Various Ciphers in Classical Cryptography

D Venkata Vidya Deepthi\textsuperscript{1}, B Homer Benny\textsuperscript{2} and K Sreenu\textsuperscript{3}

\textsuperscript{1} Asst. Prof., CSE Dept., CRRE, Eluru, W.G.Dist., A.P., India.
\textsuperscript{2} Asst. Prof., CSE Dept., CRRE, Eluru, W.G.Dist., A.P., India.
\textsuperscript{3} Asst. Prof., CSE Dept., CRRE, Eluru, W.G.Dist., A.P., India.

Email Id vvidyadd@gmail.com

Abstract. Data Encryption is often widely used tool to provide security features. It translates the clear text into code such that it can only be accessed with the person who has the appropriate key. The recovery of clear text from such an unscrambled data is deciphering. Enciphering can be implemented by using some substitution technique, shifting technique or even mathematical logics. Application of such types of techniques is difficult to retrieve clear text. In the bygone times, several symmetric key base algorithms have been developed. This paper enlightens and analyzes the substitution ciphers and transposition ciphers. With the comparison of different parameters used in the algorithms give significance of the algorithm.

Keywords— Enciphering, Deciphering, Cipher text and Clear text.

1. Introduction
Cryptography is the dissertation of securely sending raw information to concerned recipient only. The necessity to secure the data has been increased due to the emerging technologies across the networks. Data comprehended to all without any restrictions is nothing but clear text. Cryptanalysis has coevolved together with cryptography and the contest can be traced through the evolution of cryptography. The new ciphers get into limelight from the cons of previous ones and simultaneously new techniques will exist to decipher them. Classical code-breaking integrates analytical reasoning and mathematics. Cryptology underpins cryptography and cryptanalysis. At the Source enciphering has been performed with aid of shared secret key. The recipient performs the deciphering. The algorithms regarding cryptography are analyzed as secret-key cryptography and public key cryptography. This section expound about cryptographic techniques to encipher and decipher the clear text and cipher text respectively.

2. Types of encryption techniques
In cryptography, substitution cipher is a way of enciphering where the clear text is substituted with encrypted text, depending on a constant system. The recipient deciphers the text by performing the inverse substitution whereas in the transposition cipher, clear text is rearranged in a different and complex order, but the alphabets remain unaltered.

2.1. Number of keys includes
There are two types of keys in cryptography referred as public and private keys. The public key is shared between both the sender and receiver. As it is not secret. Private Key is used in situations to decipher where public key is used for enciphering.

Block Cipher and Stream Cipher are the approaches to process clear text. In Stream Ciphers, both enciphering and deciphering happens single bit at a time. In this case, the stream ciphers split the raw information into bits and randomized after that enciphering occurs. In Block Ciphers, block of clear text is enciphered at a time and vice versa. This happens as the unprocessed information is splattered into
blocks. This process is performed on the basis of block length and the key, which are provided for enciphering.

3. Principles of security
Cryptography imparts a lot of security services to data. The services of Cryptography are discussed below:

3.1. Confidentiality
This specifies only the sender and concerned recipient should be able to access the content [9]. Interception causes loss of confidentiality.

3.2. Authentication
The user’s identity and also about the origin of message is guaranteed by authentication. The loss of authentication is fabrication.

3.3. Integrity
If the message is not modified even after the sender has sent it, then the integrity is achieved. Modification causes loss of message integrity.

3.4. Access Control
Access control that should be able to access what. It relates to two areas as role management and rule management. Role management concentrates on user’s side whereas the later on resources side.

3.5. Non-Repudiation
The Sender can’t debunk about the transactions made earlier.

3.6. Availability
Availability emphasizes the resources that are obtainable to authorized parties perpetually. The loss of availability is interruption.

4. Symmetric cipher model
A Symmetric encryption model has following components as in figure 1.

4.1. Plain text
The language in which we enunciate is known as clear text. Clear text signifies the content that can be comprehended by the sender, the recipient and also to all those who have permissions. This is fed into algorithm as input.

4.2. Scrambled Message
The encrypted text can be obtained by coding the clear text using any procedure. The resultant thus obtained is send to other side over network.
4.3. Secret key
This is given as input to encipher the clear text. The key is a string of bits. Depending upon the key we will get different outputs. The techniques used to codify or not depends on the key value.

4.4. Decryption algorithm
Taking the Cipher text along with the key we can be able to retrieve clear text. This process is called as deciphering.

5. Secret key cryptography
In secret-key cryptography only single key is used for both enciphering and deciphering. Obviously both should agree before transmission begins and nobody should know about it. Asymmetric key cryptosystems are slow when compared to Symmetric key cryptosystems. The Classical Enciphering techniques are analyzed in this paper. The facets of enciphering techniques are as follows:

a) Substitution Technique: Each contents of clear message is mapped with other content which can be symbols, alphabets or even blocks. These techniques appertain to replace clear text bit patterns with encrypted text bit patterns. Substitution Ciphers stated in this paper are Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher and Polyalphabetic Cipher.

b) Transposition Techniques: In these techniques, some sorts of transpositions are applied on the clear text, in which they are altered in consistent sequence to get cipher. This technique is referred to as a transposition cipher. The simplest of such ciphers are Rail Fence technique, Column Transposition.

