DESIGN AND ANALYSIS OF CRYPTOGRAPHIC TECHNIQUE FOR COMMUNICATION SYSTEM

Final Project Report
Submitted by

Sitlendra Pratap Singh
(201810101110096)
&
Abhay Singh Chauhan
(201810101110079)

In partial fulfillment for the award of the degreeof

Bachelor of Technology

in

Computer Science and Engineering

SHRI RAMSWAROOP MEMORIAL UNIVERSITY

Under the Supervision of

Ms. Kanchan Pandey
(Assistant Professor)

BONAFIDE CERTIFICATE

Certified that this project report "DESIGN AND ANALYSIS OF CRYPTOGRAPHIC TECHNIQUE FOR COMMUNICATION SYSTEM" is the bonafide work of "Sitlendra Pratap Singh and Abhay Singh Chauhan" who carried out the project work under my supervision.

SIGNATURE OF HEAD

Dr. Shalini Agarwal
PhD (CS)
(Professor & Dean,
School of Computing Science &
Engineering)

SIGNATURE OF SUPERVISOR

Ms. Kanchan Pandey
M.Tech.
(Assistant Professor
School of Computing Science
& Engineering)

ABSTRACT

In Today's world Sensitive data is increasingly used in communication over the internet. Thus Security of data is the biggest concern of internet users. Best solution is use of some cryptography algorithm which encrypts data in some cipher and transfers it over the internet and again decrypted to original data. The field of cryptography deals with the procedure for conveying information securely. The goal is to allow the intended recipients of a message to receive the message properly while interrupt eaves-droppers from understanding the message. Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data classified and for verifying data indignity. While our conventional cryptography methods, such for AES (encryption) and RSA (signing), work well on systems which have reasonable processing power and memory capabilities, these do not scale well into a world with embedded systems and sensor networks. Thus, lightweight cryptography methods are proposed to overcome many of the problems of conventional cryptography. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext. The cryptosystem performs its encryption by encrypting the plaintext using Vigenere Cipher and further using the ciphertext to encrypt the plaintext again using Polybius Cipher.

Keywords: Encryption, Cryptography, Algorithm, Ciphers

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

Information security can be summed up to info, a group of steps, procedures, and strategies that are used to stop and observe illegal access, trouble-shooting, revelation, perturbation and adjustment of computer network sources. Enhancing the privacy, eligibility and reliability of the work requires a lot work to strengthen the current methods from constant trials to break them and to improve new ways that are resistant to most kinds of attacks if not all. Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information since the ancient days of the Romans who used similar methods to enable security on their valued information and documents

Cryptography is the art of creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it.

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus preventing un authorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

Overall Description:

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

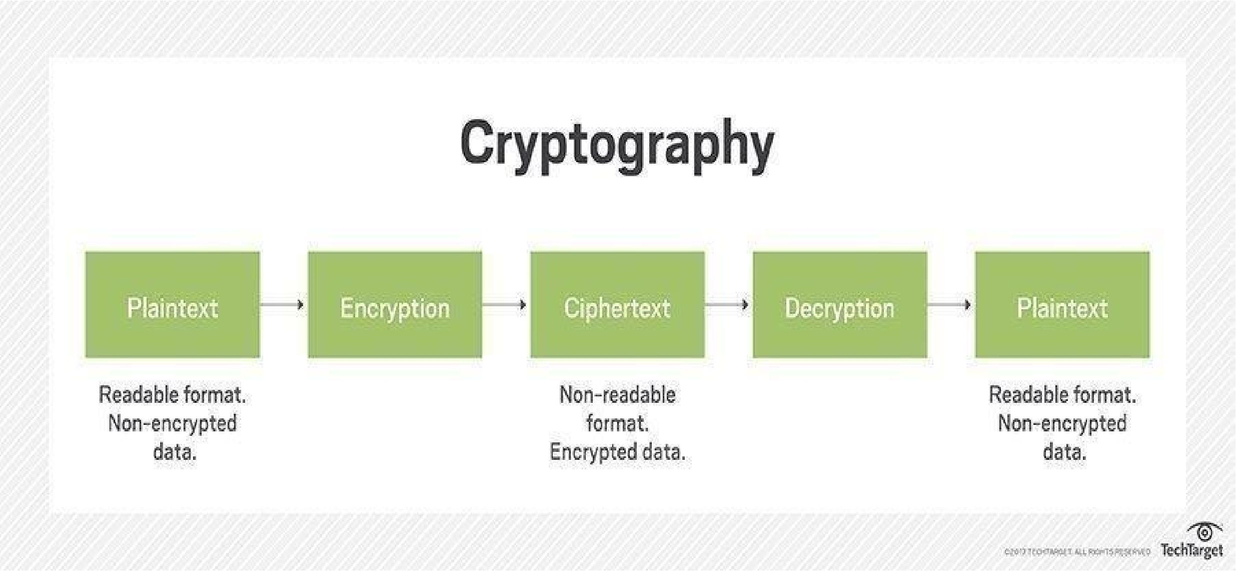
Techniques used For Cryptography: In today's age of computers, cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features of Cryptography: These are mentioned below.

- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types of Cryptography: In general there are three types of cryptography which are explained as follows.

- **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).
- **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
- **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
©2017 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

Components of a Cryptosystem: The various components of a basic cryptosystem are as follows:

- **Plaintext.** It is the original data to be protected during transmission.
- **Cipher text.** 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.
- **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.
- **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 cipher text.
- **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 cipher text 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.

Purpose: In digital world cyber-attacks are very frequent. Any social networking site, web application, etc are more prone to attacks. To counter this Study and analysis of attacks is usually important s this guide to solve major problem and make system anti attacks. Some of the attacks are given as follows.

Cryptographic Attacks: The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as *broken* or *compromised*.

Based on the methodology used, attacks on cryptosystems are categorized as follows −

- **Ciphertext Only Attacks (COA)** − In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.

. **Known Plaintext Attack (KPA)** − In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.

- **Chosen Plaintext Attack (CPA)** − In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.

- **Dictionary Attack** − this attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.
- **Brute Force Attack (BFA)** − In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is 2^8 = 256. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.
- **Man in Middle Attack (MIM)** − the targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.
  - Host *A* wants to communicate to host *B*, hence requests public key of *B*.
  - An attacker intercepts this request and sends his public key instead.
  - Thus, whatever hosts *A* sends to host *B*, the attacker is able to read.
  - In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to *B*.
  - The attacker sends his public key as *A*’s public key so that *B* takes it as if it is taking it from *A*.
- **Side Channel Attack (SCA)** − this type of attack is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem.
- **Timing Attacks** − they exploit the fact that different computations take different times to compute on processor. By measuring such timings, it

is be possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.

- **Power Analysis Attacks**: These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.
- **Fault analysis Attacks**: In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

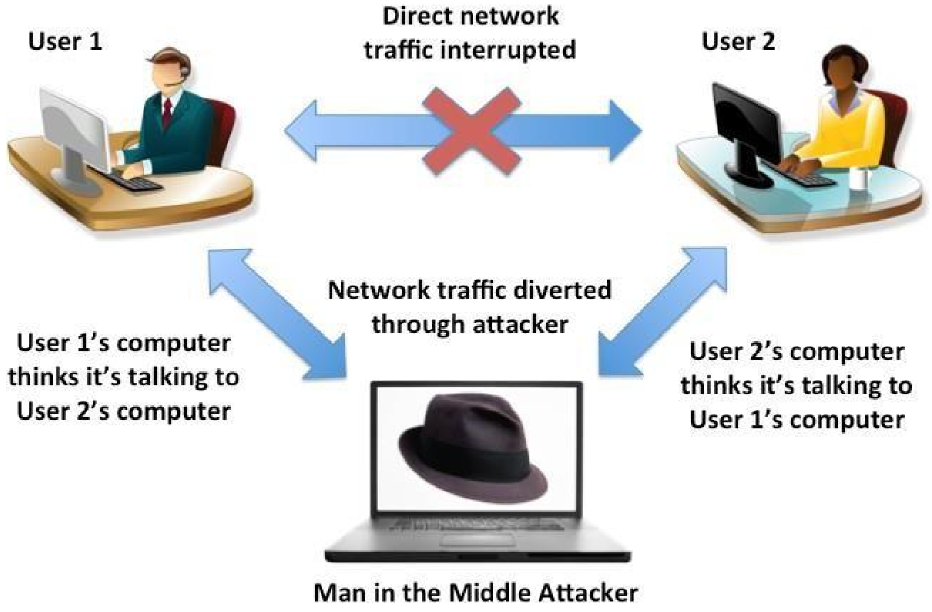

User 1
Direct network traffic interrupted
User 2
Network traffic diverted through attacker
User 1's computer thinks it's talking to User 2's computer
User 2's computer thinks it's talking to User 1's computer
Man in the Middle Attacker

Fig 2: Security Attack

Cipher –

In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information from plain text into cipher or code. In nontechnical usage, a 'cipher' is the same thing as a 'code'; however, the concepts are distinct in cryptography. In traditional cryptography, ciphers were distinguished from codes. Codes commonly substitute diverse length series of characters in the yield, while ciphers commonly substitute indistinguishable number of characters from are input. There are special cases and some cipher frameworks may utilize marginally more, or less, characters when output versus the number that were input.

There are mainly Two Traditional Ciphers such as:-

Substitution Cipher Technique:

In Substitution Cipher Technique plain text characters are replaced with other characters, numbers and symbols as well as in substitution Cipher Technique, character's identity is changed while its position remains unchanged.

