# Design and Analysis of Cryptographic Technique for Communication System

Presented To- Shubham Bainik

Presented By:
Krishna Rajoria - 21tec2cs061
Katta Pavan - 21tec2cs058
Koruprolu Gowtham - 21tec2cs60

# Abstract

Secure Communication of message from sender to receiver is one of the main security concern 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

Ciphers act as encapsulating system for message. Hybrid Algorithm will be formed from use of different types of ciphers.

The cryptosystem performs its encryption by encrypting the plaintext using Vigenere Cipher and further again processing though Polybius Cipher.

# Cryptography Definition

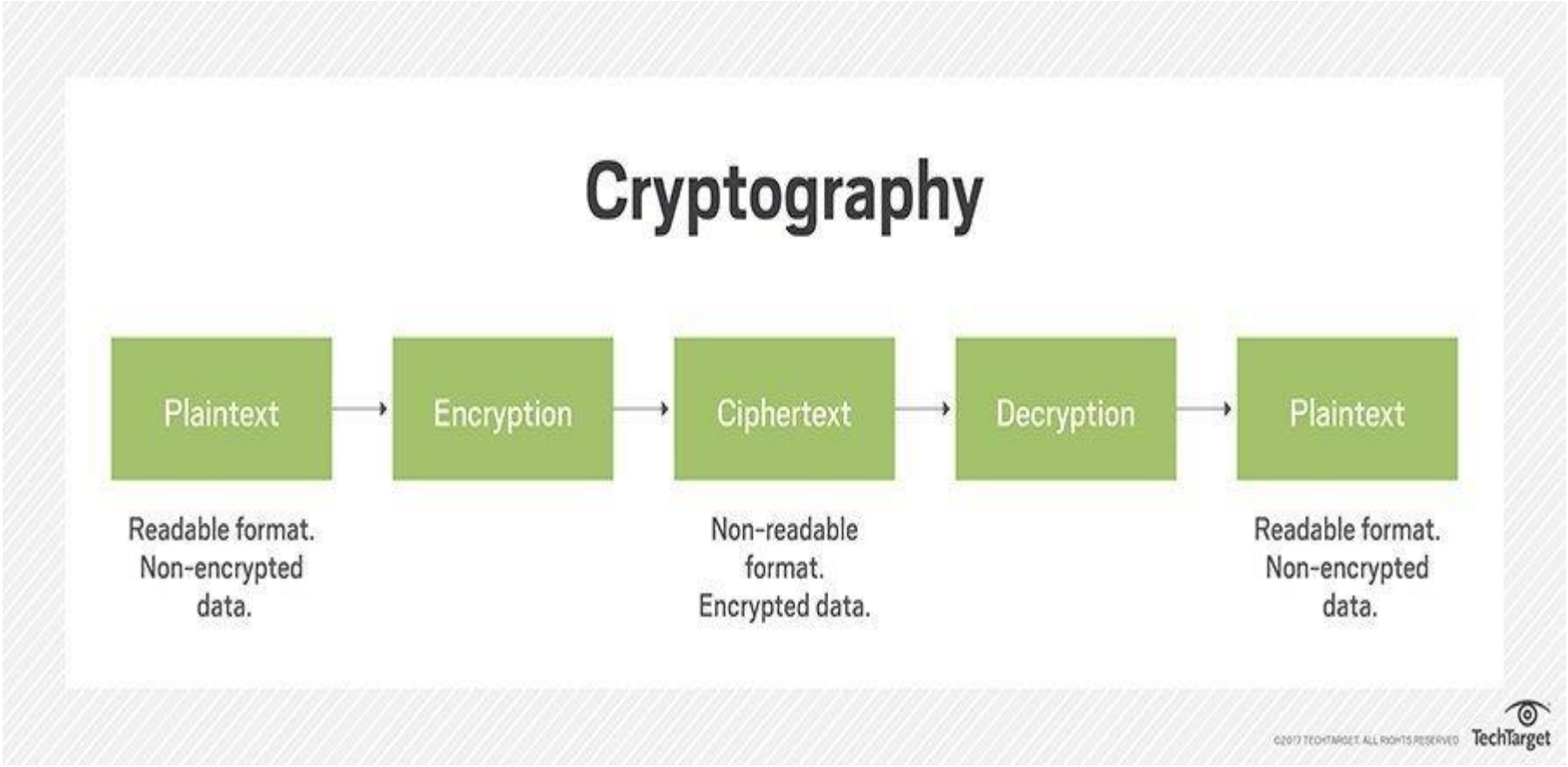
Cryptography is the science of protecting information by transforming it into a secure format. This process, called encryption, has been used for centuries to prevent handwritten messages from being read by unintended recipients.

