International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 849-853 www.ijaem.net ISSN: 2395-5252

Crptography as a Solution for a Better Security

*Hassan[1], A;Alhassan[2], M. J; Alhassan[3], Y; Sani[4], S;
[1] Department of Mathematics, Usmanu Danfodiyo University, Sokoto
[2]Department of Mathematics, kebbi State University of science and technology, Aliero
[3] Adamu Augie College of Education, Argungu
[4] Department of Computer Science, kebbi State University of science and technology, Aliero

---

Submitted: 01-12-2021 Revised: 11-12-2021 Accepted: 14-12-2021

ABSTRACT: Encryption is the process of scrambling a message so that only the intended recipient can read it. With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Caesar cipher is a mono alphabetic cipher. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter. In this paper, author modified the traditional Caesar cipher using a stacking approach and applying the transposition cipher(G_p)on the encrypted text and get another cipher text there by producing a more complex cipher text, and the decryption process is done in two phases, the first decryption will return the cipher text of the ordinary Ceaser method and the second decryption will return the original plaintext.
Keywords: encryption, decryption, cipher text, stacking, decode, padding.

I. INTRODUCTION

Cryptography was derived from two Greek words "Kryptos" which means "Hidden or Secret" and "Graphein" "to write" which is the art and science of making communication. Cryptography is a method or technique by which a message can be altered so that it becomes meaningless to anyone else but the intended recipient. This is done primarily in two basic ways, one is to change the position of letters or words in a message known as "Transposition" and the other is by substituting letters or words by different ones, known as "substitution" respectively. The science of encryption and decryption can be traced back all the way to year 2000BC in Egypt.

In 2010, using the concept of Catalan numbers the scheme for prime numbers ($p \geq 5$) was developed [7]. And furthermore some new studies on the algebraic theoretic properties were been investigated by [9],[10] and [11], the generating function was defined for $\mathbf{G_p} = \{w_1, w_2, \dots, w_{p-1}\}$for $p \geq 5$ such that $w_i = \left((1)(1+i)_{mp}(1+2i)_{mp} \dots (1+(p-1)i)_{mp}\right)$ where $m_p \coloneqq \text{modulo}_p$. Many algebraic properties of $\mathbf{G_p}$were been investigated.

In this paper, application of $\mathbf{G_p}$on the improved Ceaser cipher were been introduced, where we show that, the classical Ceaser cipher can be made more secure by applying a special transposition cipher on it after encryption function has taken effect on the plaintext and arrived at a complex cipher text that is very hard for Brute force attackers but it will be very easy for the intended receiver to retrieve the plaintext back. Transposition is often combined with the classical cryptographic techniques with the power of computers, substitution and transposition, encryption can easily be performed, and the combination of these two classical techniques provides a more and strong cipher text.

In 2014, the classical Ceaser cipher was been studied and it was been improved using a combine techniques of classical Ceaser and transposition using a random key selection of arranging numbers and produces a more secure cipher text [3],[4].

In 2017, the classical Ceaser cipher was been studied and improved by what is termed as "DIVIDE AND CONQUER APPROACH" and successfully arrived at a cipher of the improved classical Ceaser method [1][2].

Cryptography is divided into two types, Symmetric key and Asymmetric key cryptography. In Symmetric key cryptography single key is used between the sender and receiver, while the Asymmetric key cryptography each user is assigned a pair of keys, a public key and a private key, the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 849-853 www.ijaem.net ISSN: 2395-5252

public key is made known to all members, while the private key is hidden by the user (sender), the sender uses the public key to encrypt the message, while the receiver uses his own hidden (private) key to decrypt the message.
In this work, we consider Symmetric key cryptographic approach.

II. PRELIMINARIES

Let Ω be a non-empty, totally ordered and finite subset of$\mathbb{N}$. Let$\mathbf{G_p} = \{w_1, w_2, \dots, w_{p-1}\}$ be a structure such that each w_i is generated from the arbitrary set Ω for any prime$p \geq 5$, using the scheme

$$w_i = \big((1)(1+i)_{mp}(1+2i)_{mp} \dots (1 + (p-1)i)_{mp}\big)$$

Then each w_i is called a cycle and the elements in each w_i are distinct and called successors.

Example

Using the above setting, if p=5, then we have $\mathbf{G_5}$as

$\mathbf{G_5} = \{(\mathbf{12345}), (\mathbf{13524}), (\mathbf{14253}), (\mathbf{15432})\}$

Since 0 and 5 in modulo5 are equivalent, thus instead of using 0 in modulo_p we will be using p.

Cipher: - is a systematic mathematical method for encryption and decryption.

Encryption: - is the process of encoding a message or information in such a way that only authorized parties can access the meaning of the unreadable text (ciphertext).

Decryption: - is the process of transforming the ciphertext into a plaintext.

Plaintext: - is the original text from the sender's end.

