A

PROJECT REPORT OF

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

Submitted in partial fulfillment of the requirements for the award of the degree of

**MASTER OF COMPUTER APPLICATIONS**

By

#### RACHAMALLU KARTHIK (21BF1F0099)

Under the esteemed guidance of

#### K.BHUVANESWARI MCA

**Assistant Professor**



**DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS**

**SRI VENKATESWARA COLLEGE OF ENGINEERING**

**(AUTONOMOUS)**

#### (Approved by AICTE, New Delhi & Affiliated to JNTUA, Anantapuramu) Accredited by NAAC with ‘A’ Grade

**Opp.LIC Training Centre, Karakambadi Road, TIRUPATI–517507**

##### 2021-2023

\*\*\*

**SRI VENKATESWARA COLLEGE OF ENGINEERING (AUTONOMOUS)**

**(Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu)**

#### Accredited by NAAC with ‘A’ Grade

**Opp.LIC Training Centre, Karakambadi Road, TIRUPATI – 517507 DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS 2021-2023**



**CERTIFICATE**

*This is to certify that the project report entitled”* ***DESIGN OF HYBRID CRYPTOGRAPHY SYSTEM BASED ON VIGENERE CIPHER AND***

***POLYBIUS CIPHER* ”***is a bonafide record of the project work done and submitted by*

#### RACHAMALLU KARTHIK (21BF1F0099)

*for the partial fulfillment of the requirements for the award of* ***MASTER OF***

**COMPUTER APPLICATIONS** *Degree from SRI VENKATESWARA COLLEGE OF ENGINEERING (AUTONOMOUS) Affiliated to JNT Unitersity Anantapur,Anantapuramu.*

##### GUIDE HEAD OF THE DEPARTMENT

**INTERNAL EXAMINER EXTERNAL EXAMINER**

### ACKNOWLEDGEMENT

I am thankful to my guide **K. Bhuvaneswari, Assistant Professor** for her valuable guidance and encouragement. Her helping attitude and suggestions have helped me in the successful completion of the project**.**

I would like to express my sincere thanks to **Dr. E. Sreedevi,** Professor, Head of the Department of MCA, for her kind help and encouragement during the course of my study and in the successful completion of the project work.

I express my sincere thanks to **Dr. N. Sudhakar Reddy**, Principal, S.V College of Engineering, Tirupati.

Successful completion of any project cannot be done without proper support and encouragement. My sincere thanks to the Management for providing all the necessary facilities during the Course of my study.

I would like to thank my parents and friends, who have the greatest contributions in all my achievements, for the great care and blessings in making me successful in all my endeavors.

I would like to express my deep gratitude to all those who helped me directly or indirectly to transform an idea into my working project.

#### R.KARTHIK (21BF1F0099)

**DECLARATION**

I hereby declare that the project entitled **“*DESIGN OF HYBRID CRYPTOGRAPHY SYSTEM BASED ON VIGENERE CIPHER AND POLYBIUS CIPHER* ”**

submitted to the Department of MASTER of COMPUTER APPLICATIONS,

##### SRI VENKATESWARA COLLEGE OF ENGINEERING(AUTONOMOUS),

**TIRUPATI** in partial fulfillment of requirements for the award of the degree of **MASTER OF COMPUTER APPLICATIONS**.

This project is the result of my own effort and it has not been submitted to any other University or Institution for the award of any degree other than specified above.

#### Signature of the student

**R.KARTHIK**

**(21BF1F0099)**

### 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 Vigenère cipher and further again processing though Polybius cipher.

The proposed method employs use of both Vigenère cipher and Polybius squarer cipher in its encryption process. The ciphertext will first be operated on using Vigenère. 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.

|  |  |  |
| --- | --- | --- |
| **S.No** | **Contents** | **Page No** |
| 1 | Introduction  1.1 Introduction | 1 |
|  | 1.2 Scope | 2 |
|  | 1.3 Objective | 3 |
|  | 1.4 Description of the Project | 6 |
| 2 | Literature Survey | 10 |
| 3 | Types of Cryptography | 12 |
| 4 | System Analysis  4.1 Existing System | 22 |
|  | 22 |
|  | 4.2 Proposed System | 40 |
|  | 4.3 Hardware and Software Requirement | 44 |
| 5 | System Design | 45 |
|  | * 1. History of UML Diagrams   2. UML Diagrams | 45  46 |
| 6 | Implementation  6.1 Description of Modules | 48 |
|  | 48 |
|  | 6.2 Overview of Implementation of language | 52 |
| 7 | Testing | 59 |
|  | 7.1 Software Testing | 59 |
| 7.2 Testing Techniques | 61 |
|  | 7.3 Testing Strategies | 64 |
| 8 | Results | 66 |
| 9 | Conclusion And Future Work | 67 |
| 10 | Appendix | 68 |
|  | 10.1 Sample Code | 68 |
|  | 10.2 Screen shots | 72 |
| 11 | Reference | 73 |

#### LIST OF FIGURES

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Figure Name** | **Page No.** |
| 1.1 | Hieroglyph old Cryptographic technique | 7 |
| 1.2 | Steganography | 7 |
| 3.1 | Components of Cryptography | 12 |
| 3.2 | Symmetric key Cryptography | 17 |
| 3.3 | Asymmetric key Encryption | 18 |
| 3.4 | Hash Function | 19 |
| 3.5 | Types of Cryptography | 20 |
| 4.1 | Vigenère Square Table | 28 |
| 4.2 | Converting Alphabets to Numbers | 31 |
| 4.3 | Polybius Square | 36 |
| 4.4 | Polybius Square having Greek Alphabets | 37 |
| 4.5 | Polybius Square having digits | 38 |
| 4.6 | Polybius Square having key in it | 38 |
| 4.7 | Polybius Square with key line | 39 |
| 4.8 | Flowchart of Hybrid System | 40 |
| 5.1 | Symmetric Encryption | 46 |
| 5.2 | Flow chart of Hybrid Model | 47 |
| 6.1 | Representing the datatypes of python | 56 |

10.2.1 Input to the Hybrid System 72

10.2.2 Final Output of Hybrid System 72

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Table No.** | **Table Name** | **Page No.** |
| 1 | Relation between Encryption Schemes | 20 |
| 2 | Encryption using Formula | 32 |
| 3 | Decryption using Formula | 33 |

# INTRODUCTION

#### INTRODUCTION

Human being from ages had two inherent needs: (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word ‘cryptography’ was coined by combining two Greek words, ‘Krypto’ meaning hidden and ‘graphene’ meaning writing.

**Cryptography** is technique of securing information and communications through use of codes so that only those persons 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”

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, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

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 such as - a Decryption algorithm and a key.

##### SCOPE:

The scope of designing hybrid cryptography using the Polybius square and Vigenère cipher is to enhance more security, privacy, confidentiality and reliability of data. Both the Polybius square and Vigenère cipher are classical ciphers, and combining them in a hybrid approach can potentially offer enhanced security. 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, Kasis ki and Friedman assaults (attacks). Cryptanalysis, recurrence examination, men in middle attacks, frequency analysis, fault analysis attacks, design expectation and brute force attacks.

##### OBJECTIVE:

The primary **OBJECTIVE** of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

##### Confidentiality:

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy. Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption. It 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.

##### Data Integrity:

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

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:

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. Authentication service has two variants:

* Message authentication identifies the originator of the message without any regard router or system that has sent the message.
* Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

It is the safety effort planned and processed to build up the legitimacy and oneness of a transmission, message, or pre originator, or methods for checking a person’s 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.

1. **Non-repudiation**: It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party. Non- repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

It is a 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.

**(5)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 nonoperational 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 fail over 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.

##### DESCRIPTION OF THE PROJECT:

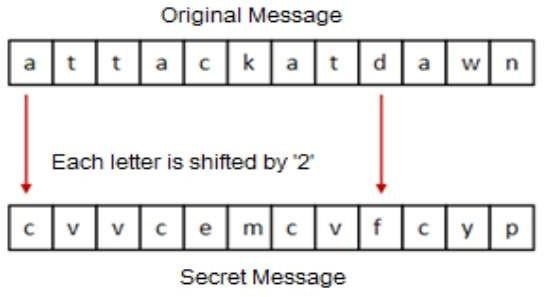
The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.

##### Hieroglyph – The Oldest Cryptographic Technique

The first known evidence of cryptography can be traced to the use of ‘hieroglyph’. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph. This code was the secret known only to the scribes who used to transmit messages on behalf of the kings.

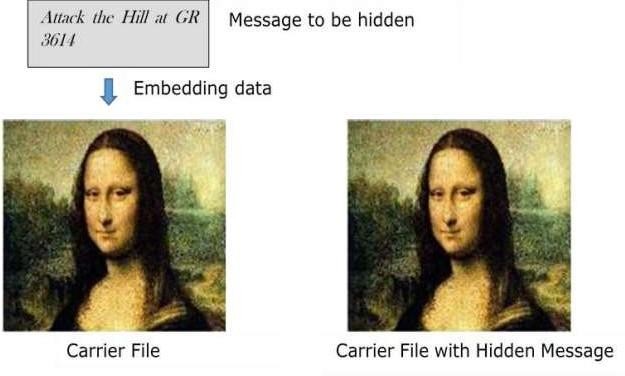
Later, the scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC. The first known use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. These consisted of complex pictograms, the full meaning of which was only known to an elite few.

This involved replacing alphabets of message with other alphabets with some secret rule. This rule became a key to retrieve the message back from the garbled message. The earlier Roman method of cryptography, popularly known as the Caesar Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.



##### Fig 1.1 Hieroglyph old cryptographic technique

1. **Steganography**:

Steganography is similar but adds another dimension to Cryptography. In this method, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists. For example, invisible watermarking. In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.

