Evaluative Study on Substitution and Transposition Ciphers

[1]Dr. Sumathy Kingslin, [2]R.Saranya,

[1]Associate Professor, [2] M.Phil Research Scholar
[1]PG & Research Dept. of Computer Science,
[1]Quaid-E-Millath Government College for Women (Autonomous), Anna Salai, Chennai 600002, Tamil Nadu, India

Abstract: With fast development over generations, encryption is one of the most trusted approaches for data protection and privacy. Data encryption strategies are meticulously applied in such a way that the original information is recovered easily using a key, referred to as decryption. Encryption can be implemented using techniques like substitution, permutation or by some mathematical operations. By applying any one of these, a cipher text thus generated goes beyond human comprehension and readability. This paper, provides a basic overview of five different substitution and transposition encryption techniques and an analysis of these algorithms based on the effectiveness of each algorithm with regard to the efficiency parameters like encryption time, decryption time, memory utilization and the avalanche effect. All the algorithms are tested using Java 2 Platform Standard Edition Development Kit 5.0.

***Index Terms* – Cryptography, Symmetric Key Encryption, Substitution Ciphers, Transposition Ciphers, Plain Text, Key, Cipher Text, Encryption and Decryption**

I. Introduction

Cryptography is the most trusted and widely practiced information protection mechanism that makes the digital data more secure, reliable and authentic over the anonymous communication channel. The term cryptography is a Greek word which means that "secret writing"[10]. Various sensitive information like banking transactions, credit card information, user profile are being transferred over internet. To protect this kind of data from being hacked and eavesdropped, there is a dire need for security, secrecy and privacy. Cryptography is one such method widely practiced to protect confidential information being sent via insecure network. It converts plain text to cipher text called encryption process and restoring the primary textual content from cipher with the help of a secret key, is referred to as decryption procedure [5]. Cryptography not only protects information it also provides authentication to the user. There are various cryptographic algorithms that are being practiced from simple to complex in nature with each day a new method being evolved. This paper compares the five most popular substitution techniques : Caesar Cipher, Monoalphabetic Cipher, Polyalphabetic Cipher, Playfair Cipher and Hill Cipher and two transposition ciphers: Rail Fence Cipher and Columnar Transposition Cipher. The commonly used terminologies in cryptography are [12]:

- Plain Text: The secret text.
- Cipher Text: The scrambled plain text.
- Key: Used for converting plain text to cipher text. Known only between the sender and the receiver.
- Encryption: Method for changing plaintext to cipher text using key.
- Decryption: Method for converting cipher text back to plaintext using key.
- Cryptanalysis: Also called code breaking. To violate cryptographic security systems and gain access to the contents of encrypted messages mainly to study the weakness of the algorithms.

II. LITERATURE REVIEW

The research to protect data through encryption is constantly evolving. The literature that discusses the results and the performances of common encryption algorithms that are widely practiced are listed in this section. Priyanka Nema et al. discussed some important and mostly useful aspects of various substitution and transposition techniques [1]. Anjlee Verma et al. in their research article describe some famous classical substitution ciphers which include Affine, Atbash, Caesar, Modified Caesar, Baconian, Poly Bius Square, Letter Number ciphers and compare their performances by encoding input files of various sizes [2]. Priyadarshini Patila et al. evaluate DES, 3DES, AES, Blowfish and RSA algorithms based on parameters like entropy, encryption and decryption time and the avalanche effect [3]. Preeti Poonia et al. gives a theoretical comparison of various substitution and transposition techniques [4].

Gaurav Yadav et al. compare AES, DES, Twofish, Blowfish, Diffihellman and RSA algorithm based on different set of parameters like encryption and decryption speed, key length size and throughput performance etc [5]. It was suggested that symmetric key encryption techniques, blowfish and Twofish algorithms give better solution in terms of security, secrecy and privacy. Akash Kumar Mandal et al. analysis the avalanche effect in plaintext of DES using binary codes [9]. Atish Jain et al. enhancing the security of Caesar cipher substitution method using a randomized approach for more secure communication [10]. K.Saranya et al. gives a theoretical comparison of available symmetric key encryption techniques based on some parameters like vulnerability to attack, uniqueness about the technique [11]. B. Padmavathi et al. analyses the performances of DES, AES and RSA Algorithm along with LSB substitution technique [12].