Ceaser cipher: - Ceaser cipher shifts all the letters in a piece of text by a certain number of places, the key for this cipher is a letter which represents the number of places for the shift, the encoding process (encryption) can mathematically use modulus operation by converting the letters into numbers as in the table below.

Table 1

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

The encryption process is given by

$$C = E(K, P) = (P + K) \bmod 26$$

While in the process of solving the code (decryption), the decryption is given by

$$P = D(K, C) = (C - K) \bmod 26$$

Where **C** is the ciphertext, **E** is the encryption function, **P** is the plaintext and K is the key.

Padding: - padding is the addition of characters in the encryption process if the letters are scarce, the padding letter is usually X.

KEY: - a key is a relatively small logical amount of information that is used by an algorithm to customize the transformation of a plaintext into the ciphertext and vice versa during the encryption and decryption process.

TRANSPOSITION CIPHER: - ciphertext is obtained by interchanging the position of each or some of the letters of a plaintext.

Example of transposition cipher is as follows.

Plaintext: **COMPRESSING**

The result of transposition cipher from

Table 2

1	2	3	4	5	6	7	8	9	10	11
C	O	M	P	R	E	S	S	I	N	G

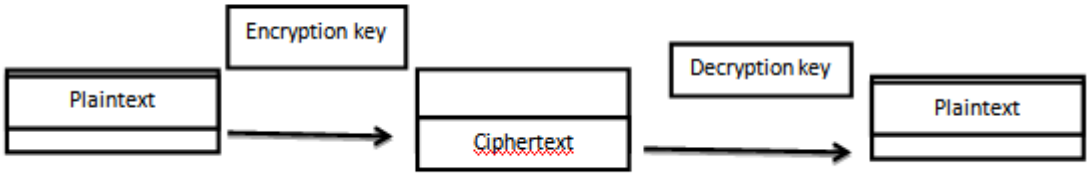
To the transposition below is

Table 3

1	3	5	7	9	11	2	4	6	8	10
C	M	R	S	I	G	O	P	E	S	N

The above table gives the result of the transposition.
The cipher text is "CMRSIGOPESN".

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 849-853 www.ijaem.net ISSN: 2395-5252



The above diagram represents Encryption and Decryption process of a Symmetric key cryptography.

III. RESULT AND DISCUSSION.

Encryption and decryption process through two processes. In the encryption process, the plaintext will be encrypted twice with the Ceaser cipher and Transposition cipher algorithm, different keys will be used for the two encryptions because the two algorithms are different and also in order to make the cipher text more secure from attackers. So different plaintext, different key.
$\mathbf{C_i}$:=Multiple cipher texts.

The encryption process will take the following steps.
(i) Apply encryption function of the Ceaser cipher on the plaintext (P) to produce ciphertext (C_0).
(ii) Stack the C_0 to produce C_1
(iii) Apply encryption function of G_p on C_1 to produce C_2, where the C_2 is the ciphertext to be sent to the receiver.

The decryption process will use the following steps.
(i) Apply the decryption function of G_p on C_2 to produce stacked ciphertext (C_1).
(ii) Reverse the stacking process to produceC_0.
(iii) Apply Ceaser decryption function on C_0 to produce the original text (plaintext)

ILLUSTRATION.
PLAINTEXT: - "WAIT FOR SIGNAL DON'T ATTACK"

ENCRYPTION STAGE:
(i) Apply the encryption function of the Ceaser cipher on the plaintext.

$$C_0 = E(K, P) = (K + P) \bmod 26, \quad k = 3$$

C_0: ZDLW IRU VLJQDO GRQW DWWAFN

(ii) Stack C_0 to produce C_1. C_1: NFAWWDWQRRGODQJLVRIWLDZ
(iii) Applying encryption function of Gp on C_1(p=23, number of characters and p is always a prime, if p is not a prime, then we pad the letters to the nearest prime)

$$G_{23} = \{w_1, w_2, w_3, \dots, w_{22}\}$$

Where w_1 is

Table 4

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
N	F	A	W	W	D	W	Q	R	R	G	O	D	Q	J	L	V	R	I	W	L	D	Z

The above table gives the arrangements of code in the transposition waiting for the execution process using transposition (G_p)

C_2: $w_1 \rightarrow w_{1+i}$, $i < p - 1$, leti $= 2$. (where i=2 represents the selected key from the range of i's)
C_2:$w_1 \rightarrow w_3$
Where w_3 is

Table 5

1	3	5	7	9	11	13	15	17	19	21	23	2	4	6	8	10	12	14	16	18	20	22
N	A	W	W	R	O	Q	L	U	I	L	Z	F	W	D	Q	G	D	J	V	R	W	D

The table above gives the cipher text of the second encryption using transposition (G_p) the code will then be written down and send to the receiver, the code to be sent is given below
The ciphertext is "NAWW ROQL UILZF WD QGD JV RWD"

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 849-853 www.ijaem.net ISSN: 2395-5252

