S^2SE: An Encryption Methodology

N.Kanagaraj
Research scholar
Computer science and Engineering,
Alagappa University, Karaikudi.

A.Padmapriya, Ph.D
Assistant professor
Computer science and Engineering,
Alagappa University, Karaikudi.

ABSTRACT

In the day to day life, Internet has become a vital part, owing to the revolutionary changes it has brought about in various fields. Transfer of critical information is also being carried out through the Internet. This enormous use of the Internet coupled with the tremendous growth in e-commerce and m-commerce has created a vital need for information security [3]. A security mechanism is any process that is designed to prevent, detect, or recover from a security attack. Examples of this security mechanism are encryption algorithms, authentication protocols and digital signatures. Encryption algorithms are used to protect blocks of data, such as messages from alteration. In this paper, we introduced a simple encryption methodology to secure the text file for longer time.

Keywords

Cryptography, Encryption, Decryption, Network Security, Symmetric encryption

1. INTRODUCTION

When, the Internet started to provide a platform for the ecommerce applications. Internet became vulnerable due to superfluous hackers / intruders. To keep the data in a safe manner, Cryptography is used for the security purpose. Cryptography is the science of using mathematics to encrypt and decrypt the data. Cryptography provides facility to store sensitive information or transmit it across insecure networks like Internet. The secured data can't be read by anyone except the intended recipient. A hacker uses the Cryptanalysis technique to interpret the messages. Cryptanalysis is the science of analysing and breaking secure communication. Cryptology embraces both cryptography and cryptanalysis.

A cryptographic algorithm is a mathematical function used in the process of encryption and decryption. It works in combination with a *key* – a word, number or phrase – to encrypt the plain text or to decrypt the cipher text. It is pictorially represented in the figure1. The security of the encrypted data is completely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key [4]. Cryptosystem comprises of a cryptographic algorithm, plus all possible keys and all the protocols that make it work. Usually, if the key is harder to discover, then the mechanism becomes more secure.

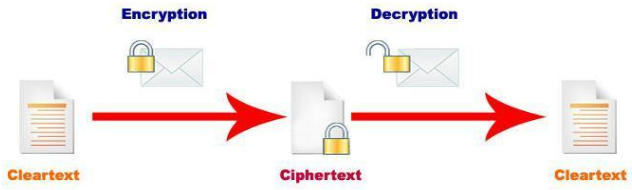

Fig1. The process of encryption and decryption

1.1 Cryptography Goals:

There are five main goals of cryptography. Each and every security system should provide a group of security functions that must promise the system's security. These functions are generally referred to as the goals of the security system. These goals of cryptography can be listed under the following five main categories: Authentication, Confidentiality, Data integrity, Non Repudiation and Access Control. [1]

1.2 Types of Cryptography:

There are two types of cryptography depending on the type of security keys used to encrypt or decrypt the data. Those two types are: Asymmetric and Symmetric encryption techniques.

1.2.1 Symmetric encryption

In this encryption process the receiver and the sender has to agree upon a single secret key (Shared Secret Key). Given a message (Plain text) and the key, encryption produces cipher text, which is about the same length as the plain text was. It uses the single key for encryption and decryption process (also called as Single key cryptography). Decryption is the reverse of encryption, and uses the same key as encryption. The process of symmetric encryption can be pictorially represented as below.

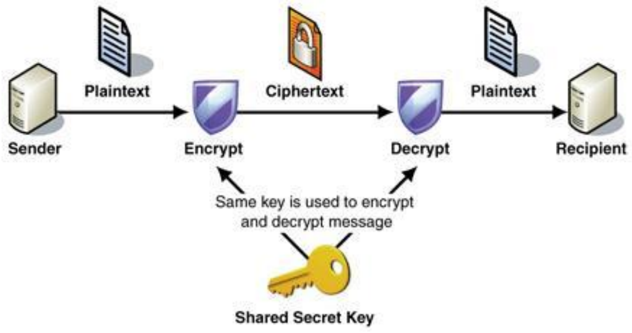

Fig.2 The process of symmetric encryption [2]

1.2.2 Asymmetric encryption

In asymmetric cryptography (also known as public key cryptography), the sender uses one key to encrypt data, and the recipient uses another key to decrypt cipher text. The encryption key and its matching decryption key are often referred to as a public/private key pair. The process of asymmetric encryption can be pictorially represented as below.

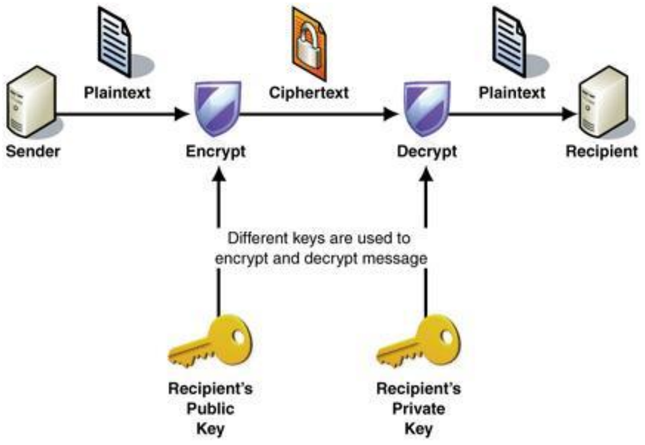

Fig.3 The process of asymmetric encryption [2]

A new symmetric key cryptography algorithm S^{2}SE (Shuffle, Shuffle, Substitution Encryption) has been proposed in this paper with its advantages and disadvantages. The paper has been divided into three phases that would describe about the proposed algorithm with an example, advantages and disadvantages of the algorithm and finally, conclusion part.