III. ENCYRPTION ALGORITHMS

There are two kinds of encryption methods namely symmetric key encryption and asymmetric key encryption based on the key used for the encryption process.

3.1 Symmetric Key Encryption

In the symmetric key encryption, same key is used for both encryption and decryption process. The sender and receiver must share the algorithm and the key. The key must be kept secret. Substitution and transposition ciphers are uses the symmetric key encryption technique [5].

3.2 Asymmetric Key Encryption

Asymmetric key encryption is the approach, wherein one set of rules is used for encryption and decryption with a couple of keys, one for encryption and one for decryption. One secret key is public and second one is the private key. They are also called as the general public key encryption [5]. For example RSA etc.

.

3.3 Symmetric Key Encryption Techniques

This paper discusses about some of the symmetric key encryption techniques, namely substitution and transposition encryption which are widely used.

3.3.1 Substitution Techniques

The substitution technique is one in which the letters of the plaintext are systematically replaced by other letter or the symbols. Some of the popular substitution ciphers are

1. Caesar Cipher
2. Monoalphabetic Cipher
3. Polyalphabetic Cipher
4. Playfair Cipher
5. Hill Cipher

3.3.1.1 Caesar Cipher

It is one of the simplest encryption techniques and invented by Julius Caesar. Each letter of a given plain text is replaced by a letter some fixed number of positions down the alphabet [1]. Encryption process can be expressed as

$$C = (P + K)\ mod\ 26 \qquad (3.1)$$

Decryption process can be expressed as

$$P = (C - K)\ mod\ 26 \qquad (3.2)$$

Where P is the plaintext, K is the key and C is the cipher text.

3.3.1.2 Monoalphabetic Cipher

In the monoalphabetic cipher each plaintext alphabet is mapped onto a cipher text alphabet [7]. For instance, if ‘S’ is encrypted as ‘Q’, for any number of incidence in that plaintext, ‘S’ will usually get encrypted to ‘Q’.

3.3.1.3 Polyalphabetic Cipher

The Vigenère cipher is probably the fine-recognized instance of a polyalphabetic cipher. The key is also a string formed from alphabets drawn from ‘A’..’Z’. The length of the key is exactly same as the length of the plaintext to be encrypted. For example the length of the plain text is 15 and the secret key is ‘SECRET’ then the key will be ‘SECRETSECRETSECRE’ which is of length 15[1].

3.3.1.4 Playfair Cipher

The Playfair cipher turned into the primary sensible digraph substitution cipher. The method encrypts pairs of letters (digraphs), in place of single letters as inside the easy substitution cipher. This algorithm [1] is based on the use of a 5 × 5 matrix of letters constructed the use of a key-word. A key word, WELCOME in this case, is stuffed in first, and the remaining unused letters of the alphabet are entered of their lexicographic order. The letters I and J count as one letter.

W	E	L	C	O
M	A	B	D	F
G	H	I/J	K	N
P	Q	R	S	T
U	V	X	Y	Z

On every digraph the following subsequent encryption steps are performed [6]:

1. If the digraph includes the identical letter two times then insert the letter "X" among the identical letters, after which hold with the relaxation of the steps.
2. If the two letters appear on the same row inside the rectangular, then update each letter by means of the letter without delay to the right of it within the square.
3. If the two letters seem within the same column within the square, then update every letter via the letter without delay below it inside the square.
4. Otherwise, each plaintext letter in a pair is changed through the letter that lies in its personal row and the column occupied by way of the other plaintext letter.

3.3.1.5 Hill Cipher

The Hill Cipher is a polygraphic substitution cipher using linear algebra. In the Hill cipher each letter corresponds to one unique number, from 0 to 25. Messages are divided into n-letter blocks. Encryption is performed by multiplication of all blocks by one n x n secret matrix, which contains also numbers from 0 to 25. All the results should be modulo 26. In the Decryption procedure one has to divide the cipher text into blocks and multiply them via the inverse of the key matrix modulo 26 [6]. The inverse of the key matrix is calculated as follows

$$K^{-1} = \mathrm{d}^{-1} * adj\ (K) \qquad (3.3)$$

3.3.2 Transposition Cipher

Transposition ciphers are block ciphers that alternate the location (or the series) of the characters or bits of the enter blocks. Transposition ciphers keep the frequency distribution of single letters [1]. The simplest such ciphers are

