PRACTICAL: 9

AIM:

A cybersecurity training program is preparing students to understand and apply cryptographic techniques in real-world scenarios. The students are tasked with using CrypTool to study various cryptographic algorithms and simulate encryption and decryption processes to gain practical insights into data security mechanisms. To explore and analyses cryptographic algorithms using CrypTool to understand their functionality, strengths, and weaknesses in securing sensitive information.

THEORY:

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption keys. Modern ciphers, such as the Advanced Encryption Standard (AES), are considered virtually unbreakable.

Monoalphabetic Cipher is a part of the substitution technique in which a single cipher alphabet is used per message (mapping is done from plain alphabet to cipher alphabet). Monoalphabetic cipher converts plain text into cipher text and re-convert a cipher text to plain text. Monoalphabetic Cipher eliminates the brute-force techniques for cryptanalysis. Moreover, the cipher line can be a permutation of the 26 alphabetic characters.

In Cryptography, various encryption techniques are used to provide data security. The classical Encryption technique is categorized into two divisions:

1. Substitution Cipher Technique

- Caesar Cipher
- Monoalphabetic Cipher
- Polyalphabetic Cipher
- Playfair Cipher
- Hill Cipher
- One-time Pad

2. Transposition Cipher Technique

The techniques which come under this division are as follows -

- Rail Fence.
- Row Column Transposition.

Types of Monoalphabetic Substitution Ciphers

Additive Cipher

It is also Known as Shift Cipher which shifts plain text to form Cipher-text.

- Mathematical Expression:
    - For Encryption: C=(P + K) mod 26 where 'P' is the character in plain text, 'K' is the key, and 'C' is the Cipher.
    - For Decryption: P=(C-K) mod 26.
- Example : Input : P= GEEKS ,Key= 4 . Output : C=KIIOW

Caesar Cipher

A type of Addictive Cipher but the value of key is always '3' here.

- Mathematical Expression:
    - For Encryption: C=(P + K) mod 26 where 'P' is the character in plain text, 'K' is the key, and 'C' is the Cipher.
    - For Decryption: P=(C-K) mod 26
- Example: Input: P=GEEKS , Output : C=JHHNV

Multiplicative Cipher

Letters are changed here using a multiplication key.

- Mathematical Expression:
    - For Encryption: C=(P * K) mod 26 where, 'P' is the character in plain text, 'K' is the key, and 'C' is the Cipher.
- Example: Input : P=VMH , Key= 3 . Output : C=HEL

Affine Cipher

A mathematical function is used to convert plain text into cipher text.

- Mathematical Expression:
    - For Encryption : C=(P * K1+K2) mod 26 where, 'P' is the character in plain text, 'K1' is the multiplicative key, 'K2' is the additive key and 'C' is Cipher.
    - For Decryption : P=((C-K2)/ K1) mod 26.
- Example : Input : P=ARM , Key1=3,Key2=5 . Output : C=HEL

Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Examples:

Input : Plaintext: ACT

Key: GYBNQKURP

Output : Ciphertext: POH

Playfair cipher, type of substitution cipher used for data encryption.

In cryptosystems for manually encrypting units of plaintext made up of more than a single letter, only digraphs (pairs of letters) were ever used. By treating digraphs in the plaintext as units rather than as single letters, the extent to which the raw frequency distribution survives the encryption process can be lessened but not eliminated, as letter pairs are themselves highly correlated. The best-known digraph substitution cipher is the Playfair, invented in 1854 by Sir Charles Wheatstone but championed at the British Foreign Office by Lyon Playfair, the first Baron Playfair of St. Andrews. Below is an example of a Playfair cipher, solved by Lord Peter Wimsey in Dorothy L. Sayers's *Have His Carcase* (1932). Here, the mnemonic aid used to carry out the encryption is a 5 × 5-square matrix containing the letters of the alphabet (I and J are treated as the same letter). A key word, MONARCHY in this example, is filled in first, and the remaining unused letters of the alphabet are entered in their lexicographic order:

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

Plaintext digraphs are encrypted with the matrix by first locating the two plaintext letters in the matrix. They are (1) in different rows and columns; (2) in the same row; (3) in the same column; or (4) alike. The corresponding encryption (replacement) rules are the following:

1. When the two letters are in different rows and columns, each is replaced by the letter that is in the same row but in the other column; i.e., to encrypt WE, W is replaced by U and E by G.
2. When A and R are in the same row, A is encrypted as R and R (reading the row cyclically) as M.
3. When I and S are in the same column, I is encrypted as S and S as X.