Example – Caesar Cipher, Polybius Cipher, Vigenere Cipher

Transposition Cipher Technique:

Transposition Cipher Technique rearranges the position of the plain text's characters. In transposition Cipher Technique, The position of the character is changed but character's identity is not changed.

Example – Rail fence Cipher

2. Literature review :-

This paper [5] the security for web keeping money, account passwords, messages accounts secret word, etc requires content protection in mechanized media. It shows the security besides; pressure for the information with the move encryption standard. The age of key has been done with the assistance of the Polybius square. The extension in number of rounds it will require increasingly computational speculation and will end up irksome for the software engineer to break the system

Caesar cipher, otherwise called the shift cipher, is one of the least complex and most generally known old style encryption systems. It is a kind of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the letters in order. For example, with a shift of 3, A would be replaced by D, B would become E, etc. The encryption step performed by a Caesar cipher is regularly joined as a component of progressively complex plans, for example, the Vigenère cipher, and still has present day application in the ROT13 framework. Similarly as with all single letters in order substitution ciphers, the Caesar cipher is effortlessly broken and in present day practice offers basically no correspondence security.[6]

In cryptography, a transposition cipher is a process of encryption by which the positions held by units of plaintext are shifted by a customary framework or example, so that the ciphertext comprises a stage of the plaintext. That is, the request for the units is changed toward the finish of the shifting process. Mathematically, a bijective function is utilized on the characters' positions to encode and an inverse function to decrypt. The letters themselves are kept unaltered, which suggests that the impact is just on their positions just, making their request inside the message mixed by a few all around characterized scheme. Numerous transposition ciphers are done as per a geometric design

In [9] changed variant of vigenere algorithm was proposed in which dispersion

is given by adding an arbitrary piece to every byte before the message is scrambled utilizing Vigenere. This strategy falls flat kasiski assault to discover the length of key on the grounds that the cushioning of message with irregular bits. The fundamental downside of this system is that the size of the scrambled message will be expanded by around 56%.

In [10] another method for executing Vigenere algorithm was presented via naturally changing the cipher key after every encryption step. In this technique progressive keys were utilized that were reliant on the underlying key an incentive during the encryption process.

In [11] adjustment of Vigenere cipher by irregular numbers, punctuations and scientific images was introduced. In proposed technique numbers, punctuations furthermore, scientific images were utilized for key instead of characters to make it increasingly hard for animal power assault. It was inferred that if irregular numbers are utilized for key what's more, to spread the range then just skilled people can recognize the message recognize the message.

Another algorithm [12] by combining Vigenere substitution cipher with Stream cipher was proposed in which repeated bits of plaintext consistently encrypted with the diverse segment of the catchphrase or binary key. The letters in odd location were encoded with stream cipher and the letters in even location with Vigenere cipher. It was inferred that proposed algorithm conceals the connection between cipher content and plain content that makes cryptanalysis much troublesome.

Tianfu [13] address that internet is one of the most unsafe communication medium due to huge connection and public network. Information protection is one the of essential requirement. At present various security algorithms are proposed to achieve security during communication. All of them have certain good point and certain bad point.

is given by adding an arbitrary piece to every byte before the message is scrambled utilizing Vigenere. This strategy falls flat kasiski assault to discover the length of key on the grounds that the cushioning of message with irregular bits. The fundamental downside of this system is that the size of the scrambled message will be expanded by around 56%.

In [10] another method for executing Vigenere algorithm was presented via naturally changing the cipher key after every encryption step. In this technique progressive keys were utilized that were reliant on the underlying key an incentive during the encryption process.

In [11] adjustment of Vigenere cipher by irregular numbers, punctuations and scientific images was introduced. In proposed technique numbers, punctuations furthermore, scientific images were utilized for key instead of characters to make it increasingly hard for animal power assault. It was inferred that if irregular numbers are utilized for key what's more, to spread the range then just skilled people can recognize the message recognize the message.

Another algorithm [12] by combining Vigenere substitution cipher with Stream cipher was proposed in which repeated bits of plaintext consistently encrypted with the diverse segment of the catchphrase or binary key. The letters in odd location were encoded with stream cipher and the letters in even location with Vigenere cipher. It was inferred that proposed algorithm conceals the connection between cipher content and plain content that makes cryptanalysis much troublesome.

Tianfu [13] address that internet is one of the most unsafe communication medium due to huge connection and public network. Information protection is one the of essential requirement. At present various security algorithms are proposed to achieve security during communication. All of them have certain good point and certain bad point. To improve the strength of encryption algorithm they proposed a hybrid model. Proposed model is combination of AES and DES. Both algorithms are symmetric key technique and itself they are

very much capable for encryption. Integration of AES and DES would give a strong level of security at encryption end. A significant improvement in results has been observed with proposed solution.

