Comparative Study of Various Substitution and Transposition Encryption Techniques

Preeti Poonia
Department of Computer Science & Engineering
BRCM CET, Bahal, MDU, India

Praveen Kantha
Department of Computer Science & Engineering
BRCM CET, Bahal, MDU, India

ABSTRACT
With the rapid development in the technology, Encryption is one the most power full approach to achieve data security and privacy. Data Encryption techniques is used to hide the original content of a data in such a way that the original information is recovered only through using a key known as decryption process. The objective of the encryption is to secure or protect data from unauthorized access in term of viewing or modifying the data. Encryption can be implemented occurs by using some substitute technique, shifting technique, or mathematical operations. By applying these techniques we can generate a different form of that data which can be difficult to understand by any one. The original data is referred to as the plaintext and the encrypted data as the cipher text. Several symmetric key base algorithms have been developed in the past year. In this paper we proposed a comparative study over symmetric key based algorithm using some parameter like algorithm strength, key size, key type attack type etc.

Keywords
Symmetric, Encryption, Decryption, Substitution, Transposition, Plaintext, Chipper text.

1. INTRODUCTION
Cryptography is the art of achieve security by encoding messages to make them non-readable [1]. It is a technique which allow human-being to encrypt the data in such a way that the decryption can be performed without the aid of sender. Cryptography not only protects the information but also provides authentication to the user. As the network technology has been greatly advanced, there is a need to send much information via the Internet. Data can be read and understood without any special measures are called plaintext. Cryptography plays an important role insecure communication over the network and it provides an best solution to offer the necessary protection against the data intruders. Cryptography is the science of securing data. Cryptography is way of implanting mathematics to encrypt and decrypt data. Cryptography provides you to store sensitive information or transmit it across the insecure networks so that cannot be read by anyone except the intend recipient. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis [3, 4]. During communication, the sender performs the encryption with the help of a shared secret key and the receiver performs the decryption. Cryptographic algorithms are broadly classified as Symmetric key cryptography and Asymmetric key cryptography. This section elucidate about services and mechanisms of cryptography, processing approaches of plaintext, key distribution and cryptanalysis.

2. VARIOUS DIMENSIONS OF CRYPTOGRAPHIC SYSTEMS
There are various independent dimensions of cryptographic system.

2.1 Type of Encryption Technique Include
I. Substitution

II. Transposition

2.2 Number of Keys Includes
I. Single-key or private

II. Two-key or public

2.3 Number of Way in Which Plaintext is processed
I. Block

II. Stream

3. SERVICE OF CRYPTOGRAPHY SYSTEM
Cryptography provides a number of security services to ensure the privacy of data. That why due to security benefit of cryptography, is widely used now a days. There are following service of Cryptography discussed below:

3.1 Confidentiality
Transmitted Information has to be accessed only by the authorized party.

3.2 Authentication
The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person.

3.3 Integrity
Only the authorized party is allowed to modify the transmitted information.

3.4 Access control
The Prevention of unauthorized use of a resource i.e. this service controls who can have access to a resource, under what condition access can occur, and what those accessing the resource are allowed to do.

3.5 Non-Repudiation
Provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication.

4. SYMMETRIC CIPHER MODEL

A symmetric encryption model has following component fig. 4.1

4.1 Plaintext

This is the original intelligible message or data that is fed into algorithm as input.

4.2 Cipher text

The encoded message send to other side over network.

4.3 Key

Information used in cipher known only to sender/receiver.

4.4 Encryption Algorithm

Performs various substitution and transformation on the plaintext to convert cipher text

4.5 Decryption Algorithm

Encryption algorithm run in reverse to recovering original message from cipher text.