i. Rail Fence Cipher
ii. Columnar Transposition Cipher

3.3.2.1 Rail Fence Cipher

The plaintext is written as a sequence of diagonals as shown below after which study off as a sequence of rows. The depth of the rail fence forms the key that desires to be exchanged among the communicating events. Suppose depth of the rail fence is chosen to be 4 [1]. Then for encryption, the plaintext “PLEASE KEEP THIS SECRET” is represented as a set of diagonals as follows

```
P  S  E  I  C
  L  E  P  S  R
    E  K  T  S  E
      A  E  H  E  T
```

Encrypted Text: PSEICLEPSREKTSEAEHET

3.3.2.2 Columnar Transposition Cipher

The Columnar transposition cipher is a rearrangement of the characters of the plaintext into columns. The order of the columns then will become the important thing to the algorithm. The order of the columns is considered as a key [1]. For example 3412 is the key, then the plaintext “HE IS A SECRET AGENT ABC” is encrypted as follows

Key	3	4	1	2
	H	E	I	S
	A	S	E	C
	R	E	T	A
	G	E	N	T
	A	B	C	Z

Encrypted Text: IETNCSCATZHARGAESEEB

IV. EVALUATION CRITERIA

Each of the encryption techniques has its own robust and susceptible points. In order to apply a suitable cryptography algorithm to a utility, knowledge concerning performance, power and weakness of the algorithms must be known. Therefore, these algorithms need to be analyzed primarily based on numerous capabilities. This paper, evaluates following metrics under which the cryptosystems may be as compared are defined beneath.

4.1 Key Length

In most cryptographic function, the key length is important security parameters and key management is the important factor to shows the how the data is encrypted [5]. The symmetric algorithm uses a different key length which is longer than asymmetric algorithm. So, the key management is a huge aspect in encryption processing for control operation of the cipher.

4.2 Time Evaluation

Time Evaluation is based on the Encryption and Decryption Time. Encryption time is the time taken to encode a plaintext. Encryption time impacts general execution of the procedure. Encryption time relies upon the length of the plaintext, key size, algorithm complexity and velocity of the processor. Encryption time must be much less influencing the contraption to quick and responsive [3].

Decryption time is the time taken to get better plaintext from cipher text. The decryption time is preferred to be much less much like encryption time to make short and responsive [3]. Encryption and Decryption time are measured in nanoseconds
.

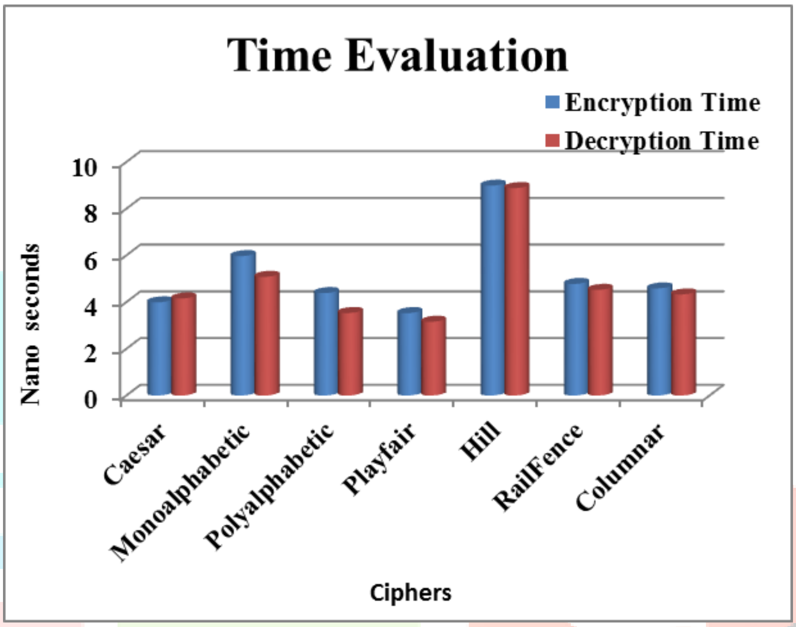

Fig 1: Analysis of Encryption and Decryption Time

4.3 Memory Utilization

Different encryption strategies require one-of-a-kind memory size for implementation. This reminiscence requirement depends on the range of operations to be carried out with the aid of the algorithm, key length used, initialization vectors used and sort of operations [3]. The memory used impacts cost of the gadget. It is suitable that the reminiscence required should be as small as possible. Memory is measured in bytes.