Jakimoski et al. [14] analyzed and evaluated the most important security techniques for data protection that are already accepted from the cloud computing providers. They classified them in four sections according to the security mechanisms that they provide: authentication, confidentiality, access control and authorization. They conclude that if all recommended measures are taken into account providing authentication, confidentiality, access control and authorization, then the cloud computing can be trusted in data protection. They focused on the security issues that should be taken into account in depth in order to have proper data security in the cloud. They recommended important security measures relating to data protection in the cloud that must be taken into account.

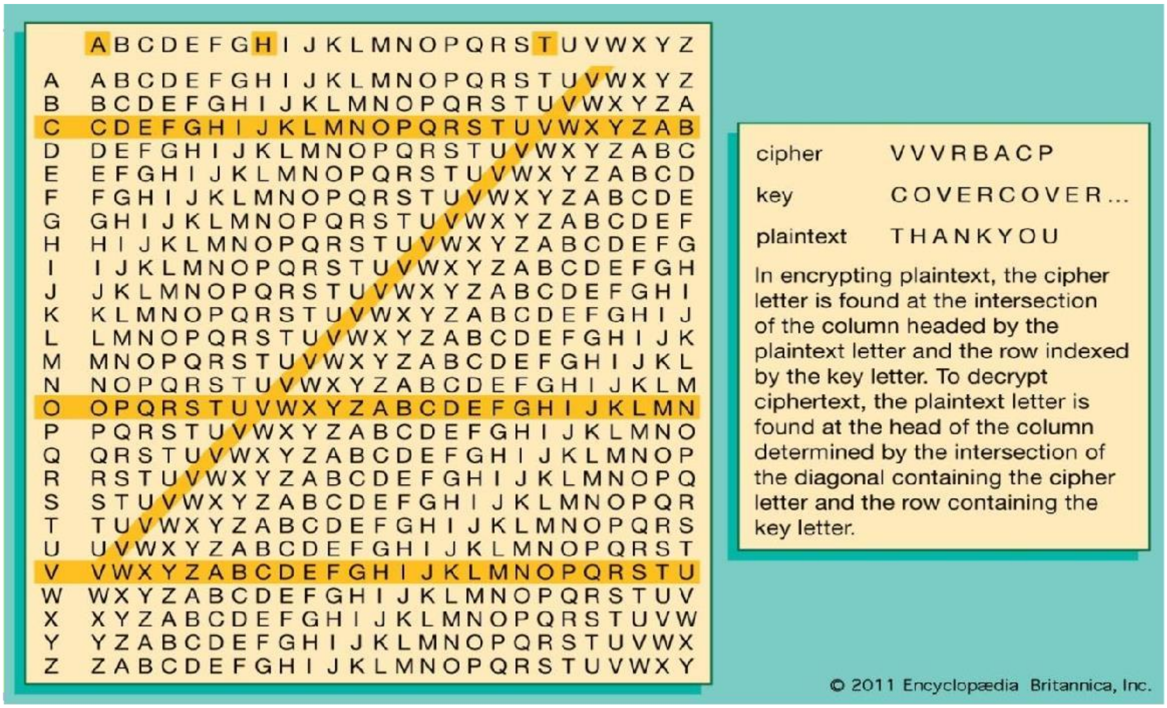
1. PROPOSED SYSTEM

Lightweight Cryptography as Ciphers is taken for Consideration for System. Two famous classical ciphers are used for the Defined plan to do Combination of Cipher in the System such as –

Vigenere Cipher

Vigenere 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*

This makes the cipher less vulnerable to cryptanalysis using letter frequencies. Blaise de Vigenère developed what is now called the Vigenère cipher in 1585. He used a table known as the Vigenère square, to encipher messages.



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

cipher	VVVRBACP
key	COVERCOVER...
plaintext	THANKYOU

In encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt ciphertext, the plaintext letter is found at the head of the column determined by the intersection of the diagonal containing the cipher letter and the row containing the key letter.

© 2011 Encyclopædia Britannica, Inc.

Fig 3: Vigenere Cipher

Example :