4. When a double letter occurs, a spurious symbol, say Q, is introduced so that the MM in SUMMER is encrypted as NL for MQ and CL for ME.

5. An X is appended to the end of the plaintext if necessary to give the plaintext an even number of letters.

Encrypting the familiar plaintext example using Sayers's Playfair array yields:

```
Plaintext: WE ARE DISCOVERED SAVE YOURSELFX
Cipher:    UG RMK CSXHMUFMKB TOXG CMVATLUIV
```

If the frequency distribution information were totally concealed in the encryption process, the ciphertext plot of letter frequencies in Playfair ciphers would be flat. It is not. The deviation from this ideal is a measure of the tendency of some letter pairs to occur more frequently than others and of the Playfair's row-and-column correlation of symbols in the ciphertext—the essential structure exploited by a cryptanalyst in solving Playfair ciphers. The loss of a significant part of the plaintext frequency distribution, however, makes a Playfair cipher harder to cryptanalyze than a monoalphabetic cipher.

substitution cipher, data encryption scheme in which units of the plaintext (generally single letters or pairs of letters of ordinary text) are replaced with other symbols or groups of symbols.

The ciphertext symbols do not have to be the same as the plaintext characters in a substitution cipher, as illustrated in Sir Arthur Conan Doyle's *Adventure of the Dancing Men* (1903), where Sherlock Holmes solves a monoalphabetic substitution cipher in which the ciphertext symbols are stick figures of a human in various dancelike poses.

The simplest of all substitution ciphers are those in which the cipher alphabet is merely a cyclical shift of the plaintext alphabet. Of these, the best-known is the Caesar cipher, used by Julius Caesar, in which A is encrypted as D, B as E, and so forth. As many a schoolboy has discovered to his embarrassment, cyclical-shift substitution ciphers are not secure, nor is any other monoalphabetic substitution cipher in which a given plaintext symbol is always encrypted into the same ciphertext symbol. Because of the redundancy of the English language, only about 25 symbols of ciphertext are required to permit the cryptanalysis of monoalphabetic substitution ciphers, which makes them a popular source for recreational cryptograms. The explanation for this weakness is that the frequency distributions of symbols in the plaintext and in the ciphertext are identical, only the symbols having been relabeled. In fact, any structure or pattern in the plaintext is preserved intact in the ciphertext, so that the cryptanalyst's task is an easy one.

There are two main approaches that have been employed with substitution ciphers to lessen the extent to which structure in the plaintext—primarily single-letter frequencies—survives in the ciphertext. One approach is to encrypt elements of plaintext consisting of two or more symbols; e.g., digraphs and trigraphs. The other is to use several cipher alphabets. When this approach of polyalphabetic substitution is carried to its limit, it results in onetime keys, or pads.

CODE:

N/A

OUTPUT:

