information. In public key cryptography, the sending computer encrypts the message to the receiver by using the selected or specified user's public key and then by using the sender's private key and the receiver computer decrypts the message by using its own private key and then using the sender's public key. The process of encryption-decryption is slower in asymmetric key cryptography than symmetric key cryptography because the length of keys i.e. the number of bits is large in asymmetric key cryptography.

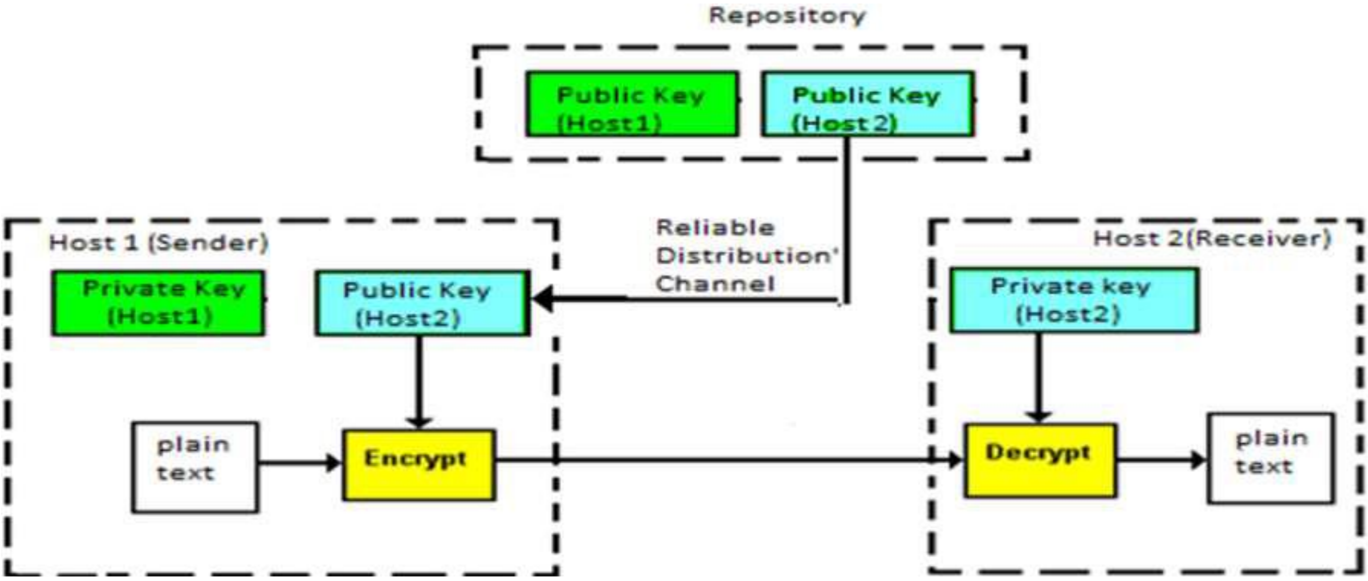

Fig.2 Asymmetric key Cryptography

VII.COMPRESSION

Data compression is the most important and vital approach for modern communication systems for reducing the communication costs and increasing the transmission rate by using the available bandwidth effectively. Compression algorithms reduce the storage space for storing the data by reducing the number of bits to represent the data and by decreasing the redundancy in data representation. In the modern era of science and technology, there has been tremendous increase in the amount of digital data transmitted via the internet representing text,images,audio,video, computer programs etc. as large number of people and organizations are moving towards the cloud. Data compression is the process of reducing the number of bits required to represent the data in order to increase the transmission rate and decrease the storage space for storing the data. There are different types of methods used for achieving for data compression. In general, Compression methods are classified as either lossless or lossy. In lossless compression, restored data and original data are identical i.e. there is no loss in the data. This method is necessary for many types of data like executable code, tabular numbers, and word processing files etc. where we cannot afford to lose even a single bit of information. E.g., Runlength coding, Huffman coding, LZW compression, Arithmetic coding, lossless predictive coding. Lossy compression is the type of compression, in which the restored data is not identical to the original data i.e. there is some loss in the data. Lossy compression is mostly used for compressing the images. It is also used for a number of applications in which some amount of error is tolerable. Further, Lossy techniques are more effective at compression than lossless techniques. E.g. transform coding, wavelet coding, Lossy predictive coding techniques.

VII. CONCLUSION

This paper shows the basic information about the cryptography and compression, and their various techniques. The combination of cryptographic and compression techniques are used for protection and security of data. Cryptography is the process that ensures the transmission of contents of the message from one party to another confidentially and without any alteration. Confidentiality means that the data transmitted between two systems remains private and only the person having decryption key can understand the data and the “no alteration” means that the original data would not be modified.

IX. ACKNOWLEGEMENT

First of all we would like to thank Almighty Allah for everything he has provided us with. A word of thanks to our college academics without which we would have not thought to go for this review paper.We would also like to thank our head of Department Ms Yasmeen for providing us with the facilities and staff members of such a caliber. We would also wish to acknowledge all the people who have worked in data security and whose work inspired me to write on this concept and whose documents gave me the path to write a this review paper.

Last but not least our heartiest thanks to our parents who always supported us by every possible way they could.

X. REFERENCES

[1] Manoj Patil, Prof. Vinay Sahu—— “A Survey of Compression and Encryption Techniques for SMS”

[2] Behrouz Forouzan. --------“Data Compression”

[3] William Stallings. ----“Cryptography and Network Security Principles and Practice”

[4] Ms. Ayushi Aggarwal, Anju “Enciphering Data for Larger Files” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 5, May 2013.

[5] R.L.Rivest, A.Sharmir, L. Adleman. ---- A method for obtaining digital signatures and public key Cryptosystems”, Tata McGraw-Hill

[6] Atul Kahate. ------Computer and Network Security

[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