Rotational Columnar Transposition Algorithm

Bhumireddy Radha Kumari[1], Dr. Ummadi Thirupalu[2]
[1]U.G student, Dept. of Computer Science and Engineering, Audisankara College of Engineering &Technology, Gudur, Andhra Pradesh, India
[2]Associate Professor, Dept. of Computer Science and Engineering, Audisankara College of Engineering& Technology, Gudur, Andhra Pradesh, India

Abstract:

The columnar technique is one of the transposition techniques which is used to secure information by rearranging plaintext characters into a grid based on the key. However, the traditional columnar method has some limitations in protecting information against modern attacks. This paper presents a modification of the columnar algorithm aimed to enhance security by adding a layer of complexity. The modified technique involves rotating the array a number of times, denoted by ‘n’. The ‘n’ value and key are sent to the receiver. The array is then read off in columns, in top-down order according to the keyword, increasing security, even when the attacker knows the key.

Key Words: Cryptography, Encryption, Decryption, Ciphertext, Plaintext, Columnar algorithm, Transposition.

1. INTRODUCTION:

Columnar is a transposition technique [1][2] in which the plain text is read into a 2D array of size determined by the key length and the cipher text is generated by reading the text from top to bottom based on key. However, this algorithm has some drawbacks. Through multiple permutations, the attacker can predict the plain text, which is not so secure.

For example, let’s say

Consider the plain text “this is a sample sentence” with the key “WORDS” (order: 52314)

Then a 2-D array of size 5X4 is created like this as per the given key:

t	h	i	s	
i	s		a	
s	a	m	p	l
e		s	e	n
t	e	n	c	e

Then the cipher text is generated by reading this array from top to bottom according to the key order.

The cipher text is:

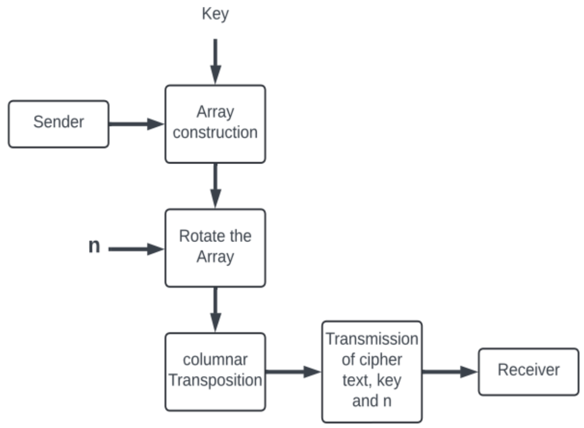
Cipher text=” sapechsa ei msn lnetiset“.

The traditional columnar algorithm has some drawbacks making it vulnerable to attacks [3]. In order to overcome the drawbacks, the algorithm need to be enhanced in such a way that the attacker cannot predict the actual text even after knowing the key.

2. Proposed System:

To further transpose the characters in the plain text, the array is rotated ‘n’ number of times(left-shifted). The value of n is determined by the sender. Then the text from the array is read in a top-down fashion based on the key just like the traditional columnar algorithm. The sender sends the cipher text, key, and ‘n’ value to the receiver.

The algorithm's flow is shown in the flow diagram below.



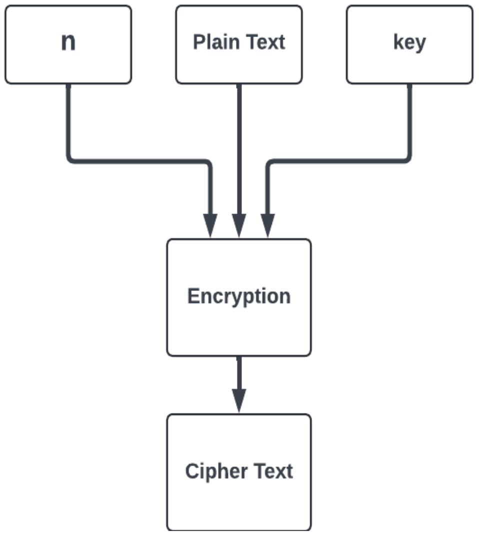
2.1 Encryption:

Plain text is encrypted by taking the plaintext, key, and n.

