SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

A HYBRID CRYPTOSYSTEM BASED ON MODIFIED VIGENERE CIPHER AND POLYBIUS CIPHER

D. Akanksha[1], Rubeena Samreen[2], G. Sai Niharika[3], A. Shruthi[4], M. Jyotsna Kiran[5]
[6]Dr. S. Venkatramulu
[1,2,3,4,5]*Students, Dept. of CSE, Kakatiya Institute of Technology and Science, Warangal.*
[6]*Associate Professor, Dept. of CSE, Kakatiya Institute of Technology and Science, Warangal.*

ABSTRACT
Nowadays, the Internet is rapidly expanding. As a result, massive amounts of data are transmitted through the Internet via networks. This information must be safeguarded. Cryptography is a technique for ensuring data security and confidentiality by transforming it into an unreadable format. Along with data security, it is also necessary to assure data authenticity, confidentiality, and protection. Because we rely so much on data, we must likewise improve our understanding of data security risks. Cryptography is an example of a data security technique. Cryptography is a Greek word that refers to the art of securing data by converting it into a jumbled and unreadable state. In this research, we use the Polybius Cipher with a modified Vigenere Cipher to create hybrid cryptography. When compared to separate ciphers, the hybrid cryptography system is more secure. We improve the Vigenere cipher key generation by removing some of its shortcomings.
KEYWORDS: *Cryptography, Vigenere cipher, Modified Vigenere cipher, Polybius cipher, Hybrid cryptosystem, Kasiski attack.*

I. INTRODUCTION

Cryptography, the use of codes and ciphers to secure secrets, dates back thousands of years. The invention of complicated mechanical and electromechanical equipment in the early twentieth century gave more sophisticated and efficient techniques of encryption, and the later introduction of electronics and computing has enabled elaborate schemes of much higher complexity. Cryptography has become an integrated layer of defence within all digital transformation activities today referred to as a digital business. Cryptography, as the foundation of modern security systems, is used to secure transactions and communications, protect personally identifiable information (PII) and other confidential data, authenticate identity, prevent document manipulation, and create trust between servers. Cryptography is one of the most significant techniques used by businesses to safeguard the systems that carry their most valuable asset – data – whether it is at rest or in motion.

The following are the fundamental cryptographic conventions and terms:

Plaintext: Anything that people can understand and/or relate to is considered plaintext. This could be as straightforward as English phrases, a script, or Java code. If you can understand what is written, it is in plaintext.

Ciphertext: Ciphertext, often known as encrypted text, is a set of randomized characters and numbers that humans are unable to comprehend.

Encryption: It is a method of securing digital data by the use of one or more mathematical procedures, as well as a password or "key" to decrypt the data. The encryption process turns data into an unreadable format using an algorithm. For example, the procedure can transform plaintext into ciphertext.

Decryption: It is the process of restoring encrypted data to its original state. It's essentially a reverse encryption procedure. Because decryption requires a secret key or password, it decodes the encrypted information so that only an authorized user can decrypt the data.

Cryptanalysis: It is the technique of analysing information systems to comprehend the systems' hidden characteristics. Even if the cryptographic secret is unknown, cryptanalysis is used to break into cryptographic security systems and get access to the contents of encrypted messages.

II. LITERATURE SURVEY

Many of the activities in the current world utilize the internet. It may involve electronic cash, bank account credentials or password, digital signatures, time stamping, email services, communication applications, and many more. Through this, we understand the importance of the encryption standards

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

for current world applications. The only way to increase the security of existing algorithms is can increase the number of rounds involved in the process of encryption. It prevents the mechanism from all the active and passive attacks.

One of the earliest and most used mechanisms in cryptography is Caesar's cipher which is also called a shift cipher. It is a replacement mechanism in which each letter of the plain text is replaced by another letter which is certain places ahead of the letter and the process is repeated for all the letters in the plain text. The number of places ahead to be used is the key to the encryption. For example, if the key is 2, then 'a' will be replaced by 'c' which is two places ahead of 'a'. This technique is used after Julius Caesar who had utilized this method for communicating with its authorities. But it is one of the least complex mechanisms known. It can be decrypted easily by the attacker using frequency analysis of letters in the decrypted text and understanding the pattern of the words.