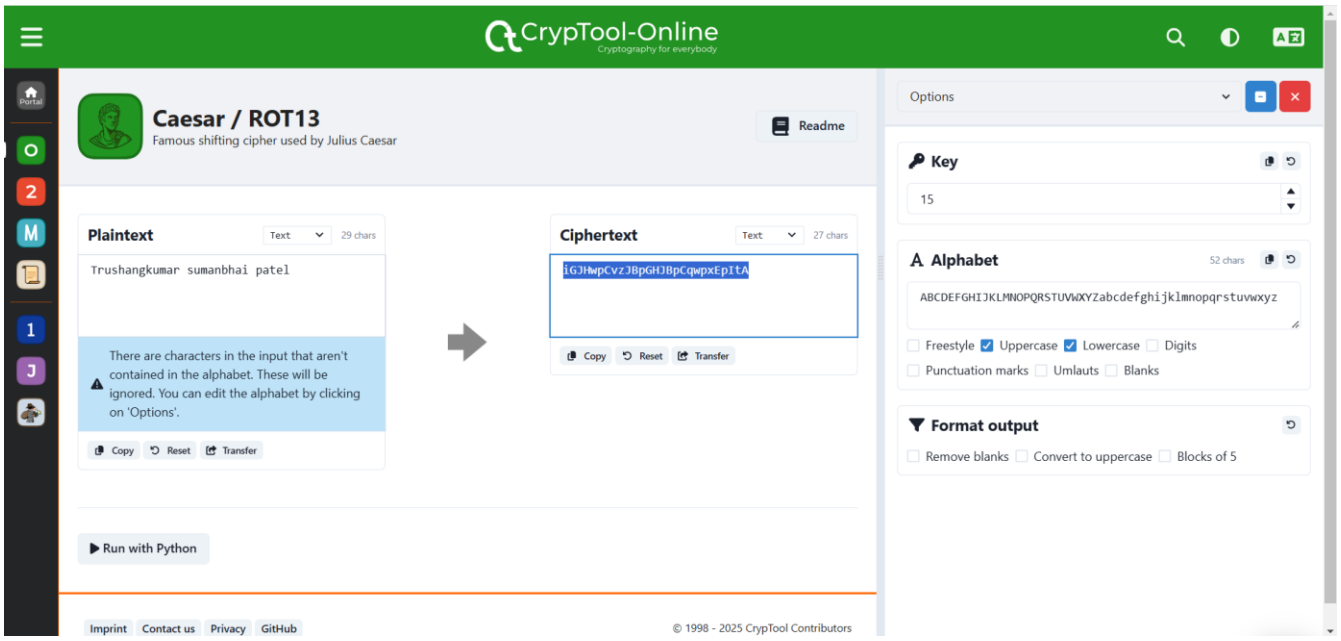

Figure 1: Encrypt the plain text using caser/Additive/shift cipher where k=15 without considering space

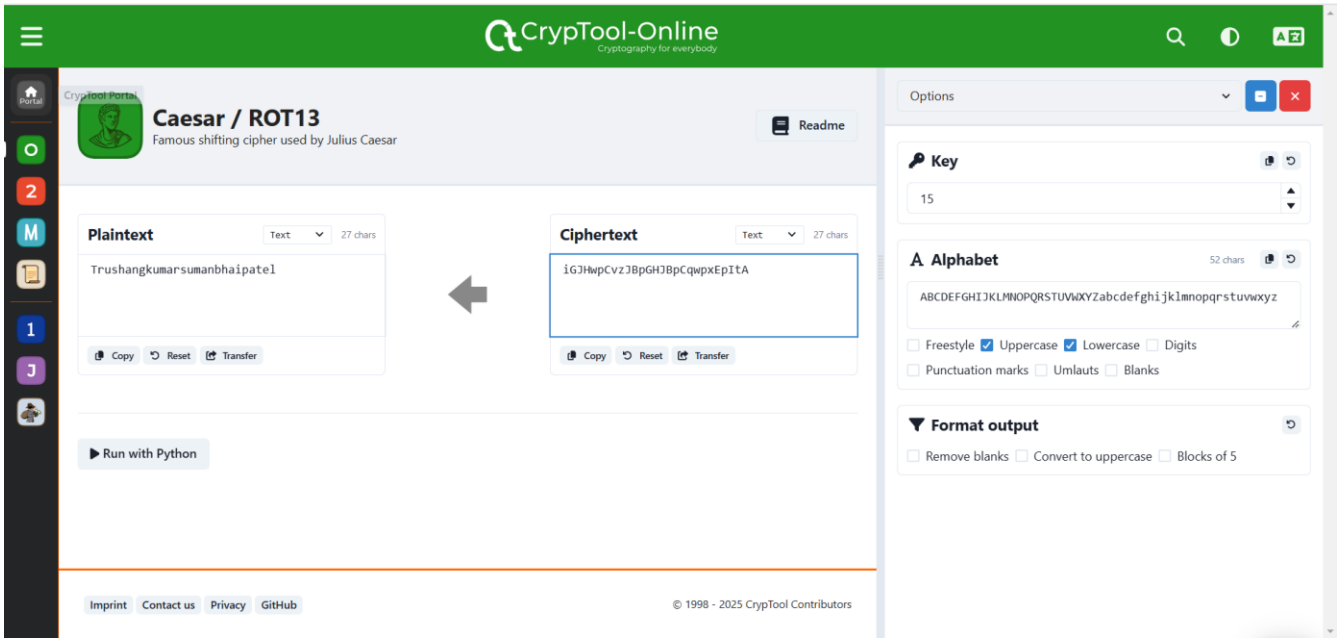

Figure 2:Decrypt the cipher text using caser/Additive/shift cipher where k=15 without considering space

