IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher

S.Naresh Goud[1] M.Pramod Kumar [2] G.Venkata Prasanth Reddy [3] K.Vishwanath [4]

20x51a04B7@srecnandyal.edu.in 20x51a04A2@srecnandyal.edu.in
viswanathvaraprasad56@gmail.com 20x55a0405@srecnandyal.edu.in

1, 2, 3, 4 students, Department of Electronics and Communication, Santhiram Engineering College, A.P, India.
Santhiram Engineering College (Autonomous) Nandyal, Ap, India, 518501 (2020-2024)

ABSTRACT:

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 Vigenere cipher and further again processing though Polybius cipher. The proposed method employs use of both Vigenere cipher and Polybius squarer cipher in its encryption process. The ciphertext will first be operated on using Vigenere. A chosen key out of random will initiate the process. At the end of the process, the resulting ciphertext then becomes a message as input for the Polybius square cipher process. This process will end up making the final ciphertext more difficult to be broken using existing cryptanalysis processes. A software program will be written to demonstrate the effectiveness of the algorithm using python programming language and cryptanalysis will be performed on the ciphertext.

INTRODUCTION: In the present direction of the world, the innovations have progressed so much that the vast majority of the people incline toward utilizing the internet as the essential intends to consign data starting with one end then onto the next over the world. There are numerous potential approaches to communicate data utilizing the internet: through messages, talks, and so on. The data change is made very snap, quick and exact utilizing the internet. In any case, one of the primary tests with sending data over the internet is the "security risk" it presents, for example, the individual or privy data can be packed away or hacked from various perspectives. In this way, it turns out to be essential to mull over data security, as it is one of the most vital variables that need consideration during the process of data transfer [1]. Security is a significant factor in the open system and cryptography assumes a significant job in this field. Cryptography is old and made sure about the system of information out in the open system. Be that as it may, the goal of cryptography is utilized not exclusively to give classification, yet in addition to giving arrangements to different issues: data trustworthiness, verification, non-denial. 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 main individual ready to recover this information is the conscious beneficiary. Cryptography is a systematic technique and procedure to hide the data and information over a communication channel. It is a craftsmanship to hide the data from outsiders. As the innovation grows step by step the need for data security over the communication channel is expanded to a high degree. Encryption is defined as a systematic procedure of changing over plain message text into ciphertext. Encryption process needs any programmed encryption algorithm and a key to change over the plain message text into cipher. In the cryptography system encryption execute at the message sender side. Encryption executes the message at sender's side before sending it to the receiver. Decryption is an opposite systematic procedure of encryption. It transforms the encrypted ciphertext into a message plaintext. In cryptography system decryption procedure execute at the receiver side. The process of decryption algorithm requires a couple of steps such as - a Decryption algorithm and a key. Cryptography is extensively isolated into two classes relying on the Key; which is characterized as the guidelines used to change over a unique book into scrambled content: Asymmetric Key Encryption and Symmetric Key Encryption. A symmetric key encryption utilizes a similar key for decryption and encryption processes. This system is a basic yet ground breaking yet key circulation is the main issue that should be addressed. While asymmetric key encryption utilizes two mathematically related keys: Public Key and Private Key for encryption. The public key is accessible to everybody

PURPOSE: PCs will be undependable if they are associated with a worldwide system, particularly the internet [2]. The locales visited a great extent have infections, malware or the like that can take singular data from a PC. Security is fundamental to keep up a key good way from data replication, stealing, visualizing, detection and intrusion. The core of PC security is done to guarantee the PC and its system to ensure the data safe and secure inside the system [13]. PC security works and incorporates a few angles, for example:

- Privacy is usually that is confidential. The fact of the matter is anticipation with the goal that unapproved individuals don't get to information and data. Avoidance is conceivable to utilize encryption innovation, so just the information proprietor can discover genuine information.

- Confidentiality involves a set of rules or a promise usually executed through confidentiality rule agreements that limit access or places restrictions on certain types of information. It shows when requested to demonstrate somebody's wrongdoing, regardless of whether the information keeper will offer information to the individual who mentioned it or keep up the customers.

