International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

DESIGN OF HYBRID CRYPTOGRAPHY SYSTEM BASED ON VIGENERE CIPHER AND POLYBIUS CIPHER

Mr. K. R. Surendra[1], V Jyothipriya[2], Tamadalapati Vijayalakshmi[3], Sankula Omkar[4], Thati Anitha[5], C Charan[6]

[1]*Assistant Professor, Dept. of ECE, S V College of Engineering, Tirupati, A.P, India.*

[23456]*B.Tech Students, Dept. of ECE, S V College of Engineering, Tirupati, A.P, India.*

ABSTRACT

This paper presents a design of hybrid cryptography system based on Vigenère cipher and Polybius cipher. Secure communication of message from sender to receiver is one of the main security concerns of internet users across world. It is because of the regular attacks and threats and most important data privacy. In order to sort out these issues, we use cryptographic algorithm which encrypts data in some cipher and transfers it over the internet and again decrypted to original data. Thus, lightweight cryptography methods are proposed to overcome many of the problems of conventional cryptography. Cryptography is the science of protecting information by transforming it into a secure format. This process, called encryption, has been used centuries to prevent handwritten messages from being read by unintended recipients. Ciphers act as encapsulating system for message. Hybrid algorithm will be formed from use of different types of ciphers. The cryptosystem performs its encryption by encrypting the plaintext using Vigenère cipher and further again processing though Polybius cipher.

Keywords: *Cryptography, Vigenère Cipher, Polybius Cipher, Python.*

1. INTRODUCTION

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. Cryptography is a term defined as encapsulating and contriving techniques which permit important information and data to be sent in a protected structure so that the individual ready to recover this information [1]. Encryption is defined as a systematic procedure of changing over plain message into cipher text. Encryption process needs any programmed encryption algorithm and a key to change the plain message text into cipher[2].

In cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing and verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

Symmetric Key Cryptography – This is also termed as Private or Secret key cryptography. Here, both the information receiver and the sender make use of a single key to encrypt and decrypt the message. The frequent kind of cryptography used in this method is AES (Advanced Encryption System). The approaches implemented through this type are completely streamlined and quicker too.

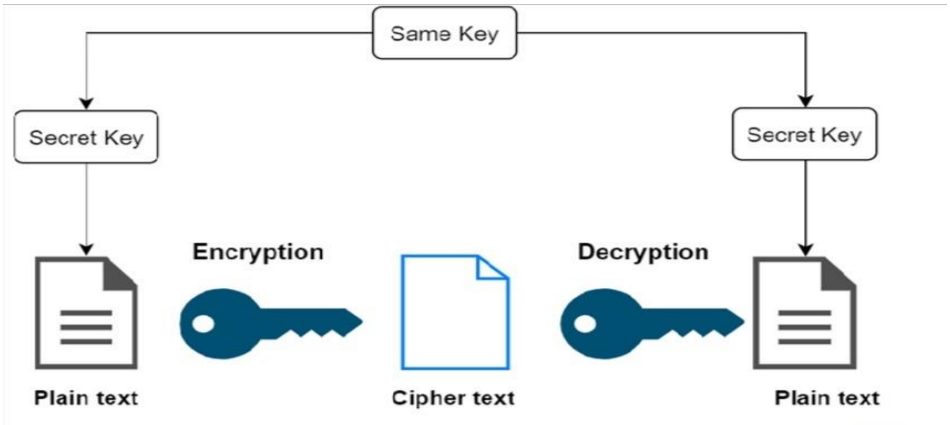

Fig .1: Symmetric Key Cryptography

2. LITERATURE REVIEW OF CRYPTOGRAPHY

Vigenère cipher algorithm was derived as scrabbled and scattering is given by combination and summation of a subjective piece of each byte and bits before the message and string are mixed using the system Vigenère cipher. This procedure crashes and burns the so called kasiski attack to find the length of the key because of the padding of the message and string with sporadic bits. The central drawback and nil improvement of this framework are that the size of the mixed text and string will be expanded by approximately calculated 56% [4].

