

Composite Cryptographic Methodologies for Data Transmission Model using Modified Vigenère and Extended Polybius Cipher

Urvi Mudliar¹, Khushi Zope², Prathamesh Lohakare³, Apeksha Tarate⁴ and Dr. Ms. Deipali V. Gore⁵

¹⁻⁵P.E.S. Modern College of Engineering /Computer, Pune, India

Email: urvimudliar12@gmail.com, Khushizope15@gmail.com, prathamesh4141lohakare@gmail.com, tarateapeksha30@gmail.com, deipali.gore@gmail.com

Abstract—Internet-based interactions in contemporary culture are increasingly using confidential information thus data security is a top concern for internet users the ideal approach is to use a cryptography technique which encrypts information in a cipher transfers it over the internet and then decrypts it to disclose the original information the area of cryptography that deals with information security also includes information transmission despite the fact that anonymity on the internet is a top concern many apps have been created and designed without making secrecy authentication and data protection their main priorities the goal is to ensure that only the authorized parties can properly interpret a message while preventing eavesdroppers from doing soon computers with enough processing power and memory our classic cryptographic approaches like Advanced Encryption Standard encryption and Rivest, Shamir, Adleman signing work well however they do not adapt well to an environment with integrated systems and wireless sensing devices thus methods for light-weight cryptography are recommended to overcome a number of problems with classical cryptography this study seeks to further the general body of knowledge in the area of classical cryptography by developing a ground-breaking hybrid approach of plaintext encryption the plaintext is first encrypted by the crypto model using the modified Vigenère cipher and then it is encrypted once more using the Extended Polybius cipher utilizing the ciphertext.

Index Terms— Cryptography, AES, RSA, Vigenère Cipher, Polybius Cipher, modified Vigenère Cipher, Extended Polybius Cipher.

I. INTRODUCTION

The process of designing or developing codes that permit content to be concealed is known as cryptography. Data can be communicated using cryptography without worrying about unauthorized parties deciphering it back into an understandable form and jeopardizing the data. Cryptography encodes data into a format that is unreadable for an unauthorized user. Cryptography is utilized in data security on multiple fronts. Without a decryption key, the data cannot be read.

The objective is to prevent intruders from deciphering a communication while enabling the authorized parties to obtain it successfully. Data can be distorted or masked using a wide range of methods in cryptography, making it only accessible to those with the ability to reconstruct the data from its original form. To overcome Vigenère cipher's limitations, we suggested an improved version called Customized Vigenère Cipher, which is much more

resistant to Friedman and Kasiski attacks. In order to improve system performance, the Vigenère Cipher is being enhanced and hybridized with other algorithms. Secure cryptographic performance is required, which is being fulfilled with this model.

The method encrypts data using a mixture of the Vigenère and Extended Polybius Square Cipher. The Vigenère cipher will be used to encrypt the text at first. A randomly chosen key will initiate the procedure. The following ciphertext eventually becomes a key for the Extended Polybius Square Cipher procedure as the process comes to a close. The final ciphertext is created using the key and the message, which is in plaintext, before decryption is completed and plaintext output is obtained.

High Security, Confidentiality, Authenticity, Data Integrity, and Non-repudiation are some advantages of this proposed approach. This procedure enables the development of new hybrid algorithms for ever-tighter security, implementation of both old and new ciphers for the mask generation of messages as well as the encryption and decryption of ciphers.

An illustration of a polyalphabetic stream cipher is the Vigenère approach. The ancient Greeks Cleoxenus and Democleitus created the Extended Polybius square, also known as the Extended Polybius checkerboard, which was made famous by the historian and scholar Extended Polybius. A table called a Extended Polybius Square enables people to change letters into numbers. The family of symmetric key ciphers includes block cipher and stream cipher, which are fundamentally encryption methods for instantly converting plaintext into ciphertext. Block ciphers take one block of plain text at a time and transform it into cipher text. By taking 1 byte of plain text at a time, the stream cipher transforms the plain text into cipher text.

II. RELATED WORK OR LITERATURE STUDIES

In the modern world, the internet is used for a lot of things. Digital signatures, time stamping, email services, communication software, bank account credentials, and many other things could be included. We can see from this how crucial the encryption standards are for the applications used in the modern world. The number of rounds used in the encryption process must be increased if present methods are to be made more secure. It guards the mechanism against all active and passive assaults. One of the earliest and most basic ciphers is the Caesar cipher. Each letter in the plaintext is "shifted" a specific number of positions down the alphabet in this kind of substitution cipher. With a shift of 1, for instance, A would become B, B would become C, and so on.