##### Fig 1.2 Steganography

**Evolution of Cryptography:**

It is during and after the European Renaissance, various Italian and Papal states led the rapid proliferation of cryptographic techniques. Various analysis and attack techniques were researched in this era to break the secret codes.

1. Improved coding techniques such as **Vigenère Coding** came into existence in the 15th century, which offered moving letters in the message with a number of variable places instead of moving them the same number of places.
2. Only after the 19th century, cryptography evolved from the ad hoc approaches to encryption to the more sophisticated art and science of information security.
3. In the early 20th century, the invention of mechanical and electromechanical machines, such as the **Enigma rotor machine,** provided more advanced and efficient means of coding the information.
4. During the period of World War II both cryptography and cryptanalysis became excessively mathematical.

With the advances taking place in this field, government organizations, military units, and some corporate houses started adopting the applications of cryptography. They used cryptography to guard their secrets from others. Now, the arrival of computers and the Internet has brought effective cryptography within the reach of common people.

##### Context of Cryptography:

Cryptology, the study of cryptosystems, can be subdivided into two branches

* Cryptography
* Cryptanalysis

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

##### Polybius Cipher:

The Polybius cipher is a simple substitution cipher that replaces each letter of the plaintext with a two-digit number, based on its position in a 5x5 grid. The main advantage of the Polybius cipher is its simplicity, making it easy to use and understand.

##### Vigenère Cipher:

The **Vigenère** cipher is a polyalphabetic substitution cipher that uses a keywordto determine different Caesar shift values for each letter in the plaintext. This makes it more secure than simple substitution ciphers like the Polybius cipher.

**2.LITERATURE SURVEY**

In the security for web keeping money, account passwords, messages account secret word, etc. requires content protection in mechanized media. It shows the security besides, pressure for the information with the move encryption standard. The Number of continuous rounds increases the greater security that can be break by active and passive attacks by software engineers, intruders and hackers. Caesar cipher, otherwise called the shift cipher, is least perplexing and large known old-style encryption systems. It is a sort of replacement cipher in which each letter in the plain text is supplanted. For instance, with a move of 2, A would be supplanted by C, B would become D, and similarly.

The encryption technique system performed by Caesar ciphers is a combination and thoroughly goes together as a disputed and complex growth plan as Vigenère Cipher and to date, it has advantages in the ROT13 framework and paraphrase system. Similarly, in substitution ciphers, the Caesar cipher is effortlessly and discreetly broken and in present-day structure, the use shows no correspondence security and protection. Caesar Cipher’s strategy is one of the soonest and least complex techniques for the encryption method. It’s a kind of replacement cipher, i.e., each letter of a given text is supplanted by a letter some fixed number of positions down the letters in order. For instance, with a move of 1, M would be supplanted by N, N would become O, and so on. Caesar cipher is effortlessly and discreetly broken and in present-day structure, the use shows no correspondence security and protection. Caesar Cipher’s strategy is one of the soonest and least complex techniques for the encryption method. Its a kind of replacement cipher, i.e., each letter of a given text is supplanted by a letter some fixed number of positions down the letters in order. For instance, with a move of 1, M would be supplanted by N, N would become O, and so on.

This technique is named after Julius Caesar, who utilized it to speak with his authorities. Accordingly, to cipher a given text we need a whole number worth, known as a move which demonstrates the quantity of position each letter of the the text has been descended. The transposition cipher is a process and adaptive system of encryption system by which location and position held by units of plaintext are moved by a standard structure or model so that the ciphertext includes a phase of the plaintext.

The location is the main substitute that is always occupied and pre location movement by given derived metric graph that can be used by string or message given by the sender. In changed variation of Vigenere cipher algorithm was` derived as scrabbled and scattering is given by combination and summation of a subjective piece to each byte and bits before the message and string are mixed using the system Vigenere 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%.

Another strategy for executing the Vigenere algorithm was` introduced and brought up as through normally and systematically for encryption and diffusion of message need key to be replaced again and again. But here primary keys act as Continuation for exchange of replaced key for the process. New technique has been Introduced in this paper as Vigenere 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.

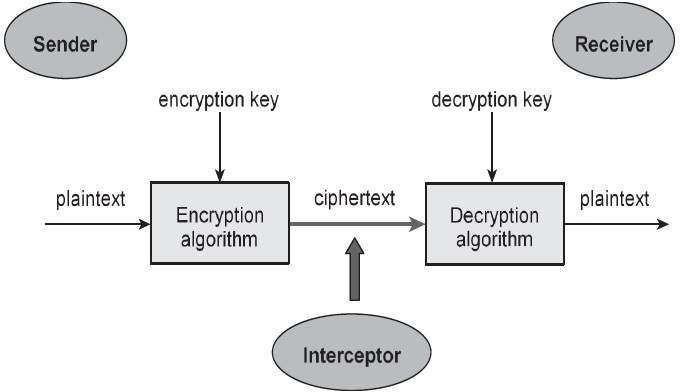
It addresses that the internet is one of the most perilous communication medium because of immense association and open system. Data assurance is one of the basic parametric prerequisite. At present different security algorithms are proposed to accomplish security during communication. Every one of them has certain valid statements and certain awful points.

To improve the quality of the 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 itself they are especially able for encryption. Reconciliation of AES and DES would give a solid degree of security at encryption end. A critical improvement in results has been seen with the proposed arrangement.

# 3.TYPES OF CRYPTOGRAPHY

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below.



##### Fig 3.1 Components of cryptography

The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

##### Components of cryptography:

The various components of a basic cryptosystem are as follows:

* **Plaintext:** It is the data to be protected during transmission.
* **Encryption Algorithm:** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
* **Ciphertext:** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
* **Decryption Algorithm:** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
* **Encryption Key:** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
* **Decryption Key:** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a key space.

An interceptor (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

##### Cryptography Types:

In **cryptography**, encryption of the information is classified as three types where those are discussed below:

* Symmetric key cryptography
* Asymmetric key cryptography
* Hash functions

**3.2Symmetric Key Cryptography** – The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. 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. Few types of Symmetric key cryptography are

* Block
* Block cipher
* DES (Data Encryption System)
* RC2
* IDEA
* Blowfish
* Stream cipher

One of the most widely used symmetric encryption ciphers is the Advanced Encryption Standard (AES), defined as a U.S. government standard by the National Institute of Standards and Technology (NIST) in 2001. AES supports three different key lengths, which determine the number of possible keys: 128, 192, or 256 bits. Cracking any AES key length requires levels of computational power that are currently unrealistic and unlikely ever to become so. AES is widely used worldwide, including by government organizations like the National Security Agency (NSA).

##### Data Encryption Standard (DES):

The most common SKC scheme used today, DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES is a block- cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well-designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

##### Advanced Encryption Standard (AES):

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack.

The features of AES are as follows −

* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details

AES has been adopted by the U.S. government. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric key algorithm, meaning the same key is used for both encrypting and decrypting the data.

The number of rounds depends on the key length follows:

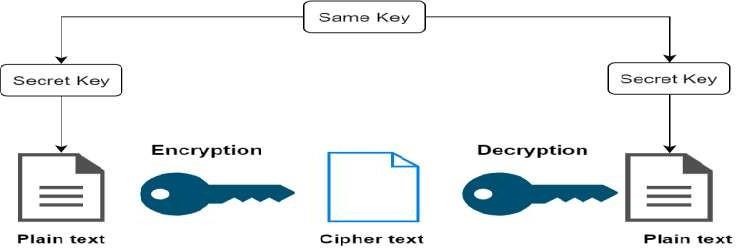
* 128 bit key – 10 rounds
* 192 bit key – 12 rounds
* 256 bit key – 14 rounds

##### Challenge of Symmetric Key Cryptosystem:

There are two restrictive challenges of employing symmetric key cryptography.

* Key establishment – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
* Trust Issue – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

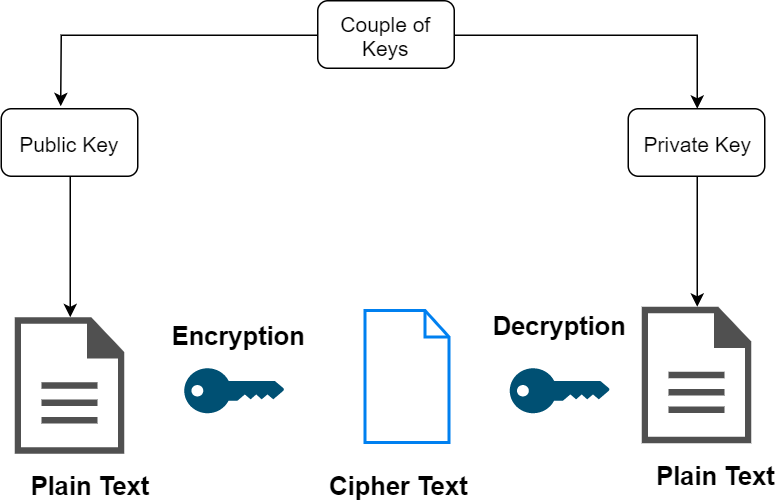


##### Fig 3.2 Symmetric key cryptography

* 1. **Asymmetric key cryptography:**

This is also termed as Public-key cryptography. It follows a varied and protected method in the transmission of information. Using a couple of keys, both the sender and receiver go with encryption and decryption processes. The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. A private key is stored with each person and the public key is shared across the network so that a message can be transmitted through public keys. The frequent kind of cryptography used in this method is RSA. The public key method is more secure than that of a private key. Few of the kinds of Asymmetric key cryptography are:

