Quest Journals
Journal of Research in Applied Mathematics
Volume 7 ~ Issue 10 (2021) pp: 08-12
ISSN(Online) : 2394-0743 ISSN (Print): 2394-0735
www.questjournals.org

Research Paper

A Combined Technique of an Affine Cipher and Transposition Cipher

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

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. Affine cipher is a mono-alphabetic substitution cipher, wherein each later in an alphabet is mapped outs number equivalent, encrypted using a simple mathematical function and decrypted back to a letter. In this paper, authorsuses an Affine cipher technique for the first encryption and later apply 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 Affine method and the second decryption will return the original plaintext.*

KEYWORDS: *encryption, decryption, cipher text, plaintext, transposition.*

Received 20 September, 2021; Revised: 03 October, 2021; Accepted 05 October, 2021 © The author(s) 2021. Published with open access at www.questjournals.org

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.

Cryptography is the study of methods for sending messages in secret (namely, in enciphered or disguised form) so that only the intended receipt can re-move the disguise and read the message (or decipher). Cryptography has, as its etymology, kryptos from the Greek, meaning hidden, and graphein, meaning to write. The original message is called the plaintext, and the disguised message is called cipher text. The original message, encapsulated and sent, is called cryptogram. The process of transforming plaintext into cipher text is called encryption or enciphering. The reverse process of turning cipher text into plaintext, which is accomplished by the recipient who has the knowledge to remove the disguise, is called decryption or deciphering. On the other hand, the study of mathematical techniques for attempting to defeat cryptographic methods is called cryptanalysis. Those practicing cryptanalysis (usually termed the "enemy") are called cryptanalyst. The term cryptology is used to embody the study of both cryptography and cryptanalysis, and the practitioners of cryptology are cryptologist. The etymology of cryptology is the Greek kryptos meaning hidden and logos meaning word. Also, the term cipher (which we will use interchangeably with the term cryptosystem) is a method for enciphering and deciphering. Later in this section we will mathematically formulize the notion a cryptosystem.

A "substitution" cipher replaces plaintext symbols with other systems to produce cipher text. As a simple example, the plaintext might be QZYZXW when a,c,e,l,p are replaced by Z,X,W,Y,Q, respectively. With a "transposition" cipher, we permute the places where the plaintext letters sit. What this means is that we do not change the letters but rather move them around, transpose them, without introducing new letters. Here is a simple illustration. Suppose that we have thirteen letters in our plaintext, and the following is a permutation that tells us how to move the thirteen positions around. The way to read the following is that the symbol in the position number in the top row gets replaced by the symbol in the in the position number below it in the second raw.

$$\begin{pmatrix} 1\ 2\ 3\ 4\ \ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13 \\ 1\ 2\ 3\ 4\ 10\ 7\ 8\ 9\ 5\ 6\ \ 11\ 12\ 13 \end{pmatrix}$$

Now, suppose our plaintext is the jurisdictions. Then the cipher text will be juriictsdons. Notice that the first four and last four of three plaintext letters remain in the same position as dictated by the above permutation, but the s in position 5 gets replaced by i in position 10, then d in the position 6 gets replaced by i in position 7 and so on, so this an easy-to-understand method of depicting transposition ciphers depend upon the permutation given, such as the one above, so often transposition ciphers are called permutation ciphers. Although the ancients Greeks made no claim to actually using any of the substitution on ciphers that they invented, the first use in both military and domestic affairs of such ciphers is well documented by Romans. In the lives of the twelve Ceasers. If there was occasion for secrecy, he wrote in ciphers, that is, he uses the alphabet in such a manner, that not a single word could be made out. The way to decipher those ciphers was to substitute the fourth for the first letter, as d for a, and so for the other letters respectively. What is been described here is a simple substitution cipher used by Julius Ceaser. He used them not only in domestic affairs but also in his military affairs as he documented in his own writing of the Gallic wars.

Permutation pattern have been used in the past decade to study mathematical structures. For instance Audu (1986), Ibrahim (2006) studied the concept of permutation pattern using some elaborate scheme to determine the order of precedence and the position of each of the elements in a finite set of prime size. Similarly an idea of an embedment as an algebraic structure has yielded some interesting results by Ibrahim (2005). Garba and Ibrahim (2010), studied the structure and developed a scheme for the range of such cycles and use it to investigate further number theoretic and algebraic properties of$\boldsymbol{G}_P$.

Furthermore, a group theoretical properties of $\boldsymbol{G}_{\boldsymbol{p}}'$was also investigated by Garba and Abubakar (2015), the concept of fuzzy nature and of $\boldsymbol{G}_{\boldsymbol{p}}'$ alpha-level cut has also been studied by Aremu, Ejima and Abdullahi (2017), and the fuzzy nature and modified fuzzy membership function on $\boldsymbol{G}_P$ was investigated by Garba, Zakari and Hassan (2019) and also some algebraic theoretic properties were also been investigated by Garba(2018) and Ibrahim(2021).

