Volume-7,Issue-4, (Apr-17)
ISSN (O) :- 2349-3585

Survey on various substitution techniques for Cryptography

Mr. Rajendra S.Navale[1], Mr. Adilshah N.Jalgeri[2], Mr. Balkrushna B.Jagadale[3]
[1,2,3]Asst. Prof. at FTCOER, Sangola.

Abstract:With the faster development in the technology, to achieve data security and privacy Encryption is one of the most power full approach . Data Encryption techniques are 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 main aim of the encryption is to secure or protect data from unauthorized access in term of viewing or modifying the data. Encryption can be implemented by using some substitute technique, transposition 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 have referred to as the plaintext and the encrypted data as the cipher text. a number of symmetric key base algorithms have been developed in the past year. In this paper, we anticipated a relative 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, Cipher text, Vigenere cipher, Stream cipher.

1. INTRODUCTION

Cryptography is the fine art of attain security by programming messages to make them non-readable [1].Etymologically talking, the word cryptography comes from the Greek origin. It is an amalgamation of two words Crypto and Geography. Crypto means Secret and Graphy means Writing [2].As information is transferred from one user to another user the data or the information becomes highly susceptible to every kind of threats caused by adversaries (third party interventions). Now the data communication between two entities can be secured if an encryption and decryption technique is used at two end points[3] Symmetric and Asymmetric are the two types of encryption. In symmetric encryption techniques, we use the same key for both encryption and decryption purpose[4].Asymmetric-key encryption using public and private keys, the public key is announced to all members while the private key is kept secure by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his\her own private key to decrypt the message[4].In symmetric method, there are two techniques (substitution and transposition) used as a classical methods. Substitution technique maps the Plaintext elements into cipher text elements. Substitution has further two types, Monoalphabetic and polyalphabetic cipher. In monoalphabetic the character in the Plaintext changes to the same character in the Ciphertext. In polyalphabetic cipher a single character in the Plaintext is changing to many characters in the Ciphertext[5]. Permutation technique is one in which the Plaintext remains the same, but the order of characters is shuffled around to get the Ciphertext[5].Also the symmetric ciphers can be divided into Stream ciphers and block ciphers, as a modern cipher[5].The following figure shows the general structure of cryptography.Here in the below figure, plaintext stands for the data which is to be transferred to the receiver end by the sender. In encryption , the plaintext will be converted into the ciphertext by using any encryption algorithm. The encryption algorithm takes the two different inputs, i.e. plaintext and key. The ciphertext is the output of the encryption algorithm which is nothing but the garbled data.

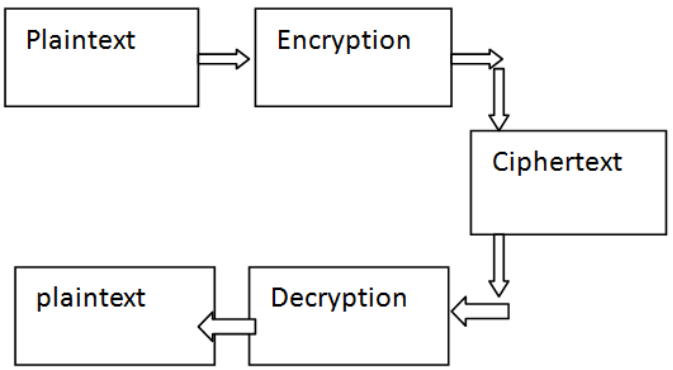

Fig1: Encryption & Decryption in Cryptography

The decryption algorithms takes the garbled data and key as input and produces the original data called as plaintext. The

decryption algorithm generally works in the inverse of the encryption algorithm.Ciphertext is also known as encrypted or encoded informationbecause it contains a form of the original plaintext that isunreadable by a human or computer without the proper cipher to decrypt it[7]. Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with codetext because the latter is a result of a not a cipher[7].

2.SERVICES OF CRYPTOGRAPHY SYSTEM

Cryptography provides a quantity of security services to make sure the secrecy of data. That's why due to the security benefit of cryptography, is widely used now a day. Following are the services of Cryptography discussed in detail:

2.1 Confidentiality

Transmitted Information has to be accessed only by the official party.

2.2 Authentication

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

2.3 Integrity

Only the official party is permitted to modify the transmitted information.

2.4 Access control

The Prevention of unofficial 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.

2.5 Non-Repudiation

Provides shielding against denunciation by one of the entities involved in a communication of having participated in all or part of the communication.