* RSA
* DSA
* PKCs
* Elliptic curve techniques



##### Fig 3.3 Asymmetric Key Encryption Challenge of Public Key

**Cryptosystem**:

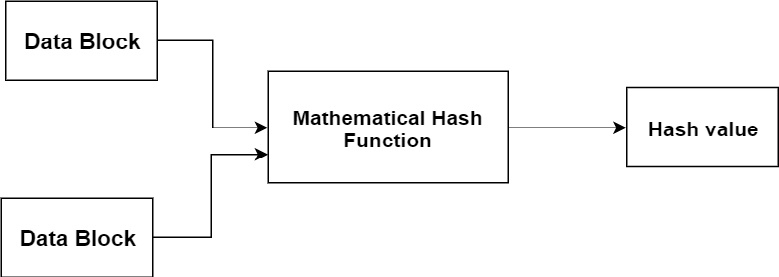
Public-key cryptosystems have one significant challenge: the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party. This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process - that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

##### Hash Function

Taking the arbitrary length of the message as input and delivering a fixed length of the output is the algorithm followed by a hash function. It is also termed as a mathematical equation by taking numerical values as input and produce the hash message. This method will not need any kind of key as it functions in a one-way scenario. There are various rounds of hashing operations and every round considers input as an array of the recent block and generates last round activity as output. Few of the functionalities of the hash are:

* Message Digest 5 (MD5)
* RIPEMD
* Whirlpool
* SHA (Secure hash Algorithm)



##### Fig 3.4 Hash Functions

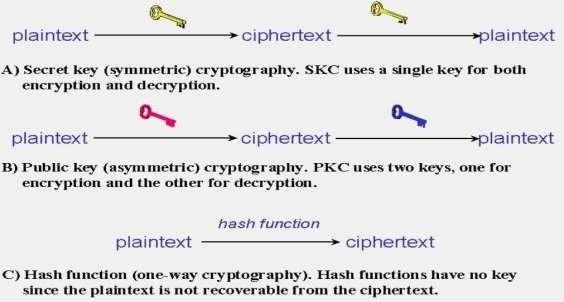
* 1. **Relation between Encryption Schemes**

A summary of basic key properties of two types of cryptosystems is given below –

|  |  |  |
| --- | --- | --- |
|  | **Symmetric Cryptosystems** | **Public Key Cryptosystems** |
| **Relation**  **between Keys** | Same | Different, but mathematically related |
| Encryption Key | Symmetric | Public |
| Decryption Key | Symmetric | Private |

##### Table 1 Relation between Encryption Schemes

Due to the advantages and disadvantage of both the systems, symmetric key and public- key cryptosystems are often used together in the practical information security systems.



##### Fig 3.5 Types of Cryptography

* 1. **Types of Attacks in Cryptography:**

There are two types of cryptography attacks, passive and active attacks.

**1.Passive attack:** In a passive attack, the intruder can only see the private data but can hardly make any changes to it or alter it. Passive attacks are more dangerous because the intruder only sees the message without altering it. Then no one will ever know that an attack is taking place, and their hidden messages will no longer be hidden.

* **Snooping:** Also known as message content leakage, snooping is a nonaggressive attack where the intruder can only read a message. This jeopardizes the security goal of confidentiality**.**

**2.Active attack:** In this type of attack, the intruder can alter the private data**.**

**3.Masquerade:** The intruder will try to gain as much access to the computer system as possible. Masquerade is an active attack that threatens the security goal of credibility.

**4.Brute force attack**: A brute force attack occurs when hackers use computers to feedback loop over each letter in a character set systematically. A character set can consist of letters, numbers, symbols, or anything else that the hackers may desire. In the most general terms, a brute force attack is a method of trial and error that attempts all possible password combinations. This method works well for short passwords, but it takes a long time to try all possible passwords.

**5.Dictionary attack**: It is a quick and easy password attack. Hackers generate thousands of candidate digests and their pre-matched plaintext passwords using a dictionary. These candidate digits are compared to those in a stolen digest file by hackers. If a match is found, they are given the password. Although this method appears to be feasible if done manually, computers are capable of processing millions of words in a matter.

**4.SYSTEM ANALYSIS**

* 1. **EXISTING SYSTEM**

##### 4.01 Introduction to Cipher:

**Cipher**: Any method of transforming a message to conceal its meaning. The term is also used synonymously with ciphertext or cryptogram in reference to the encrypted form of the message. A brief treatment of ciphers follows. For full treatment, see cryptology.

All ciphers involve either transposition or substitution, or a combination of these two mathematical operations—i.e., product ciphers. In transposition cipher systems, elements of the plaintext (e.g., a letter, word, or string of symbols) are rearranged without any change in the identity of the elements. In substitution systems, such elements are replaced by other objects or groups of objects without a change in their sequence.

In systems involving product ciphers, transposition and substitution are cascaded; for example, in a system of this type called a fractionation system, a substitution is first made from symbols in the plaintext to multiple symbols in the ciphertext, which is then super encrypted by a transposition. All operations or steps involved in the transformation of a message are carried out in accordance to a rule defined by a secret key known only to the sender of the message and the intended receiver.

Cipher devices or machines have commonly been used to encipher and decipher messages. The first cipher device appears to have been employed by the ancient Greeks around 400 BCE for secret communications between military commanders. This device, called the scytale, consisted of a tapered baton around which was spirally wrapped a piece of parchment inscribed with the message. When unwrapped the parchment bore an incomprehensible set of letters, but when wrapped around another baton of identical proportions, the original text reappeared. Other simple devices known as cipher disks were used by European governments for diplomatic communications by the late 1400s.

These devices consisted of two rotating concentric circles, both bearing a sequence of 26 letters. One disk was used to select plaintext letters, while the other was used for the corresponding cipher component.

In 1891 Étienne Bazeries a French cryptologist, invented a more sophisticated cipher device based on principles formulated by Thomas Jefferson of the United States nearly a century earlier. Bazeries’s so-called cylindrical cryptograph was made up of 20 numbered rotatable disks, each with a different alphabet engraved on its periphery. The disks were arranged in an agreed-upon order on a central shaft and rotated so that the first 20 letters of the message plaintext appeared in a row; the ciphertext was then formed by arbitrarily taking off any other row. The remaining letters of the message were treated in the same way, 20 letters at a time.

Advances in radio communications and electromechanical technology in the 1920s brought about a revolution in crypto devices - the development of the rotor cipher machine. One common type of rotor system implemented product ciphers with simple monoalphabetic substitution ciphers as factors. The rotors in this machine consisted of disks with electrical contacts on each side that were hardwired to realize an arbitrary set of one-to-one connections (monoalphabetic substitution) between the contacts on opposite sides of the rotor.

The rotor cipher machine was used extensively by both the Allied and the Axis powers during World War II, with the most notable such device being the German Enigma machine. The application of electronic components in subsequent years resulted in significant increases in operation speed though no major changes in basic design. Since the early 1970s, cryptologists have adapted major developments in microcircuitry and computer technology to create new, highly sophisticated forms of crypto devices and cryptosystems, as exemplified by the Fibonacci generator and the implementation of the Data Encryption Standard (DES) through the use of microprocessors.

##### VIGENERE CIPHER

Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of [polyalphabetic substitution.](https://en.wikipedia.org/wiki/Polyalphabetic_cipher) 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 compared to the previous alphabet, corresponding to the 26 possible [Caesar Ciphers.](https://www.geeksforgeeks.org/caesar-cipher/)
* At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
* The alphabet used at each point depends on a repeating keyword.

A Vigenère Cipher is an extended Caesar Cipher where a message is encrypted using various Caesar shifted alphabets. A polyalphabetic cipher is known cipher that is dependent on replacement, utilizing numerous replacement letter set. The encapsulation of the first plaintext is finished utilizing the Vigenère square table.

##### History of Vigenère cipher:

The very first well-documented description of a polyalphabetic cipher was by Leon Battista Alberti around 1467 and used a metal cipher disk to switch between cipher alphabets. Alberti's system only switched alphabets after several words, and switches were indicated by writing the letter of the corresponding alphabet in the ciphertext. Later, Johannes Trithemius, in his work Polygraphy (which was completed in manuscript form in 1508 but first published in 1518), invented the tabula recta, a critical component of the Vigenère cipher. The Trithemius cipher, however, provided a progressive, rather rigid and predictable system for switching betweencipher alphabets.

In 1586 Blaise de Vigenère published a type of polyalphabetic cipher called an autokey cipher

– because its key is based on the original plaintext – before the court of Henry III of France. The cipher now known as the Vigenère cipher, however, is that originally described by Giovan Battista Bellaso in his 1553 book La cifra del Sig. Giovan Battista Bellaso. He built upon the tabula recta of Trithemius but added a repeating "countersign" (a key) to switch cipher alphabets every letter. Whereas Alberti and Trithemius used a fixed pattern of substitutions, Bellaso's scheme meant thepattern of substitutions could be easily changed, simply by selecting a new key. Keys were typically single words or short phrases, known to both parties in advance, or transmitted "out of band" along with the message. Bellaso's method thus required strong security for only the key. Asit is relatively easy to secure a short key phrase, such as by a previous private conversation, Bellaso's system was considerably more secure.

In the 19th century, the invention of Bellaso's cipher was misattributed to Vigenère. David Kahn, in his book, The Codebreakers lamented this misattribution, saying that history had "ignored this important contribution and instead named a regressive and elementary cipher for him [Vigenère] though he had nothing to do with it".

The Vigenère cipher gained a reputation for being exceptionally strong. Noted author and mathematician Charles Lutwidge Dodgson (Lewis Carroll) called the Vigenère cipher unbreakable in his 1868 piece "The Alphabet Cipher" in a children's magazine. In 1917, Scientific American described the Vigenère cipher as "impossible of translation". That reputation was not deserved. Charles Babbage is known to have broken a variant of the cipher as early as 1854 but did not publish his work. Kasiski entirely broke the cipher and published the technique in the 19thcentury, but even in the 16th century, some skilled cryptanalysts could occasionally break the cipher.



Cryptographic slide rule used as a calculation aid by the Swiss Army between 1914 and 1940.