Azzam and Sumarsono (2017), study combine technique of Hill cipher and Ceaser cipher and arrived at a secure cipher text since the two algorithms are combined. And Sriramoju Ajay Babu.(2017), build a prototype of data security (cryptography) for passwords using a modified method of affine ciphers and cryptography password is encrypted and decrypted using a modified method of affine cipher.

In view of the above comes the motivation for this research, where we will use the nature of$\boldsymbol{G}_P$ on the combined technique of affine cipher and transposition cipher on$\boldsymbol{G}_P$.

II. PRELIMINARIES

Let Ω be a non empty, totally ordered and finite subset of N. Let $\boldsymbol{G}_{\boldsymbol{P}} = \{\boldsymbol{\omega}_{\mathbf{1}}, \boldsymbol{\omega}_{\mathbf{2}}, \boldsymbol{\omega}_{\mathbf{3}}, \dots \boldsymbol{\omega}_{\boldsymbol{p}-\mathbf{1}}\}$be a structure such that each $\boldsymbol{\omega}_{\boldsymbol{i}}$ is generated from the arbitrary set $\boldsymbol{\omega}$ for any prime **p≥5**, using the scheme$\boldsymbol{\omega}_{\boldsymbol{i}} = ((\mathbf{1})(\mathbf{1}+\boldsymbol{i})_{\boldsymbol{mp}}(\mathbf{1}+\mathbf{2}\boldsymbol{i})_{\boldsymbol{mp}} \dots (\mathbf{1}+(\boldsymbol{p}-\mathbf{1})\boldsymbol{i})_{\boldsymbol{mp}})$then each $\boldsymbol{\omega}_{\boldsymbol{i}}$is called a cycle andthe elements in each$\boldsymbol{\omega}_{\boldsymbol{i}}$ are distinct and called successors.

2.1 **Modular Arithmetic**

A modulo of one number in terms of another (i.e. *a mod b*) for*a,b* integers, means that, if
a number *a* is divided by *b* gives another number and a remainder then the remainder is the answer. If *a mod b =r,* then it implies that *ab = c+r.* Example. *80 mod 26=2.*

2.2 **Modular Inverse**

In modular arithmetic a number a has a modular inverse a^{-1} for a number m if $(a.a^{-1})mod_m$ =1. The table below shows all the possible modular inverses of mod_{26}

Table 1

A	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

for instance the modular inverse of *9* is *3* since *9 × 3 = 27*, and *27mod26=1.*

2.3 **Cipher**

Cipher is a systematic mathematical method for encryption and decryption.

- **Plaintext** is the original text
- **Encryption** is the process of encoding a message or information in such a way that only authorized parties can access it, and those who are not authorized cannot.
- **Decryption** is the process of transforming the cipher text into a plaintext

2.4 **Affine Cipher**

Affine cipher is a monoalphabetic substitution cipher, wherein each later in an alphabet is mapped touts number equivalent, encrypted using a simple mathematical function and decrypted back to a letter. After a simple scheme is used. The table below shows the place values of alphabets in affine cipher substitution.

Table 2

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

Encryption Function.
E (c) = $(ap + b)_{modm}$
Where,
c = Cipher text… as a number
p = Plaintext Character… as a number
m = Size of the alphabets
a => any number 1 ≤ a ≤ m… great common divisor of (a, m) = 1
b = any number 1 ≤ b ≤ m
Decryption Function.
p = $a^{-1}(c - b)_{modm}$
c = Cipher text… as a number
p = Plaintext Character… as a number
m = Size of the alphabets
b = any number 1 ≤ b ≤ m
a^{-1} = Inverse of a.

2.4 **Padding**

Padding is the addition of characters in a permutation when the letters are scarce.

2.5 **Key**

Key A relatively small amount of information that is used by an algorithm to customize the transformation of plain text into the cipher text during encryption or decryption.

III. RESULT AND DISCUSSION.

Encryption and decryption process through two processes. In the encryption process, the plaintext will be encrypted twice with the Affine 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.

Mathematically the process of encryption and decryption for the affine cipher we have

$$E(c) = (ap + b)_{modm} = C_1$$

$$D(p) = a^{-1}(c - b)_{modm}$$

Now encrypt the plaintext to get the cipher text, we arrived atC_1 we take it our ciphertext, then we apply G_P transposition on the ciphertext and result to new cipher text C_2.

ENCRYPTION ON G_P

Since $\boldsymbol{G}_P = \{\omega_1, \omega_2, \omega_3, \dots \omega_{p-1}\}$ then for the encryption process we can define a relation:

$$C_2 : \omega_1 \rightarrow \omega_{(1+i)} \qquad \text{Where } i < p-1$$

Where

$$\omega_1 = C_1$$

DECRYPTION ON G_P

Since $\boldsymbol{G}_P = \{\omega_1, \omega_2, \omega_3, \dots \omega_{p-1}\}$ then for the decryption process we have:

$$P : \omega_{(1+i)} \rightarrow \omega_1$$

ILLUSTRATION

Encryption stage let
p = "PLEASE CALL ME"
$C_1 = MCUHNUZHCCLU$
C_1 =is the first ciphertext.

