A Survey on Classic Cipher in Cryptography

Payal Chhabra

P.G. Student, Department of Information Technology, College of Technology, G.B Pant University of Agriculture and Technology, Pantnagar, Uttarakhand, India

ABSTRACT: Today, in the admirable growth of internet environment, information security and data security is most challenging aspects that uses in many areas like computers, e-mail and communication. Cryptography is a technique of hiding the information that is recognized as encryption. Security is sharing or transferring of data without any alteration or hacking done by illegal operators. Here, there are several cryptographic algorithms [9] which send the information as cipher text and cannot be unstated by the introducers. Cryptography preserved confidentiality, authentication, integrity, availability and identification and also provide security and privacy of data to the user. Cryptography compromises the necessary protection in contradiction of the data intruders. The plain text is encrypted into a cipher text at receiver site and then cipher text is decrypted into plain text at receiver site for security purpose. In this paper, study of various encryption techniques has conceded out for providing data and information security.

KEYWORDS: Cryptography, Substitution and Transposition techniques, Comparison analysis.

I. INTRODUCTION

The word cryptography is derived from the Greek word in which ‘crypto’ means “hidden or secret” and ‘graphy’ means "writing". In cryptography only those can read and process it for which it is intended. Cryptography [7] is an art and science that protect the information in such a way that only anticipated recipient able to repossess this information. It is very convincing to encrypt the message so that intruder cannot recite the message. Cryptography is an art of hiding information through translating the message. The art of secret writing or hiding information into an unreadable format called cipher text. Only those who keep a secret key can decrypt the message into plain text. The system in which plain text in encrypted at sender side and cipher text is decrypted at receiver side using a unique key is called a Cryptographic system. Steganography and Cryptography are closely related and it also scrambles messages so that they cannot be understood by unauthorized user. According to Kerckhoff's law for cryptography “the superiority of a cryptographic system is only be determined by small part of information called secret key i.e. other information of the system did not give any information about the existence of hidden messages”. Knowledge of the key is mandatory to uncover or identify a message.

Cryptographic systems are characterized into three extents:

1. The type of operations used for transforming plaintext to cipher text. Entirely encryption algorithms are based on two general ethics: first one is substitution, which mapped each element in the plaintext into another element, and another is transposition, which rearranged the elements in the plaintext.

2. The number of keys used. Symmetric, single-key, secret-key, or conventional encryption in which both sender and receiver uses same key. Asymmetric or public key encryption in which sender and receiver uses a different key.

3. The way in which the plaintext is processed. Processes one input block of elements at a time, producing an output block for each input block is called block cipher. Processes the input elements continuously and producing output one element at a time is called stream cipher.
Types of cryptography
Cryptography algorithms play an essential role in information security. It divided into Symmetric and Asymmetric key cryptography.

Symmetric Key Cryptography (Secret Key Cryptography)
In Symmetric key encryption similar key is used for encryption and decryption. The key is circulated before transmission between two parties. Key plays a major role in encryption and decryption process. Uncertainty a feeble key is used in the algorithm then data can be decrypted. The size of the key decides the asset of Symmetric key encryption. In SKC, the sender and the receiver aware with that same secret code or key and messages are encrypted by the sender and decrypted by the receiver through same secret key. It can be of 2 types: Stream Buffer in which digits of a message is encrypted one at a time. Block cipher in which number of bits is encrypted as a single unit.

Asymmetric Key Cryptography (Public Key Cryptography)
In asymmetric key encryption two different keys are used, one key for encryption and another key for decryption and users acquire the Key from a Certificate Authority. Asymmetric key (or public key) encryption solve the key distribution problem. In PKC private keys and public keys are used. For encryption public key is used and for decryption private key is used. Public key is known to public and private key is known to the user.

Objectives of cryptography:
1) **Confidentiality:** Confidentiality is a provision used to preserve the content of information by authenticating the sender and receiver before sending and receiving data. Secrecy is similar to confidentiality and privacy. There are numerous methodologies to providing confidentiality so that no one can recite the message except the intentional receiver. It means that only the genuine people are able to understand the message content and no one else.

2) **Integrity:** Data is free from any kind of modification among sender and receiver so data should be transmit between sender and intended receiver without any alteration being perceived. Data integrity is a service which discourses the unauthorized alteration of data. To guarantee data integrity, one must have the capacity to detect data manipulation by unauthorized parties. Data manipulation comprises such things like insertion, deletion, and substitution. Receiver assuring that the received message has not been altered in any way from the original.