The Vigenère cipher is simple enough to be a field cipher if it is used in conjunction with cipher disks. The Confederate States of America, for example, used a brass cipher disk to implement the Vigenère cipher during the American Civil War. The Confederacy's messages were far from secret, and the Union regularly cracked its messages. Throughout the war, the Confederate leadership primarily relied upon three key phrases: "Manchester Bluff", "Complete Victory" and, as the war came to a close, "Come Retribution".

A Vigenère cipher with a completely random (and non-reusable) key which is as long as the message becomes a one-time pad, a theoretically unbreakable cipher. Gilbert Vernam tried to repair the broken cipher (creating the Vernam - Vigenère cipher in 1918), but the technology he used was so cumbersome as to be impracticable.

This type of substitution cipher used for data encryption in which the original plaintext structure is somewhat concealed in the ciphertext by using several different monoalphabetic substitution ciphers rather than just one; the code key specifies which particular substitution is to be employed for encrypting each plaintext symbol. Such resulting ciphers, known generically as polyalphabetic, have a long history of usage. The systems differ mainly in the way in which the key is used to choose among the collection of monoalphabetic substitution rules.

The cipher was invented in 1553 by the Italian cryptographer Giovan Battista Bellaso but for centuries was attributed to the 16th-centuryFrench cryptographer Blaise de Vigenère, who devised a similar cipher in 1586. For many years this type of cipher was thought to be impregnable and was known as *le chiffre indéchiffrable,* literally “the unbreakable cipher.”

##### Vigenère cipher encryption and decryption

The Vigenère cipher uses a 26×26 table with **A** to **Z** as the row heading and column heading This table is usually referred to as the Vigenère Tableau, Vigenère Table or Vigenère Square. We shall use Vigenère Table. The first row of this table has the 26 English letters. Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. For example, when **B** is shifted to the first position on the second row, the letter **A** moves to the end.

So, the first row of the Vigenère square table is ABCDEFGHIJKLMNOPQRSTUVWXYZ and the second row of the Vigenère square table is BCDEFGHIJKLMNOPQRSTUVWXYZA and soon the table continues 26 times...

The simpler and easier approach is to view Vigenère log- arithmetically and changing over alphabets [A-Z] into numerically as [0-25].

**Encryption** of Vigenère cipher using the formula:

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

𝐸𝑖 = (𝑃𝑖 + 𝐾𝑖) modulus26

W

h 𝑃𝑖 = plaintext

e

r 𝐾𝑖 = key

e

𝐸𝑖 = encrypted text

Decryption of Vigenère cipher using the formula:

## 𝐷𝑖 = (𝐸𝑖 − 𝐾𝑖+ 26) modulus26

W

h 𝐸𝑖= encrypted text

e

r 𝐾𝑖 = key

e

𝐷𝑖 = decrypted text / original text



##### Fig 4.1 Vigenère square table

Input: Plaintext: COMMUNICATION

Keyword: TABLE Output: Ciphertext: VONXYGIDLXBOO

For generating key, the given keyword is repeated in a circular manner until it matches the lengthof the plain text.

The keyword "TABLE" generates the key "TABLETABLETAB".

##### Encryption:

The plain text is then encrypted using the process explained below

The main letter of the plaintext, alphabet C is that is in a row combined with alphabet T is the key that is a column, the primarily given letter of the sender and receiver side key that results in the output as V. Then O is a row and key A is a column now it will result as O in the crossover of both rows as Message by sender and column as the key. Similarly, other letters will be processed in the same format and will result in encoded message.

Let’s take the simple example to describe how we calculate the cipher text using the Vigenère cipher table.

Plaintext: CITY Key: ON

Here the length of the key is less than the length of the plaintext. Length of the key is 2 and the length of the plaintext is 4 so we repeat the key until it matches the length of the plaintext. So, the key becomes ONON.

|  |  |  |  |
| --- | --- | --- | --- |
| C | I | T | Y |
| O | N | O | N |

##### Encryption:

The first letter of the plaintext is combined with the first letter of the key. The column of plain text "C" and row of key "O" intersects the alphabet of "Q" in the Vigenère table, so the first letter of ciphertext is "Q".

Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "I" and row of key "N" intersects the alphabet of "V" in the Vigenère table, so the second letter of ciphertext is "V".

This process continues continuously until the plaintext is finished.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 |

We took the first letter of the plaintext C and the first letter of the key O and they are compared along the rows and columns and they interchange at the Q so the cipher text is Q for this and it continues for remaining letters also…

##### Decryption:

Decryption is done by the row of keys in the Vigenère table. First, select the row of the key letter, find the ciphertext letter's position in that row, and then select the column label of the corresponding ciphertext as the plaintext.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ciphertext | Q | V | H | L |
| Key | O | N | O | N |

For example, in the row of the key is "O" and the ciphertext is "Q" and this ciphertext letter appears in the column "C", that means the first plaintext letter is "C".

Next, in the row of the key is "N" and the ciphertext is "V" and this ciphertext letter appears in the column "I", that means the second plaintext letter is "I". This process continues continuously until the ciphertext is finished

##### Encryption and Decryption using formula:

When the Vigenère table is not given, the encryption and decryption are done by Vigenère algebraically formula in this method (convert the letters (A-Z) into the numbers (0-25)).



##### Fig 4.2 converting alphabets to numbers

Encryption formula is Ei = (Pi + Ki) mod 26

Let the plain text be DESCRIPTIVE and the key is IMAGINE. We have to match the length of the key and the plaintext so the key becomes IMAGINEIMAG.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | D | E | S | C | R | I | P | T | I | V | E |
| Plaintext value (P) | 03 | 04 | 18 | 02 | 17 | 08 | 15 | 19 | 08 | 21 | 04 |
| Key | I | M | A | G | I | N | E | I | M | A | G |
| Key value (K) | 08 | 12 | 00 | 06 | 08 | 13 | 04 | 08 | 12 | 00 | 06 |
| Ciphertext value (E) | 11 | 16 | 18 | 08 | 25 | 21 | 19 | 01 | 20 | 21 | 10 |
| Ciphertext | L | Q | S | I | Z | V | T | B | U | V | K |

##### Table 3.1 Encryption using formula

The value of first letter of plaintext D is 03 and the value of the first letter of key is 08 and the ciphertext can be calculated by substituting the above values in the below formula:

Encrypted Ei = (Pi + Ki) modulus 26

= (03 + 08) modulus 26

= (11) modulus 26

= 11

The alphabet that has the value 11 is L so the first alphabet of the cipher text is L and the procedure continues for the other alphabet of plaintext and key and the final cipher text is LQSIZVTBUVK.

**Decryption using formula:** Di = (Ei - Ki+26) mod 26

Ciphertext: LQSIZVTBUV

Key: IMAGINEIMAG

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext | L | Q | S | I | Z | V | T | B | U | V | K |
| Ciphertext value (E) | 11 | 16 | 18 | 08 | 25 | 21 | 19 | 01 | 20 | 21 | 10 |
| Key | I | M | A | G | I | N | E | I | M | A | G |
| Key value (K) | 08 | 12 | 00 | 06 | 08 | 13 | 04 | 08 | 12 | 00 | 06 |
| Decrypted value(D) | 03 | 04 | 18 | 02 | 17 | 08 | 15 | 19 | 08 | 21 | 04 |
| Decrypted text | D | E | S | C | R | I | P | T | I | V | E |

##### Table 3.2 Decryption using formula

The value of the first letter of the cipher text L is 11 and the value of the first letter of key is 08 and the decrypted text can be calculated by substituting the above values in the below formula:

Decrypted Di = (Ei-ki+26) mod 26

= (11-08+26) mod 26

= (03+26) mod 26

= 03

The alphabet that has the value 03 is D so the first alphabet of the decrypted text is D and the procedure continues for the other alphabet of the ciphertext and key and the final decrypted text is DESCRIPTIVE.

##### Measuring the complexity of the Vigenère cipher:

This encryption method is certainly more complex than the Caesar cipher that you looked at earlier. To assess how secure the Vigenère cipher is, consider the key areas that you were introduced to in the previous step.

**Key length**: The key in a Vigenère cipher can vary in length from two characters to the length of the plaintext. The longer the key is and the more random it is, the harder the scheme is to crack. With short keys, you are likely to encrypt similar words or parts of words in the plaintext with the same part of the key, giving an attacker some clues as to what the key might be.

**Algorithmic complexity:** The encryption and decryption algorithms require multiple steps for each character. These extra steps mean that it will take an attacker longer to test their guesses at the key. For each character in the plaintext, there are many more permutations to try, adding more steps and more complexity.

##### Attacks on Vigenère cipher:

The idea behind the Vigenère cipher, like all other polyalphabetic ciphers, is to disguise the plaintext letter frequency to interfere with a straightforward application of frequency analysis. For instance, if P is the most frequent letter in a ciphertext whose plaintext in English, one might suspect that P corresponds to e since e is the most frequently used letter in English. However, by using the Vigenère cipher, e can be enciphered as different ciphertext letters at different points in the message, which defeats simple frequency analysis.

The primary weakness of the Vigenère cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length *n*, the cipher text can be treated as *n* interleaved Caesar ciphers which can easily be broken individually. The key length may be discovered by brute force testing each possible value of n, or Kasiski examination and the Friedman test can help to determine the key length.