3. SYMMETRIC CIPHER MODEL

Before surveying the various substitution techniques, we must first understand the concept of symmetric cipher model. Actually, in this type of cryptography the same key is used for encryption and decryption. Only because the same key is shared between two parties , we call this type of cryptography as symmetric cryptography[9]. Here in this symmetric model , We consider the plaintext as ‘X’, ciphertext as ‘Y’, key as ‘K’, encryption algorithm as ‘E’ and decryption algorithm as ‘D’. Then the equation for the encryption in symmetric model will look like as-

$Y = E(K,X)$……(1)

And the equation for the decryption in symmetric model will look like as –

$X = D(K,Y)$……(2)

Now, the explanation of equation (1) is shown in the figure.2 and the explanation of equation(2) is shown in the figure.3. The terms plaintext, ciphertext, key, encryption and decryption algorithms are same as explained in introduction section of this paper. There are two requirements for secure use of conventional encryption:-

1.We need a strong encryption algorithm.

2.The sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

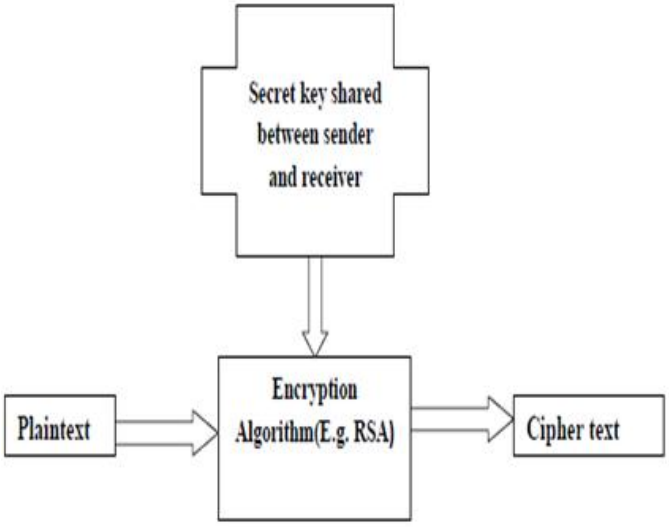

Fig.2 Encryption

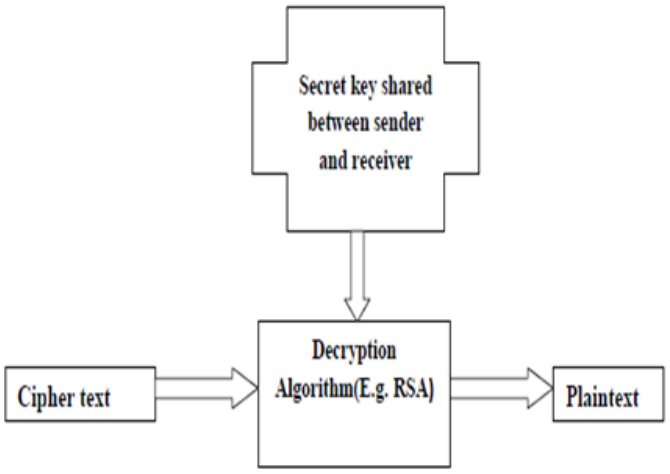

Fig.3 Decryption

4.Attacks on Symmetric Cipher Model

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. Here in this section , we try to explain the two different possible attacks on the Symmetric Cipher model. And those are Cryptanalysis attack and Brute force attack.

1.Cryptanalysis attacks: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

2.Brute force attack:- The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average , half of all possible keys must must be tried to achieve success.If either type of attack succeeds in deducing the key, the effect is catastrophic : All future and past messages encrypted with that key are compromised.

5.Classical encryption techniques

There are two main encryption techniques available:-

5.1 Substitution Techniques and

5.2 Transposition Techniques.

5.1.Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols[9]. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

5.2.Transposition Techniques

it is as very different kind of mapping and is achieved by performing some sort of permutation on the plaintext letters.

Now in this paper, we are only concentrating on the substitution techniques. So here , we first try to explain some substitution techniques in detail and then it will be summarized on the basis of some terms.

5.1.1.Caesar Cipher

It was invented by Julius Caesar. It is the earliest known and simplest use of a substitution cipher. In this technique ,we replace each letter of the alphabet with the letter standing three places further down the alphabet. For example:-

Plaintext:- Raj Navale

Ciphertext:-UDM QDYDOH

Here for the sake of convenience, we have written the ciphertext in capital letters.

If we assign numerical equivalent to each letter, then the Ceaser Cipher can be expressed as-

C= E(3,P)= (P+3)Mod 26……..(3)

Where,

C= Ciphertext , P= Plaintext and E= encryption algorithm.

In this technique, shift may be of any amount instead of the third letter down the order in plain text.