New technique has been Introduced in this paper as Vigenère Cipher constitute alphabetic numerical and punctuation marks as colon, comma, semicolon, question marks, underline, full stop and brackets are used as the key instead of character to formed it increasingly hard for active and passive assault and attacks and spreading this spread the rang, so literate people who understand basic of cryptography can recognize the message [5]

In the security for web keeping money, account pass words, messages account secret word, etc requires content protection in mechanized media [3]. It shows the security besides, pressure for the information with the move encryption standard. To improve the quality of encryption algorithm they proposed a hybrid model.

The proposed model is a blend combination of AES and DES algorithmic cryptographic. The two algorithms are symmetric key procedure and reconciliation of AES and DES would give a solid degree of security of encryption end. A critical improvement in results has been seen with the proposed arrangement [6].

3. EXISTING METHOD

Vigenère Cipher:

Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table. The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left

ISSN: 2454-9665

compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. If the length of the key is less than the length of the message then the key, then the key is repeated until it matches the length of the message.

Encryption: We can convert the plaintext to ciphertext using the formula

$$Ei = [Pi + Ki] + \text{modulus } (26)$$

The plaintext(P) and key(K) are added to the modulus of 26. For example

Plaintext: INDIA

Key: TIGER

Ciphertext: BVJMR

The main letter of the plaintext, alphabet I is in a row is combined with the alphabet T is the key that is a column and results in the output B. Similarly, another letter will be processed in the same format and will result in encoded message.

Decryption: We can convert the ciphertext to plaintext using the formula

$$Di = (Ei - Ki + 26) \text{ modulus} 26$$

Where E is the Encrypted text

In row the key, alphabet T is combined with the ciphertext alphabet B, which will result in the output I of the plaintext. The simpler and easier approach is to view Vigenère logarithmically by changing over alphabets[A-Z] into numeric as [0-25].

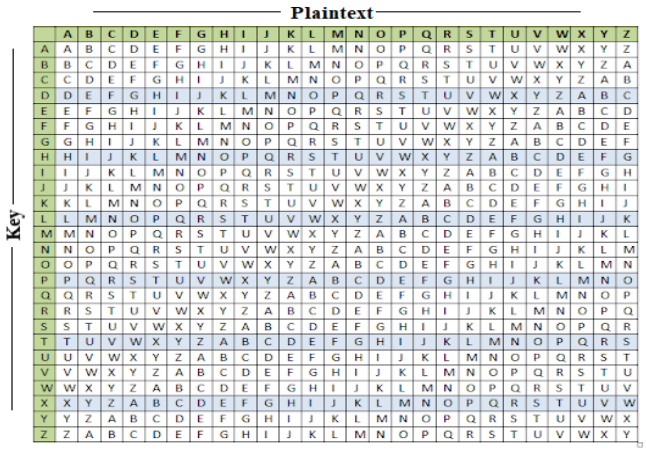

Fig. 2: Vigenère Square Table

Polybius Cipher:

A Polybius square is a table that allows someone to convert letters into numbers. To make the encryption little harder, this table can be randomized and shared with the recipient. In order to fit the 26 letters of the alphabet into the 25 cells created by the table, the letters ‘i’ and ‘j’ are usually combined into a single cell. Originally there was no such problem because the ancient Greek alphabet has 24 letters.

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

	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. 3: Polybius square

Example- ORDER

O is placed in row 3 and column 4 so output code is 34, R is placed in row 4 and column 2 so output code is 42 and soon. The resultant output for ORDER is 34 42 14 15 42.

To increase the security of the Polybius cipher we change the Polybius table using the key.

If the key is INTER, then we can change the Polybius square table to the below table

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

Fig. 4: Polybius Square Using Key

Example- ORDER

O is placed in row 4 and column 1, R is placed in row 1 and column 5 and soon. The resultant output for ORDER after using the key is 41 15 24 14 15.

4. PROPOSED METHOD

The method employs use of both Vigenère Cipher and Polybius Square Cipher in its encryption process. Message and the key are given to the Vigenère cipher and the cipher text is in return given to Polybius cipher. This process will reverse at the receiver side first the Polybius cipher is executed and then the Vigenère cipher. The modified hybrid of Polybius cipher and Vigenère cipher program software give outputs that show the difficulty of breaking the cipher text. The program written was used to encrypt a message and the result was analyzed by various methods of cryptanalysis. This is called Hybrid cryptography because it combines both Vigenère cipher and Polybius cipher.