To encrypt a message, you will replace each letter in the message with another letter, chosen by finding the intersection of the correct row and column. To choose the row, find the letter of your message in the first column. If your message was "hello", the first letter would be encrypted using the row beginning with the letter 'h'. You need your key in order to select the right column. Choose the column that begins with the first letter of your key for the first letter in your message, the second letter in your message for the column that begins with the second letter of your key, and so forth. For instance, if your key was "RPI," the first letter of the message would be encrypted using the column that starts with "R," the second letter would be encrypted using the column that starts with "P," and the third letter would be encrypted using the column that starts with "I." Simply repeat the letters in your key in the correct order if the message is longer than your key.

The letter "h" is encoded as "y," and the letter "e" is encoded as "t" using this method. The second "l" becomes "c," while the first "l" also becomes "t." The letter "o" finally becomes the letter "d." This converts the word "hello" into the symbol "yttcd."

The process is reversed to decode a message by first locating the row that the current letter in the key belongs to, then navigating along that row until you locate the corresponding letter in the ciphertext. The plaintext letter is the one at the top of this column.

Start with column "R" and locate the location of the letter "y" in this column to decrypt the ciphertext "yttcd."

The letter "h," which represents the first letter of the plaintext, begins this row. When you reach the end of the key, you wrap around and use the initial letter once more, just like during the encryption procedure.

The Caesar cipher is undoubtedly simpler than this encryption technique.

For each character, the encryption and decryption methods call for several steps. Because of these additional processes, testing an attacker's key guesses will take longer. There are numerous additional permutations to try for each character in the plaintext, which increases the number of steps and complexity.

The Extended Polybius square, also known as the Extended Polybius checkerboard, is a method for fractionating plaintext characters so that they can be represented by a smaller set of symbols that was developed by the Ancient Greek historian and scholar Extended Polybius and described in Hist. X.45.6 ff.

The Greek alphabet was used in the original square, but it can be used with any script. In actuality, hiragana in Japanese has also been employed with it (see cryptography in Japan).

The coordinates of each letter in the grid are then used to represent it. "BAT," for instance, becomes "12 11 44." In order to round down to the next lowest square number because 26 characters do not quite fit in a square, we typically combine the letters I and J.

A keyword similar to the Playfair cipher can be used with the Extended Polybius cipher. Even when employed with a mixed alphabet, the Extended Polybius square is not particularly secure by itself. When combined, the digit pairs simply create a simple substitute whose symbols just so happen to be digit pairs. However, a Extended Polybius square has the potential for fractionation, which can result in the confusion and dispersion theorized by Claude E. Shannon. As a result, it serves as a helpful component in a number of ciphers, including the ADFGVX, Nihilist, and bifid ciphers.

Since the same letter is substituted by the same set of coordinates, this encryption is likewise simple to crack. They are easily broken by attackers using frequency analysis.

Thus, the Vigenère and Extended Polybius cipher each have benefits and drawbacks. These two methods can be combined to create a hybrid cryptography system that creates a stronger algorithm than either method working alone. The enhanced version of each separate encryption algorithm is the hybrid system. It is challenging to break because the combination produces a high amount of intricacy and ambiguity. Additionally, it somewhat mitigates the drawbacks of the various algorithms.

III. MOTIVATION

The proposed Hybrid Cryptographic model can be used in real world as follows:

- Chat applications in security agencies: Security agencies like Research and Analysis Wing, Police department and Indian army can use this communication model for secure data transmission.
- Banking applications: Customers can raise their queries online through this chat application for secure and fast communication and therefore they can get their queries solved faster.
- This point is based on Reference [5]. Many operations, whether they are military, police, fire dept, intelligence, rescue, or other field operations, it is necessary for online situation awareness to be efficient due to the growth in structural complexity in modern cities. Since the digital data gathered from these devices is sensitive, security issues related to its transfer through both protected and unprotected communication channels must be addressed. We suggest a hybrid cryptographic encryption method in this paper[5].
- General Data Protection Regulation Act- This point is based on Reference [6], By choosing to encrypt personal data, businesses can lessen the likelihood of a data breach and, consequently, lower their risk of future fines. Naturally, there is some risk involved in the handling of personal data. Particularly now, when firms larger than a certain size almost always experience cyberattacks. Data encryption is suitable for these businesses, among other methods, and risk management is thus playing an ever-larger part in IT security. In theory, the term "encryption" refers to the process of utilizing a key to hash plaintext into a code, and only the appropriate key can make the code readable once it has been sent. Due to the fact that encrypted contents are essentially illegible for other parties without the right key, this reduces the likelihood of an incident occurring during data processing. The best method for securing data during transport and one method for keeping stored personal information private is encryption. As access is restricted to those with the proper key and authorization, it also lowers the potential of fraud within an organization proposed communication model is also in accordance to the GDPR act [6].