5.1 Types of substitution & transposition techniques

5.1.1. Caesar Cipher. The Caesar Cipher technique is one of the preliminary methods. In this technique, a given text is replaced by a letter with constant number of positions down the letter. Consider a shift of 1, D would be modified by E; E would become F, and so on. Therefore to cipher a given text we need a value, which indicates the number of positions each letter of the text has been progressed. The first step is to transmute the alphabets into numeric where a be zero, b be one and so on up to z.

Mathematically enciphering is given below:

\[ e_n(x) = (x + n) \mod 26 \]

Similarly deciphering is as follows:

\[ d_n(x) = (x - n) \mod 26 \]
Here in the above both cases of enciphering and deciphering alter should be done with n positions.

5.1.2. Monoalphabetic Cipher. The simple substitution cipher depends on precise modification. In the clear text, alphabet matches to dissimilar random cipher text alphabet. Therefore, if ”k” is enciphered to ”s”, then wherever we come across “k” in clear text then it is modified as “s” in the encrypted text.

5.1.3. Playfair Cipher. Draw a Polybius Checker board and also along with it the sender should have a keyword to encipher clear text as in figure 2.

Keyword: QUEST

Using the keyword fill the 5x5 matrix by writing row-by-row. Continue the rest of the spaces with remaining alphabets. Duplication of any alphabet is not allowed. Don’t write I OR J. Pair the clear text, hence GOLD becomes GO LD. Look into the Clear text and follow the instructions. If any two letters are in the same row then write the letters which are besides to the right side of it. If in the same column then replace it with the letter that is down to it. If it forms the rectangle replace it with corner sided ones.

Using the keyword fill the 5x5 matrix by writing row-by-row. Continue the rest of the spaces with remaining alphabets. Duplication of any alphabet is not allowed. Don’t write I OR J. Pair the clear text, hence GOLD becomes GO LD. Look into the Clear text and follow the instructions. If any two letters are in the same row then write the letters which are besides to the right side of it. If in the same column then replace it with the letter that is down to it. If it forms the rectangle replace it with corner sided ones.

GO - HN LD
KE

The resultant cipher text is HNKE.

5.1.4. Hill Cipher. Hill cipher works on multiple alphabets at the uniform time and it is vulnerable to known plain text attack. Each letter is represented by numeric mod 26. The first step is to transmute the alphabets into numeric where a be zero, b be one and so on up to z. To encipher a message, each block of n letters is multiplied by an invertible n × n matrix, against mod 26. To decipher the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for enciphering is the cipher key. In the set of invertible n × n matrices (mod 26), the key is chosen aperiodically.

Cipher text=key * clear text mod 26 where the key is nxn matrix, the plaintext and cipher text are nx1 matrix. 5.1.5. Polyalphabetic Cipher. Polyalphabetic cipher has multitudinous letters to encipher. If two letters are the same in the cipher text it does not mean they must decipher to the same plain text letter.

5.1.6. Rail Fence technique. In this method, the clear text is written diagonally from left to right side onwards. After that look through row after row from left to right and then write it down. Here we consider clear text as college.
Example:

Clear Text: "college"

C l e e

o l g

Cipher text is cleeolg

5.1.7. Row-Column Transpose technique. In the row-column transpose technique we get in touch with the clear text message row-by-row in a rectangular box of definite size and look through columns randomly as in figure 3. If we use with multiple rounds then it will become complex.

Clear Text: willing

Random order 3, 6, 5,1,2,4
Cipher text is lniwgil

6. Different symmetric key Encryption techniques & its comparison table

This paper enlightens and analyzes the substitution ciphers and Transposition ciphers. The technique used in bygone times does not provide Interception but the modern ones are providing the principles of security. The rounds in an algorithm follow the same set of instructions. We can easily understand the processing of round with the block diagram. The analysis of different techniques plays a crucial role in order to select the best one which meets our requirements. To achieve it certain parameters are taken into considerations as shown in table1. Classical encryption techniques are distinguished in Table 1.
| Techniques/Parameter | Caesar cipher | Play fair Cipher | Hill Cipher | Polyalphabetic Cipher | Rail-fence | Columnar transposition |
|----------------------|---------------|------------------|-------------|-----------------------|------------|------------------------|
| Key Type             | 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          | BruteForce attack | Cipher text only(frequency distribution) | Known plain text attack | Cipher text and plain text 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 in 1929 | Leon Battista Alberti in around 1467 | - | - |
| Key Factor (Uniqueness) about the technique | Simple substitution with Alphabet | Use pair of letters and substitute with 5x5 matrix designed with key and remaining alphabets | Based on Linear algebra, Convert plain text into matrix based on ASCII value | Plain text is replaced by another one where it is modified cyclically & it depends on a current position of the modified letter | Plain text is written downwards on successive “rails” of an imaginary fence, then moving up when we get to the bottom rail then read off it in rows | The Plain text 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 Classical Encryption Algorithm pros and cons are enlightened. The techniques used in bygone times provide only confidentiality but the modern ones provides the principles of security. The
analysis of different techniques plays a crucial role in order to select the best one which meets our requirements. With the comparison of different parameters used in the algorithms give significance of the algorithm. The main focus of this paper is to give foundation and analyze cryptographic techniques.

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. Dubey ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile Computing IJCSMC, 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] 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.
[7] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. Dubey ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 8, August 2015.
[8] 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.
[9] Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill Publication company Ltd., New Delhi.