Input: Plaintext : INDIA

Key: AYUSH

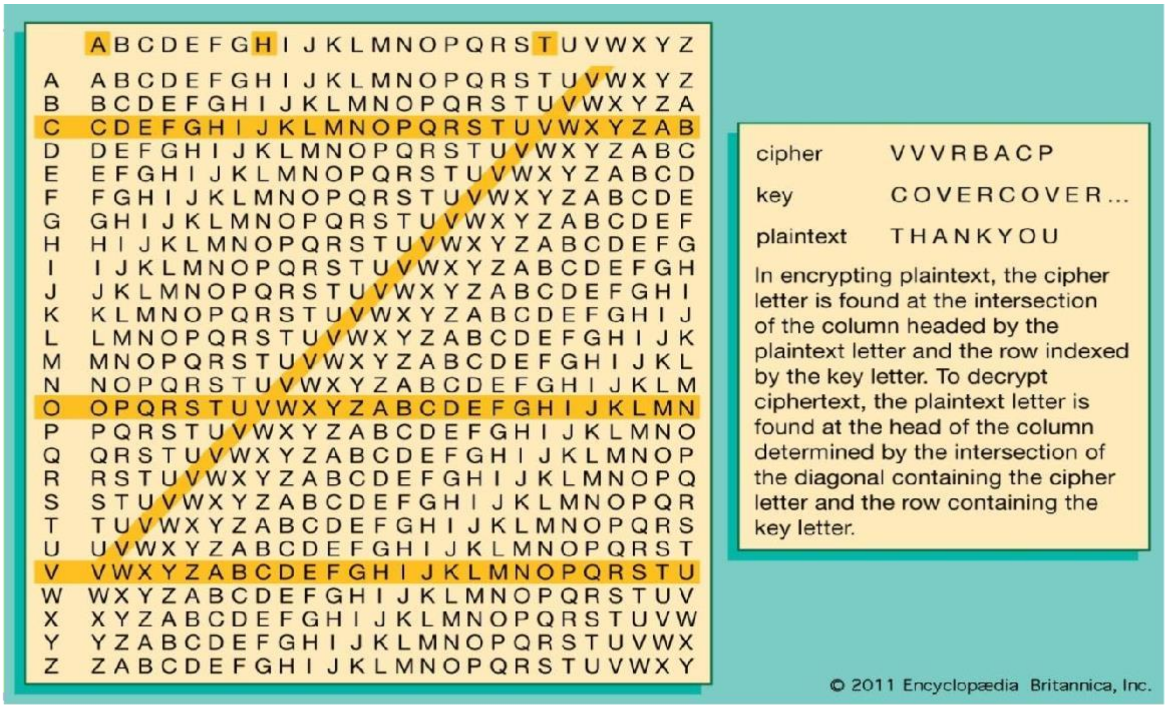
2. PROPOSED SYSTEM

Lightweight Cryptography as Ciphers is taken for Consideration for System. Two famous classical ciphers are used for the Defined plan to do Combination of Cipher in the System such as –

Vigenere Cipher

Vigenere 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*

This makes the cipher less vulnerable to cryptanalysis using letter frequencies. Blaise de Vigenère developed what is now called the Vigenère cipher in 1585. He used a table known as the Vigenère square, to encipher messages.



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

cipher	VVVRBACP
key	COVERCOVER...
plaintext	THANKYOU

In encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt ciphertext, the plaintext letter is found at the head of the column determined by the intersection of the diagonal containing the cipher letter and the row containing the key letter.

© 2011 Encyclopædia Britannica, Inc.

Fig 3: Vigenere Cipher

Example :

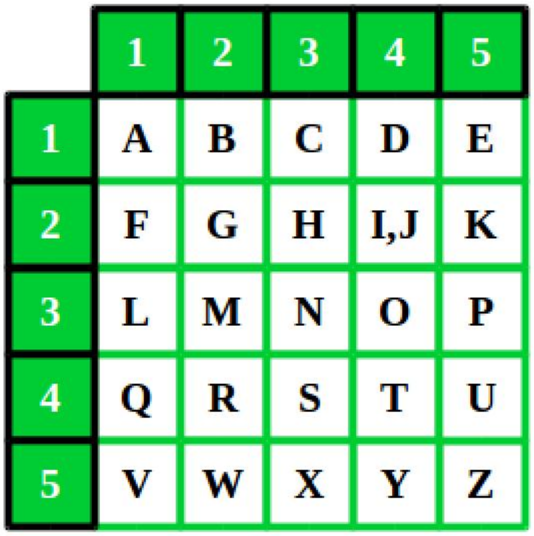
Input: Plaintext : INDIA

Key: AYUSH

Output: ILXAH

Polybius Square 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. A table of bigger size could be used if a language contain large number of alphabets.[4]



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

Fig 4: Polybius Cipher

Example**:** Input:

BUS Output:

124543

Now, this both two Vigenere and Polybius cipher will be done summation and combination for formation of hybrid cipher system. This combination makes use of alphabetic substitution that is vigenere Cipher and polyalphabetic Numerical Cipher that is Polybius Square Cipher which make the message and plain text to encrypted message which is very confusing, unstructured and diffused that cannot be easier to break.

3. METHADOLOGY

The message as plaintext and Key is send through sender in two phase for execution and working of System as in first phase it will proceed through Vigenere 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 numerical and the Input that proceed in first phase was alphabetic letters this all confuses and doesn't allow the intruders, detectors, thefts, hackers and cyber crime to commit any assaults and attacks on system and doesn't allow them to steal Information.