IV. PROBLEM DOMAIN

The problem field is based on Cyber Security. Cyber security, in its most basic definition, is the attempt to guard the web systems, including their technology, software, and data transmission, from online attacks. The practice of securing corporate data transmission and avoiding knowledge loss due to illegal entry is known as data security. This entails securing your data from assaults that can alter or damage it, as well as assaults that can encode or erase it, like ransomware. The proposed model works well against the cyberattacks such as Kasiski and Friedman assaults. Kasiski examination is a technique used in cryptosystems to break polyalphabetic substitution ciphers like the Vigenère cipher.

V. PROBLEM DEFINITION

This study introduces a novel technique. Due to its extensive association and open structure, the internet is mentioned as one of the riskiest communication tools. One of the fundamental requirements for a parameter is

data assurance. Various security mechanisms are now being suggested to achieve security during communication. Each of them makes some good points as well as some terrible ones. They suggested a hybrid model to enhance the encryption algorithm's quality.

VI. STATEMENT

To build a Hybrid Cryptographic Communication System using Substitution Cipher Techniques such as modified Vigenère and Extended Polybius Cipher Algorithm.

VII. INNOVATIVE CONTENT

This point is based on Reference[1]. The strategy utilizes a combination of Vigenère cipher and Polybius Square Cipher in its encryption process. The ciphertext will initially be worked on utilizing Vigenère cipher. A picked key out of arbitrary will start the process. Toward the finish of the process, the subsequent ciphertext then turns into a key for the Polybius Square Cipher process. The key is used to work on the message which is the plaintext to create the last ciphertext. This process will wind up making the last ciphertext progressively hard to be broken utilizing existing cryptanalysis processes. Decryption will be done by the receiver in reverse order for retrieval of a message from the sender[1].

This point is based on Reference[2]. This article offers a security technique that can be applied to data transfer that includes letters, numbers, and some unique symbols. An examination of the Polybius encryption that is now in use and cryptography. The current Polybius cypher is based on the use of a 5X5 letter matrix created using the numerals 1 through 5. This field will only accept text that contains alphabets. Due to this, we have suggested a modification to the current Polybius encryption that allows for the creation of an 8X8 matrix[2].

This point is based on Reference[3]. To protect data many cyphers have been devised by creating a novel modified hybrid method of encryption of data this study aims to add to the body of knowledge in the field of classical cryptography big key spaces a large number of rounds and numerous complex processes may increase security but they can slow down operations therefore a modified hybrid of the Caesar and Vigenère cyphers is proposed in this work with dissemination and confusion that the classical cyphers cannot claim in order to incorporate alphabets numerals and symbols into the updated cypher the Caesar and Vigenère cyphers were changed and expanded at the same time a complete conflation and diffusion were added the qualities of current cyphers can be added to classical cyphers to make them more secure and effective the qualities of a contemporary cypher were added to a classical cypher in this study therefore the suggested scheme is a hybrid of traditional and contemporary cypher qualities in which the modified hybrid of the Caesar cipher and Vigenère cipher is now made a highly strong cypher and challenging to crack using a frequency approach brute force etc.[3].

This point is based on Reference[4]. To implement encryption methods, a hybrid approach is adopted in this paper. The employment of various algorithms, including symmetric and substitution cyphers, is widespread. By studying numerous well-known data encryption techniques, enhancing some of them, and putting them in the right order, the system's security is significantly increased. Avalanche Effect is selected as a metric for evaluating the effectiveness of the suggested algorithm and its use[4].

This point is based on Reference[5]. The following reference includes the various applications of hybrid crypto models. Hybrid cryptographic model is applicable in varied streams like military, banking and numerous fields. The security issues involved in transmission of digital data[5].