* + 1. **Kasiski examination:** In 1863, Friedrich Kasiski was the first to publish a successful general attack on the Vigenère cipher. Earlier attacks relied on knowledge of the plaintext or the use of a recognizable word as a key. Kasiski's method had no such dependencies. Although Kasiski was the first to publish an account of the attack, it is clear that others had been aware of it. The Kasiski examination also called the Kasiski test, takes advantage of the fact that repeated words are, by chance, sometimes encrypted using the same key letters, leading to repeated groups in the ciphertext

Key: **ABCDAB**CDABCDABCD**ABCDAB**CDABCD Plaintext: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY Ciphertext: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

There is an easily noticed repetition in the ciphertext, and so the Kasiski test will be effective. The distance between the repetitions of CSASTP is 16. If it is assumed that the repeated segments represent the same plaintext segments, that implies that the key is 16, 8, 4, 2, or 1 character long. (All factors of the distance are possible key lengths; a key of length one is just a simple Caesar cipher, and its cryptanalysis is much easier.) Since key lengths 2 and 1 are unrealistically short, one needs to try only lengths 16, 8 or 4. Longer messages make the test more accurate because they usually contain more repeated ciphertext segments. The following ciphertext has two segments that are repeated:

Ciphertext: **VHVS**SP**QUCE**MRVBVBBB**VHVS**URQGIBDUGRNICJ**QUCE**RVUAXSSR

The distance between the repetitions of VHVS is 18. If it is assumed that the repeated segments represent the same plaintext segments, that implies that the key is 18, 9, 6, 3, 2 or 1 character long. The distance between the repetitions of QUCE is 30 characters. That means that the key length could be 30, 15, 10, 6, 5, 3, 2 or 1 character long. By taking the intersection of those sets, one could safely conclude that the most likely key length is 6 since 3, 2, and 1 are unrealistically short.

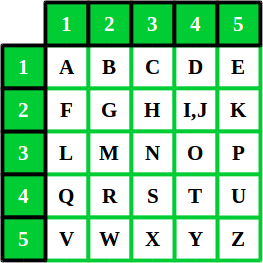
##### Frequency analysis:

Once the length of the key is known, the ciphertext can be rewritten into that many columns, with each column corresponding to a single letter of the key. Each column consists of plaintext that has been encrypted by a single Caesar cipher. The Caesar key (shift) is just the letter of the Vigenère key that was used for that column. Using methods similar to those used to break the Caesar cipher, the letters in the ciphertext can be discovered.

An improvement to the Kasis ki examination, known as Kerchkoff’s method, matches each column's letter frequencies to shifted plaintext frequencies to discover the key letter (Caesar shift) for that column. Once every letter in the key is known, all the cryptanalyst has to do is to decrypt the ciphertext and reveal the plaintext. Kerckhoffs' method is not applicable if the Vigenère table has been scrambled, rather than using normal alphabetic sequences, but Kasiski examination and coincidence tests can still be used to determine key length.

* 1. **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.



##### Fig 4.3 Polybius square

* + 1. **History of Polybius cipher:**

The **Polybius square**, also known as the **Polybius checkerboard**, is a device invented by the ancient Greeks Cleoxenus and Democleitus, and made famous by the historian and scholar Polybius. The device is used for fractionating plaintext characters so that they can be represented by a smaller set of symbols, which is useful for telegraphy, steganography, and cryptography. The device was originally used for fire signaling, allowing for the coded transmission of any message, not just a finite number of predetermined options as was the convention before.

Letters are represented by two numbers from one to five, allowing the representation of 25 characters using only 5 numeric symbols.

The original square used the Greek alphabet laid out as follows:

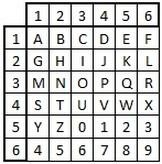


##### Fig 4.4 Polybius square having Greek alphabets

The Polybius Square is an ancient Greek invention, discovered by a scholar named Polybius. For the Greek alphabet of 24 letters, it consisted of a 5 by 5 grid where each square of the grid was filled by a single letter.

In the English Alphabet of 26 letters, we have one too many letters. To get round this we combine two letters, traditionally "i" and "j". It is also possible to combine other pairs, such as "v" and "u". Another alternative to the Polybius Square for English is to include the digits 0-9, so we have 36 characters.

This encryption is standard, and so far, has no key, and thus is easily broken. We need to introduce the idea of a key to the Polybius Square to make it more secure (Kerckhoffs's Principle).



##### Fig 4.5 Polybius square having digits

We reorder the alphabet in the same way as we did for the Mixed Alphabet Cipher before we put it in the grid. That is, we use the letters of the keyword first, ignoring any repeat So using a keyword of **sample** we get the mixed square below.

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

##### Fig 4.6 Polybius square having key in it

* + 1. **Encryption without key:**

Plaintext: DRAW

From the above figure of Polybius square the letter D is placed in row 1 and column 4

So, the output of the first letter D is 14. Next letter R is placed in row 4 and column 2 so its code is 11 and soon. The final Polybius output for the text DRAW is 14 42 11 53.

**Decryption:** Code: 23 15 11 14

23 visualize for 2st line and 3nd column, as result letter H, 15 visualize for 1th line and 5th column that result E and continues as same. Decrypted message result as HEAD.

In order to increase the security and reduce the attacks on the Polybius cipher we insert the key into the Polybius square so that the Polybius square table depends on the key and guessing the table each time becomes difficult.

##### Polybius square with key:

Plaintext: DRAW

The normal Polybius output without key is 14 42 11 53. Key: LINE

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

##### Fig 4.7 Polybius square with key LINE

The letter D is placed in row 2 and column 3 so the code is 23 and letter A is placed in row 1 and column 5 so its code is 15 and soon. The Polybius output with key for the text DRAW is 23 43 15 53.

**Decryption:** Code: 23 43 15 53

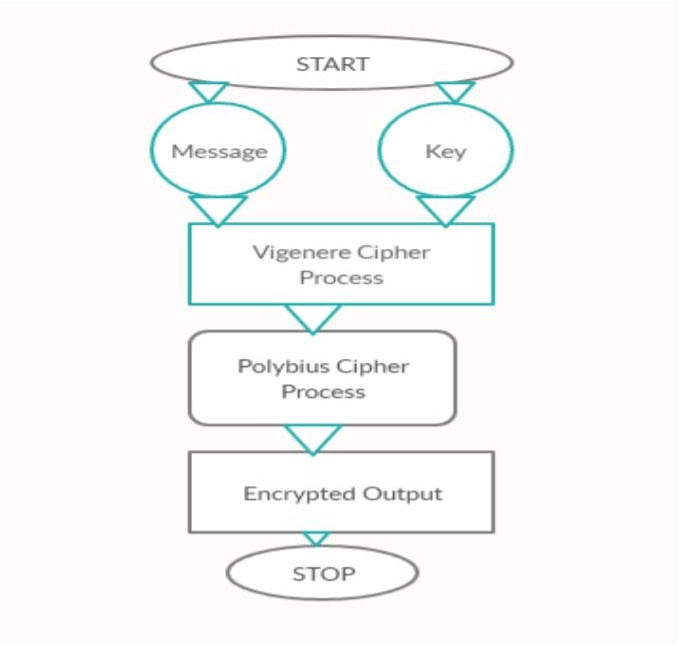
23 visualize for 2st line and 3nd column, as result letter D, 43 visualize for 4th line and 3th column that result R and continues as same. Decrypted message result as DRAW.

#### PROPOSED SYSTEM

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.

The flowchart representing the process of the proposed system is given below:



##### Fig 4.8 Flow chart of hybrid system

First the message and key are given to the Vigenère cipher and the output of Vigenère 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 Vigenère. After entering the key, the original plaintext, the sender sent is displayed.

##### 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 15 54 11 14

From the figure 3.1 (Vigenère table) The first letter of the plaintext is combined with the first letter of the key. The column of plain text "C" and row of key "S" intersects the alphabet of "U" in the Vigenère table, so the first letter of ciphertext is "U".

Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "A" and row of key "T" intersects the alphabet of "T" in the Vigenère table, so the second letter of ciphertext is "T" and soon.

The Vigenère cipher output is U T P B X S E. By using the encryption formula of the Vigenère cipher we construct the below table.

We can see output is in a NUMERICAL format where sender has sent as in ALPHABETICAL format. Even the Vigenère cipher result outputs as in distributed, it is jumbled and unformatted ALPHABETS which is also secured but again passing that treating Vigenère outputs as Polybius input and then result in numerical format that makes it greater secure and complex than the use of single ciphers.

The output of Vigenère U T P B X S E is given as input to Polybius cipher.

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

From the above figure of Polybius square the letter U is placed in row 5 and column 1. So, the output of the first letter U is 51. Next letter T is placed in row 1 and column 2 so its code is 12 and soon. The final Polybius output for the text U T P B X S E is 51 12 43 15 54 11 14.

##### Decryption:

Phase 1 (Polybius Cipher)

MESSAGE- 51 12 43 15 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

DECRYPTED OUTPUT- CAPITAL

From the above table of Polybius square with key we convert the 51 12 43 15 54 11 14 to alphabets51 visualize for 5th line and 1st column, as result letter U, 12 visualize for 1st line and 2nd column that result T and continues as same. Output of the Polybius is U T P B X S E.

This is given as input to Vigenère along with key and the decrypted output is CAPITAL. We can see decode output is arriving after reversing the process of through first and foremost Polybius cipher and then Vigenère cipher. This makes complexity for intruders, ` attackers and hackers to confuse them and stop them to Replicate, copy, or harm the system through various types of active and passive attacks.

##### Advantages of Proposed System:

* As we combine both the Vigenère 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.