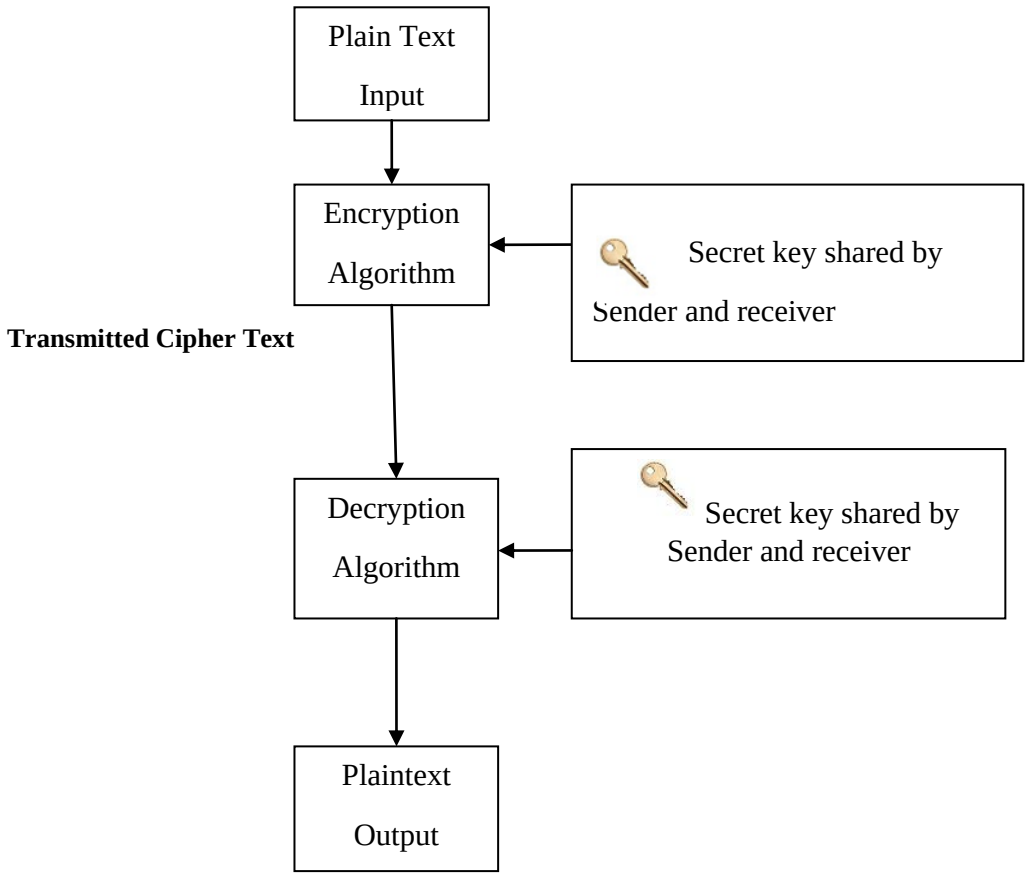

Figure: 4.1 Simplified Model of Conventional Encryption

5. SYMMETRIC CRYPTOGRAPHY

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encrypt them. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. The block cipher mode provides, whole data is divided into number of blocks. This is based on the block length and the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems [2]. In this paper we examine only called classical encryption techniques .A study of this technique enables us to illustrate the basic approaches to symmetric encryption used today. There are two building blocks of all encryption techniques are-

a).Substitution Technique: A substitution technique is one in which the letters of plaintext are replaced by other letters or by number or symbols .If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. There are following substitution technique – Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher , Polyalphabetic Cipher etc.

b).Transposition Techniques: A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters in which plaintext characters are shifted in some regular pattern to from cipher. This technique is referred to as a transposition cipher. The simplest such

cipher is the Rail Fence technique, Column Transposition, Odd-Even, Plaintext.