A python programming is written and executed for the working of System. Google Colab as Online and Sypder IDE on Independent System are taken for Execution of process. Flowchart of Hybrid Algorithm-

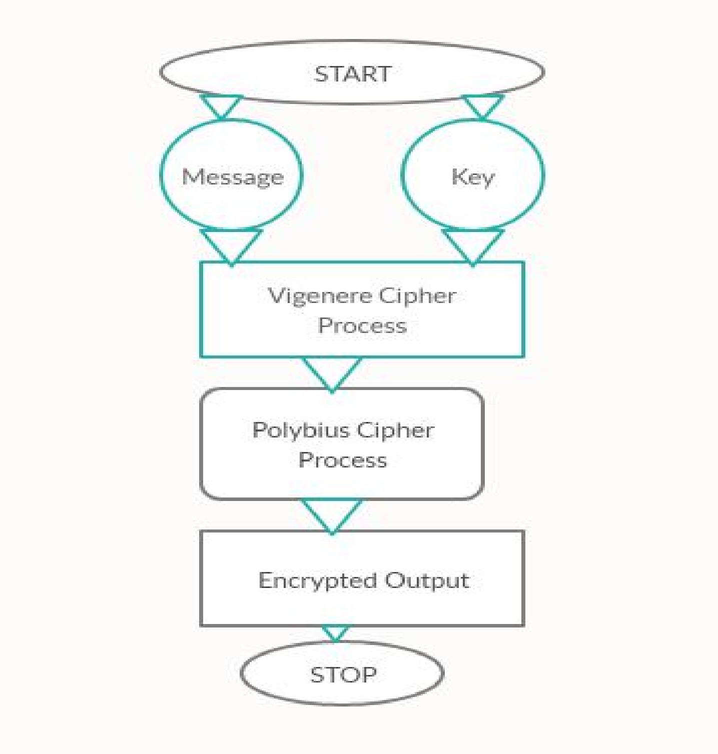


Fig 5: Hybrid System

4. IMPLEMENTATION

Python programming is written for Implementation of Hybrid System.

Step 1 : Vigenere Cipher

```
# Python code to implement
# Vigenere Cipher

# This function generates the
# key in a cyclic manner until
# it's length isn't equal to
# the length of original text
def generateKey(string, key):
  key = list(key)
  if len(string) == len(key):
    return(key)
  else:
    for i in range(len(string) -
          len(key)):
      key.append(key[i % len(key)])
  return("" . join(key))

# This function returns the
# encrypted text generated
# with the help of the key
def cipherText(string, key):
  cipher_text = []
  for i in range(len(string)):
    x = (ord(string[i]) +
      ord(key[i])) % 26
    x += ord('A')
    cipher_text.append(chr(x))
  return("" . join(cipher_text))

# This function decrypts the
# encrypted text and returns
# the original text
def originalText(cipher_text, key):
  orig_text = []
  for i in range(len(cipher_text)):
    x = (ord(cipher_text[i]) -
      ord(key[i]) + 26) % 26
    x += ord('A')
    orig_text.append(chr(x))
  return("" . join(orig_text))


# Driver code
if_name_== "_main__":
  string = "GEEKSFORGEEKS"
  keyword = "AYUSH"
  key = generateKey(string, keyword)
  cipher_text = cipherText(string,key)
  print("Ciphertext :", cipher_text)
  print("Original/Decrypted Text :",
    originalText(cipher_text, key))
```

Step 2 : Polybius Cipher

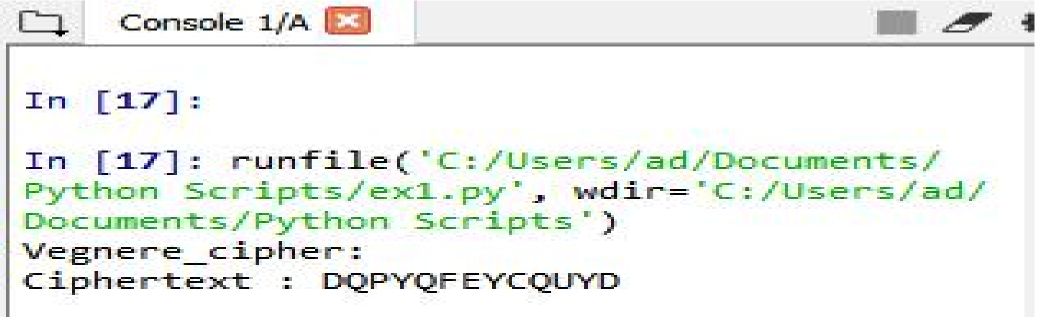
```
def codes_table(char):
    table = {
        "A": 11, "B": 21, "C": 31, "D": 41, "E": 51,
        "F": 12, "G": 22, "H": 32, "I": 42, "K": 52,
        "L": 13, "M": 23, "N": 33, "O": 43, "P": 53,
        "Q": 14, "R": 24, "S": 34, "T": 44, "U": 54,
        "V": 15, "W": 25, "X": 35, "Y": 45, "Z": 55, "J": 0,

        11: "A", 21: "B", 31: "C", 41: "D", 51: "E",
        12: "F", 22: "G", 32: "H", 42: "I", 52: "K",
        13: "L", 23: "M", 33: "N", 43: "O", 53: "P",
        14: "Q", 24: "R", 34: "S", 44: "T", 54: "U",
        15: "V", 25: "W", 35: "X", 45: "Y", 55: "Z", 0: "J"
    }

    return table[char]


def encoding(text):
    text, finished_text = text.upper(), ""
    for symbol in text:
        if symbol in alphabet:
            finished_text += str(codes_table(symbol)) + " "

    return finished_text
```

```
def decoding(text):
    text, finished_text = text.upper(), ""
    for symbol in list(map(int, text.split())):
        finished_text += codes_table(symbol)

    return finished_text


def assembly(mode):
    text = str(input("[+] Enter your text - "))

    if mode == 0:
        finished_text = encoding(text)
    else:
        finished_text = decoding(text)

    print("\n »» The result of encoding by algorithm. ««")
    print(finished_text)


def main():
    print("[x] Polybius Square cryptography algorithm. [x]")
    print(" • 0. Encoding mode.\n • 1. Decoding mode.")

    mode = int(input("[?] Select program mode - "))
    assembly(mode)


_      if name__== '___main___':
    main()
```