Today, cryptography is used to protect digital data. It is a division of computer science that focuses on transforming data into formats that cannot be recognized by unauthorized users.

Two Types of Cryptography:

- Symmetric Cryptography
- Asymmetric Cryptography

# Pictorial View of Cryptography



# Merits

Highly Secure

Confidentiality

Authentication

Data Integrity

Non-repudiation

## Demerits

Less use of hybrid algorithms

Selective access control also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.

Cryptography comes at cost and time

Less deployment of system through Deep Learning (Neural Networks)

Difficult to access even for a legitimate user at a crucial time of decision-making.

Threats that emerge from the poor design of systems.

# Issue and Challenges in Communication System

**State of Insecurity** – Increase in Adaption and Development of fragmented attached attack on daily basis on communication system.

**Data Replication** – Re-writing and Copying of data from Back End server even It is protected by Data saving applications.

**Sense of Message Stealing**- Important Message of huge Key length stealing or blocking & Jamming of server.

New threats and Attacks such as Eavesdroping, DOS attack and kasiski attacks

**Congestion** – Message overlapping and re accessing receiver channel without their knowledge.

**Wireless Spoofing attacks**- attacker uses information obtained by a wireless sniffer to impersonate another machine on the network.

# Literature and Survey

In [1], modified version of vigenere algorithm was proposed in which diffusion is provided by adding a random bit to each byte before the message is encrypted using Vigenere. This technique fails kasiski attack to find the length of key because the padding of message with random bits. The main drawback of this technique is that the size of the encrypted message will be increased by around 56%.

In [2], the Caesar Cipher and Vigenere Cipher have been modified and expanded by including alphabets, numbers and symbols and at the same time introduced a complete confusion and diffusion into the modified cipher developed. It was concluded that cipher text generated by proposed hybrid technique is very difficult to break using a frequency method, brute force attack etc.

Vigenere cipher is one of the most popular ciphers in the past because of its simplicity and resistance to the frequency analysis test of letters that can crack simple ciphers like Caesar cipher. But with the increase in the cryptanalytic skills, Vigenere cipher is no longer taken as secure cipher and is not popularly used. The most weak point of Vigenere cipher is the use of

# DIFFIE HELLMAN KEY EXCHANGE ALGORITHM

The Diffie–Hellman Key Exchange Method (hereafter called the D-H method) allows two parties agree upon a shared secret number, a symmetric key, over an insecure communications channel/medium, where attackers/hackers might be listening in.

The benefit of using a symmetric key over public key cryptography lies in the fact that encryption of a plaintext message into a ciphertext message and decryption of the ciphertext message back to the original plaintext message happens much faster using a symmetric key.

# Vigenere Cipher

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.

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.

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.

# Vigenere Table

| | 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 |

# 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.

| | 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 |

# Proposed Work

The method employs use of both Vegenere Cipher and Polybius Square Cipher in its encryption process.

