International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 11 | Nov 2022 www.irjet.net p-ISSN: 2395-0072

Text Encryption and Decryption Technique using Columnar Transposition and Substitution

Shruti Gawas

Student, Dept. of Electronics and Telecommunication Engineering,
MKSSS's Cummins College of Engineering for Women, Pune, Maharashtra, India

---

Abstract - *We live in an age of information technology and high connectivity. Viruses, hackers, electronic wiretapping and fraud are inevitable. To be protected, information must be confidential, available, and maintain its integrity. The areas of computer security, data security, and information security design utilize software, hardware, and human resources to address this problem. Recognition of the importance of data security has led to the development of cryptography for practical, ready-to-use applications for enforcing network security. In this paper, I proposed a cipher that encrypts text using substitution, columnar transposition, and rail-fence transposition techniques of the basic encryption. Generation of random numbers and random words make the algorithm more difficult to crack. This eliminates the need for the user to define fixed keys, making the algorithm secure. It also facilitates sending the key to the receiver while appending it to the cipher texts at random locations.*

Key Words: — Cipher, Cipher Text, Information Technology, Security, Encryption, Decryption, Plain Text, Random Number, Substitution, Columnar Transposition, Key.

1. INTRODUCTION

The rise of hackers in our tech-dependent world is not just affecting individual consumers, but businesses and governments as well. With the need to properly organize information about every aspect of our lives, there is absolutely no time when safety can be considered secondary. Information security is a critical issue in today's world.

Over the past three decades, computer networks have revolutionized the use of information. Information is currently distributed. Authorized individuals can send and retrieve information remotely over computer networks. While his three aforementioned requirements - confidentiality, integrity, and availability - have not changed, there are now some new aspects. Not only do we need to keep information confidential, but we also need a way to maintain confidentiality when transferring information from one computer to another. The privacy challenge is using data while protecting individual privacy settings and personally identifiable information. From email to cellular communications, from secure web access to digital cash, encryption is an integral part of today's information systems. As the foundation of modern security systems, encryption protects transactions and communications, protects personally identifiable information (PII) and other sensitive data, authenticates identities, prevents document tampering, and protects servers from tampering, used to establish trust in Encryption is one of the primary tools organizations use to protect systems, including their most important assets (data), whether they are at rest or in motion. Encryption helps provide accountability, impartiality, accuracy, and confidentiality. Prevent e-commerce fraud and ensure the legitimacy of financial transactions. Protect your anonymity or prove your identity. In the future, as commerce and communications continue to move to computer networks, cryptography will become more and more vital.

2. SHORTCOMINGS OF THE PREVIOUS ALGORITHM

- Previous algorithm uses fixed key for encryption which is defined by the user itself. This can be easily decoded by the attacker.
- The sequence of different encryption techniques is fixed which makes the decryption very easy for attacker once the key is known.
- The algorithm uses user defined fixed letter range (e.g. A=1, B=2… Z=26).
- The previous algorithm can only encrypt and decrypt capital letters which can be easily intruded.
- The time complexity of previous algorithm depends on the user defined letter range.

3. MY CONTRIBUTION

The algorithm proposed by me uses the key for encryption which is derived from the message itself. In contrary to this, the previous algorithm required the key to be defined by the user which could have been an overhead for the user. Once the text is encrypted using the key, it needs to be passed on to the receiver's end to be used for decryption. This algorithm uses the concept of random number generation and random text generation in order to improvise the security. The random number generated decides the order of the encryption techniques that needs to be applied on the text. The algorithm uses simple substitution, rail fence

transposition technique and columnar transposition technique. The length of the original message decides the key for encryption. If the length of message is even, the key will be added at the beginning and the notation used for random number will be placed at the end of message else the notation will be stored at the beginning and key at the end. The notation for random number will be zero if it is even and one if it is odd.

The decryption algorithm on the other hand will separate the key and the random number used for the cipher text by counting its length. Once they are separated, the cipher text will undergo decryption rounds on the basis of random number notation.

4. ENCRYPTION ALGORITHM

Step 1: Generate a Random Number R.

Step 2: If R is Even, go to Step 3. Else: go to Step 12.

Step 3: Count the length of String

Step 4: If length is even, go to Step 5. Else go to Step 9.

Step 5: Generate a random word.

Step 6: Apply Columnar Transposition to the plain text using the random word.

Step 7: Calculate key (K) for substitution by looking for Letter at Position n/2 and letter at position (n/2)+1, Calculate decimal ASCII value of (n/2 + (n/2)+1)/2 and go to Step 8.

Step 8: Apply Substitution using formula C=(p+k) mod 254; where C is cipher text , p is transposed text and key K and go to step 19.

Step 9: Calculate Key (K) for substitution by looking for Letter at Position (n+1/2), Calculate a ASCII value by considering NUL(null)=0, SOH(start of header)=2…..DEL(delete)=127. **Step 10:** Apply Substitution using formula C=(p+k) mod 254; where c is cipher text , p is plain text and key K.

Step 11: Apply Rail Fence Transposition Technique on result of Step 10 and go to Step 15.

Step 12: Apply rail-fence transposition to the Plain Text.

Step 13: Apply Columnar Transposition to the result of step 12.

Step 14: Count the length of string.

Step 15: if length is even, go to Step 16. Else go to Step 17.

Step 16: Calculate key (K) for substitution by looking for Letter at Position n/2 and letter at position (n/2)+1, Calculate decimal ASCII value of (n/2 + (n/2)+1)/2 and go to Step 19.