#### HARDWARE and SOFTWARE REQUIREMENTS

* + 1. **SOFTWARE REQUIREMENTS PROGRAMMING LANGUAGE :**

#### PYTHON 3.11.4

**OPERATING SYSTEM :**

#### WINDOWS.

* **MAC OS.**

#### LINUX, UNIX.

**IDE:**

#### SPYDER

* + 1. **HARDWARE REQUIREMENTS PROCESSOR :**

#### Dual Core 1.6 GHz

* **Ryzen AMD**

#### Intel

**RAM : 4 GB**

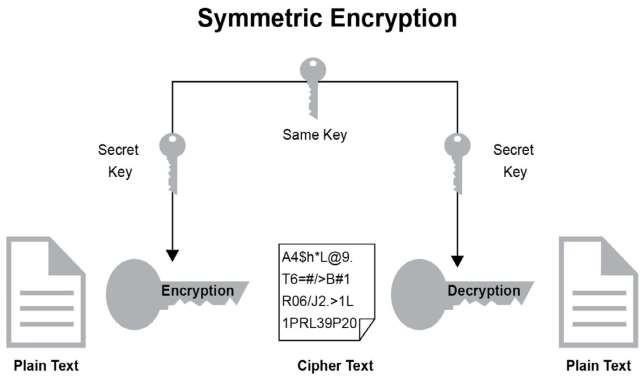
**HARD DISK : 256GB**

# 5.SYSTEM DESIGN

#### History of UML Diagrams

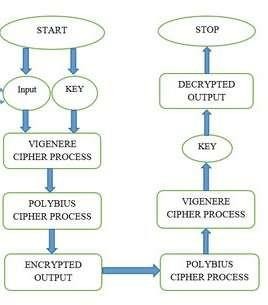
UML stands for Unified Modeling Language. UML is a standardized general purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The Unified Modeling Language is a standard language for specifying, visualization, constructing and documenting the artifacts of software systems, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing object-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects. The overall logical structure of a database can be expressed graphically by an ER diagram. The relative simplicity and pictorial clarity of this diagramming technique may well account in large part for the widespread use of the E-R model. Such a diagram consists of the following major components

#### UML DIAGRAMS



**Fig 5.1 Symmetric Encryption**

we have same key which is used by both sender and receiver in other words same key is used by both encryption and decryption since same key is used by both encryption and decryption “this key will kept Secret and it will be a private key” since private key is only used by the both encryption and decryption algorithms (or) Sender and the Receiver. We call this Cryptographic method as “Private (or)Symmetric Key Cryptography”.



#### Fig 5.2 Flow chart of Hybrid Model

The figure shows the flow of our model which consists of sending an plain text as input, encryption of the input through Vigenère and Polybius cipher, and then decryption using the Polybius and Vigenère cipher by using the same key to obtain the original contents

The input as plain text having any size and Key is send through sender in two phase for execution and working of System as in first phase it will proceed through Vigenère Cipher and then the new instructed and disputed encrypted cipher comes and then in second phase it became the input of Polybius cipher which result as output as Numerical encrypted Cipher that is confusing and scrambled mix numerical. This Output from Polybius at last phase is allow the to steal Information. In the same way decryption is first done through Polybius cipher and then with Vigenère Cipher. So Original contents will be received. We have applied 2 algorithms:

1. Encryption and decryption using Vigenère cipher.
2. Encryption and decryption using Polybius cipher.

# 6. IMPLEMENTATION

#### DESCRIPTION OF MODULES

**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.

**Vigenère Square:** The Vigenère Square is a table that contains the alphabet repeated multiple times, each time shifted by one position to the right. The rows and columns of the square represent the letters of the alphabet. This square is used to determine the encryption and decryption of the message.



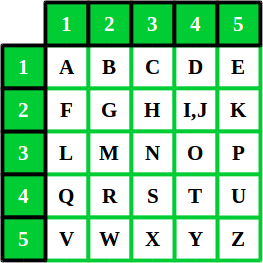
**Key:** The key is a word or phrase used to determine the shift value for each letter in the plaintext. The key is typically shorter than the message itself and is repeated to match the length of the plaintext. Each letter of the key corresponds to a specific column in the Vigenère Square.

**Encryption:** To encrypt a message using the Vigenère cipher, you align the key with the plaintext, repeating the key as necessary. Each letter of the plaintext is then shifted by the corresponding letter in the key, using the Vigenère Square to determine the new letter. The encrypted message is formed by taking the letters from the Vigenère Square based on the row of the plaintext letter and the column of the key letter.

**Decryption:** Decryption in the Vigenère cipher follows a similar process as encryption. The key is aligned with the ciphertext, repeating the key as necessary. Each letter of the ciphertext is then shifted backward by the corresponding letter in the key, using the Vigenère Square to determine the original letter. The decrypted message is formed by taking the letters from the Vigenère Square based on the row of the ciphertext letter and the column of the key letter.

**Alphabet:** The alphabet used in the Vigenère Square typically consists of the 26 letters from A to Z. The letters are arranged in the square in a specific pattern, with each row shifted by one position to the right compared to the previous row.

The **Polybius cipher** is a substitution cipher that uses a 5x5 grid to encrypt and decrypt messages. Each letter of the alphabet is represented by a pair of coordinates corresponding to its position in the grid.



Here are the main components or modules of the Polybius cipher:

**Grid:** The grid is a 5x5 square matrix used to map the letters of the alphabet. It consists of 25 cells, each containing a unique letter, usually excluding the letter 'J'(to reduce ambiguity with 'I').

**Encoding:** To encode a message using the Polybius cipher, you need to find the coordinates (row and column) of each letter in the grid. The row number represents the first digit of the encoded pair, while the column number represents the second digit.

**Decoding:** To decode an encoded Polybius message, you reverse the process. You take the pairs of digits and find the corresponding letter in the grid using the row and column values.

**Alphabet:** The alphabet used in the Polybius cipher typically consists of the 25 letters from A to Z (excluding J). The letters are arranged in the grid according to a specific pattern.

**Key:** In some variants of the Polybius cipher, a key may be used to rearrange the letters in the grid. The key determines the order in which the letters are placed in the grid, adding an additional layer of complexity to the encryption and decryption process.

These modules work together to encode and decode messages using the Polybius cipher. By assigning pairs of digits to each letter, the original message is transformed into a series of numbers, making it harder to decipher without the key and knowledge of the grid arrangement.

#### OVERVIEW OF IMPLEMENTATION OF LANGUAGE

**Implementation** of the Encryption and Decryption process of the Hybrid cipher process that flows systematically through Polybius and Vigenère cipher system**. Python** Program is written as for the Implementation of Hybrid cipher.

**Python** is a [high-level,](https://en.wikipedia.org/wiki/High-level_programming_language) [interpreted,](https://en.wikipedia.org/wiki/Interpreter_(computing)) [general-purpose programming language.](https://en.wikipedia.org/wiki/General-purpose_programming_language) Its design philosophy emphasizes [code readability](https://en.wikipedia.org/wiki/Code_readability) with the use of [significant indentation.](https://en.wikipedia.org/wiki/Off-side_rule)

Python is [dynamically-typed](https://en.wikipedia.org/wiki/Type_system#DYNAMIC) and [garbage-collected](https://en.wikipedia.org/wiki/Garbage_collection_(computer_science)). It supports multiple [programming](https://en.wikipedia.org/wiki/Programming_paradigm) [paradigms,](https://en.wikipedia.org/wiki/Programming_paradigm) including [structured](https://en.wikipedia.org/wiki/Structured_programming) (particularly [procedural](https://en.wikipedia.org/wiki/Procedural_programming)), [object-oriented](https://en.wikipedia.org/wiki/Object-oriented_programming) and [functional](https://en.wikipedia.org/wiki/Functional_programming) [programming.](https://en.wikipedia.org/wiki/Functional_programming) It is often described as a "batteries included" language due to its comprehensive [standard library.](https://en.wikipedia.org/wiki/Standard_library)

[Guido van Rossum](https://en.wikipedia.org/wiki/Guido_van_Rossum) began working on Python in the late 1980s as a successor to the [ABC](https://en.wikipedia.org/wiki/ABC_(programming_language)) [programming language](https://en.wikipedia.org/wiki/ABC_(programming_language)) and first released it in 1991 as Python 0.9.0. Python 2.0 was released in 2000 and introduced new features such as [list comprehensions,](https://en.wikipedia.org/wiki/List_comprehension) [cycle-detecting](https://en.wikipedia.org/wiki/Cycle_detection) garbage collection, [reference counting,](https://en.wikipedia.org/wiki/Reference_counting) and [Unicode](https://en.wikipedia.org/wiki/Unicode) support. Python 3.0, released in 2008, was a major revision that is not completely [backward-compatible](https://en.wikipedia.org/wiki/Backward_compatibility) with earlier versions. Python 2 was discontinued with version 2.7.18 in 2020.

Python consistently ranks as one of the most popular programming languages

##### History of Python

Python was conceived in the late 1980s by [Guido van Rossum](https://en.wikipedia.org/wiki/Guido_van_Rossum) at [Centrum Wickende &](https://en.wikipedia.org/wiki/Centrum_Wiskunde_%26_Informatica) [Informatica](https://en.wikipedia.org/wiki/Centrum_Wiskunde_%26_Informatica) (CWI) in the [Netherlands](https://en.wikipedia.org/wiki/Netherlands) as a successor to the [ABC programming language,](https://en.wikipedia.org/wiki/ABC_(programming_language)) which was inspired by [SETL,](https://en.wikipedia.org/wiki/SETL) capable of [exception handling](https://en.wikipedia.org/wiki/Exception_handling) and interfacing with the [Amoeba](https://en.wikipedia.org/wiki/Amoeba_(operating_system)) operating system. Its implementation began in December 1989. Van Rossum shouldered sole responsibility for the project, as the lead developer, until 12 July 2018, when he announced his "permanent vacation" from his responsibilities as Python's "[benevolent dictator for life](https://en.wikipedia.org/wiki/Benevolent_dictator_for_life)", a title the Python community bestowed upon him to reflect his long-term commitment as the project's chief decision- maker. In January 2019, active Python core developers elected a five-member Steering Council to lead the project.

Python 2.0 was released on 16 October 2000, with many major new features. Python 3.0, released on 3 December 2008, with many of its major features [backported](https://en.wikipedia.org/wiki/Backporting) to Python 2.6.x and

2.7.x. Releases of Python 3 include the 2 to 3 utility, which automates the translation of Python 2 code to Python 3.

Python 2.7's [end-of-life](https://en.wikipedia.org/wiki/End-of-life_(product)) was initially set for 2015, then postponed to 2020 out of concern that a large body of existing code could not easily be forward-ported to Python 3.