So in general, Ceasar algorithm is-

C = E(K,P)= (P+K)Mod26…….(4)

Where K= key and its value ranges from 1 to 25.

The decryption algorithm is simply as –

P = D(K,C) = (C-K)Mod26……(5)

Advantages

1.Easy to implement.

2.Take a little time for implementation.

Disadvantages

1.Brute force cryptanalysis is easily performed by simply trying all possible 25 keys.

5.1.2.Monoalphabetic Cipher

The Ceasar cipher is far from secure with only 25 possible keys. To increase the key space,here in this technique, developer has used arbitrary substitution. To achieve arbitrary substitution, with this technique, developer has used the permutation concept from set theory.

Permutation

A permutation of a finite set of elements ‘s’ is an ordered sequence of all the elements of ‘S’, with each element appearing exactly once. If S = {a,b,c} then, there are six permutations of S. And those are- abc, acd, bac,bca,cab,cba.

In general, there are n! permutations of a set of ‘n’ elements because the first element can be chosen in one of ‘n’ ways, the second in n-1 ways, the third in n-3 ways and so on.. If we consider 26 letters for plaintext, then 26! Possible keys will be there for encryption. This approach is referred to as a monoalphabetic cipher , because a single cipher alphabet is used per message.

ISSN:-2349-3585 |www.ijrdt.org

Advantages

1.Brute force cryptanalysis is highly impossible.

2.Easy to implement as compared to Playfair cipher.

Disadvantages

1.Complex to implement as compared with Ceasar cipher.

2.More time consuming.

5.1.3.Playfair Cipher

It is the best known multiple letter encryption algorithm. Playfair ciphertext, which treats digrams in the plaintext as single units and translated these into units into ciphertext diagrams. It is based on the use of a 5X5 matrix of letters constructed using a keyword.The matrix is constructed by filling in the letters of the keyword. From left to right and from top to bottom. Then fill the remainder of the matrix with the remaining letters in alphabetic order. Here, the letters 'I and J' count as one letter. The plaintext is encrypted two letters at a time, according to the some rules and the rules are-

1.same pair with a filler letter, such as X, so that balloon would be treated as- balX lo on.

2.Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right , with the first element of the row circularly following the last.

3.Two plaintext letters that fall in the same coloum are each replaced by the letter beneath with the top element of that coloumn circularly following the last.

4.Otherwise , each plaintext letter in a pair is replaced by the letter that lies in its own row and the coloumn occupied by the other plaintext letter.

Advantages

1.it is a great advance over simple monoalphabetic ciphers.

2.It is unbreakable.

3.Identification of individual diagram is more difficult.

Disadvantages

1.Complex to implement as compared with monoalphabetic cipher.

Conclusion

In this paper, we have done surveys on three different substitution techniques of cryptography: Ceasar cipher, Monoalphabetic cipher and Playfair cipher.Also, we studied the advantages and disadvantages of each technique in detail. Every technique is having its own features and it works accordingly.

References

[1] PreetiPoonia and PravinKantha, " Comparative study of various substitution and transposition encryption techniques", International Journal of Computer Applications, ISSN: 0975-8887, vol. 145-No.10, July 2016.

[2] S.S.Dhenakaran, M. Ilayaraja, "Extension of playfair cipher using 16X16 matrix", International Journal of Computer Applications (0975 – 888)
Volume 48– No.7, June 2012.

[3] Harinandan Tunga, Arnab Saha, Akash Ghosh, Swashata Ghosh, " Novel Modified Playfair Cipher using a Square Matrix", International Journal of Computer Applications (0975 – 8887) Volume 101– No.12, September 2014

[4] Fairouz Mushtaq Sher Ali, Falah Hassan Sarhan, " Enhancing Security of Vigenere Cipher by Stream Cipher",International Journal of Computer Applications (0975 – 8887) Volume 100– No.1, August 2014

[5] Malay B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition", International Journal of Computer Applications (0975 – 8887) Second National Conference on Recent Trends in Information Security, GHRCE, Nagpur, India, Jan-2014

[6] Orooba Ismaeel IbraheemmAl –Farraji, "
New algorithm for encryption based on substitution cipher and transposition cipher", International Journal of Current Research Vol. 7, Issue, 12, pp.23610-23612, December, 2015

[7] Kashish Goyal, Supriya Kinger, "
Modified Caesar Cipher for Better Security Enhancement",
International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013

[8]. Book of cryptography and network security by William Stallings.

[9] Behroz A.Forozon, Debdeep Mukhopadhyay, " Cyber and Network Security" McGraw Hill education, 2nd Edition.

[10]WWW.google.com