Step 17: calculate Key (K) for substitution by looking for Letter at Position (n+1)/2, Calculate a ASCII value by considering NUL(null)=0, SOH(start of header)=2 …..DEL(delete)=127.

Step 18: Apply Substitution to the result of Step 13 using formula C=(p+k) mod 254; where c is cipher text , p is plain text and key K.

Step 19: STOP

Final Cipher text will be the output of previous Step

5. ENCRYPTION AND DECRYPTION RESULTS

Example: Consider the plaintext message “Encipher$123”. The Encryption and Decryption results produced by the Algorithm are as follows –

- A Random key is generated by random function. Let, key generated be 6. Since the random key is even, columnar transposition technique will be applied first and then substitution will be applied on the plain text.
- Now the length of original string “Encipher$123” is counted, which is 12.
- Since 12 is an even number, the Key is generated using (n/2) + ((n/2) +1) i.e. (12/2=6) and ((12/6) +1 = 7).
- Now the key i.e. letter at position 6 is ‘h’ and letter at position 7 is ‘e’, and key chosen will be 102 (i.e. absolute value of (h (104) + e (101))/2).

For Columnar Transposition, considering random word “TABLES”.

For Columnar Transposition,

(6) (1) (2) (4) (3) (5)

T A B L E S

E n c i p h

e r $ 1 2 3

Result after 1 round of encryption – **nrc$p2i1h3Ee**

Key (k) = 102

Table I. Encryption – Substitution Technique

Original Text	Position in English	C = (p+k) mod 254	Corresponding English Alphabet in C
n	110	(110+102)mod 254 = **212**	**Ô**
r	114	(114+102)mod 254 = **216**	**Ø**
c	99	(99+102)mod 254 = **201**	**É**
$	36	(36+102)mod 254 = **138**	**Š**
p	112	(112+102)mod 254 = **214**	**Ö**
2	50	(50+102)mod 254 = **152**	**~**
i	105	(105+102)mod 254 = **207**	**Ï**
1	49	(49+102)mod 254 = **151**	**—**
h	104	(104+102)mod 254 = **206**	**Î**
3	51	(51+102)mod 254 = **153**	**™**
E	69	(69+102)mod 254 = **171**	**«**
e	101	(101+102)mod 254 = **203**	**Ë**

Final Cipher Text	**Ô Ø É Š Ö ~ Ï — Î ™ « Ë**

For Decryption,

Table II. Decryption

Characters	Position in English	C = |p-k| mod 254	Corresponding English Alphabet in C
Ô	212	|110-102|mod 254 = **110**	**n**
Ø	216	|114-102|mod 254 = **114**	**r**
É	201	|99-102|mod 254 = **99**	**c**
Š	138	|36-102|mod 254 = **36**	**$**
Ö	214	|112-102|mod 254 = **112**	**p**
~	152	|50-102|mod 254 = **50**	**2**
Ï	207	|105-102|mod 254 = **105**	**i**
—	151	|49-102|mod 254 = **49**	**1**
Î	206	|104-102|mod 254 = **104**	**h**
™	153	|51-102|mod 254 = **51**	**3**
«	171	|69-102|mod 254 = **69**	**E**
Ë	203	|101-102|mod 254 = **101**	**e**

Result after 1 round of decryption – nrc$p2i1h3Ee

Length of the encipher text = 12,

Length of the random keyword generated = 6,

Therefore, No. of rows of the matrix = 2 (12/6),

No. of columns = 6

	(6)	(1)	(2)	(4)	(3)	(5)
	T	A	B	L	E	S
(1)	E →	n →	c →	i →	p →	h
(2)	e →	r →	$ →	1 →	2 →	3

Original Text	**E n c i p h e r $ 1 2 3**

6. ADVANTAGES OF THE ALGORITHM

- The algorithm uses simple substitution and columnar transposition technique.
- Since the key is not predefined by the user, and instead generated efficiently on the basis of length of text, it becomes difficult to identify for the outside sources.
- Easy implementation of the algorithm.
- Encryption sequence based on random number generator enhances security.
- Requires less time complexity as compared to the previous algorithm.

7. CONCLUSION

The objective of cryptography is to make it difficult for an eavesdropper to understand the communication. The sequence and technique of encryption depends on the random number which makes it less easy to hack. The keys are random and not pre-defined by the user which makes them difficult to identify. The implementation of algorithm is achieved with simple and compact code which does not lead to large processing delay and time complexity. The algorithm leads to high security for message such that they cannot be interpreted during transfer.

REFERENCES

[1] Behrouz A. Forouzan, "Data Communications and Networking," *Fifth-edition.*

[2] "Encipher - A Text Encryption and decryption Technique Using Substitution-Transposition and Basic Arithmetic and Logic Operation" by Devendra Prasad, Govind Prasad Arya, Chirag Chaudhary, Vipin Kumar- International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2334-2337.

[3] Behrouz A. Forouzan, "Cryptography and Network Security," *Fifth-edition.*

[4] "Logical Description of Encryption and Decryption Technique using substitution-transposition with basic arithmetic and logical operation" by Sumit Pawar, Sumit Chaudhary and Hamid Ali- Golden Research Thoughts ISSN 2231-5063, Vol. 4, Issue-6, Dec 2014.

[5] "A Secure and Fast Approach for Encryption and Decryption of Message Communication" by Ekta Agarwal and Dr. Parshu Ram Pal – International Journal of Engineering Science and Computing, Vol. 7, Issue-5, ISSN- 2321 3361.

[6] "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" by Ezeofor C. J.1, Ulasi A. G.2. International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753, Vol. 3, Issue 12, December 2014.