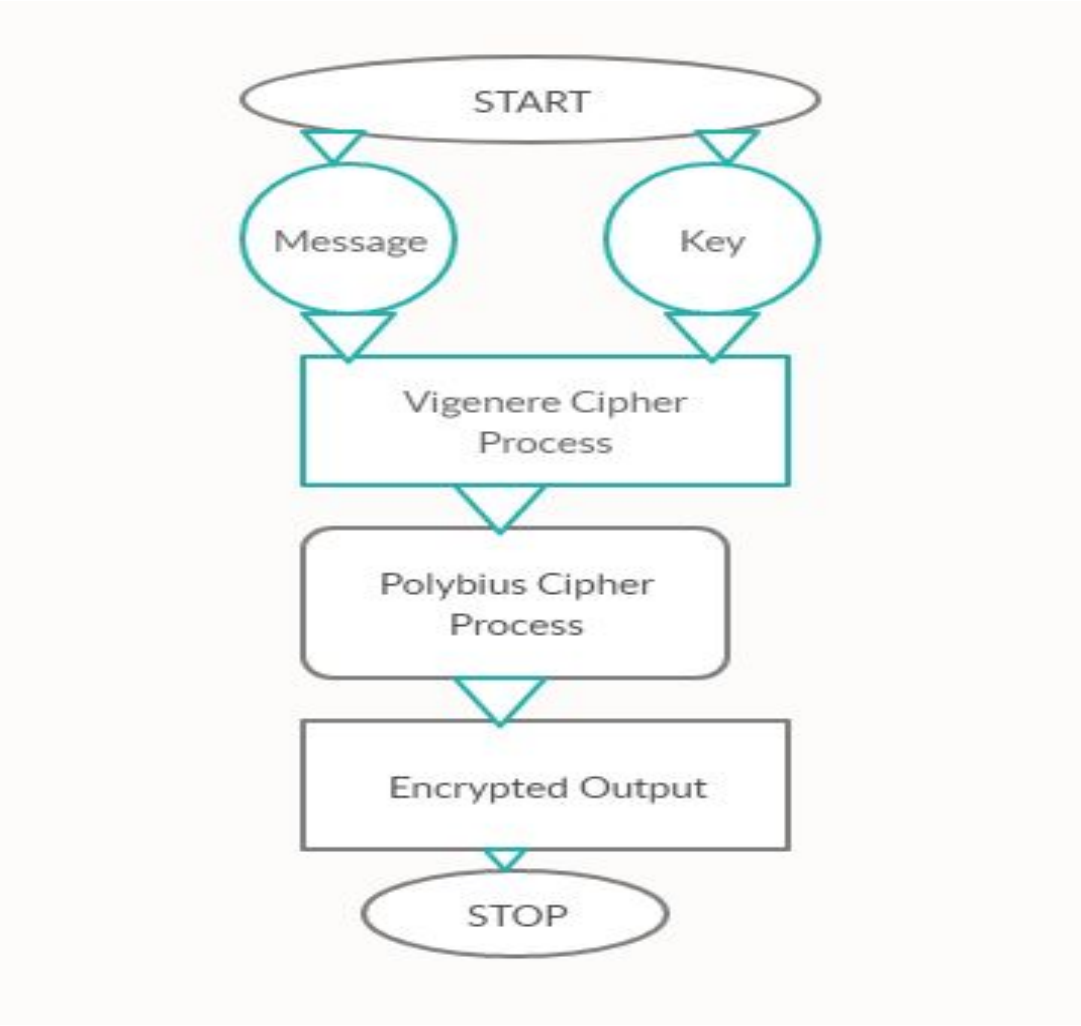
The ciphertext will first be operated on using Vegenere. A chosen key out of random will initiate the process.

At the end of the process, the resulting ciphertext then becomes a message as Input for the Polybius Square Cipher process.