3) **Non-repudiation:** Sender cannot contradict his or her intents in the creation or transmission of the information. Non-repudiation is a service which prevents an entity from denying previous obligations or actions. Once disputes arise due to an entity denying then certain actions were taken, a means to resolve the situation is necessary. It is a mechanism to
prove that the sender really sent this message. Means that neither the sender nor the receiver can untruthfully deny that they have sent a definite message

4) **Authentication**: The sender and receiver confirm each other’s identity. Sender and receiver should be authenticated before sending and receiving data. Authentication is a service associated to identification. This function smears to both entities and information itself. Two parties entering into a communication should identify each other. Information sent over a channel should be authenticated for instance origin, date of origin, data content, time sent, etc.

II. **OVERVIEW OF CLASSICAL SYMMETRIC CRYPTOGRAPHY**

Cryptographic algorithms [6, 2] are classified as classical cryptographic techniques and modern cryptographic techniques. Classical cryptographic techniques are developed in the most primitive days to provide confidentiality to the information. Modern cryptographic techniques are providing enhanced services like confidentiality, authentication, etc., to the information.

**Substitution Techniques**

Substitution ciphers analytically replace letters or groups of letters with other letters or groups of letters.

**Caesar Cipher**: Caesar cipher is also recognized as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most usually known as encryption techniques. In this technique each letter in the plaintext is replaced with the letter standing some fixed number of places further down the alphabet. This substitution cipher was earliest use by Julius Caesar in which only 25 keys to try.

A shift may be of any amount, so that the encryption and decryption algorithm is:

Encryption: \( C = E (p) = (p + k) \mod (26) \) where \( k \) takes on a value in the range 1 to 25.

Decryption: \( p = D(C) = (C - k) \mod (26) \)

For example: \( k=3 \)

Plain text: HELLO

Cipher text: KHOOR

**Monoalphabetic Ciphers**: Caesar cipher is not so protected because of 25 possible keys. A melodramatic increase in the key space can be completed by allowing an arbitrary substitution. A Monoalphabetic cipher customs fixed substitution for each letter of the alphabet over the entire message. Monoalphabetic substitution cipher or simple substitution cipher depend on a fixed replacement structure. Hence, if “a” is encrypted to “B” then every time the letter “a” in the plaintext replace with the letter “B” in the cipher text.

Example:

Plaintext: HELLO MESSAGE

Cipher text: IFMMP NFTTBHF

There are lots of different Monoalphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter.

**Play fair Cipher**: Play fair cipher was the first example of a digraph substitution cipher which is based on the use of a square matrix of 5X5 alphabetic letters arranged in a suitable manner [10]. Following are the steps of play fair cipher:

1. Select a key and place it in the matrix, the remaining letters of English alphabet are then one by one positioned in the matrix of Play fair cipher.

2. Disrupt the plain text into pairs and if a pair is same, then acquaint with a filler letter like ‘x’ after the first letter, otherwise if the pair are reside in the same row of matrix then each letter is interchanged by the immediate right respectively.

3. If the pair of letters is in same column of matrix then each letter is replaced by the immediate below respectively.
**International Journal of Innovative Research in Science, Engineering and Technology**  
*(An ISO 3297: 2007 Certified Organization)*  
*Website: www.ijirset.com*  
*Vol. 6, Issue 5, May 2017*

4. Pair of letters is neither in same column nor in same row then are they replaced with the letter on the same row respectively.  
Example: key=play fair  
```
P L A Y F
I R E X M
B C D G H
K N O Q S
T U V W Z
```  
Plain text: Hide the gold pairing: Hi de the goldx  
Cipher text: bm odzbxdnage

**Hill Cipher:** Another curious multiletter cipher is a polygraphic substitution cipher which is based on linear algebra called Hill cipher. Hill cipher [3] was the first polygraphic cipher in which more than three codes can be performed at one time. This encryption algorithm takes “m” uninterrupted plaintext letters and substitutes for “m” ciphertext letters. The replacement is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, … z = 25). For m = 3, the system can be described as follows:

\[
C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \mod 26  
C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \mod 26  
C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \mod 26  
\]

**Encryption:**  
\[C = KP \mod 26\]

**Decryption:**  
\[P = K^{-1}C \mod 26\]

Example: key=GYBNQKURP  
message= ACT  
<table>
<thead>
<tr>
<th>6</th>
<th>10</th>
<th>20</th>
<th>13</th>
<th>16</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>67</td>
<td>222</td>
<td>319</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>14</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ciphertext is:  
```
2 6 19
```  

**One-Time Pad:** This encryption technique uses a random key which is as equivalent as the message being sent with no repetition. The word “pad” derives from early implementations where the key material was dispersed as a pad of paper, so that the top sheet could be easily decided and cracked once use. This technique is unbreakable or cannot be cracked because of indiscriminate output generated by OTP has no statistical relationship with plaintext and that plaintext is paired with a random secret key or one-time pad. Ciphertext holds no information about the plaintext apart from the maximum possible length of the message; there is ultimately no approach to break the code. In this technique, every bit or character of the plaintext is encoded by its equivalent bit or character from the pad by modular addition. If the key is accurately random as long as the plaintext, then that key is certainly not reused in process and entirely undisclosed, then the resulting ciphertext will be challenging to decrypt or break. It has also been definite that any cipher with the faultless secrecy property must use keys with meritoriously the same requirements as OTP keys.