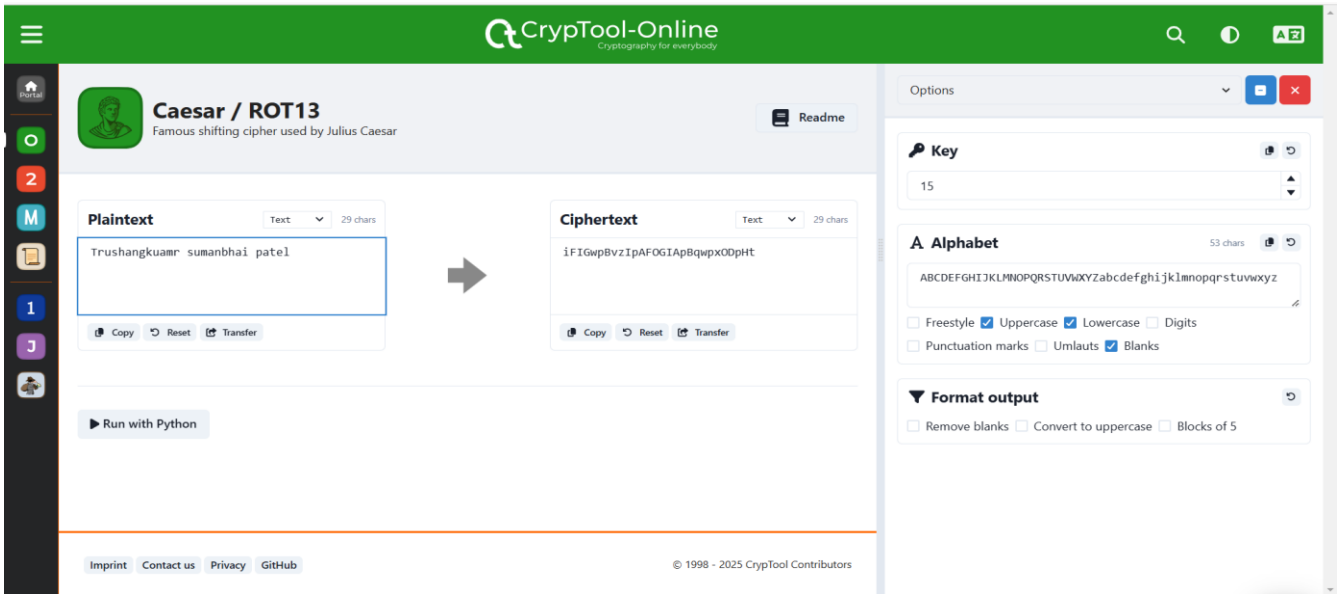

Figure 3:Encrypt the plain text using caser/Additive/shift cipher where k=15 with considering space

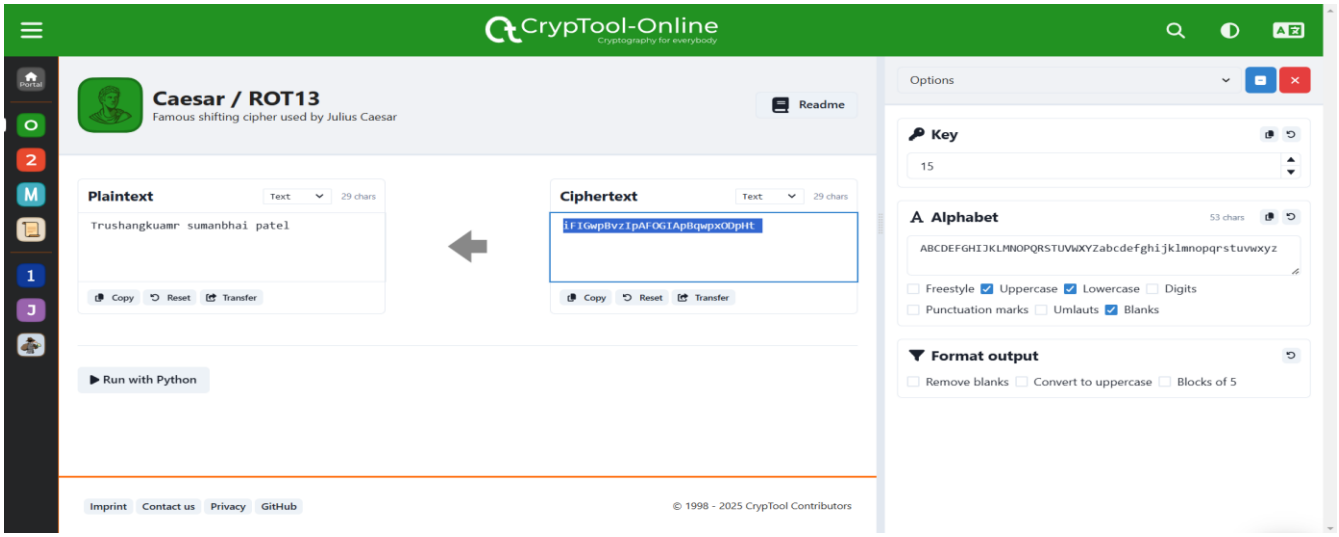

Figure 4:Decrypt the cipher text using caser/Additive/shift cipher where k=15 with considering space