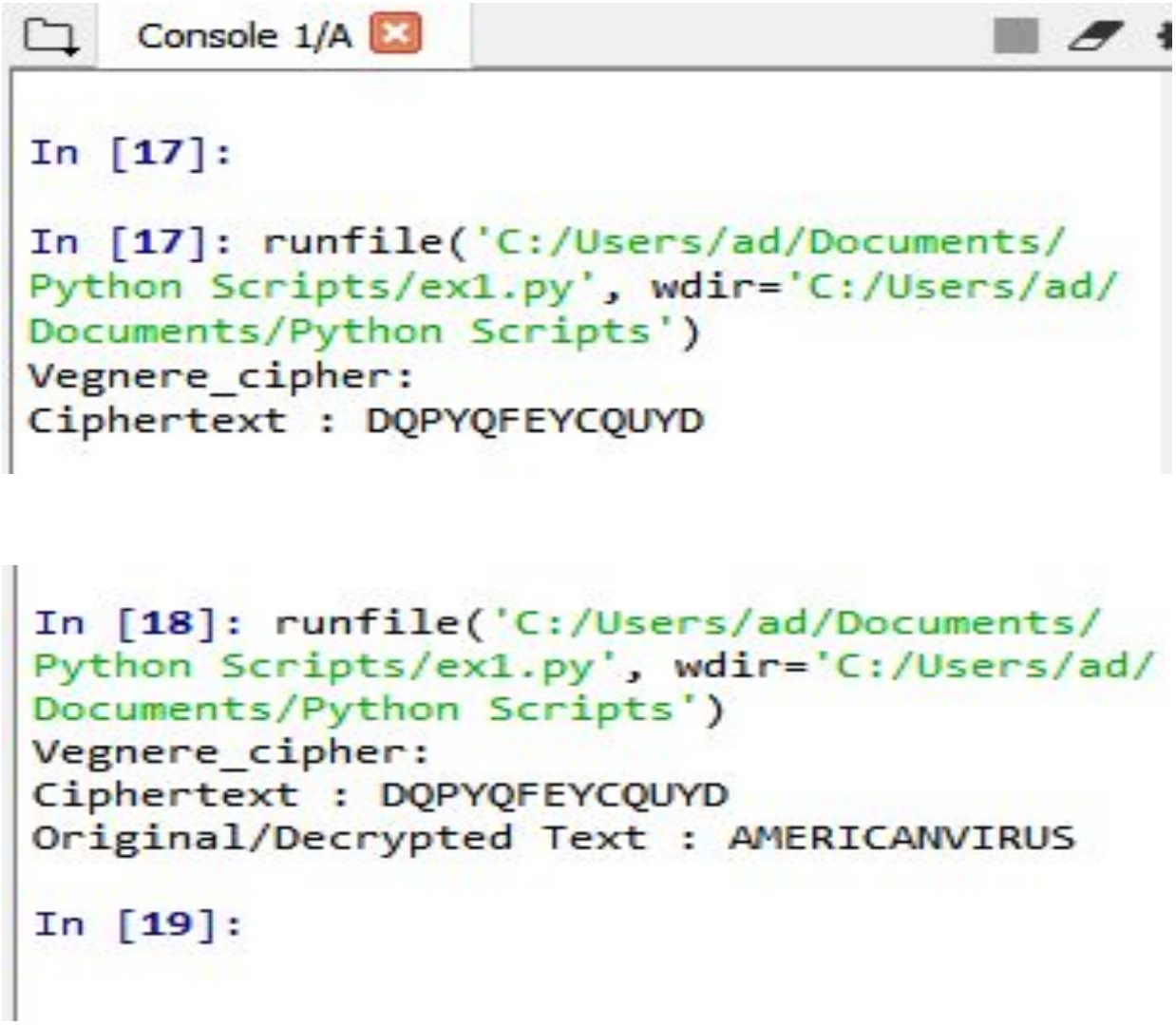
This process will end up making the final ciphertext more difficult to be broken using existing cryptanalysis processes.

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.