A transposition cipher is a process where the location of letters in the plain text is changed by following a certain model and hence the encrypted text contains the letters same as plain text but are interchanged between them. Vigenere cipher is a type of polyalphabetic substitution in which each letter in the plain text is substituted using a key and Vigenere table. It is considered one of the unbreakable ciphers for a longer time. This cipher was invented by Blaise de Vigenere and was named after him. The disadvantage of this cipher is that the key is repeated until it matches the length of the plain text. The identical pair of plain text letters and key letters produces the same encrypted text letters. Hence by understanding the frequency we can predict the key length used. With sufficient ciphertext, an attacker can easily guess the key. This attack is also called the kasiski attack. We can overcome this disadvantage using a key that doesn't have repeating letters.

Polybius cipher is also a substitution cipher that converts the plain text letters into a pair of numbers utilizing the Polybius square. Polybius square is invented by ancient Greeks and was made famous by Polybius. Polybius square consists of alphabets arranged in the form of a grid. This cipher is also easy to break since the same letter is replaced by the same pair of coordinates. By doing frequency analysis, attackers can easily break them. Hence Vigenere and Polybius cipher each have their advantages and disadvantages. If we combine these two techniques to form a hybrid cryptography system, it forms a stronger algorithm than the individual algorithms. The hybrid system is the upgraded variant of the individual encryption algorithms. The combination results in a high level of complexity and confusion making it hard to break. It also overcomes the disadvantages of the individual algorithms to some extent.

III. THEORIES

When PCs are connected to a global system, particularly the internet, they become unreliable. Infections, malware, and other malicious software can steal personal information from a computer. Data replication, theft, visualization, detection, and intrusion are all threats that require security. The primary goal of PC security is to ensure that the computer and its operating system keep data safe and secure.

PC security works from several perspectives, including:

1. **Confidentiality**
   This property of cryptography ensures that the data will be only accessed by the intended users or authenticated users. It comprises rules that the data will only be visible or accessed by the intended users. The confidential data must not be known or understood by the third person since it contains valuable information.
2. **Privacy**
   This property of cryptography ensures that the personal information of an individual is protected from visibility to the public. There will be a lot of personal data for the individual which they wish to be not disclosed to the public. The main difference between confidentiality and privacy is that confidential information can be accessed by a range of people upon the permission of the user to whom the information belongs. Whereas privacy ensures that the information of the individual is kept to the individual.
3. **Integrity**
   This property of cryptography ensures that the information is not altered while it is being sent from the sender to the receiver. Even if the information is changed it must be known to the sender and receiver. This property ensures the protection of data from modification by attackers. If the integrity of the data is lost, wrong information may be communicated to the receiver and causes severe damage. It represents the dependability and reliability of data being transferred. It protects the legitimacy and the precision of the data.
4. **Non-repudiation**
   Sometimes people may deny it after they have sent the data or received data. Even after receiving the information receiver may deny that he did not receive the data. The non-repudiation property of cryptography ensures that the sender or receiver cannot deny the fact that they have sent or received information. It is like making a mark on the message when it is sent or received so that the user cannot deny the fact.
5. **Authentication**
   This property of cryptography verifies the sender or receiver as authenticated users before sending or receiving the information. Only after successful authentication, the information will be sent to them. It protects the legitimacy and oneness of transmission or message. Authentication helps in protecting the data from unauthorized users.
6. **Availability**
   This property of cryptography ensures that the data is always available for the user when he requests it. Sometimes attackers may interfere with the services provided such that the authorized requests will also be failed due to heavy load on the server. The attacker will make the server unavailable such that the data cannot be accessed by the authenticated users. Hence, we must ensure a mechanism for the availability of data for the authorized users.

A cipher is an algorithm for encrypting and decrypting data in cryptology, the field concerned with the study of cryptographic methods. Symmetric key encryption, often known as secret key encryption, is based on the usage of symmetrical

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

ciphers. The encryption key is also used for decryption. Ciphers can be classified in a variety of ways, including Block ciphers which encrypt data in blocks of consistent size, and Stream ciphers which are used to encrypt data streams that are often received and transferred over the internet.

Ciphers have traditionally employed two forms of transformation: Transposition ciphers maintain all of the original data bits in a byte but alter their order. Substitution ciphers substitute alternative data sequences for certain data sequences. One method of replacement, for example, is to change all bits with a value of 1 to a value of 0, and vice versa. A cipher transforms plaintext, a readable message, into ciphertext, a random string of letters, using a set of established rules which is an encryption algorithm. The algorithm and a secret key are utilized by the encryption algorithm to change data as it is encrypted in modern cipher implementations. A key is such an important aspect of an encryption algorithm that it is kept secret rather than the algorithm in real-world ciphering.