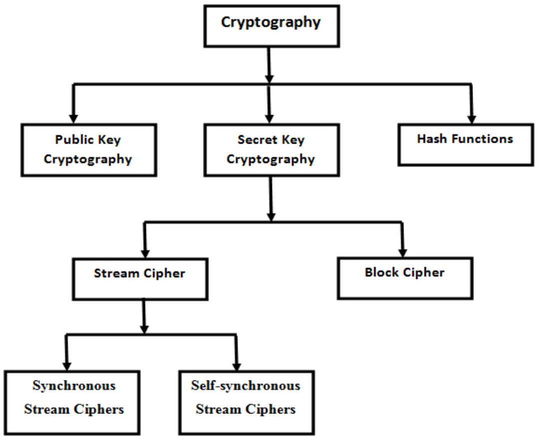
- Non-repudiation is the process that sides to the capacity to guarantee that involved with an agreement or a communication can't prevent the realness from securing their mark on an archive or the sending of a message that they started. To disavow intends to deny. For a long time, specialists have looked to make repudiation unthinkable in certain circumstances. We may send enlisted mail, for instance, so the beneficiary can't deny that a letter was conveyed. Thus, an authoritative archive regularly expects observers to mark with the goal that the individual who signs can't deny having done as such. On the Internet, an advanced mark is utilized not exclusively to guarantee that a message or report has been electronically marked by the individual that implied to sign the archive, yet additionally, since a computerized mark must be made by one individual, to guarantee that an individual can't later deny that they outfitted the mark.

- Integrity, Data integrity defines as alludes to the dependability and reliability of data all through its lifecycle. It can portray the condition of your data e.g., substantial or invalid or the process of guaranteeing and protecting the legitimacy and precision of data.

- Authentication is a safety effort planned and processed to build up the legitimacy and oneness of a transmission, message, or pre originator, or methods for checking a persons authorization to get explicit classifications of data. It is done to verify the login user who is trying to log in for the procurement of the message. It checks first the user details for login as username and password. Then after checking the whole details, it allows entering the system. It is an important process for the protection of Information.

- Availability ensures that systems, applications and data are accessible to clients when they need them. The most widely recognized assault that impacts accessibility is disavowal of administration in which the assailant interferes with access to data, framework, gadgets or other network assets. A refusal of administration in an inward vehicular network could bring about an ECU not having the option to access the data expected to work and the ECU could become non operational or even most noticeably terrible it could carry the framework to a hazardous state. To keep away from accessibility issues, it is important to incorporate repetition ways and failover procedures in the planning stage, just as to incorporate interruption avoidance systems that can monitor network traffic design, decide whether there is an abnormality and square network traffic when required. Cryptography has four fundamental parts, for example: 1. The plaintext is defined as a message that can be perused. 2. The ciphertext is a random unscripted, disputed and an informal message that is unable to be perused. 3. The key is a vital aspect for defining the cryptographic techniques such as symmetric and asymmetric. 4. An algorithm is a procedural solution to execute encryption and decryption algorithms in the system. Cipher: cryptography, a cipher (or cipher) is an algorithm for performing encryption or decryption (unscrambling) a progression of very much characterized advances that can be followed as a method. Another option, less regular term is encipherment. To encipher or encode is to change over data from plaintext into cipher or code. In nontechnical use, a ’cipher’ is a similar thing as a ’code’; nonetheless, the ideas are unmistakable in cryptography. In customary cryptography, ciphers were recognized from codes. Codes usually substitute differing length arrangement of characters in the yield, while ciphers regularly substitute an unclear number of characters from are input. There are exceptional cases and some cipher systems may use possibly more, or less, characters when yield versus the number that was input.