This point is based on Reference[6]. It describes the GDPR Act in detail. It gives all the details about the various policies involved in the GDPR Act which implies secure data transmission[6].

VIII. PROBLEM FORMULATION OR REPRESENTATION OR DESIGN.

A. Mathematical Model

TABLE I. MODIFIED VIGENÈRE MATHEMATICAL MODEL TABLE

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
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

By using the above table, we assign the alphabets in the format of list. In the list, we include characters from 0 to 51 in the order of A to z.

Example:

The first letter in plaintext hello is h and its corresponding letter in key is "B". when we look at the Vigenère table we can see that the cross-referenced character in the Modified Vigenère Mathematical Model Table is i. Similarly, according to below equation 1, p refers to the plaintext letter at index i. In given example the value of plaintext letter "h", at index i is 33. furthermore k refers to the key letter at index i. hence the value of key letter "B" at index 1 is 1. Therefore the value of E which refers to the encrypted letter at index i is $34 \bmod 52$ which is equal to 34. Now if we look at the table, we get same cross-referenced character "i" in Modified Vigenère Mathematical Model table.

According to below decryption formula, E_i is the encrypted letter at index i, here in given equation the value for encrypted letter "i" at index 1 is 34 and K_i is the key letter at index i. so the value of key letter B at index 1 is 1. Hence the above equation becomes $33 \bmod 52$ which gives us 33. So, we get decrypted value in below table as "h".

Extended Polybius Mathematical Model.

By the using the below table [3], we find indexing of particular alphabets.

Example:

For extended Polybius encryption by using below table no.3 we take column and row index we get value of h as 25. Again for decryption Search first integer i.e., 2 in column and second integer i.e., 5 in row and check for the cross-referenced character here in given example we get letter h. Similarly, we need to decrypt another character

IX. SOLUTION METHODOLOGIES OR PROBLEM SOLVING

A. Vigenère Cipher

Giovan Battista Bellaso initially explained the process in 1553. It was one of the unbreakable ciphers for a longer period of time. It was additionally referred to as a "indecipherable cipher." Unbreakable until 1863, this cipher. Friedrich Kasiski published a general approach to deciphering the Vigenère cipher in 1863. It involves the two operations of encryption and decryption, just like any other cryptographic algorithm.

Using a key and Vigenère table, the Vigenère cipher in cryptography transforms plain text into ciphertext. It resembles polyalphabetic replacement in certain ways. In order to extract the encoded letter from the modified Vigenère table, every letter in the plain text and every letter in the key are cross-referenced as the appropriate row and column.

B. Problems Solved by Modified Vigenère Model

- Modified Vigenère Algorithm overcomes the problem of not accepting lower case alphabets as an input.
- This modified algorithm also accepts space in the plaintext and encodes and decrypts the space using salt technique.
- salt technique- As an additional input to a one-way function that hashes a passphrase, a salt is random data that is used in cryptography.

C. Encryption

A modified Vigenère table, plain text, and a key are needed for the modified Vigenère cipher's encryption procedure. A table called a modified Vigenère table has 52 rows and 52 columns. In the modified Vigenère table, we can link to a letter by defining the row alphabet and column alphabet.

The modified Vigenère table, which is utilized in the Vigenère encoding, is the one seen above. The following steps are used in the encryption process:

Plain text, a key, and a modified Vigenère table must all be provided as inputs. The key is repeated and enlarged until it is the same length as the plain text if its length is less than that of the plain text. Let's now assume that the letter in plain text is X and that the letter in the key is Y. The modified Vigenère table's column indexes must first be searched for the X, and then its row indexes must be searched for the Y. The encrypted alphabet is a cross-reference of both coordinates.

The modified Vigenère encryption formula is best understood as follows:

$$E_i = [P_i + K_i] \bmod 52 \quad (1)$$

In the formula above, E_i stands for the encrypted letter at index i, P_i for the letter at index I in plain text, and K_i for the key letter at index i.