VIGENERE CIPHER

Vigenere cipher is a strategy in cryptography that converts the plain text into ciphertext using a key and Vigenere table. It is a kind of polyalphabetic substitution. Because every letter in the plain text and every letter in the key is cross-referenced as row and column correspondingly for obtaining the encrypted letter from the Vigenere table. The method was first described by Giovan Battista Bellaso in 1553. For a longer time, it was considered one of the unbreakable ciphers. It was also called an "indecipherable cipher". This cipher was unbreakable until 1863. In 1863, Friedrich Kasiski published a general method that can decode the Vigenere cipher. As with any other cryptographic algorithm, it involves two processes encryption and decryption.

Encryption

The encryption process in the Vigenere cipher requires a Vigenere table, plain text, and a key. Vigenere table is a table consisting of 26 rows and 26 columns. We can refer to a letter in the Vigenere table by specifying the row alphabet and column alphabet.

	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

Fig. 1 Vigenere Table

The above table is the Vigenere table which is used in the Vigenere cipher. The encryption process involves the following process:

The inputs required are plain text, key, and Vigenere table. If the length of the key is less than the length of plain text, the key is repeated and expanded until it matches the length of the plain text. Now let us consider the letter in plain text as X and its corresponding letter in key as Y. We need to look for the X in the row indexes and then we need to look for the Y in the column indexes of the Vigenere table. The cross-reference of both coordinates is the encrypted alphabet.

Example:

Plaintext: CRYPTOGRAPHY

Key: TIGER

Expanded Key: TIGERTIGERTI

Cipher text: DSDAFZECEMXE

The key is repeated until it matches the length of plain text since its length is smaller than the length of the plain text. The first letter in plain text is "C" and its corresponding letter in the key is "T". Look for the "C" row and "T" columns in the Vigenere table, we can see that the cross-referenced alphabet in the table is "V". Similarly, we need to find the encrypted letters for remaining letters in the plain text.

The formula for Vigenere encryption can be interpreted as follows:

$E_i = [P_i + K_i]$ modulus (26)

In the above formula, E_i refers to the encrypted letter of index i, P_i refers to the plain text letter at index I, and K_i refer to the key letter at index i.

Decryption

The decryption process in the Vigenere cipher also requires a Vigenere table. The process involved in Vigenere decryption includes the following process:

The inputs required for Vigenere decryption are ciphertext, key, and Vigenere table. Consider the letter in the key as the row index of the Vigenere table. Then look for its corresponding ciphertext letter in that particular row. The location at which the ciphertext letter is located, its corresponding column index is the decrypted letter.

Example:

Expanded Key: TIGERTIGERTI

Cipher text: DSDAFZECEMXE

Plain text: CRYPTOGRAPHY

"T" is the first letter in the key, look for the "T" indexed row in the Vigenere table. Its corresponding letter in the ciphertext is "V", look for the location of "V" in the "T" indexed row and then look for its column index. The column index is "C" which

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

is the decrypted first letter of the ciphertext. Similarly, we need to decrypt the remaining letters.
The formula for Vigenere decryption can be interpreted as:
$D_i = (E_i - K_i + 26)$ modulus 26
In the above formula, D_i is the decrypted letter at index i, E_i is the encrypted letter at index i, and K_i is the key letter at index i.

KASISKI ATTACK

By studying the recurring cryptograms in the ciphertext, the kasiski approach aids in determining the length of the key. English plain text has the problem of repeating plain text. The letter "THE" may appear several times in the sentence, for example. This allows for the creation of cryptograms that are repeated.
The kasiski attack consists of the following steps:

- If the ciphertext is lengthier, look for all the recurring cryptograms inside it.
- Calculate the distance between the cryptograms that repeat.
- Find the distance's factors or divisors.
- Calculate the slices of the dividing factor set. The number that occurs on all of the distance dividing factors is represented by the value in the slice. This value could represent the length of the key.

Example:

Plaintext:
CRYPTOISSHORTFORCRYPTOGRAPHY

Key: ABCD

Cipher text:
CSASTPKVSIQUTGQUCSASTPIUAQJB

In the above example, the cryptogram "CSASTP" is repeated twice and the distance between the repetition is 16. For calculating the distance, start calculating from the beginning of the string which is repeated. "CSASTPKVSIQUTGQU" is repeated in the next occurrence. 16 is the multiple of 4 which is the key length. We can overcome this by producing the key length equal to that of the plain text.