**Transposition Techniques**  
Transposition techniques [11] rearrange the order of letters in a message and performing some sort of permutation on the plaintext letters to achieve different kind of mapping.

**Rail fence:** Rail fence or zigzag technique is a simplest technique in which the plaintext is written downwards and diagonally on consecutive "rails" of an imaginary fence and then read off as a sequence of rows. For example: Plaintext "meet me after the toga party" with a rail fence of depth 2.

\[m \atilde{e} \tilde{n} \tilde{t} \tilde{e} m \tilde{a} \tilde{t} \tilde{e} \tilde{r} \tilde{t} \tilde{h} \tilde{r} \tilde{t} \tilde{e} \tilde{g}\tilde{y} \tilde{p}\tilde{r}\tilde{t}\tilde{y}\]

Copyright to IJIRSET  
DOI:10.15680/IJIRSET.2017.0605020  
7419
Ciphertext: MEMATRHTGPRYETEFETEOAAT
This sort of thing would be insignificant to cryptanalyze.

**Simple column Transposition Technique**: An extramultifarious technique in which message is written out in a rectangle, row by row, and then read out by column by column, also permute the direction of the columns. Key of the algorithm is the order of the columns.

For example: Key: ZEBRA  permutation: 3 4 2 1 5 6  
Plaintext: come home tomorrow  
Ciphertext: 1 2 3 4 5 6  
c o m e h o =mteowoercmrmoo  
m e t o m o  
row

### Comparison of Various Techniques

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Key Type</th>
<th>Key Size</th>
<th>Attack Type</th>
<th>Developed by</th>
<th>Advantage</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caesar cipher</td>
<td>Substitution</td>
<td>25 keys</td>
<td>Brute force</td>
<td>Julius Caesar</td>
<td>One of the easiest methodologies used in cryptography.</td>
<td>Cracked by brute force attack because of 25 possible selections of key.</td>
</tr>
<tr>
<td>Hill cipher</td>
<td>Substitution</td>
<td>25 keys</td>
<td>Known plaintext attack</td>
<td>Lester S. Hill</td>
<td>Extensively more numerical nature than a portion of the others.</td>
<td>Encrypts identical plaintext blocks to identical ciphertext blocks</td>
</tr>
<tr>
<td>Playfair</td>
<td>Substitution</td>
<td>25 keys</td>
<td>Brute force attack, Frequency analysis</td>
<td>Charles Wheatstone</td>
<td>Convenient since it needs no special tools to use.</td>
<td>There is a minor bit of ambiguity in decryption process.</td>
</tr>
<tr>
<td>Monoalphabeti c</td>
<td>Substitution</td>
<td>-</td>
<td>Known Plaintext Attack</td>
<td>-</td>
<td>Easier to evoke the key phrase than unplanned permutation of letters.</td>
<td>Easy to breakdown since they reflect the frequency data of the original alphabet</td>
</tr>
<tr>
<td>One time pad</td>
<td>Substitution</td>
<td>Equal To plaintext size</td>
<td>Key and ciphertext chosen</td>
<td>Frank Miller</td>
<td>Key is used one and only one time.</td>
<td>Only secure if each key is used to encrypt a single message</td>
</tr>
<tr>
<td>Rail fence</td>
<td>Permutation</td>
<td>-</td>
<td>Known cipher text, Chosen plaintext</td>
<td>-</td>
<td>Letters arranged in a zigzag manner which increase the difficulty of cracking the code.</td>
<td>number of possible solutions are so small that a cryptanalyst can try them all by hand</td>
</tr>
</tbody>
</table>
III. CONCLUSION

After studied all the above definite cryptography techniques it can be concluded that Cryptography provides secure communication, integrity, authentication and confidentiality over an internet. This criticism showed that Caesar cipher is not so good because it gives a difference of 1 bit and it is also seen that Playfair giving better results by giving a difference of 7 bits. The purpose of this paper is to provide the fundamental knowledge about the cryptography algorithms and comparison of available symmetric key encryption techniques based on some parameters like limitation attack, Key factor, pros and cons etc. Symmetric is faster and simpler as compared to asymmetric. The Playfair is significantly harder to break as well as stronger than a Monoalphabetic substitution cipher. The future work can be done in comparative study of various Asymmetric algorithms based on different factors like flexibility, speed, encryption time, scalability, etc. which found out best technique to provide better security to the complicated or unsecured network.

REFERENCES