TABLE II. MODIFIED VIGENÈRE TABLE

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	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z				
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	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z					
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	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z						
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	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z							
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	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z								
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	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z									
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	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z										
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	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z											
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	m	n	o	p	q	r	s	t	u	v	w	x	y	z												
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	n	o	p	q	r	s	t	u	v	w	x	y	z													
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	o	p	q	r	s	t	u	v	w	x	y	z														
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	p	q	r	s	t	u	v	w	x	y	z															
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	q	r	s	t	u	v	w	x	y	z																
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	r	s	t	u	v	w	x	y	z																	
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	s	t	u	v	w	x	y	z																		
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	t	u	v	w	x	y	z																			
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	u	v	w	x	y	z																				
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	v	w	x	y	z																					
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	w	x	y	z																						
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	x	y	z																							
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	y	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	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	z																										
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																											
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																												
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																													
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																														
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																															
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																																
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																																	
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																																		
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																																			
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																																				
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																																					
m	n	o	p	q	r	s	t	u	v	w	x	y	z																																						
n	o	p	q	r	s	t	u	v	w	x	y	z																																							
o	p	q	r	s	t	u	v	w	x	y	z																																								
p	q	r	s	t	u	v	w	x	y	z																																									
q	r	s	t	u	v	w	x	y	z																																										
r	s	t	u	v	w	x	y	z																																											
s	t	u	v	w	x	y	z																																												
t	u	v	w	x	y	z																																													
u	v	w	x	y	z																																														
v	w	x	y	z																																															
w	x	y	z																																																
x	y	z																																																	
y	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	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	z
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	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	
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	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z		
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	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z			
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	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z				
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	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z					
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	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z						
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	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z							
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	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z								
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	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z									
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	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z										
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	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z											
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	m	n	o	p	q	r	s	t	u	v	w	x	y	z												
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	n	o	p	q	r	s	t	u	v	w	x	y	z													
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	o	p	q	r	s	t	u	v	w	x	y	z														
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	p	q	r	s	t	u	v	w	x	y	z															
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	q	r	s	t	u	v	w	x	y	z																
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	r	s	t	u	v	w	x	y	z																	
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	s	t	u	v	w	x	y	z																		
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	t	u	v	w	x	y	z																			
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	u	v	w	x	y	z																				
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	v	w	x	y	z																					
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	w	x	y	z																						
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	x	y	z																							
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	y	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	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	z																										
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																											
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																												
d	e	f	g	h	i	j	k	l	m	n	o																																								

Example:

```
Plaintext: - I love India
Key: -
wrWejcknRRaiwHbnsebfLVLzOOduKrS
Expansion Key: - wrWejcknRRaiwH
Cipher text: - ERxPXXONsZNLeh
```

The key is iterated until its length equals that of the plain text since it is shorter than that of the plain text first letter in plain text is “R” and, in the key, it corresponds to “w” in the Vigenère table look for the “R” column and the “w” rows to see that “N” is indeed the cross-referenced letter finding the encrypted characters for the remaining plain-text letters is similar.

D. Decryption

A modified Vigenère table is also necessary for the modified Vigenère cipher's decryption operation. The following steps are a part of the modified Vigenère decryption process:

Ciphertext, a key, and a modified Vigenère table are the necessary inputs for the modified Vigenère decryption. Think of the row index in the modified Vigenère table as being the letter in the key. Then scan that row for the ciphertext letter that corresponds to it. The decrypted letter is found at the same location as the ciphertext letter, and its associated column index.

It is possible to read the modified Vigenère decryption formula as

$$D_i = (E_i - K_i) \text{ modulus } 52 \quad (2)$$

In the above equation, D_i is the letter that has been decrypted, E_i is the letter that has been encrypted, and K_i is the letter that has been assigned the key.

Cipher text: - ERxPXXONsZNLeH
Expansion Key: - wrWejcknRRaiwH
Plaintext: - I love India

Example:

Since "w" is the first letter in the key, seek for the Vigenère table entry that is "w" indexed. Look for the location of "N" in the "w" indexed row, then look for its column index. Its corresponding letter in the ciphertext is "N". The decrypted first letter of the ciphertext, "R," serves as the column index. We must similarly decipher the letters that are left.

E. Kasiski Attack

The Kasiski method aids in determining the length of the key by examining the recurrent cryptograms in the ciphertext.

Plain text repetition is an issue with English plain text. For instance, the word "THE" may appear more than once in the sentence. As a result, it is possible to create repeated cryptograms.

The following steps make up the Kasiski attack:

Search through the ciphertext for all of the recurrent cryptograms if it is longer.

Determine the separation between the repeating cryptograms.

Find the factors or divisors of the distance.