MODIFIED VIGENERE CIPHER

To overcome the above kasiski attack, in this project we generate a different key for each word in a sentence that is of equal length to that of the word. Through this approach, we can avoid expanding the key and the occurrence of the same cryptogram. According to the test results presented in the paper given in [1] reference, it has been proven that the above change has a positive change on the strength of the Vigenere cipher. According to the modification, the Vigenere cipher can be described as follows with an example:

Example:

Plaintext:
CRYPTOISSHORTFORCRYPTOGRAPHY

Key:
EJWICNESPQQRVDXWNHJFBYJFULEU

Ciphertext:
GAUXVBMKHXEIOILNPYHUUMPWUALS

In the above example, a separate key is generated for each word to avoid the repetition of the key.

POLYBIUS CIPHER

Polybius cipher also called Polybius square cipher is a strategy in cryptography that converts the letters into a pair of coordinates. It utilizes polyalphabetic substitution since each letter in the plain text is substituted by pair of coordinate numbers. Polybius encryption and decryption process is based on Polybius square also called as Polybius checkerboard. Polybius square is invented by ancient Greeks and was made famous by historian and scholar Polybius.

Encryption:

The encryption in the Polybius cipher converts the plain text letters into numbers utilizing the Polybius square. Polybius square is a matrix consisting of 5 rows and 5 columns. The matrix consists of 26 alphabets. Since it is a 5 X 5 matrix, it can only fit 25 letters. Hence, I, and J are kept in the same cell of the matrix.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fig. 2 Polybius Square

The above figure depicts the Polybius square. Indexing in the Polybius square is done through numbers. We can locate each letter in the Polybius square with its coordinates which are row index and column index. For example, the letter "A" can be represented by 11. "A" row coordinate is 1 and column coordinate is 1.

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

Example:

Plaintext: CSE

Cipher text: 134315

This encryption process does not include any key. It just involves mapping from the Polybius square.

Decryption

The decryption process in the Polybius cipher involves the location of coordinates in the Polybius square and finding its corresponding letter.

Example:

Cipher text: 134315

Plaintext: CSE

IV. METHODOLOGY

A hybrid cryptography system is based on the strategy of combining two different existing cryptographic techniques to overcome the disadvantages of the individual classical encryption techniques. It helps in enhancing the strength of the cryptographic algorithm and increases the complexity making it hard to break. In this project, we have built a hybrid cryptography system based on the modified Vigenere cipher and Polybius cipher. The main goal of the project is to prove that the combination of algorithms is stronger than the individual ones. The steps involved in the process of hybrid cryptosystem using modified Vigenere cipher and Polybius cipher involve four main steps:

I. Modified Vigenere encryption
II. Polybius encryption
III. Polybius decryption
IV. Modified Vigenere decryption

Encryption:

The encryption process in the hybrid cryptosystem using modified Vigenere cipher and Polybius cipher involves two rounds of encryption. First, we need to encrypt the plain text using the modified Vigenere encryption and then the output obtained from the modified Vigenere encryption is given as an input to the Polybius encryption. The output obtained from Polybius encryption is the obtained ciphertext which will be sent to the receiver. If the input message is a sentence, then we should break it into an array of words. We can understand the encryption process involved with an example.

Example:

ENCRYPTION

Phase 1 (Modified Vigenere Cipher)

STEP 1: Plaintext- ONLINE

STEP 2: Key- UQMUUR

STEP 3: Output- IDXCHV

Phase 2 (Polybius Cipher)

STEP 4: Text- IDXCHV

STEP 5: Output- 24 14 53 13 23 51

Fig. 3. Flowchart for encryption

Decryption:

The decryption process of a hybrid cryptography system using modified Vigenere cipher and Polybius cipher involves the reverse process of encryption. The ciphertext is first decoded using the Polybius cipher. Through Polybius decryption, the numbers will be converted into a string of letters. The output obtained from Polybius decryption is given as an input to the modified Vigenere decryption process. For Vigenere decryption, we also need to provide the key which should be sent from sender to receiver securely. In this project, for the key exchange mechanism between the sender and receiver, we have used email. As soon as the message is encrypted, the key will be sent to the authenticated user's email address, then he decrypts the messages using the key. The output obtained after the modified Vigenere decryption is the plain text which is to be communicated with the receiver. We can understand the process of decryption by continuing the example we discussed in the previous section.