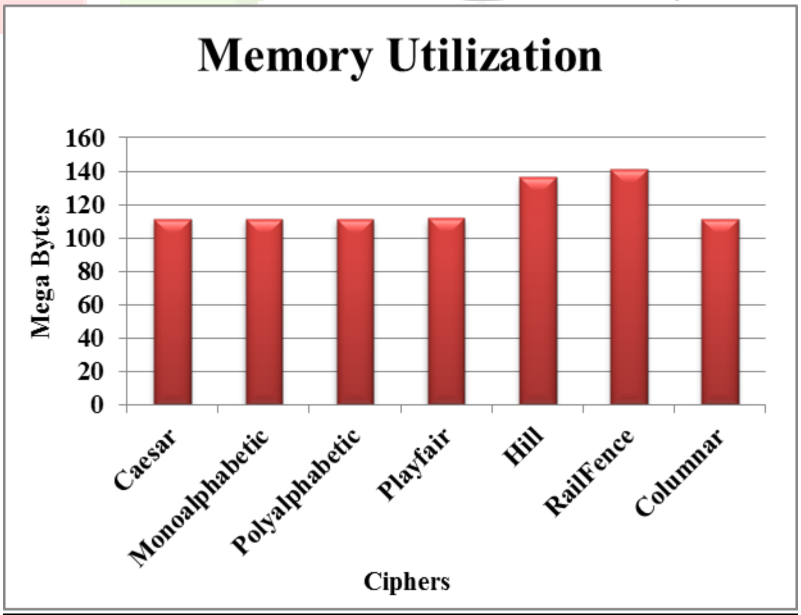

Fig 2: Analysis of Memory Utilization

4.4 Avalanche Effect

A desirable property of any encryption algorithm is that small change in either the plaintext or the key should produce a significant change in the cipher text. In fact, for one bit change in plaintext or key, many bits should change in the cipher-text. This effect is called Avalanche Effect [9].

$$\text{Avalanche Effect} = (\text{No of changed bits in cipher text} \div \text{Total no of bits in cipher text}) \times 100 \qquad (4.1)$$

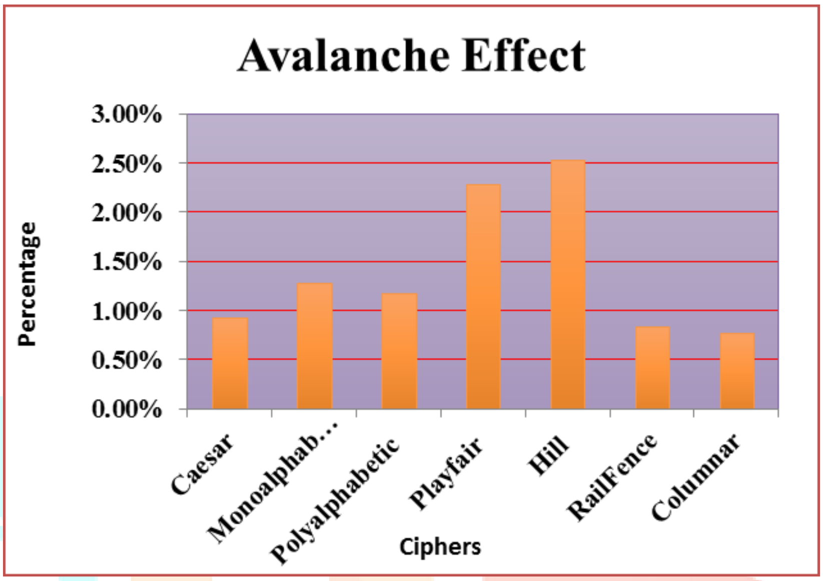

Fig 3: Analysis of Avalanche Effect.

4.5 Strength of the Algorithms

Knowing the set of rules must no longer allow the cipher textual content to be broken. Knowledge of the set of rules ought to no longer reduce the energy of the cipher, but will appreciably lessen the resources required to interrupt the crypto device. A determination of algorithm strength need to think about the fine recognized methods of attack and the period of time required to carry out the ones attacks the usage of modern-day technology.