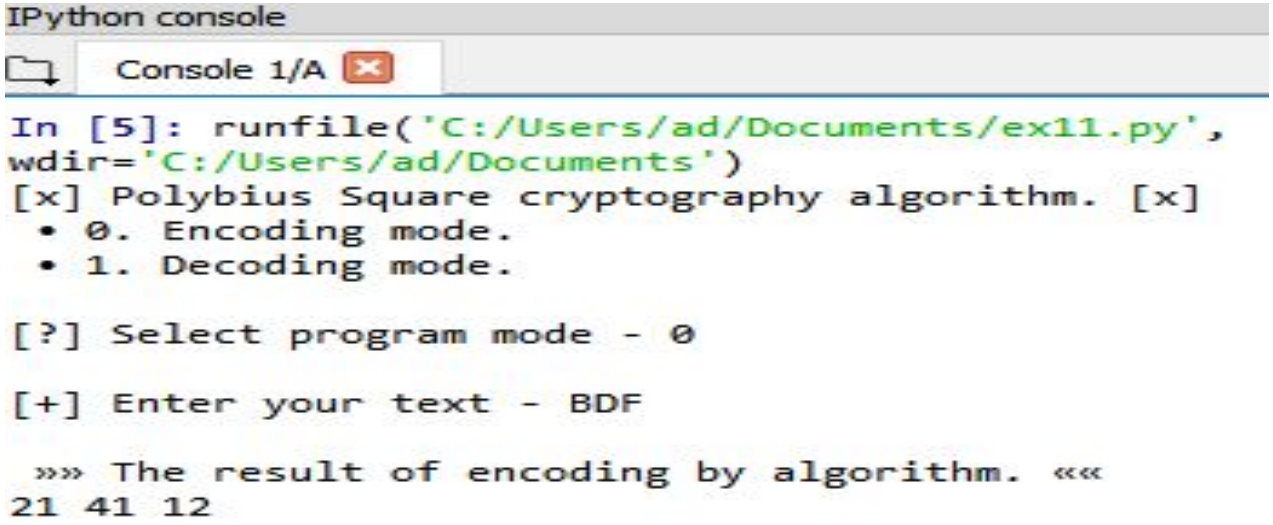
# Pictorial View

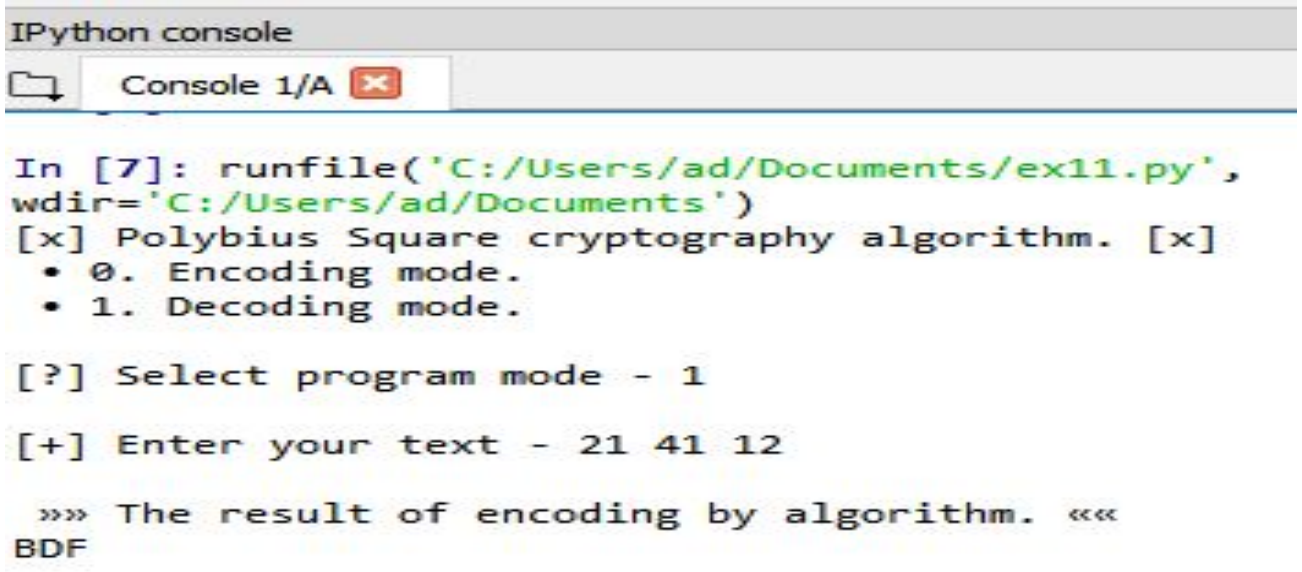


# Vegenere Cipher Output



# Polybius Cryptography Output



# Hybrid Cipher

Hybrid Process though Combination of Vigenere and Polybius Square Cipher takes Encoding Mode where it governs on [A-Z] Aplhabetic letters and Numerical Both in the System.

This Hybrid Cipher makes the System tough and unbreakable for any Assaults and attacks from Outside

```
[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
```

# Conclusion

Cryptography is the widely used method for the security of data.

Diffie Hellman Exchange Key Algorithm will determine numbers of secret message to transfer.

Vigenere cipher is one of the cryptographic method that is considered simplest and weakest due to many limitations.

To overcome the limitations of Vigenere cipher we proposed Summation of Polybius Cipher that makes much secure against Kasiski and Friedman attacks. 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.

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 analysis.