International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 05
May 2015

Data Encryption and Decryption

Nitigya Grover
Student (B.Tech 6th sem) Department of Electronics and Computers Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email: nitigyagrover01@gmail.com

Nitin Garg
Student (B.Tech 6th sem) Department of Electronics and Computers Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email: ngarg1910@gmail.com

Abstract

The Process of Encryption and Decryption is performed by using Symmetric key cryptography and public key cryptography for Secure Communication. Cryptography is an art of scrambling the data in order to provide security and confidentiality. Cryptography is being used in order for the securely transmission of the data. It is impossible to provide security as the hacker or the attackers can easily get the data as they are easily able to know key and if key get key they will be able to decrypt your whole important data. In this paper, we studied that how the process of Encryption and Decryption is perform in case of Symmetric key and public key cryptography using algorithms.

Keywords: Encryption, Decryption, Cryptography, Key.

Introduction

There are many methods that have been proposed that provide security during communication using random number generators, using secure key, using large length key which is very difficult to break.

Encryption is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the
unintelligible ciphertext back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext. Cryptography is the practice and study of techniques for secure communication in the presence of third parties or we can say that it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.

Types of Cryptography

a) Symmetric-Key Cryptography

Symmetric-key cryptography is also known as the secret key cryptography or private key cryptography. It refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

b) Asymmetric-Key Cryptography

Asymmetric-key cryptography is also known as the public key cryptography. In this the pair of keys are used one is to encrypt the data at the sender side and other is to decrypt the data at the receiver side. In this the data at the sender side is encrypted using the public key and encrypted data at the receiver side is decrypted using the private key.
Nowadays as the communication is increasing and our lots of sensitive information is being sent over the network or internet so there is a need of information security and safety.

Conclusion

In today's world security is an imperative part of our life. With the advancement in the communication, security is the only thing that is needed by everyone in order to keep their communication secure. There are many ways of providing security but most of them provide the secure way of key distribution. As there is other problem that the key that is being distributed if get to know by the third party then that will lead to the leak of the information. So I am trying in my proposed work to provide the best way of key generation that will provide the security without any overhead of key distribution by adding randomness to the key. MREA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted. Main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect
guess of encryption key makes decryption impossible.

Refrences

[1]. William Stallings (2004), "Network Security Essentials (Applications and Standards)", Pearson Education.

[2]. M.G. MADIESH, M.L. MCGUIRE, S.W. NEVILLE," SECRET KEY GENERATION WITHIN PEER-TO-PEER NETWORK OVERLAYS", P2P, PARALLEL, GRID, CLOUD AND INTERNET COMPUTING (3PGCIC), 2012 SEVENTH INTERNATIONAL CONFERENCE, PP 156-163, IEEE 2012.

[3]. www.google.com