International Journal of Inventive Engineering and Sciences (IJIES)
ISSN: 2319-9598 (Online), Volume-11 Issue-11, November 2024

A Study on Encryption in Poly Alphabetic Ciphers

Syed Usman Basha, S. Brintha Rajakumari

Abstract: ***Internet in nowadays has been in use in all departments of a society and it has been used by people of all ages for different purposes. With its increasing usage, security has become a major concern for secure data transfer over the internet. At this juncture, the importance of cryptography peeks in. Poly alphabetic cipher is one among the types of cryptography in which an alphabet can be substituted to any other alphabet. This article focuses light on different methods of generating Cipher text on the basis of Poly Alphabetic Cipher.***

Keywords: Cryptography, Poly Alphabetic, Cipher, Alberti, Trithemius, Vigenère

I. INTRODUCTION

Cryptography in Greek means "secret writing". It is a technique to achieve confidentiality of messages [1]. Most of the people around the globe use cryptography on a daily basis to protect data and information knowingly or unknowingly. Cryptography is the method of converting a normal message to unrelated and inconsequent ciphertext. The process of converting a plain text to coded text is termed as Encryption. The reverse process of converting back the coded text to normal message is termed as Decryption. The code in general is termed as Cipher [2]. The conversion is done using the plain text and a key. If same key used for both encryption and decryption, then it is termed as Symmetric Key Cryptography. If Public key used for encryption and Private key used for decryption., then it is termed as Asymmetric Key Cryptography. The conversion can be performed in two ways. Cipher generated by converting each digit of the plain text one at a time is termed as Stream Cipher. Cipher which is generated by converting the plain text as blocks is termed as Block Cipher. If the Cipher is obtained by changing the position of alphabets in the main text, it is called as Transposition cipher. If the Cipher is obtained by replacing the alphabets of the plain text to other alphabets using formulas and computations, it is termed as Substitution Cipher. The security of the encrypted message depends on the strength of cryptographic algorithm. Algorithms of cryptography from traditional to modern methods mostly make use of alphabets. In this article Poly Alphabetic ciphers are discussed, in which each alphabet is substituted for more than one alphabet.

Manuscript received on 16 August 2024 | Revised Manuscript received on 03 November 2024 | Manuscript Accepted on 15 November 2024 | Manuscript published on 30 November 2024.
*Correspondence Author(s)
Syed Usman Basha*, Research Scholar, BIHER, Chennai (Tamil Nadu), India. Email ID: syed.usman.mca@gmail.com, ORCID ID: 0000-0002-6406-9387
Dr. S. Brintha Rajakumari, Department of Computer Science, BIHER, Chennai (Tamil Nadu), India. Email ID: brimtha.ramesh@gmail.com, ORCID ID: 0000-0003-4381-3493

II. LITERATURE REVIEW

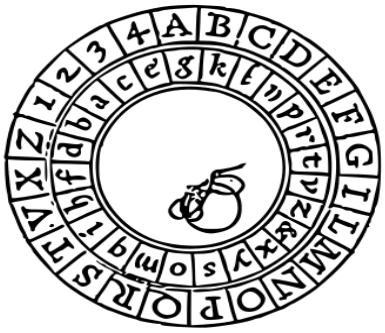
Poly Alphabetic means, each alphabet takes more than one form [3]. The first description of a polyalphabetic cipher was contained in the work of Al-Qalqashandi. Early Polyalphabetic cipher include Alberti cipher found by Leon Battista Alberti. For encrypting a message, Alberti used mixed alphabets, alphabet switching was done random intervals [4]. A decoder device was used by Alberti for implementing polyalphabetic substitution with mixed alphabets. The device was cipher disk. Johannes Trithemius invented a progressive key polyalphabetic cipher called the Trithemius cipher [5]. In this method, cipher are obtained by shifting each letter of the message. A tabula recta was used for switching of letters of the plain text. The Trithemius Cipher is an incredibly important step in the development of very secure ciphers. But it is quite weak due to lack of key. One of the biggest advances in cryptography is the Vigenère Cipher [6]. It is a method of converting a normal text to coded text using series of interwoven Caesar Cipher. It was first developed by Giovan Battista Bellaso. It was termed as the indecipherable cipher as it was tough to decode. Even though it was decoded by Friedrich Kasiski, still it is a very secure cipher.