Table 4.1: Comparison of Substitution and Transposition Encryption techniques

Cipher/Factors	Caesar [4,11]	Monoalphabetic	Polyalphabetic [4]	Playfair [4,11]	Hill [4,11]	RailFence [4,11]	Columnar Transposition [4,11]
Developed By	Julius Caesar	-	Leone Battista Alberti	Charles Wheatstone	Lester S.Hill	Anonymous	Anonymous
Year	19th century	-	1467	1854	1929	-	-
Key Type	Substitution	Substitution	Substitution	Substitution	Substitution	Permutation	Permutation
Encryption Speed	Fast	Slow	Medium	Very Fast	Very Slow	Medium	Medium
Decryption Speed	Medium	Slow	Fast	Very Fast	Very Slow	Medium	Medium
Memory Utilization	Low	Low	Very Low	Medium	High	Very High	Medium
Avalanche Effect	Weak	Medium	Medium	Strong	Very Strong	Weak	Very Weak
Possible Type of Attack	Brute force attack	Cipher text only attack	Cipher text and plaintext known attack	Brute force attack, Frequency analysis	Known plaintext attack	Known cipher text, Chosen plaintext	Known plaintext, chosen cipher text.
Uniqueness about the Ciphers	Simple substitution with alphabet	Single alphabet replacement with fixed substitution	Arrange the letters in 26*26 matrix and perform substitution with	Use pair of letters and substitute with 5×5 matrix	Based on Linear algebra, Convert plaintext	Plaintext is written downwards on successive	The plaintext is written out in rows of a fixed length, and then read

			pair of letters	designed with key and remaining alphabets	into matrix based on ASCII value	"rails" of an imaginary fence, then moving up when we get to the bottom.	out again column by column, and the columns are chosen in some scrambled order.

V.CONCLUSION

Each of the encryption techniques discussed has its very own strong and susceptible points. This paper discusses some crucial and in most cases beneficial components of various substitution and transposition strategies and analyses some important effects which might be very useful in case of security of facts transmission. Based at the experimental results, Playfair cipher and Caesar cipher takes very less encryption and decryption time. From the experiment outcomes, the memory required for implementation is smallest in case of polyalphabetic cipher. After evaluating the algorithms based on Avalanche effect, Hill Cipher scores maximum and hence can be used in applications where confidentiality and integrity is of highest priority. If time and memory is a major factor Caesar cipher, Playfair cipher and the Polyalphabetic cipher are the best suited.

REFERENCES

[1] Priyanka Nema et al. “A Comparative Survey on Various Encryption Techniques for Information Security “, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 11, November - 2013, pp. 725-730

[2] Anjlee Verma et al. “A Comparative Study of Classical Substitution Ciphers” International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 9, September- 2014

[3] Priyadarshini Patila et al. “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish” International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

[4] Preeti Poonia et al. “Comparative Study of Various Substitution and Transposition Encryption Techniques”, International Journal of Computer Applications(0975 – 8887), Volume 145 – No.10, July 2016.

[5] Gaurav Yadav et al. “A Comparative Study of Performance Analysis of Various Encryption Algorithms”, International Conference on Emanations in Modern Technology and Engineering (ICEMTE-2017) Volume: 5 Issue: 3.

[6] William Stallings “Cryptography and network security principles and practice”, fifth edition , 2006 Pearson Education, Inc., publishing as Prentice Hall.

[7] P.S.Gill “Cryptography and Network Security” First Edition 2011, Macmillan Publishers India Ltd.

[8] Atul Kahate “Cryptography and Network Security” Second Edition, Tata McGraw Hill Education Private Limited.

[9] Akash Kumar Mandal et al. “Analysis of Avalanche Effect in Plaintext of DES using Binary Codes” , International journal of Emerging Trends & Technology in Computer Science(IJETTCS) , Volume 1, Issue 3, September – October 2012.

[10] Atish Jain et al. “Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication”, International Journal of Computer Applications (0975 – 8887) Volume 129 – No.13, November 2015.

[11] K.Saranya et al. “A Review on Symmetric Key Encryption Techniques in Cryptography”, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March2014.

[12] B. Padmavathi et al. “A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique”, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 4, April 2013.