6. DIFFERENT SYMMETRIC KEY ENCRYPTION TECHNIQUE AND COMPARISON TABLE

This paper describes about some of the substitution and transposition encryption techniques which are already available. In general cryptographic encryption techniques are classified as classical encryption techniques and modern cryptographic techniques based on the periods that are developed/used . Classical cryptographic techniques are developed in the earliest days, but still some of the algorithms are used for providing confidentiality to the information. Modern cryptographic techniques are developed in recent years for providing better services like confidentiality, authentication, etc., to the information. In order to increase the degree of security, the modern cryptographic techniques algorithms are incredibly complex than classical cryptographic algorithms. Some of modern cryptographic algorithms are designed in such a way that repeats same procedure for many rounds, for example Feistel network, etc. Besides, symmetric encryption techniques also have encryption algorithms in both of classical and modern cryptographic techniques. For example play fair cipher, one time pad, hill cipher, etc. are comes under classical cryptographic techniques, and DES, AES, etc are modern cryptographic techniques. Here existing symmetric encryption algorithms are compared based on the parameters like block size, size of key, vulnerability to attacks and uniqueness of the technique, which are depicted as tabulation. Table I portrays the comparison of classical encryption techniques that are already exist.

Techniques/ Parameter	**Caesar cipher**	**Play fair cipher**	**Hill cipher**	**Polyalphabetic cipher**	**Rail-fence**	**Columnar transposition**
Key Type	Substitution	Substitution	Substitution	Substitution	permutation	Permutation
Block Size	1	2	m	Variable length	Variable length (depth)	Equal to key size
Key Size	Fixed Number	Fixed (25!)	variable	Equal to message length	Depth size is variable	Variable
Attack Type	Brute-Force attack	Cipher text only (frequency distribution)	Known plaintext attack	Cipher text and plaintext known attack	Brute-Force attack	Frequency analysis attack
Algorithm Strength	Only 25 keys possible	26*26=676 diagrams possible	Hide single letter frequency distribution	multiple cipher text letters for each plaintext letter	Depth size	Multiple encryption are possible To a single message
Encryption & Decryption Process	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric
Developed by	Julius Caesar in 19th century	Charles Wheatstone in 1854	Lester S. Hill I1n 1929	Leon Battista Alberti in around 1467	-	-
Key Factor (Uniqueness) about the technique	Simple substitution with Alphabet	Use pair of letters and substitute with 5×5 matrix designed with key and remaining alphabets	Based on Linear algebra, Convert plaintext into matrix based on ASCII value	Plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get	Plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom.	The plaintext is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.

7. CONCLUSION

In this paper, the limitations and weaknesses of classical encryption algorithms like Caesar cipher and Transposition cipher are described. It is used to achieve the mains of security aim like confidentiality, integrity, authentication, non-repudiation. In order to achieve these goals, Several algorithms have been developed in the past year and by comparison of different parameters used in algorithms give

significance of the algorithms In which some of the algorithms are succeed and others failed due to lack of security. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated. The main aim of this paper is to provides the fundamental knowledge about the cryptographic algorithms and comparison of available symmetric key encryption techniques based on some parameters like brute force attack, Key factor of Uniqueness about the technique, etc.

8. REFERENCES

[1] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010.

[2] Mohit Mittal, "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, ISSN 0975-8887.

[3] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. DubeyASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile ComputingIJCSMC, Vol. 4, Issue. 8, August 2015.

[4] Mohammad ShahnawazNasir, Prakash Kuppuswamy "Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm "International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013.

[5] William Stallings "Cryptography and Network Security: Principles and Practices", PHI Learning Private Limited, Forth Edition, 2009, pp 64 - 86.

[6] Satish Kumar Garg" Modified Encryption and Decryption Using Symmetric Keys at Two Stages: Algorithm SKG 1.2" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6, June 2014 ISSN: 2277 128X.

[7] SomdipDey "An Integrated Symmetric Key Cryptographic Method Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm" I.J.Modern Education and Computer Science, 2012, 5, 1-9 Published Online June 2012 in MECS.

[8] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. DubeyASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile ComputingIJCSMC, Vol. 4, Issue. 8, August 2015.

[9] William Stallings "Cryptography and Network Security: Principles and Practices", PHI Learning Private Limited, Forth Edition, 2009, pp 64 - 86.

[10] Senthil, K., K. Prasanthi, and R. Rajaram . "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research(ICCIC), 2013 IEEE International Conference on. IEEE,2013.