Determine the slices of the set of dividing factors. The value in the slice corresponds to the number that appears on each of the distance-dividing variables. The length of the key might be represented by this value.

F. Polybius Cipher

The Polybius cipher, also known as the Polybius square cipher, is a cryptographic technique that turns each letter into a pair of coordinates. Since each letter in the plain text is replaced with a pair of coordinate numbers, polyalphabetic substitution is used. The Polybius square, also known as the Polybius checkerboard, serves as the foundation for the Polybius encoding and decoding process. Ancient Greeks created Polybius Square, which became well-known thanks to historian and thinker Polybius.

G. Problems Solved by Extended Polybius Model

- The Extended Polybius model overcomes the issues faced by Polybius i.e. the mapping to smaller case letters is now possible.
- The separation of the letters I and j in the same block cleared the ambiguity that was faced by original Polybius

H. Encryption of Extended Polybius Model

Utilizing the Polybius square, the encryption in the Extended Polybius cipher turns the letters in plain text into numbers. A matrix called the Extended Polybius square has eight rows and eight columns. There are 52 alphabets total in the matrix. As in the 8*8 matrix there are 62 blocks and the total number of alphabets are only 52, 12 remaining blocks are left empty, which are further filled with null character.

The Extended Polybius square is seen in the above figure. In the Extended Polybius square, indexing is done using numbers. With the help of each letter's row index and column index, we can find it in the Extended Polybius square. For instance, the number 11 can be used to represent the letter "A." The "A" row and column coordinates are both 1.

TABLE III. EXTENDED POLYBIUS TABLE

	1	2	3	4	5	6	7	8
1	A	B	C	D	E	F	G	H
2	I	J	K	L	M	N	O	P
3	Q	R	S	T	U	V	W	X
4	Y	Z	a	b	c	d	e	f
5	g	h	i	j	k	l	m	n
6	o	p	q	r	s	t	u	v
7	w	x	y	z	\0	\0	\0	\0
\0	\0	\0	\0	\0	\0	\0	\0	\0

Example:

Plaintext: - I love India Cipher text: - 12 65 16 86 74 12 85 64 35 34

There are no keys involved in this encryption procedure. Simply mapping from the Extended Polybius square is required.

I. Decryption of Extended Polybius Model

TABLE IV. COMPARISON OF VARIOUS INPUT SETS

Input	Modified Vigenère Encryption	Extended Polybius Encryption	Extended Polybius Decryption	Modified Vigenère Decryption	Expected Output
INDIA	EEZmj	51 51 24 75 45	EEZmj	INDIA	INDIA
Mumbai	IIIFJK	12 65 12 61 22 32	IIIFJK	Mumbai	Mumbai
mysore	ipOSaG	35 26 72 33 34 71	ipOSaG	mysore	Mysore

Finding the coordinates in the Extended Polybius square and the associated letter are steps in the decryption procedure for the Polybius cipher. The alphabet associated with the indexed number will be given as the decrypted output.

Example:

Cipher text: - 12 65 16 86 74 12 85 64 35 34 Plaintext: - I love India

X. RESULTS AND SENSITIVITY ANALYSIS

- In order to facilitate secure communication, we have integrated the hybrid crypto system we developed utilizing the Modified Vigenère and Extended Polybius ciphers into a real-world application named Webchat. It is the user interface designed to display the outcomes of the hybrid crypto model.

XI. DATA MODEL

The Extended Polybius and modified Vigenère ciphers were used to create a hybrid algorithm. In this case, encryption and decryption were performed twice. Hence, it was essentially double encryption and double decryption. The first encryption was carried out using the modified Vigenère cipher and a key that produces alphabets. Key generator generates a key wherein if the length of the keyword and the plaintext matches, then assume the keyword as key. If it does not match, then an expanded key is generated by appending the keyword

till the length of plaintext. The next encryption was carried out using extended Polybius, a program that turns alphabets into integers.