2. PROPOSED ALGORITHM

A text file that contains plain text is passed to the encryption phase of the system. The words in the text file are shuffled in even or odd order (i.e) the first word moved to the third word, continues till last and works on a circular way; in case of odd order chosen. Then the first and last characters are being moved to the last and first character of the next word. If the next word has only one character then the first character will be moved as said above and the last character been unchanged. In the next stage the text file is divided into the user chosen times ('n'). The keys (Kn) generated in a random way (i.e) using ASCII values from 32 to 126. In another way the keys (Kn) can be chosen from another table that holds the copy of ASCII table with a newly denoted values to the existing symbols. It makes the hacker, harder to guess the keys generated by this table. Using the keys generated, the each and every parts of the file encrypted with different keys. Here, substitution process takes place and then the encrypted file has been generated. The encrypted file can be sent to anyone using the mail servers already available.

After the receiver receives the encrypted file, the encrypted file is passed through the decryption phase of the system. The key file that holds the data like keys (Kn) used , original/ copied table used, number of partitions(n), shuffled order. The key file can be encrypted using one time pad encryption methodology for better security but it needs another key file to decrypt the first key file. Even though the security increases; the processing time dramatically increases and the system might slows down. Using the key file the decryption process starts. The keys can also been represented in negative so that the keys must be multiplied with minus one. Then the substitutions processes starts and in the next phase the shuffled words and characters are rearranged and at last the original plain text file has been generated.

2.1 Algorithm for encryption:

Step 1: Input: Text file (Plain text in .txt
format) Step 2: Shuffling the words (Odd /even
order) Step 3: Moving the character position
Step 4: Dividing the file into 'n' divisions
Step 5: Generating keys (Kn) for 'n'
divisions
Step 6: Substitution of characters using Keys (Kn)
Step 7: Output: Text file (encrypted text in .txt
format)

2.2 Algorithm for decryption:

Step 1: Input: Text file (encrypted text in .txt
format) Step 2: Multiplying the key (Kn) by minus
one
Step 3: Substitution of characters using (-Kn)
Step 4: Rearranging the characters position and
words Step 5: Text file (Plain text in .txt format)

2.3 Example

In an intuitive manner, the plain text has a sentence like "America is going to attack on Cyria this weekend". The words are shuffled in odd/even order. In this case, the order is even, the sentence become "this America going is attack to Cyria on weekend". In the next phase, the characters get shuffled and the sentence becomes "dhiw smerict aoinA gg sttaci ka oyrit aC neekeno". Now in the next phase the sentence is divided into 'n' times; consider 'n' as 2. The keys (K2) are generated. Consider K_1 as (+3) and K_2 as (-5) and consider the substitution takes place with already existing ASCII vales. Then the same sentence becomes "gklz vphulfw drlqD jj noo\^d f\ jtmdo \> i``fij". This would be the final cipher text.

In the decryption process, the keys needs to multiplied by minus one to revert the substitution. Then the keys, K_1 and K_2 become -3 and +5 respectively. In the next two phases, the shuffle of characters and words are rearranged to acquire the plaintext.

3. ADVANTAGES AND DISADVANTAGES

In this section the advantages and disadvantages of using our encryption are pointed out.

3.1 Advantages

1. The algorithm is very simple in nature.
2. CRC checking in receiving ends is easier.
3. For a small amount of data this algorithm will work very smoothly.
4. If the redefined table used for substitution process; the possibilities to break the system is very less.

3.4 Disadvantages

5. It becomes inefficient for larger data and if the cryptanalysis uses the very high-end processors.

4. CONCLUSION

Cryptography is used to achieve the goals like Confidentiality, Data integrity, Authentication, Access control, Non repudiation of the data send. In order to achieve these goals various cryptographic algorithms are developed by various researchers. For a small amount of data those algorithms wouldn't be cost effective because those are not designed for small amount of data. The objective of this work was to design a new algorithm to address this kind of issue. By having this kind of issue in mind, the algorithm is designed in a simple manner without sacrificing the security issues too. A single key is used for both encryption and decryption i.e., it falls under the secret key cryptographic algorithm category. Literally, the public key cryptography algorithms are more secured than secret key cryptography algorithms. So our next objective would be to develop a simple and proficient public key cryptographic algorithm.

5. REFERENCES

[1] Cryptography and Network Security - Principles and Practice, Fifth edition, William Stallings, Pearson Publication.

[2] http://msdn.microsoft.com/en-us/library/ff650720.aspx - Symmetric and Asymmetric encryption process figures.

[3] Sheena, Mathew; Dr. Poulose Jacob, K, Studies,Design and Development of Network Security Enhancement Services Using Novel Cryptographic Algorithms , Dtd: 2008-06. Online available at http://dyuthi.cusat.ac.in/purl/2689

[4] Online available at: http://en.kryptotel.net/encryption.html