Plain text: The original message you want to encrypt.

Key: A word or phrase to determine the order of columns.

n: A number provided by the sender, that is used to rotate the array.



Encryption Algorithm:

Step 1: Array Construction

Arrange the plaintext into a grid based on the length of the key.

Step 2: Rotate the Array

Rotate the grid 'n' times. The value of n is chosen by the sender itself.

Step 3: Columnar Transposition

Read the columns in a bottom-up order according to the key.

Step 4: Transmission

Send the cipher text along with the key and value of 'n' to the receiver.

Let us apply this algorithm to the previous example.

Example:

Plain text=" this is a sample sentence"

Key =" WORDS"

Order=52314

Then a 2-D array of 3 rows and 4 columns is created like this as per the given key:

t	h	i	s	
i	s		a	
s	a	m	p	l
e		s	e	n
t	e	n	c	e

Let's rotate this array 3 times, so n=3

Then the resultant array looks like this:

s		t	h	i
a		i	s	
p	l	s	a	m
e	n	e		s
c	e	t	e	n

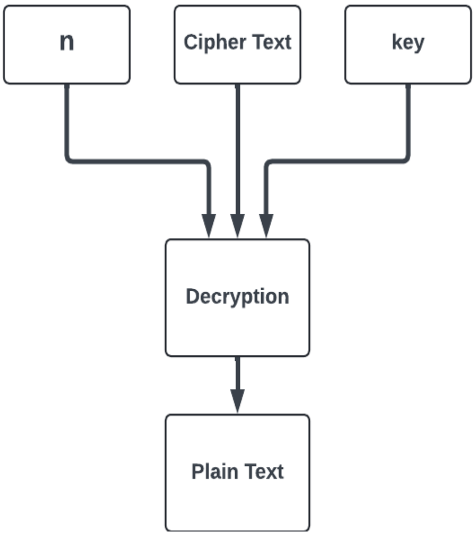
Then the cipher text is generated by reading this array from top to bottom according to the key order.

The cipher text is:

Cipher text= ”hsa e lnetiseti msnsapec “.

2.2 Decryption:

The cipher text is decrypted by using the key and n to produce plain text.



Decryption Algorithm:

Step 1: Array Construction

Arrange the cipher text into an array based on the key.

Step 2: Right shift Array

Right shift the array elements by the value of n times.

Step 3: Read the Array

Read the elements of the array from left to right.

Example:

Cipher text= ” hsa e lnetiseti msnsapec “.

Key =” WORDS”

Order=52314

s		t	h	i
a		i	s	
p	l	s	a	m
e	n	e		s
c	e	t	e	n

The array is right shifted by 3 times.

The resultant array is:

t	h	i	s	
i	s		a	
s	a	m	p	l
e		s	e	n
t	e	n	c	e

Plain text= “this is a sample sentence”

As the array is rotated n times and the value of n is not disclosed, the attacker would not know how many times the array is rotated. Even if the attacker tries to predict the actual text by performing multiple permutations, they would not know the value of n.

In traditional columnar algorithm if the key is known then the information is leaked. But in this Rotational columnar algorithm even if the key is known to the attacker, the attacker still needs to find one more value, that is the value of ‘n’ to decode the message. So, an additional layer of security is added. The information is more secure than the traditional columnar algorithm.

3.CONCLUSIONS:

The proposed enhancement to the traditional columnar algorithm adds an extra layer of security by incorporating an array rotation step. This method effectively addresses the vulnerabilities of traditional transposition techniques, providing a more secure means of protecting sensitive information against cryptographic attacks. Future research may explore further modifications and their impact on the cipher’s security and efficiency.

REFERENCES:

[1] Implementation of Cryptography Technique using Columnar Transposition, Malay B. Pramanik.

[2] Columnar Transposition Cipher: An Introduction, David W. Agler, November 29, 2023.

[3] Attacks on the Transposition Ciphers Using Optimization Heuristics, A. Dimovski1, D. Gligoroski2.