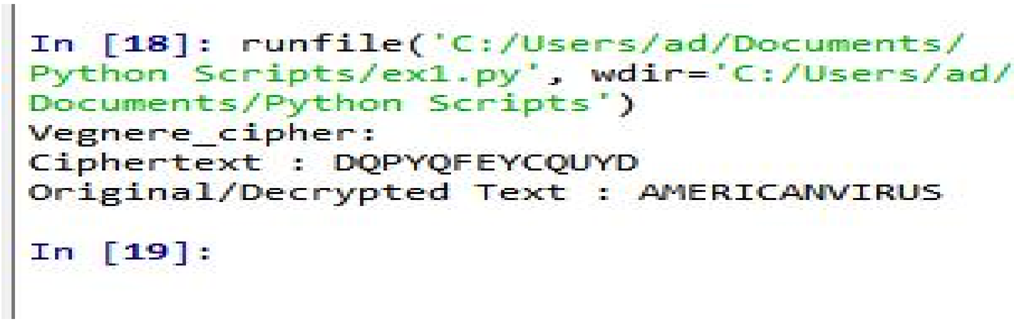
The output will be Encrypted text as Cipher text will be generated from the system. This two combination of cipher program will be executed back to backto get cipher text. It can be implemented on any System, IDE, Interpreter, and Compiler or on Cloud System such as Jupyter, Anaconda, Google collaboratory, etc

1. OUTPUTS

VIGENERE CIPHER ENCRYPTION:

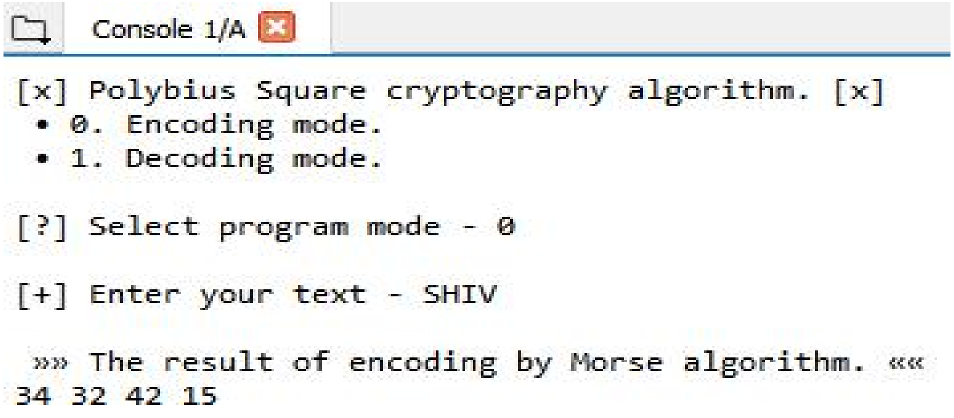


```
In [17]:

In [17]: runfile('C:/Users/ad/Documents/
Python Scripts/ex1.py', wdir='C:/Users/ad/
Documents/Python Scripts')
Vegnere_cipher:
Ciphertext : DQPYQFEYCQUYD
```