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

Example:

DECRYPTION

Phase 1 (Polybius Cipher)

STEP 1: Plaintext- 24 14 53 13 23 51

STEP 2: Output- IDXCHV

Phase 2 (Vigenere Cipher)

STEP 3: Text- IDXCHV

STEP 4: Key- UQMUUR

STEP 5: Output- ONLINE

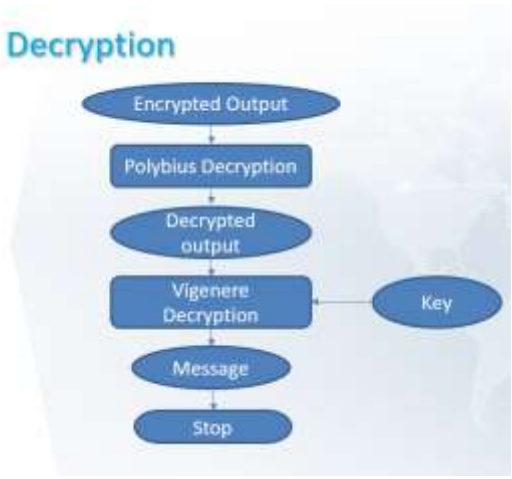

Fig. 4. Flowchart for decryption

V. RESULTS

We have implemented the created hybrid cryptosystem using Vigenere cipher and Polybius cipher in a real-world application called military communications. It is the UI developed to show the results of the hybrid cryptosystem.

Fig. 5. The landing page of UI

In this application, military officials such as majors, brigadiers, and colonels can sign up, and then their accounts will be approved by their higher officials. After the approval, users can log into the application and send messages or view the messages they received.

Fig. 5. Sending encrypted message

As shown in the above figure, we can choose the receiver and then fill in the subject and message of the input to be sent. On submitting, the message will be encrypted using a hybrid cryptosystem and sent to the receiver.

Fig. 6. Decryption screen

The above screen is the UI design for the decryption where the user needs to enter the key from their email and then decrypt the message.

Fig. 7. Decrypted output

The above screen shows the decrypted message at the receiver's end.

VI. CONCLUSION

Because the Internet is continually expanding, there is an enormous quantity of data being transmitted across the network that must be protected and secured. A hybrid cryptography system is one of the approaches for data secrecy. The Vigenere Algorithm and the Polybius Algorithm are combined in this algorithm. This combination will increase the difficulty of an

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

attacker breaking the system. The limitations of individual cryptographic methods are likewise overcome by the hybrid cryptography system. The Vigenere encryption has also been modified and used in cryptography. Cryptography is a dynamic field that requires new and increasingly complex methods to keep data secure.

VII. REFERENCES

1. *April Lia Hananto, Arip Solehudin, Agung Susilo Yuda Irwan, Bayu Priyatna, "Analyzing the kasiski method against Vigenere cipher", International Journal of Computer Techniques—Volume 6 Issue 6, November 2019.*
2. *Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma, "Design of Hybrid Cryptography System based on Vigenere cipher and Polybius cipher", 2020 International Conference on Computational Performance Evaluation(ComPE), North-Eastern Hill University, Shillong, Meghalaya, India. July 2—4,2020.*
3. *Bhavana K V, Banushree D J, Bhumika D, Chaitanya K B, Prof. Raghu B R , "A Cryptosystem using Vigenere and Polybius cipher", International Journal of engineering applied science and technology, 2021, Vol.6, Issue 2.*
4. *S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, "A research paper on new hybrid cryptography algorithm."*
5. *A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., "An extended hybridization of vigenere and caesar cipher techniques for secure com- ´ munication," Procedia Computer Science, vol. 92, pp. 355–360, 2016.*
6. *Q.-A. Kester, "A cryptosystem based on vigenere cipher with varying ` key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, no. 10, pp. 108–113, 2012.*
7. *C. Bhardwaj, "Modification of vigenere cipher by random numbers, ` punctuations & mathematical symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278–0661, 2012.*
8. *F. M. S. Ali and F. H. Sarhan, "Enhancing security of vigenere cipher ` by stream cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 1–4, 2014.*
9. *A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigenere cipher for ` data security," Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.*
10. *P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.*