No further security patches or other improvements will be released for it. With Python 2's [end-of-life,](https://en.wikipedia.org/wiki/End-of-life_(product)) only Python 3.6.x and later were supported.

Later, support for 3.6 was also discontinued. In 2021, Python 3.9.2 and 3.8.8 were expedited as all versions of Python (including 2.7) had security issues leading to possible [remote code](https://en.wikipedia.org/wiki/Remote_code_execution) [execution](https://en.wikipedia.org/wiki/Remote_code_execution) and [web cache poisoning.](https://en.wikipedia.org/wiki/Cache_poisoning)

In 2022, Python 3.10.4 and 3.9.12 were expedited and so were older releases including 3.8.13, and

3.7.13 because of many security issues in 2022. Python 3.9.13 is the latest 3.9 version, and from now on 3.9 (and older; 3.8 and 3.7) will only get security updates.

Python uses [dynamic typing](https://en.wikipedia.org/wiki/Dynamic_typing) and a combination of [reference counting](https://en.wikipedia.org/wiki/Reference_counting) and a cycle-detecting garbage collector for [memory management.](https://en.wikipedia.org/wiki/Memory_management) It uses dynamic [name resolution](https://en.wikipedia.org/wiki/Name_resolution_(programming_languages)) ([late binding](https://en.wikipedia.org/wiki/Late_binding)), which binds method and variable names during program execution.

#### Syntax of Python:

Python is meant to be an easily readable language. Its formatting is visually uncluttered and often uses English keywords where other languages use punctuation. Unlike many other languages, it does not use [curly brackets](https://en.wikipedia.org/wiki/Curly_bracket_programming_language) to delimit blocks, and semicolons after statements are allowed but rarely used. It has fewer syntactic exceptions and special cases than [C](https://en.wikipedia.org/wiki/C_(programming_language)) or [Pascal.](https://en.wikipedia.org/wiki/Pascal_(programming_language))

##### Indentation:

Python uses [whitespace](https://en.wikipedia.org/wiki/Whitespace_character) indentation, rather than [curly brackets](https://en.wikipedia.org/wiki/Curly_bracket_programming_language) or keywords, to delimit [blocks.](https://en.wikipedia.org/wiki/Block_(programming)) An increase in indentation comes after certain statements; a decrease in indentation signifies the end of the current block. Thus, the program's visual structure accurately represents its semantic structure. This feature is sometimes termed the [off-side rule.](https://en.wikipedia.org/wiki/Off-side_rule) Some other languages use indentation this way; but in most, indentation has no semantic meaning. The recommended indent size is four spaces.

##### Comments:

* + Comments can be used to explain Python code.
  + Comments can be used to make the code more readable.
  + Comments can be used to prevent execution when testing code.

Comments starts with a #, and Python will ignore them:

Example:

#This is a comment print ("Hello, World!")

Comments can be placed at the end of a line, and Python will ignore the rest of the line: Example:

Print ("Hello, World!") #This is a comment

A comment does not have to be text that explains the code, it can also be used to prevent Python from executing code:

Example:

#Print ("Hello, World!")print ("Cheers, Mate!")

##### Variables

1. Variables are containers for storing data values. Python has no command for declaring a variable. A variable is created the moment you first assign a value to it.

Example:

x = 5

y = "John" print(x) print(y)

1. Variables do not need to be declared with any particular *type*, and can even change type after they have been set.

Example:

x = 4 # x is of type int

x = "Sally” # x is now of type str print(x)

1. You can get the data type of a variable with the type () function. Example: x = 5

y = "John" print(type(x))print(type(y))

1. Variable names are case-sensitive.

Example:

a = 4

A = "Sally"

#A will not overwrite a

1. String variables can be declared either by using single or double quotes.

##### Data Types

Built-in Data Types: In programming, data type is an important concept. Variables can store data of different types, and different types can do different things.

Python has the following data types built-in by default, in these categories:

|  |  |
| --- | --- |
| 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 |

##### Fig 6.1 Representing the datatypes of python

* + 1. **Python IF ELSE:**

Python supports the usual logical conditions from mathematics:

* + Equals: a == b
  + Not Equals: a! = b
  + Less than: a < b
  + Less than or equal to: a <= b
  + Greater than: a

These conditions can be used in several ways, most commonly in "if statements" and loops. Example:

a= 200

b= 33

if b>a:

print("b is greater than a") elif a == b:

print("a and b are equal")else:

print("a is greater than b")

##### Python Loops:

Python has two primitive loop commands:

* + while loops
  + for loops

The while Loop: With the while loop we can execute a set of statements as long as a condition is true.

Example:

I = 1

while I < 6:

print(I) I += 1

The For loop: A for loop is used for iterating over a sequence. Example: fruits = ["apple", "banana", "cherry"]for x in fruits:

print(x)

#### Modulus Operator:

The modulus operator is added in the arithmetic operators in C, and it works between two available operands. It divides the given numerator by the denominator to find a result. In simpler words, it produces a remainder for the integer division. Thus, the remainder is also always an integer number only.

Example:

8%5 = 3

7%2 = 1

When we perform the modulus operator between 8 and 5, means 8 % 5, it returns the remainder 3 because when 8 is divided by 5, it returns 1 as the quotient and 3 as the remainder. Similarly, 7

% 2 returns 1 as a remainder because when 7 is divided by 2, it returns 3 as quotient and 1 as remainder.

# 7.TESTING

#### SOFTWARE TESTING

Software Testing is a method to check whether the actual software product matches expected requirements and to ensure that software product is defect free. These are the benefits of software testing.

* Cost-effectiveness
* Customer Satisfaction
* Security
* Product Quality

Testing is the process of attempting to find every possible flaw or error in a work product. It allows you to test the functionality of parts, subassemblies, assemblies, and/or finished products. It is a method of writing code with the goal of ensuring that the software meets its requirements and user expectations and does not fail in an unfavorable way. There are numerous types of tests.

Each check sort reports a specific testing demand. Before releasing or deploying any software application the testers use various testing processes and techniques for testing and validation. This process is known as software testing procedure.

It can be done either manually or by using automated tools. Software testing is essential because it allows any faults or errors in the software to be found early and fixed before the software product is delivered. Reliability, security, and high performance are all provided by properly tested software, which also leads to time savings, cost effectiveness, and customer pleasure.

Software testing is a crucial process in the development of software that aims to evaluate and validate the quality and functionality of a software application. The primary goal of software testing is to identify defects, errors, or discrepancies between expected and actual outcomes, ensuring that the software meets the specified requirements and works as intended.

The primary goal of testing is to identify a large number of errors in a systematic and time- efficient manner. Formally, we can say that testing is the process of running a program in order to find and fix errors.

* A successful test is one that identifies a previously unknown error.
* A good test case is one that has the potential to uncover an error, if one exists.
* The test is insufficient to detect potential errors.
* The software largely conforms to the quality and unwavering standards.

Software testing is a crucial process in the development of software that aims to evaluate and validate the quality and functionality of a software application. Theprimary goal of software testing is to identify defects, errors, or discrepancies between expected and actual outcomes, ensuring that the software meets the specified requirements and works as intended.

#### TESTING TECHNIQUES

Software Testing Techniques help you design better test cases. Since exhaustive testing is not possible; Manual Testing Techniques help reduce the number of testcases to be executed while increasing test coverage. They help identify test conditions that are otherwise difficult to recognize.

##### Black Box Testing:

In this technique, testers focus solely on the external behavior of the software without considering its internal code structure. Testers create test cases based on the software's specifications and requirements. Black box testing is useful for functional, integration, and acceptance testing.

##### White Box Testing:

Also known as "Clear Box Testing" or "Glass Box Testing," this technique involves examining the internal structure of the software code. Testers design test cases based on the code's logic, branches, and paths. White box testing is suitable for unit testing and ensuring code coverage.

##### Gray Box Testing:

Gray box testing is a combination of black box and white box testing. Testers have partial knowledge of the internal code structure and use that information to design test cases. This approach helps find defects from both an external and internal perspective.

##### Equivalence Partitioning:

This technique divides the input data into groups or partitions, assuming that the software behaves the same way for all inputs within each partition. Test cases are then designed to represent each partition, reducing the number of test cases needed.

##### Boundary Value Analysis:

Test cases are designed using data at the boundaries of equivalence partitions. These boundary values are more likely to cause errors, so testing them helps identify issues with boundary conditions.

##### Mutation Testing:

This technique involves making small modifications (mutations) to the software code and running the test suite. The objective is to check if the test suite can detect these artificial defects. If not, it indicates a weakness in the test suite.

##### Exploratory Testing:

Exploratory testing is an informal testing approach where testers explore the software, interact with it, and test it on the fly. Testers use their domain knowledge, creativity, and intuition to identify defects and potential issues.

##### Ad Hoc Testing:

Ad hoc testing is an unplanned and informal testing technique where testers perform testing without following any predefined test cases or test plan. It is often used to quickly identify critical defects.

##### Regression Testing:

After making changes to the software, regression testing verifies that the modifications did not introduce new defects and that the existing functionalities still work correctly.

##### Load Testing:

Load testing checks the software's performance under anticipated or simulated load conditions. It helps identify performance bottlenecks and potential issues related to high user loads.

##### Stress Testing:

Stress testing involves testing the software beyond its normal operational capacity to determine its robustness and stability under extreme conditions.

##### Usability Testing:

Usability testing evaluates how user-friendly and intuitive the software is from an end-user perspective.

These are just a few examples of software testing techniques, and various other specialized techniques exist, depending on the nature of the software being tested and the testing objectives. Effective testing often involves combining multiple techniques to ensure comprehensive coverage and a high-quality end product.