DECRYPTION STAGE:

(i) Apply the decryption function of **Gp on** the C_2 to produce C_1

$C_1^{'}:\ w_{1+i} \rightarrow w_1$

Where w_3 is

Table 6

1	3	5	7	9	11	13	15	17	19	21	23	2	4	6	8	10	12	14	16	18	20	22
N	A	W	W	R	O	Q	L	U	I	L	Z	F	W	D	Q	G	D	J	V	R	W	D

The table above shows the arrangement of letters waiting for the receiver to start the decoding the code, when the key is imputed correctly then the code will transform tow_1, we have the following transformation of w_1

Table 7

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
N	F	A	W	W	D	W	Q	R	R	G	O	D	Q	J	L	V	R	I	W	L	D	Z

The above table gives the reverse of the process of table 5 using decryption algorithm of the transposition (G_p) process.

(ii) Reverse the stacking process to produce C_0:- "ZDLW IRU VLJQ DOGR QWDW WAFN"

(iii) Apply Ceaser cipher decryption function on C_0 to produce **P.**

P: "WAIT FOR SIGNAL DON'T ATTACK"

IV. RESULT AND DISCUSSION

Encryption and decryption process goes through 3 processes, in the encryption stage, the original text(plaintext) will be encrypted twice together with the stacking process which is the improvement of the classical Ceaser cipher technique code after encryption function of the Ceaser cipher is been applied and finally a special transposition cipher is then be applied to the stack result there by producing an alphabetic ciphertext which is more complex for Brute force attackers but simply be decrypted for the intended recipient.

Mathematically the process of encryption and decryption are as follows.

$C_0 = E(K, P) = (K + P) \bmod 26$, Encryption stage of the Ceaser cipher.

$P = D(K, C) = (C - K) \bmod 26$ Decryption stage of the Ceaser cipher.

C_2: $w_1 \rightarrow w_{1+i}$, Encryption state of **Gp.**

$C_1^{'}:\ w_{1+i} \rightarrow w_1$, Decryption stage of **Gp.**

C_1,Is the result of the stack.

V. CONCLUSION AND SCOPE OF FUTURE WORK

Data security is a very important aspect, the formulation of keys in a cryptography plays an important role in designing ciphers, this paper presents modified Ceaser cipher, it is a substitution cipher, the use of internet and network is fast growing, therefore there are more requirements to secure data that is been transmitted all over different networks that uses different services. To provide the security to the network and data different encryption techniques are used, in this paper Ceaser cipher technique is used for security. It is unique on its own way; security provided by this algorithm can be enhanced further, if more than one algorithm is applied to data. Future work will explore this concept of Ceaser and **Gp** combination to a more complex ciphertext which produces an **alphanumeric** ciphertext which is more secure for data storage and retrieval.

REFERENCES

[1]. Pooja S and Pintu S. (2017), Enhancing security of Ceaser cipher using "Divide and Conquer Approach". International Journal of Advance Research in Science andEngineering. **06**(02):144-150.

[2]. Fahrul I, K., Hassan F, S., Toras P and Rahmat W. (2017), Combination of Ceaser Cipher Modification with Transposition Cipher. Advances in Science Technology and Engineering Systems Journal. **2**(5): 22-25.

[3]. Rajput Y., Naik D. and Mane C. (2014), An improved cryptographic technique to encrypt Text message using double encryption. International Journal of Computer Applications**86**(6):24-28.

[4]. Shahid B. D. (2014), enhancing the security of Ceaser cipher using double substitution method. International Journal of Computer Science and Engineering Technology.**5**:772-774.

[5]. Kashish G and Supriya K.(2013) Modified Ceaser Cipher for a Better Security Enhancement. International Journal of Computer Application.**73**:26-31

[6]. Mishra A. (2013), Enhancing security of Ceaser cipher using different methods.International Journal of Research in Engineering and Technology **2**(09):327-332.

[7]. Garba A. I and Ibrahim A. A. (2010), A new method of constructing a Variety of Finite Group Based on some succession scheme. Internal Journal of Physical Science, **2**(3):23:26.

[8]. Massoud S., Sokouti B. and Saeid P. (2009), An Approach in Improving Transposition cipherSystem. Indian Journal of Science and Technology. **2**(8):9-15.

[9]. Ibrahim A. A; Garba A. I; Alhassan M. J; Hassan A. (2021), Some Algebraic Theoretic Properties on Gamma 1 Non Deranged Permutation, IOSR journal of mathematics, 17:58-61.

[10]. Garba A.I, Zakari, Y. and Hassan, A. (2019), on the fuzzy nature of constructed algebraic structure G_p. Bayero Journal of Pure and applied sciences,12(1):146-150

[11]. Garba A. I, Yusuf A and Hassan A. (2018), Some Topological Properties of a Constructed Algebraic Structure. Journal of the Nigerian Association of Mathematical Physics, 45:21-26