As we combined both Vigenère cipher and Polybius cipher the security of the system is increased and it is safe from the attacks.

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

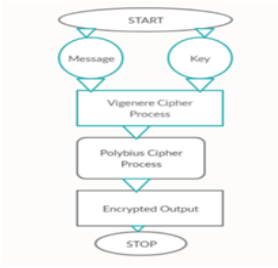

Fig. 5: Flowchart of hybrid algorithm

5. METHODS OR TECHNIQUES USED

Programming language used: Python

Python is a high-level, interpreted, general-purpose programming language. Python has a simple syntax similar to the English language. Python is dynamically typed and garbage collected. Python has syntax that allows developers to write programs with fewer lines than some other programming languages. Python runs on an interpreter system, meaning that code can be executed as soon as it is written. we use the python version Python 3.

6. RESULT

A. Encryption:

Phase 1 (Vigenère Cipher)

MESSAGE – CAPITAL

KEY- STATE

VIGENERE CIPHER OUTPUT- U T P B X S E

Phase 2 (Polybius Cipher)

TEXT- U T P B X S E

POLYBIUS OUTPUT- 51 12 43 20 54 11 14

B. Decryption:

Phase 1 (Polybius Cipher)

MESSAGE- 51 12 43 20 54 11 14

OUTPUT- U T P B X S E

Phase 2 (Vigenère Cipher)

TEXT- U T P B X S E

KEY- STATE

VIGENERE OUTPUT- CAPITAL

The modified hybrid of Polybius cipher and Vigenère cipher program software give outputs that show the difficulty of breaking the cipher text. The program written was used to encrypt a message and the result was analyzed by various methods of cryptanalysis.

7. ADVANTAGES OF PROPOSED SYSTEM

1. As we combine both the Vigenère cipher and Polybius cipher the security of the message is increased, hacking also become difficult.

ISSN: 2454-9665

2. Cryptanalysis, frequency analysis, pattern prediction and brute attack on proposed technique are also much difficult due to use of Combination of two Cipher for encryption.
3. As we build the Polybius table using key it is difficult to attack without knowing the key.

8. APPLICATIONS

1. Army
2. Police System

9. CONCLUSION

Cryptography is the generally utilized technique for the security, privacy, confidentiality and reliability of data. Single classic ciphers are cryptographic techniques that are viewed as least complex. Vigenère cipher is the famous cipher but also has few drawbacks. Vigenère cipher is one of the cryptographic methods that is considered simplest and weakest. So, combination of two ciphers provides more security. Combination of Polybius cipher and Vigenère that is a lot more secure against attacks like Active, passive, Kasiski and Friedman assaults (attacks). Cryptanalysis, recurrence examination, men in middle attacks, frequency analysis, fault analysis attacks, design expectation and brute force attacks.

10. FUTURE SCOPE

Although there are many cryptographic methods but this domain still requires serious attention of research community for the improvement of data security. In future our aim is to provide validation of proposed approach by performing security and performance.

11. REFERENCES

[1] K. Jakimoski, “Security techniques for data protection in cloud computing,” International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.

[2] A. A. Soofi, I. Riaz, and U. Rasheed, “an enhanced Vigenère cipher for data security,” Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.

[3] P. Kumar and s. B. Rana, “development of modified aes algorithm for data security,” Optik, vol. 127, no. 4, pp. 2341–2345, 2016.

[4] C. Sanchez-Avila and R. Sanchez-Reillol, “The Rijndael block cipher (aes proposal): a comparison with des,” in Proceedings IEEE 35th annual2001 International Carnahan Conference on Security Technology (cat.no. 01ch37186). IEEE, 2001, pp. 229–234.

[5] C. Bhardwaj, “Modification of Vigenère cipher by random numbers, punctuations & mathematical symbols,” Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278–0661, 2012.

[6] P. Gutmann, “Cryptographic security architecture: design and verification”. Springer Science & Business Media, 2003