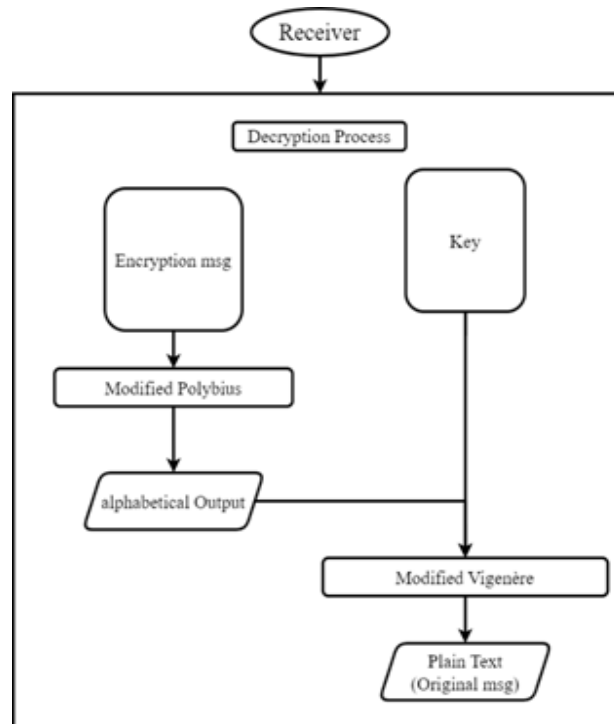


Figure 1. Modified Vigenère Process

The reverse process of decryption was carried out in the same way. The encrypted cipher was used as the input for the Extended Polybius cypher, which produced a numerical encrypted cipher with confusing and mixed-numerical scrambling as the output.

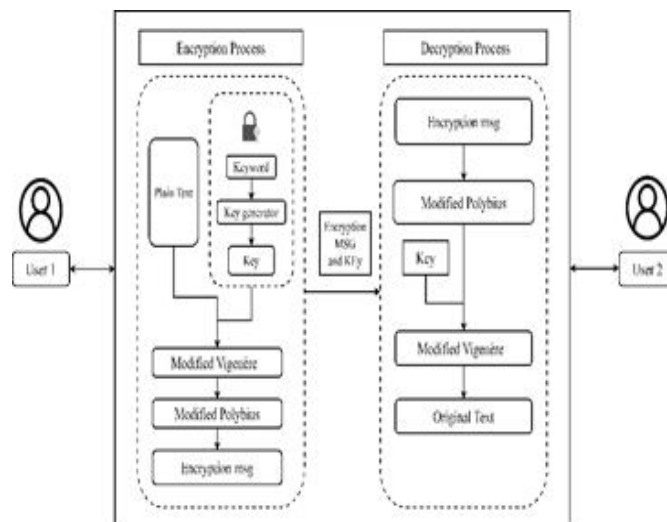


Figure 2. Extended Polybius Process

The diagram is a modified hybrid cryptographic architectural diagram. above is a pictorial representation of extended composite crypto model when user 1 transmits a message it takes the plaintext and keyword as input user 1 then sends the keyword to the key generator using the expanded key plaintext modified Vigenère and extended Polybius algorithms the diagram above is a modified hybrid cryptographic architecture diagram user 2 receives the enlarged key and plaintext when the encryption is completed and user 2 then decrypts the message to acquire the final result.

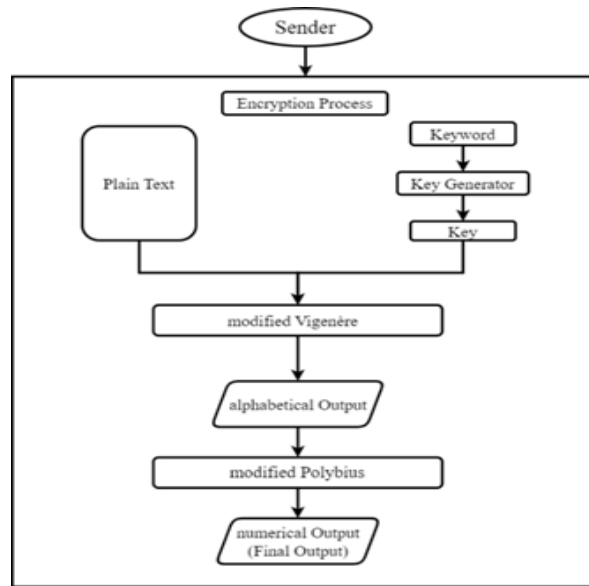


Figure 3. Modified Hybrid Cryptographic Architectural Diagram

XII. COMPARISON OF RESULTS

TABLE V. COMPARISON BETWEEN NORMAL AND MODIFIED HYBRID MODELS

Parameters	Old Vigenère Cipher	Modified Vigenère Cipher	Polybius Cipher	Extended Polybius Cipher
Small Case alphabet	Does not accept smaller case alphabets as input	Does accept smaller case alphabets as input	mapping to smaller case alphabets is not possible	mapping to smaller case alphabets is possible
White Space	Does not accept space	Does accept Spaces	Does not accept space	Does accept Spaces

XIII. JUSTIFICATION OF THE RESULTS.

As mentioned in the reference [reference model], the modified hybrid cryptographic model incorporates the disadvantages faced in the normal hybrid crypto model. In the normal hybrid crypto model, smaller case alphabets and white spaces were not allowed. In the modified hybrid crypto model, the smaller case alphabets and white space are included as input.