III. METHODOLOGY

Each cipher has its own method of derivation. Each method is different form one another. In this section we discuss about the three main Polyalphabetic ciphers.

A. Alberti Cipher

It traditionally consists of a movable inner disc and immovable outer disc. Inner disc consists of Alphabets in Lower case. The outer disc consists of Upper case Alphabets. The encryption process is as follows: The disc is set in one position. The initial shift corresponds to number of letters shifted at the beginning. Each alphabet of the plain text found on the outer disc is replaced by the corresponding alphabet aligned with it in the inner ring. By default for every four characters, the disk is rotated clockwise of one alphabet.



[Fig.1: Alberti Disc]

The following methodology describes encryption of the text “Cipher World”. Lets assume that the Outer disc letter ‘A’ is in line with inner movable disc letter ‘g’ [7].

Rotation – I: Let the disc be static. Firs three letters are to be encrypted. C on the outer disc corresponds to l on the inner disc [8]. I on the outer disc corresponds to u on the inner disc. P on the Outer disc corresponds to s on inner disc.

Table 1: Phase-1 Alberti Disc Encryption(R-I)

Plain Text	C	I	P	H	E	R	W	O	R	L	D
Cipher Text	l	u	s								

Rotation – II: Let the disc be rotated clockwise to two positions. Four letters to be encrypted from H to W. H is not present in the outer disc. So the cipher text will have same letter in uppercase format. E in the Outer disc corresponds to l in the inner disc. R in the outer disc corresponds to s in the inner disc. W is not present in the Outer disc. So the cipher text will have the same letter in uppercase [9].

Table 2: Alberti Disc Encryption(R-II)

Plain Text	C	I	P	H	E	R	W	O	R	L	D
Cipher Text	l	u	s	H	l	s	W				

Rotation – III: Let the disc be rotated clockwise to three positions. Two letters, O, R to be encrypted. O in the outer disc corresponds to t in the inner disc. R in the outer disc corresponds to & in the inner disc [10].

Table 3: Alberti Disc Encryption(R-III)

Plain Text	C	I	P	H	E	R	W	O	R	L	D
Cipher Text	l	u	s	H	l	s	W	t	&		

Rotation – IV: Let the disc be rotated clockwise to one position. Final two letters L, D to be encrypted. L in the outer disc is not present. So its encrypted to the same letter in Uppercase. D in the outer disc is matched with a in the inner disc [11].

Table 4: Alberti Disc Encryption(R-IV)

Plain Text	C	I	P	H	E	R	W	O	R	L	D
Cipher Text	l	u	s	H	l	s	W	t	&	L	a

The final result of the encryption of the Plain Text CIPHERWORLD is l u s H l s W t & L a.

B. Trithemius Cipher

A special was proposed by Trithemius instead of using random combination of letters. This table was later named as tabula recta. The 1st row contains all alphabet letters in normal order. The following rows contain all the alphabets in each row and in each row letters are shifted to left by one position [12].

Table 5: Tabula Recta

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

The first letter of the Plain text is encrypted with its equivalent letter in the row which has no shift. The second letter of the plain text is encrypted with its equivalent letter in the second row which is shifted by one position. The third letter of the plain text is encrypted with its equivalent letter in the third row which is shifted by two positions and so on.

Table 6: Trithemius Cipher Encryption

Plain Text	T	R	I	T	H	E	M	I	U	S
Cipher Text	T	S	K	W	L	J	S	P	C	B

An encryption has been performed using Trithemius Cipher. From Figure.4 we could analyze the method of Trithemius. First letter T is encrypted with the first letter of the column T. the result is also T. The second letter R is encrypted to the second letter of the column R. The result is S. The third letter I is encrypted to the third letter of the column I. The result is K. This process continues till the last letter S is encrypted as B.

C. Vigenère Cipher

This cipher again uses the Tabula Recta. A key is assumed randomly. It can be of a single letter or a set of letters. . The letters of the key are repeated until it matches the number of characters in the plain text. Each letter in the plain text is matched with the key text using Tabula Recta Columns and Rows respectively. Each letter in the plain text is selected from the column list. Each letter from the key is selected from the row list. The intersection of the column and row for each letter in the tabula recta is the cipher text.