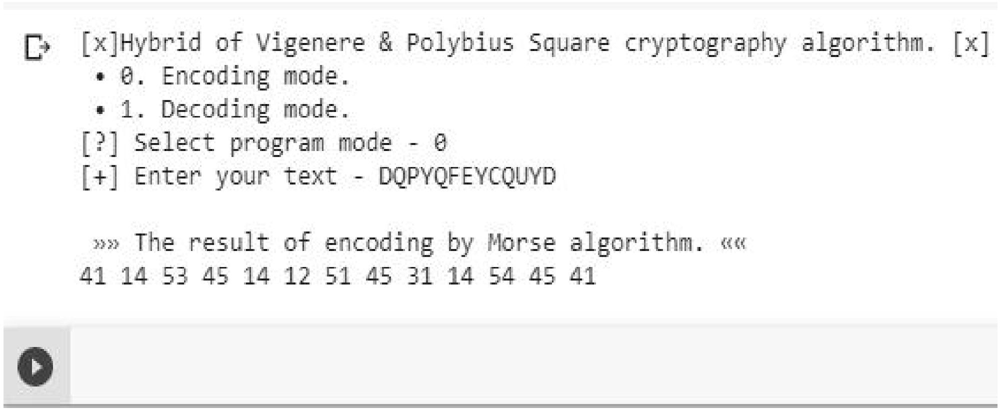
```
In [18]: runfile('C:/Users/ad/Documents/
Python Scripts/ex1.py', wdir='C:/Users/ad/
Documents/Python Scripts')
Vegnere_cipher:
Ciphertext : DQPYQFEYCQUYD
Original/Decrypted Text : AMERICANVIRUS

In [19]:
```

POLYBIUS CIPHER ENCRYPTION:



```
[x] Polybius Square cryptography algorithm. [x]
 • 0. Encoding mode.
 • 1. Decoding mode.

[?] Select program mode - 0

[+] Enter your text - SHIV

 »» The result of encoding by Morse algorithm. ««
34 32 42 15
```

HYBRID COMBINATION OF VIGENERE CIPHER AND POLYBIUS CIPHER -



```
[x]Hybrid of Vigenere & Polybius Square cryptography algorithm. [x]
 • 0. Encoding mode.
 • 1. Decoding mode.
[?] Select program mode - 0
[+] Enter your text - DQPYQFEYCQUYD

 »» The result of encoding by Morse algorithm. ««
41 14 53 45 14 12 51 45 31 14 54 45 41
```

7. CONCLUSION AND FUTURE ENHANCEMENT-

Cryptography is the generally utilized technique for the security of data. Vigenere cipher is one of the cryptographic techniques that are viewed as least complex and most vulnerable because of numerous impediments. To conquer the impediments of Vigenere cipher we proposed an upgraded variant as Combination of Polybius cipher that is a lot of secure against Kasiski and Friedman assaults. Cryptanalysis, frequency analysis, pattern prediction and brute attack on proposed technique are also much difficult due to use of multiples tables for encryption. The modified hybrid of both the Caesar Cipher and Vigenere Cipher, there is now a high percentage of Diffusion and Confusion in the algorithm that generates them making it a very strong cipher and difficult to break. In spite of the fact that there are numerous cryptographic strategies yet this space still requires genuine consideration of research network for the improvement of data security. In future our point is to give approval of proposed approach by performing security and performance analysis.

8. REFRENCES-

[1] Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryptography Algorithm.

[2] Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing." International Journal of Grid and Distributed Computing 9.1 (2016): 49-56.

[3]https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

[4]https://en.wikipedia.org/wiki/Polybius_square

[5] Puneet Kumar, Shashi B. Rana, Development of modified AES algorithm for data security, Optik - International Journal for Light and Electron Optics, Volume 127, Issue 4, 2016, Pages 2341-2345, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2015.11.188. (http://www.sciencedirect.com/science/article/pii/S0030402615018215)

[6] Encryption. Wellesley college Computer Science Department lecture note retrieved from : http://cs110.wellesley.edu/lectures/L18-encryption/.

[7] Classical cipher, Transposition ciphers, Retrieved from http://en.wikipedia.org/wiki/Classical_cipher

[8] Transposition ciphers, columnar transposition Retrieved from http://en.wikipedia.org/wiki/Transposition_cipher

[9] C. Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AES proposal): a comparison with DES," in Security Technology, 2001 IEEE 35th International Carnahan Conference on, 2001, pp. 229-234.

[10] Q.-A. Kester, "A cryptosystem based on Vigenère cipher with varying key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, pp. pp: 108-113, 2012.

[11] C. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278-0661, 2012

[12] F. H. S. Fairouz Mushtaq Sher Ali, "Enhancing Security of Vigenere Cipher by Stream Cipher," International Journal of Computer Applications, vol. 100, pp. 1-4, 2014

[13] P. Gutmann, ―Cryptographic Security Architecture: Design and Verification‖. Springer-Verlag,2004.

[14] Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing." International Journal of Grid and Distributed Computing 9.1 (2016): 49-56.

[15] M. Abror, "Pengertian dan Aspek-Aspek Keamanan Komputer," 2018. [Daring]. Tersedia pada:https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputer-lengkap/. [Diakses: 01-Okt-2018].

[16]V.Beal.(2009,Encryption.Available:Http://www.webopedia.com/TERM/E/
encryption.ht