XIV. CONCLUSION.

The profitability of your firm depends on the safety of important business information. This algorithm combines the Vigenère Algorithm and the Extended Polybius Algorithm. Combining these two factors will make it more challenging for an intruder to breach the system. The hybrid cryptography model also eliminates the disadvantages of individual cryptographic techniques. This Cryptographic model also uses a modified version of the Vigenère encryption. Data security in the dynamic field of cryptography necessitates new and more complicated techniques.

FUTURE WORK

Future research may concentrate on the modified Vigenère cipher's execution time trade-off. Additionally, researchers can employ the Extended Polybius cipher, which provides a much safer conversion of message.

REFERENCES

- [1] Shivam Vatshayan, Raza Abbas haidri, Jitendra Kumar Verma "design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher" 2020 International Conference on Computational Performance Evaluation (ComPE)

- [2] Tabu S. Kondo, Leonard J. Mselle "An Extended Version of the Polybius Cipher" International Journal of Computer Applications (0975 – 8887) Volume 79 – No 13, October 2013
- [3] O.E. Omolara, A.I. Oludare and S.E. Abdulah "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication" Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.5, No.5, 2014
- [4] Gurpreet Singh, Supriya "Modified Vigenere Encryption Algorithm and its Hybrid Implementation with Base64 and AES" 2013 Second International Conference on Advanced Computing, Networking and Security
- [5] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo M. Eghan, and Nii Narku Quaynor "A Hybrid Cryptographic Encryption Technique for Securing Surveillance Digital Images in Mobile Urban Situation Awareness Systems"
- [6] <https://gdpr-info.eu/issues/encryption/>
- [7] Sanjeev Kumar Mandal, A.R. Deepti "A Cryptosystem Based On Vigenere Cipher By Using Multilevel Encryption Scheme" International Journal of Computer Science and Information Technologies, Vol. 7 (4), 2016, 2096-2099
- [8] Jan Carlo T. Arroyo, Cristina E. Dum Dumaya, Allemar Jhone P. Delima "Polybius Square in Cryptography: A Brief Review of Literature" International Journal of Advanced Trends in Computer Science and Engineering
- [9] Khairun Nahar, Partha Chakraborty "A Modified Version of Vigenere Cipher using 95×95 Table" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020
- [10] Abhishek Mishra, Abhishek Rai, Dheeraj Gurjar "Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher" International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
- [11] Dr. Aradhana. D, Chaithra. V. N, Evelyn Arpitha Joseph, Gouri Pooja. H. M "CRYPTOGRAPHIC TECHNIQUE FOR COMMUNICATION" International Journal of Scientific Research and Engineering Development— Volume X Issue X, Year
- [12] Chandan Kumar, Sandip Dutta, Soubhik Chakraborty "A Hybrid Polybius-Playfair Music Cipher" International Journal of Multimedia and Ubiquitous Engineering Vol.10, No.8 (2015), pp.187-198
- [13] D. Akanksha, Rubeena Samreen, G. Sai Niharika, A. Shruthi, M. Jyotsna Kiran Dr. S. Venkatramulu "A HYBRID CRYPTOSYSTEM BASED ON MODIFIED VIGENERE CIPHER AND POLYBIUS CIPHER" EPRA International Journal of Research and Development (IJRD) Volume: 7 Issue: 6 June 2022
- [14] Moumita Maity "A MODIFIED VERSION OF POLYBIUS CIPHER USING MAGIC SQUARE AND WESTERN MUSIC NOTES" International Journal for Technological Research In Engineering Volume 1, Issue 10, June-2014
- [15] Aized Amin Soofi, Irfan Riaz, Umair Rasheed "An Enhanced Vigenère Cipher for Data Security" International Journal of Scientific & Technology Research Volume 5, Issue 03, March 2016.