Analysis and Comparison of Substitution and Transposition Cipher

[1]K.Renuka devi & [2]G.N.Harshini
[1,2]Master of Engineering
[1]Dept. of Computer Science, [1]Dr.Mahalingam College of Engineering and Technology, Tamilnadu, India

Received: January 31, 2019 Accepted: March 01, 2019

ABSTRACT: *In the cutting edge technology world,sending and receiving secured information is one of the herculeantasks and it demands a staunch concept to root out this issue. Network security is the prevailing concept highly used for protecting information and denies the intruders access. Most used methods to encrypt the given data are substitution and transposition techniques. The prevailing network applications are enlisted as Caesar cipher, Rail fence cipher, Hill cipher, AES and many more. This paper utilizesCaesar cipher and columnar transposition cipher to encrypt, analyze and compare the given data in order to decide which one makes best method to transmit the information in a secure way.*

Key Words: *Substitution, Transposition, Caesar cipher, Columnar Transposition, Encryption, Decryption.*

I. Introduction

The NIST computer security handbook defines the term computer security as, "The protection afforded to an automated information system inorder to obtain the applicable objectives of preserving integrity, availability and confidentiality of information security resources" [1].

Three main objectives of network security includes:

a) Confidentiality:

Only authorized users can access the information being transmitted.

b) Integrity:

Only authorized users can make changes to the information and programs being transmitted.

c) Availability:

The authorized users can make use of all the services provided by the system and permission should not be denied.

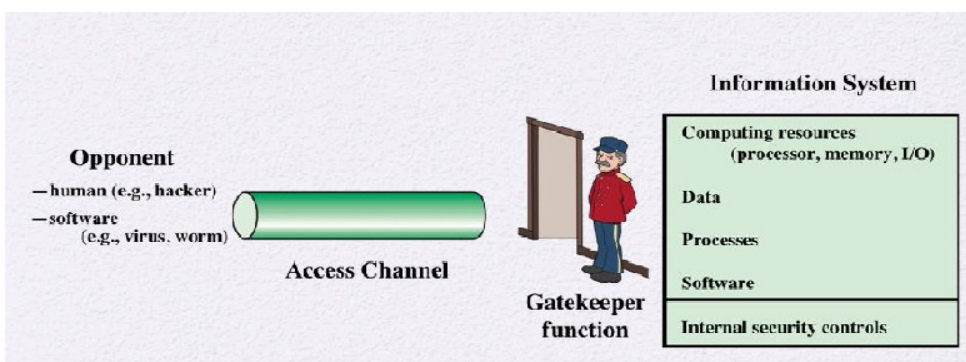

Fig.1 Network Access Security Model

Many organizations adhere to Network Access Security model for protecting the information the networking channel.The two main actors in the communication model are the sender and the receiver. In Figure 1, the opponent (such as hacker or software) accesses the information system through the access channel, while the gate keeper function arrives to protect the system without being hacked. Information System contains many resources such as Processor, Memory, I/O, Software, Data etc.,

Security Attacks:

An attack is an attempt to alter, disable, steal the information or even gain unauthorized access to make use of data being sent through the communication channel. There are different forms of attacks prevails which shows how the intruders access the user's information.

Two types:

Passive attack: The passive attack permits the intruders to utilize the information completely but deny

alteration of system resources.

Categories:

a) Release of message contents.
b) Traffic analysis.

Active attack: The active attack allows the intruders to make use of information and also alter the system resources.

Categories:

a) Masquerade.
b) Replay.
c) Modification of messages.
d) Denial of service.

II. Encryption techniques

In this section, two encryption techniques are to be discussed for encrypting the user's message. Two encrypting techniques include substitution and transposition [2].

a) Substitution technique:

The former one is a cryptographic technique which involves the replacement of given letters of plaintext to the other letters, numbers or symbols."Plain-text bit patterns are replaced by Cipher-text bit patterns".

b) Transposition technique:

The latter one involves some sort of permutation on plaintext letters. There are different kinds of transposition techniques available. One such technique is that "columnar transposition cipher" [10].

a.1 Caesar cipher:

- Caesar cipher is one of the best and most used substitution technique. In comparison to other technique it is more simple and easier to be processed [3,8].
- This involves the replacement of letters of plaintext to the letter that is placed at the key position across the alphabet[11].

Example:
Plain-text: She gave me a book.
Key: 2

Table 1Alphabet

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Cipher-text: vjgicxgogcdqqm

b.1 Columnar Transposition Cipher

- This is one of the complex schemeto process the plain-text.
- The plain-text is written in a rectangle as a row according to the key count and read the message across column with respect to key position [5].