#### TESTING STARTEGIES

##### UNIT TESTING:

A unit is the smallest piece of testable source code. It is also known as a module because it is made up of many lines of code that are processed by a single programmer. The primary goal of unit testing is to demonstrate that a specific unit Deep Learning for Classification and Localization Of does not meet the specified functional requirements and also to demonstrate that the structural implementation differs from the projected structure designed.

##### INTEGRATION TESTING:

Integration tests are designed to test incorporated programming segments to determine whether they truly run as one system. Testing is event driven and is more concerned with the fundamental outcome of screens or fields. Reconciliation tests demonstrate that, despite the fact that the parts were fulfilled separately, as demonstrated by effectively unit testing, the combination of segments is correct and complete. Integration testing is specifically designed to reveal issues that arise from the combination of components.

##### SYSTEM TESTING:

System testing ensures that the entire coordinated programming framework satisfies the requirements. It tests a design to ensure predictable and unsurprising results.

##### ACCEPTANCE TESTING:

To obtain customer sign-off so that software can be delivered and payments received. Types of Acceptance Testing are Alpha, Beta &Gamma Testing.

##### Alpha Testing

Alpha testing is an internal checking done by the in-house development or QA team, rarely, by the customer himself. Its main purpose is to discover software bugs that were not found before. At the stage of alpha testing, software behaviour’s verified under real-life conditions by imitating the end users’ actions. It enables us to get fast approval from the customer before proceeding to product delivery.

##### Beta Testing

Beta testing can be called pre-release testing. It can be conducted by a limited number of end-users called beta testers before the official product delivery. The main purpose of beta testing is to verify software compatibility with different software and hardware configurations, types of network connection, and to get the users’ feedback on software usability and functionality.

There are two types of beta testing:

* open beta is available for a large group of end-users or to everyone interested .
* closed beta is available only to a limited number of users that are selected especially for beta testing.

##### Gamma Testing

Gamma testing is the final stage of the testing process conducted before software release. It makes sure that the product is ready for market release according to all the specified requirements. Gamma testing focuses on software security and functionality. But it does not include any in-house QA activities. During gamma testing, the software does not undergo any modifications unless the detected bugis of a high priority and severity.

# 8.RESULTS

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.

# 9.CONCLUSION AND FUTURE WORK

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 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. 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.

# 10.APPENDIX

#### SAMPLE CODE

##### def generateKey(message, key):key = list(key) if len(message) == len(key):return(key)

**else:**

##### for i in range(len(message) -

**len(key)): key.append(key[i % len(key)]) return("" . join(key))**

##### # vigenere cipher encryption def cipherText(message, key):cipher\_text = [] for i in range(len(message)): x = (ord(message[i]) +

**ord(key[i])) % 26**

##### x += ord('A') cipher\_text.append(chr(x)) return("" . join(cipher\_text))

**# vigenere cipher code decryption def originalText(cipher\_text, key):** **orig\_text = []**

##### for i in range(len(cipher\_text)):x = (ord(cipher\_text[i]) -

**ord(key[i]) + 26) % 26x += ord('A') orig\_text.append(chr(x)) return("" . join(orig\_text))**

##### # Driver code

**if name == " main ":**

##### message = input("enter the message").upper() keyword = input("enter the keyword").upper()key = generateKey(message, keyword) cipher\_text = cipherText(message,key) print("vigenere cipher output :", cipher\_text) #polybius cipher codeimport string

**alpha = string.ascii\_uppercase**

##### print(alpha)square = [] for i in keyword:

**if i not in square: square.append(i)** **for i in alpha:**

##### if i not in square: square.append(i) print(''.join(square))plain = cipher\_text #cipher = [] #for i in plain:

**# n = square.find(i) + 1 # row,col = divmod(n,5)**

##### # cipher.append(str(row+1)+str(col)) #print("polybius cipher output",' '.join(cipher))

**sq= [] k= [4,9,14,19,24,25]**

##### temp= []

**for i in range(len(square)):**

##### if i in k: temp.append(square[i]) sq.append(''.join(temp))temp=[] else:

**temp.append(square[i])#print(sq)** **cipher= []**

##### for i in cipher\_text:for j in sq:

**if i in j:**

##### cipher.append(str(sq.index(j)+1)+str(j.index(i)+1))print("polybius cipher output",' '.join(cipher))

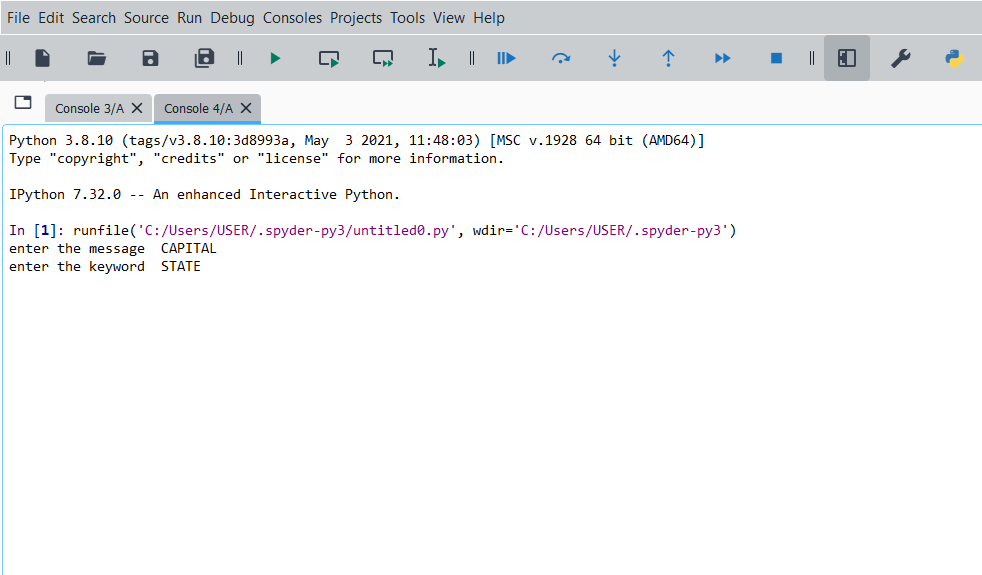
**plain= []**

##### for i in cipher:

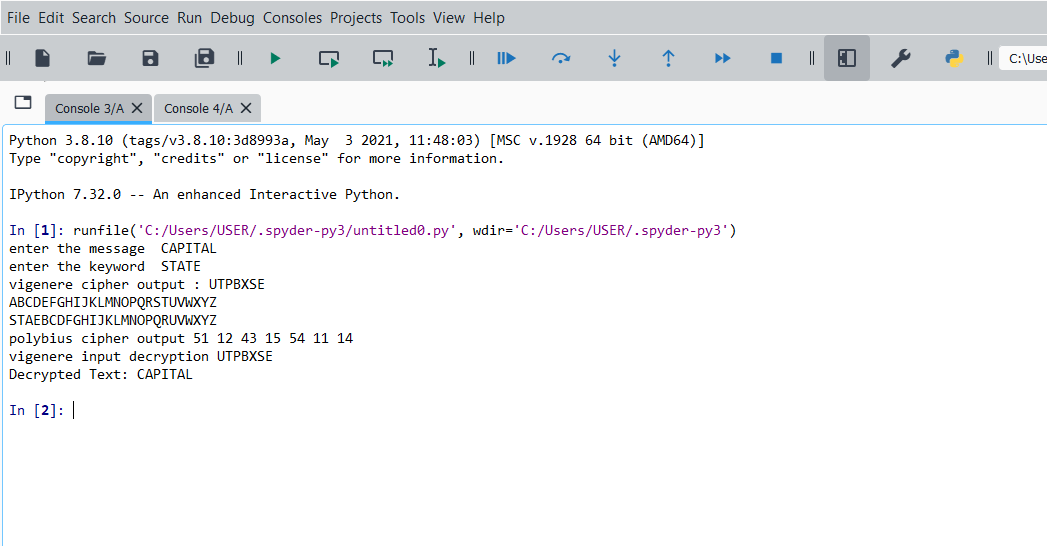
**plain.append(sq[int(i[0])-1][int(i[1])-1])**

**print ("vigenere input decryption",''.join(plain)) print("Decrypted Text:",originalText(cipher\_text, key))**

#### SCREENSHOTS



##### Fig 10.2.1 Input to the Hybrid System



**Fig 10.2.2 Final Output of Hybrid System**

# 11.REFERENCES

1. S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, “A research paper on new hybridcryptography algorithm.”
2. 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.
3. 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.
4. P. Kumar and s. B. Rana, “development of modiﬁed aes algorithm for data security,” Optik, vol. 127, no. 4, pp. 2341–2345, 2016.
5. A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., “An extended hybridization of Vigenère and Caesar cipher techniques for secure communication,” Procedia Computer Science, vol. 92, pp.355–360, 2016.
6. J. Chen and J. S. Rosenthal, “Decrypting classical cipher text using markov chain monte carlo,”statistics and computing, vol. 22, no. 2, pp. 397–413, 2012.
7. M. B. Pramanik, “Implementation of cryptography technique using columnar transposition,” International Journal of Computer Applications, vol. 975, p. 8887, 2014.
8. C. Sanchez-Avila and R. Sanchez-Reillol, “The Rijndael block cipher (aes proposal): a comparison with des,” in Proceedings IEEE 35th annual2001 International Carnahan Conferenceon Security Technology (cat.no. 01ch37186). IEEE, 2001, pp. 229–234.
9. Q.-A. Kester, “A cryptosystem based on Vigenère cipher with varying key,” International Journal of Advanced Research in Computer Engineering & technology (IJARCET), vol. 1, no. 10,pp. 108–113, 2012.
10. C. Bhardwaj, “Modiﬁcation of Vigenère cipher by random numbers, punctuations & mathematical symbols,” Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278–0661, 2012.
11. P. Gutmann, “Cryptographic security architecture: design and verification”. Springer Science& Business Media, 2003