Then this result of Affine cipher is encrypted with $G_p$transposition with i=1 as a key to the transposition in order to arrived at $w_{2,}$ sincethe result of the just concluded algorithm is 12 and our w_2 requires 13 characters then the (plaintext=c_1)will be padded with a letter "X" so that it can execute as usual.
$C_1 = MCUHNUZHCCLU$

$C_2 : \omega_1 \to \omega_{(1+i)}$ Where $i<$ *p-1*and also$\omega_1 = C_1$
Whereω_1, $\omega_{(1+i)} \in \boldsymbol{G}_P$ and *p* is the number of letters in a text and also *p*is always a prime, we pad letter “X” to make the number prime.
$C_2 : \omega_1 \to \omega_{(1+i)}$*leti=1where i< p-1 then*
Workingwith$\boldsymbol{G}_{13} = \{\omega_1, \omega_2, \omega_3, \dots \omega_{12}\}$,
$\omega_1 = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13)$

Table 3

1	2	3	4	5	6	7	8	9	10	11	12	13
M	C	U	H	N	U	Z	H	C	C	L	U	X

And$\omega_2 = (1, 3, 5, 7, 9, 11, 13, 2, 4, 6, 8, 10, 12)$, using w$_2$ as our new transposition then the table below shows how the transposition works.

Table 4

1	3	5	7	9	11	13	2	4	6	8	10	12
M	U	N	Z	C	L	X	C	H	U	H	C	U

$C_2 = MUNZCLXCHUHCU$
The above C$_2$ gives us the final cipher text which is to be sent to the receiver, and the receiver will then request for the two keys which he will use to decode the coded message.

Decryption stage
In the decryption state, the receiver after receiving the two keys for the Transposition and an Affine algorithm, then start with the transposition decryption algorithm which is given by the equation below.
$C_1 : \omega_2 \to \omega_1$
The table below shows the w$_2$ which is the second cipher text of which the receiver has received.

Table 5

1	3	5	7	9	11	13	2	4	6	8	10	12
M	U	N	Z	C	L	X	C	H	U	H	C	U

$C_1 : \omega_{(1+i)} \to \omega_1$
$\omega_1 = C_1$

$$C_1 = MCUHNUZHCCLU$$

The above code is the result of first decryption method, the code will then be decrypted using decryption algorithm of an Affine cipher.

Table 6

M	C	U	H	N	U	Z	H	C	C	L	U
12	2	20	7	13	20	25	7	2	12	11	20

The table above uses alphabet arrangements under Affine algorithm and will be used to find the Plaintext message.
Using this equation p = $a^{-1}(c-b)_{modm}$ to Decrypt the cipher texts, we arrived at

Table 6

P	L	E	A	S	E	C	A	L	L	M	E
15	11	4	0	18	4	2	0	11	11	12	4

The above table gives us the original message of which the sender sends to the receiver.

IV. CONCLUSION

From the above explanation, it is known that the original plaintext and final cipher text have different number of characters and in the process occurs two times encryption where each process occurs with a cipher text. So, the result of cipher text is very complex and to solve it there are so many possibilities that should be tried by crptanalis such as: they must find the sequence of algorithms used, determine the added character part, determine the characters that were been added in each encryption stage, this is not simple, because different plaintext, different keys will be used.

REFERENCES

[1]. Audu M.S. (1986), Generating Sets for Transitive Permutation groups of prime-power order. The Journal of Mathematical Association of Nigeria Abacus, **17**(2), 22-26.

[2]. Aremu K.O., Ejima O, and Abdullahi M. S (2017), On the fuzzy T^1 non Deranged Permutation Group of G_T1 Asian Journal of Mathematics and Computer Research, **18**, 152-157.

[3]. Azzam A and Sumarsono (2017), A Modifying of Hill Cipher Algorithm with 3 Substitution Ceaser Cipher. Proceedings International Conference of Science and Engineering, Indonesia.**1**: 157-163.

[4]. 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.

[5]. Garba A. I. and Abubakar J. (2015), Construction of an Algebraic Structure Using a Concatenation Map. Nigerian Journal of Basic and applied Science (December, 2015), 23(2), 177-120.

[6]. 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

[7]. GarbaA.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

[8]. Ibrahim A. A. and Audu M. S. (2005), Some Group Theoretic Properties of Certain Class of (123) and (132) Avoiding Patterns of Certain Numbers: An Enumeration Scheme. African Journal of Natural Science, 8:34-39

[9]. Ibrahim A. A. (2006), Correspondence between the Length of some Class of Permutation patterns and Primitive Elements of Automophism Group modulo n, Abacus. The Journal of mathematical Association of Nigeria, 33:143-154.

[10]. 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.

[11]. Sriramoju Ajay Babu. (2017), modification affine ciphers algorithm for cryptography password, Programmer Analyst , Randstad Technologies, EQT Plaza 625 Liberty Avenue, Suite 1020 ,Pittsburgh, Pennsylvania -15222, USA.