Example:
Plain-text: She gave me a book.
Key: 4 3 1 2 5

Table 2 Transposition technique

4	3	1	2	5
t	r	a	n	s
p	o	s	i	t
i	o	n	e	d

Cipher-text: asnnierootpistd

This technique would be more advantageous by applying several rounds of transposition to improve its security.It cannot be easily reconstructed because of its complex permutation [6].

III. Implementation

a) Caesar cipher:

a.1 Encryption algorithm:

Encryption is the process which reads the plain-text or any other type of data and converts from the readable form to the cipher-text by accessing the given key. It is one of the important method to provide data security and protection of user's information from unauthorized persons [7].

ALGORITHM:

1. Read the block of plain-text(p).
2. Divide the plain-text into letters.
3. Read the sender's secret key(s).
4. Initialize m=0
5. Read the key value(k).
6. Check for plain-text letter position (pos) across the alphabet(n).
7. Add pos with k to get s.
8. Interchange p[m] with n[s].
9. Increment m.
10. Repeat steps 6 to 8.

a.2 Decryption algorithm:

Decryption is the reverse process of encryption. It decodes the data from encrypted data which is of unreadable format. An authorized persons can only be able to make decryption because it requires a secret key.

ALGORITHM:

1. Read the cipher-text(c).
2. Read the receiver's secret key(r).
3. If s = = r, perform decryption.
4. Else go to step 12
5. Initialize i=0
6. Divide the cipher-text into letters
7. Read the key value(k).
8. Check for cipher-text letter position(pos) across the alphabet(n).
9. Subtract k from pos to get s.
10. Interchange c[i] with n[s].
11. Increment i
12. Repeat steps 7 to 9.
13. Exit.

b) Columnar transposition cipher:

b.1 Encryption algorithm:

Encryption is the process which reads the plain-text or any other type of data and converts from the readable form to the cipher-text in accordance with the permutation of order of key.

ALGORITHM:

1. Read the block of plain-text(p).
2. Read the key count(n).
3. Read the key value(k[n])
4. Divide the plain-text into letters.
5. Arrange the plain-text in a matrix as a row according to key count(n).
6. Read the message across column with respect to key position k[n].

b.2 Decryption algorithm:

Decryption is the reverse process of encryption. It decodes the data from encrypted data which is of unreadable format.

An authorized persons can only be able to make decryption because it requires a secret key and makes decryption in accordance with the permutation of order of key.

ALGORITHM:

1. Read the cipher-text(c).
2. Read the receiver's secret key(r).
3. If s = = r, perform decryption.
4. Else goto step 8.

5. Divide the cipher-text into letters.
6. Arrange the cipher-text in a matrix as a column according to key position(k[n]).
7. Read the message across row with respect to key position(k[n]).
8. Exit.

IV. RESULTS

a) Substitution technique:

```
Enter the plain text
hellowar
Enter the secret key
123
h
e
l
l
o
w
a
r

Enter the key
2
Encrypted message
jgnnqyctIt took 4132  milliseconds for encryption

Enter the sender's secret key:
123

Decrypted message:hellowar
It took  5654  milliseconds for encryption
```

Fig.2 Caesar Cipher

The Figure 2 shows the implementation of Caesar cipher in java with the key length as 2 and its secret key as 123.

b) Transposition technique:

```
run:
Enter the plain text
hellowar
Enter the secret key:
123
Enter the key
0
2
3
4
1
h
e
l
l
o
w
a
r
x
x
Encrypted message
hwlrlxoxea
It took  7117  milliseconds for encryption

Enter the sender's secret key
123
Decrypted messagehellowar
It took 8473  milliseconds for encryption
```

Fig.3 Columnar transposition Cipher

The Figure 3 shows the implementation of Columnar transposition cipher in java with key as [0,2,3,4,1] and its secret key as 123.

V. ANALYSIS

a) Encryption:

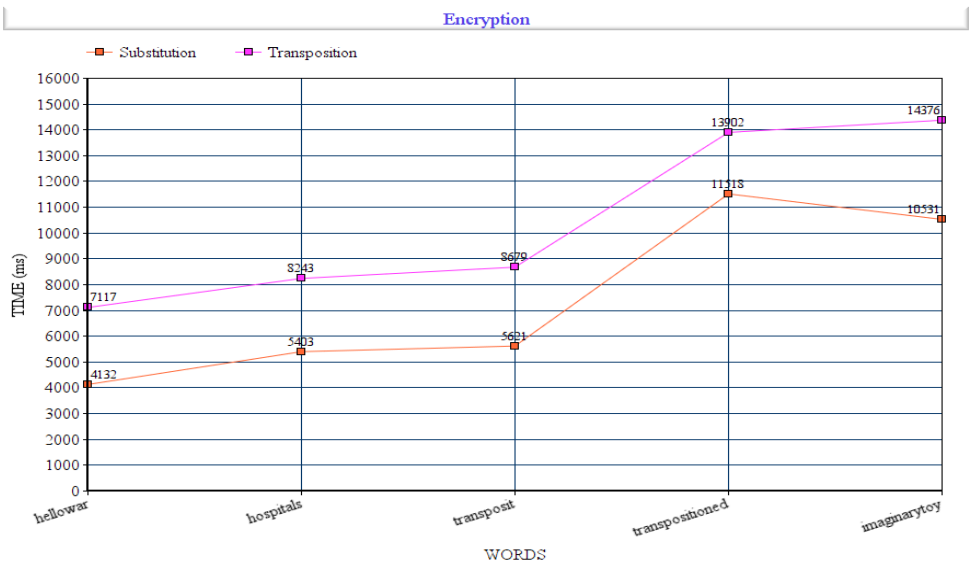

Fig.4 Encryption-time complexity

The Figure 4 shows the time complexity of encryption technique for both substitution and transposition cipher. The encryption time for substitution techniqueis less than that of transposition technique. This shows that encryption technique is simpler for substitution cipher.Eventhough, its encryption time of substitution is less than transposition, it is feasible for intruders to crack the encryption code.

b) Decryption:

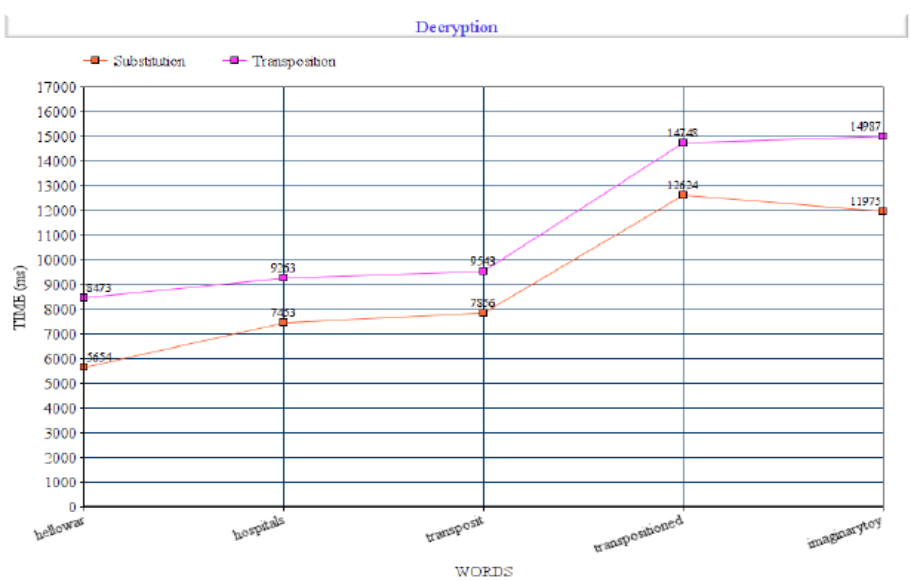

Fig.5 Decryption-time complexity

The Figure 5 shows the time complexity of decryption for both substitution and transposition cipher. The decryption time for substitution is less than that of transposition technique. As both encryption and decryption time of transposition technique is larger than that of substitution technique, it shows that transposition cipher is complex than substitution cipher to crack the code.

c) Comparison of Substitution and transposition techniques:

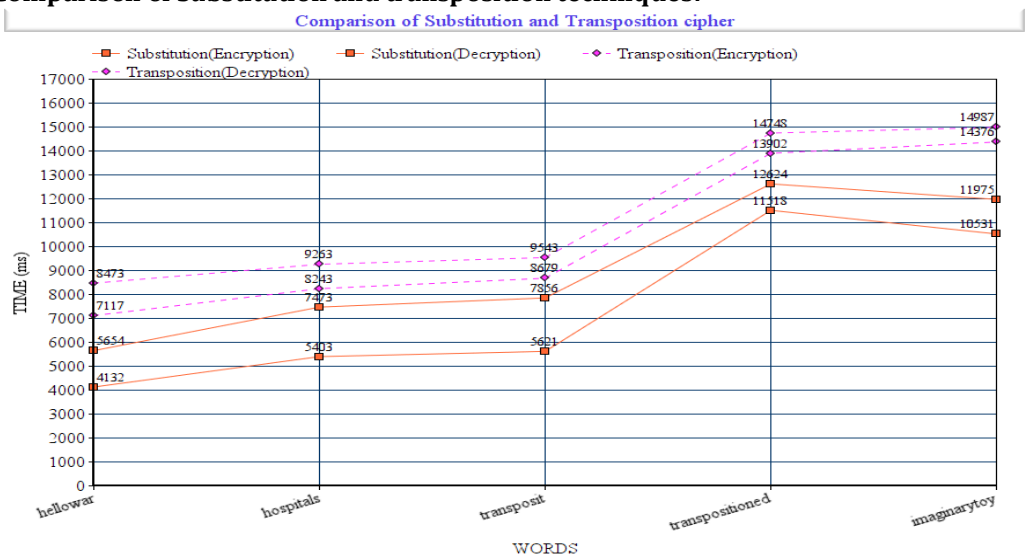

Fig.6 Comparison-time complexity of both Substitution and transposition techniques

The Figure 6 shows the time complexity of encryption and decryption for both Substitution and transposition techniques. The result shows that substitution (i.e.)Caesar cipher holds less time for both encryption and decryption process than that of transposition (i.e.)columnar transposition cipher. The time depends on text size and the key length. This shows that transposition technique is complex for unauthorized persons to break the code.

Table 3 comparison of substitution and transposition technique

Substitution technique	**Transposition technique**
Changes its identity but retain its position.	Changes its position but retain its identity.
Simple process.	Complex than substitution technique.
Easy to crack the code.	Difficult to crack the code.
Unauthorized users can easily access the data.	Difficult for intruders to access the information.
The time complexity of Encryption and decryption is less.	**The time complexity of Encryption and decryption is high.**
Example: Caesar cipher	Example: Columnar transposition cipher.

VI. INFERENCE

- Encryption and decryption holds less time for substitution (i.e.) Caesar cipher.
- Encryption time depends on the key length for both the techniques.
- As encryption is time is less for Caesar cipher, it is easy to crack the code by the unauthorized users.
- Larger the key size, larger the encryption and decryption time.

VII. CONCLUSION

The proposed work makes use of encryption techniques such as substitution (i.e.) Caesar cipher and transposition ciphers
(i.e.) columnar transposition cipher. The encryption time is less for substitution (Caesar cipher) but it paves way for intruders to easily crack the code. The transposition technique is complex as well as secure than substitution technique. So, transposition technique is the best suitable for encrypting the message. As a future work, plan to encrypt the given message through AES algorithm and then perform the transposition technique to improve the security.

References

[1] William Stallings, "Cryptography and network Security:principles and practice"; Pearson Publication, london, pp. 148-183, 2011.

[2] AnjleeVerma, Navjot Kaur.2014. A Comparative Study of Classical Substitution Ciphers. International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 9, pp 360-364.

[3] Falguni Patel, Mohammed Farik. 2016. A New Substitution Cipher - Random-X. International Journal Of Scientific &Technology Research, Vol. 5, Issue 11, pp 125-128.

[4] UmangBhargava, Aparna Sharma, RaghavChawla, Prateek Thakral.2017. A New Algorithm Combining Substitution & Transposition Cipher Techniques for Secure Communication. International Conference on Trends in Electronics and Informatics,pp 619-624.

[5] UvarajArutkumaran.S. 2018. Network Based Cryptographic Techniques. International Journal of Research and Analytical Reviews (IJRAR). Vol 5, Issue 3, pp 96-99

[6] SreeparnaChakrabarti, Dr. G.N.K. Suresh Babu. 2018. A Review On Encryption Algorithms For Secured Data Communication. International Journal of Research and Analytical Reviews (IJRAR). Vol 5, Issue 4. pp 656-663.

[7] Shaikh Abdul Hannan, Ali Mir Arif Mir Asif. 2017. Analysis of Polyalphabetic Transposition Cipher Techniques used for Encryption and Decryption. International Journal of Computer Science and Software Engineering (IJCSSE), Vol 6, Issue 2,pp 41-46.

[8] Gyan Singh Yadav, AparajitaOjha. A Novel Visual Cryptography Scheme Based on Substitution Cipher. Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), pp 640-643.

[9] NishantKambhatla, AnahitaMansouriBigvand, AnoopSarkar. 2018. Decipherment of Substitution Ciphers with Neural Language Models. Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing, pp 869–874.

[10] MassoudSokouti, BabakSokouti, SaeidPashazadeh. 2009. An approach in improving transposition cipher system. Indian Journal of Science and Technology. Vol.2, Issue 8, pp 9-15.

[11] Atish Jain, RonakDedhia, AbhijitPatil. 2015. Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. International Journal of Computer Applications, Vol 129, Issue 13, pp 6-11.

[12] SaritaKumari. 2017. A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science. Vol. 6, Issue 4. pp 20915-20919.