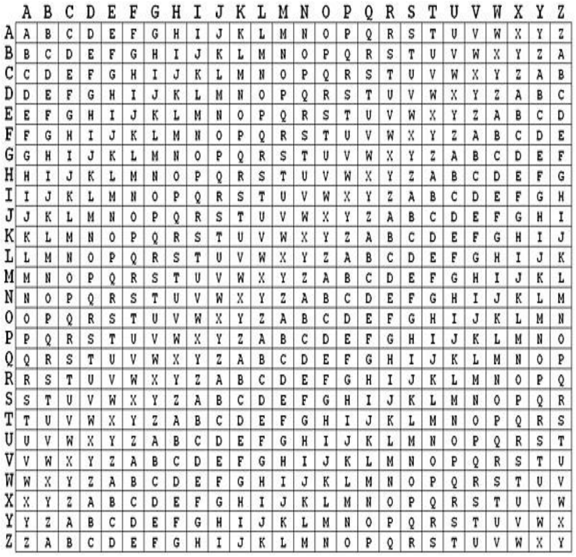
PROPOSED SYSTEM: The method employs use of both Vigenere Cipher and Polybius Square Cipher in its encryption process. Message and the key are given to the Vigenere cipher and the cipher text is in return given to Polybius cipher. This process will reverse at the receiver side first the Polybius cipher is executed and then the Vigenere cipher. The modified hybrid of Polybius cipher and Vigenere 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 Vigenere cipher and Polybius cipher. As we combined both Vigenere cipher and Polybius cipher the security of the system is increased and it is safe from the attacks. The flowchart representing the process of the proposed system is given below:



First the message and key are given to the Vigenere cipher and the output of Vigenere cipher i.e., cipher text. This ciphertext is given as input to the Polybius cipher for converting the alphabets to numerical format. The output of the Polybius cipher is the final encrypted output. At the receiver the entire process reverses first Polybius cipher converts the numerical data to alphabets and this output is given as input to Vigenere. After entering the key, the original plaintext, the sender sent is displayed. 1

ENCRYPTION:

Phase 1 (Vigenere 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 15 54 11 14



	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.Vigenere cipher

DECRYPTION:

Phase 1 (Polybius Cipher)

MESSAGE- 51 12 43 15 54 11 14

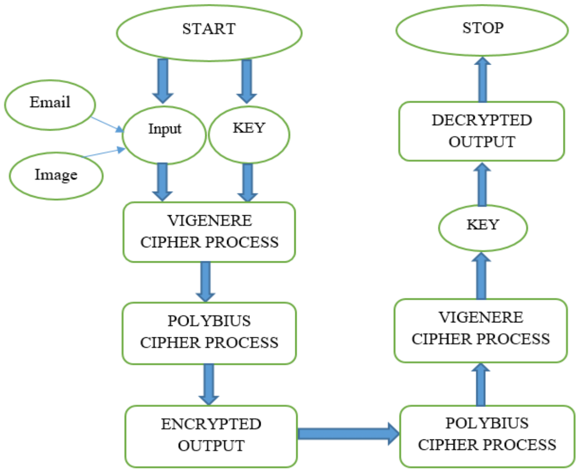
OUTPUT- U T P B X S E

Phase 2 (Vigenere Cipher)

TEXT- U T P B X S E

KEY- STATE DECRYPTED

OUTPUT- CAPITAL



ADVANTAGES OF PROPOSED SYSTEM:

- As we combine both the Vigenere cipher and Polybius cipher the security of the message is increased, hacking also becomes difficult.
- 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.

- As we build the Polybius table using key it is difficult to attack without knowing the key.

TECHNICAL SPECIFICATIONS:

SOFTWARE:

Text Type: str

Numeric Types: int, float, complex

Sequence Types: list, tuple, range

Mapping Type: dict

Set Types: set, frozen set

Boolean Type: bool

Binary Types: bytes, byte array, memory view
None Type: NoneType

FEATURES OF PYTHON:

1. Easy to Code

2. Easy to Read

3. Free and Open-Source

4. Robust Standard Library

5. Interpreted

6. Portable

7. Object-Oriented and Procedure-Oriented

8. Extensible

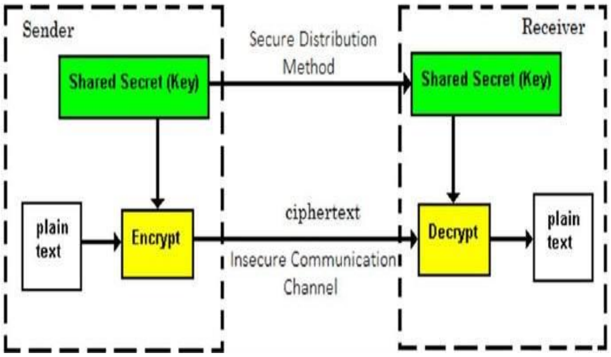
9. Expressive

10. Support for GUI

11. Dynamically Typed

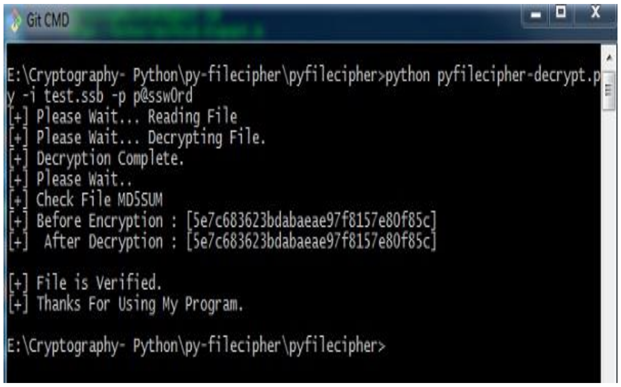
12. High-level Language

BLOCKDIAGRAM:



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. Vigenere 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 Vigenere 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. 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.

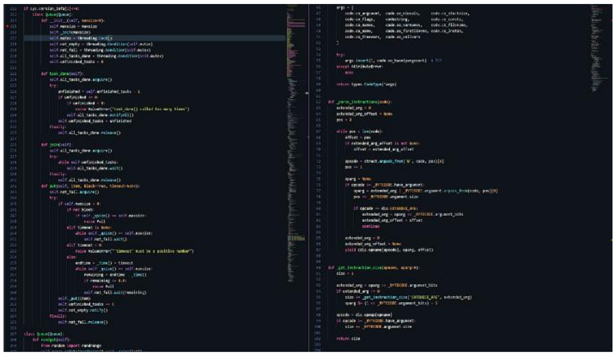
RESULT:



```
E:\Cryptography- Python\py-filecipher\pyfilecipher>python pyfilecipher-decrypt.p
y -i test.ssb -p p@ssw0rd
[+] Please Wait... Reading File
[+] Please Wait... Decrypting File.
[+] Decryption Complete.
[+] Please Wait..
[+] Check File MD5SUM
[+] Before Encryption : [5e7c683623bdabaeae97f8157e80f85c]
[+]  After Decryption : [5e7c683623bdabaeae97f8157e80f85c]

[+] File is Verified.
[+] Thanks For Using My Program.

E:\Cryptography- Python\py-filecipher\pyfilecipher>
```



REFERENCES:

[1] S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, “A research paper on new hybrid cryptography algorithm.”

[2] A. A. Soofi, I. Riaz, and U. Rasheed, “an enhanced Vigenere cipher for data security”.

[3] A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., “An extended hybridization of Vigenere and Caesar cipher techniques for secure communication”.

[4] J. Chen and J. S. Rosenthal, “Decrypting classical cipher text using markov chain monte carlo,” statistics and computing.

[5] M. B. Pramanik, “Implementation of cryptography technique using columnar transposition,” International Journal of Computer Applications.

[6] Q.-A. Kester, “A cryptosystem based on Vigenere cipher with varying key,” International Journal of Advanced Research in Computer Engineering & technology (IJARCET).

[7] F. M. S. Ali and F. H. Sarhan, “Enhancing security of Vigenere cipher ` by stream cipher,” International Journal of Computer Applications.

[8] A. P. U. Siahaan, “Protection of important data and information using gronsfeld cipher,”2018.

[9] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, “Data security using Vigenere cipher and goldbach codes algorithm,” ` Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.

[10] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, “An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher,” in 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018, 2018.

[11] J. David and S. Kumar, "Investigation on secondary memory management in wireless sensor network", Int. J. Computer. Eng. Res. Trends, vol. 876, no. 6, pp. 387-391, 2015.