Table 7: Vigenère Encryption

Plain Text	A	T	T	A	C	K
Key	G	O	G	O	G	O

The plain text is assumed to be ATTACK. The Key is assumed as GO and is repeated until all the characters in the plain text are assigned a letter in the key as shown in Figure 4.1. The first letter in the plain text is A. Column A is selected. The key for the first letter is G. Row G is selected. The intersection of the column and row gives the cipher text G. The next letter of the plain text is T. Column T is selected. The corresponding key is O. Row O is selected. The intersection of the column and row represents the Cipher letter H as shown in figure 4.2. The Plain text, Key and Cipher text are highlighted.

Table 8: Vigenère Encryption for letter T

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Similar method is followed for the entire plain text. The next letter of the plain text is T. Column T is selected. The corresponding key is G. Row G is selected. The intersection of the column and row represents the Cipher letter Z. The next letter of the plain text is A. Column A is selected. The corresponding key is O. Row O is selected. The intersection of the column and row represents the Cipher letter O. The next letter of the plain text is C. Column C is selected. The corresponding key is G. Row G is selected. The intersection of the column and row represents the Cipher letter I. The next letter of the plain text is K. Column K is selected. The corresponding key is O. Row O is selected. The intersection of the column and row represents the Cipher letter Y. The final result of the plain text ATTACK is GHZOIY.

IV. CONCLUSION

This paper presented the three important polyalphabetic ciphers namely Alberti cipher, Trithemius cipher and Vigenère Cipher. By understanding the methods of these three ciphers, one can formalize a new methodology in each of the above three to make the ciphers more secure and unbreakable from attacks. While formulating new methodology, both encryption and decryption techniques need to be formalized. New algorithms need to be generated to make modification in the level of security of the messages sent over any network.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Bellare, Mihir, Rogaway, Philip, " Introduction to Modern Cryptography", p.10, September 2005.
2. Khan, David, " The Codebreakers", 1967, ISBN 978-0-684-83130-5.
3. Lenon, Brian, " Passwords: Philology, Security, Authentication", p. 26, 2018, ISBN: 978-0-674-98537-7.
4. Sands, Kevin, " Top 10 Codes, Keys and Ciphers", September 2015.
5. Salomon, David, " Data Privacy and Security", p. 63, ISBN 0-387-00311-8.
6. Laurence Dwight Smith, " Cryptography: The Science of Secret Writing", p. 81, 1955, ISBN 978-0-486-20247-1.
7. Salomon, David, " Coding for Data and Computer Communications", ISBN 0-387-21245-0. Doi: https://doi.org/10.1007/b102531
8. Kartha, R. S., & Paul, Dr. V. (2020). New Polyalphabetic Substitution Scheme for Secure Communication. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 3, pp. 3303–3310). https://doi.org/10.35940/ijitee.C9043.019320
9. Onome, Dr. O. A. (2022). Advanced Cyber Exploitation and Mitigation Methodology. In International Journal of Emerging Science and Engineering (Vol. 10, Issue 4, pp. 8–15). https://doi.org/10.35940/ijese.C2525.0310422
10. K Priyadharshini, R Aroul Canessane, Data Integrity, Data Privacy and Data Confidentiality Issues in Multi-User Cloud. (2019). In International Journal of Engineering and Advanced Technology (Vol. 8, Issue 6, pp. 1705–1708). https://doi.org/10.35940/ijeat.F8421.088619
11. Garg, S., & Mondal, T. (2024). Review on Data Privacy, Protection, and Security Challenges in Blockchain Adoption Across Diverse Domains. In International Journal of Management and Humanities (Vol. 10, Issue 7, pp. 20–38). https://doi.org/10.35940/ijmh.G1696.10070324
12. Manna, A., Sengupta, A., & Mazumdar, C. (2019). A Methodology for Eliciting Data Privacy Requirements and Resolving Conflicts. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 4, pp. 8366–8374). https://doi.org/10.35940/ijrte.D9049.118419