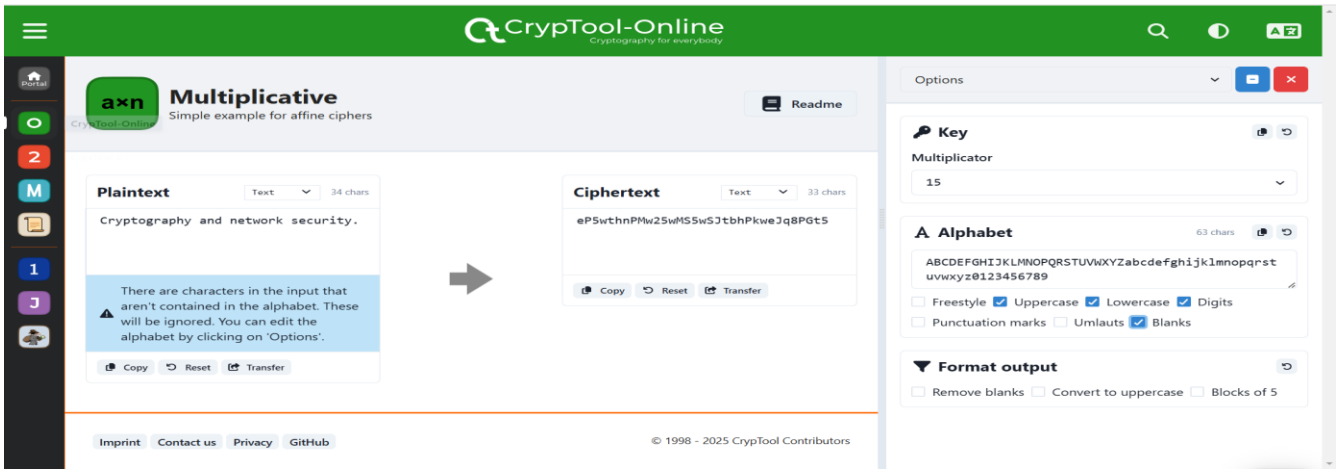

Figure 5:Encrypt message using Multiplicative cipher considering Uppercase and lowercase and key=15

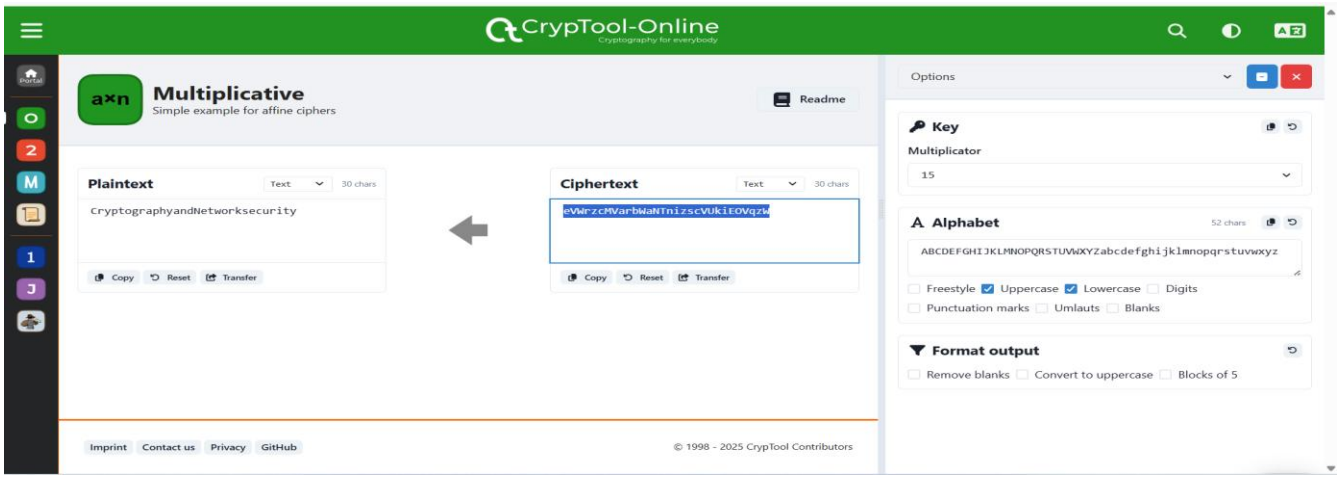

Figure 6:Decrypt message using Multiplicative cipher considering Uppercase and lowercase and key=15

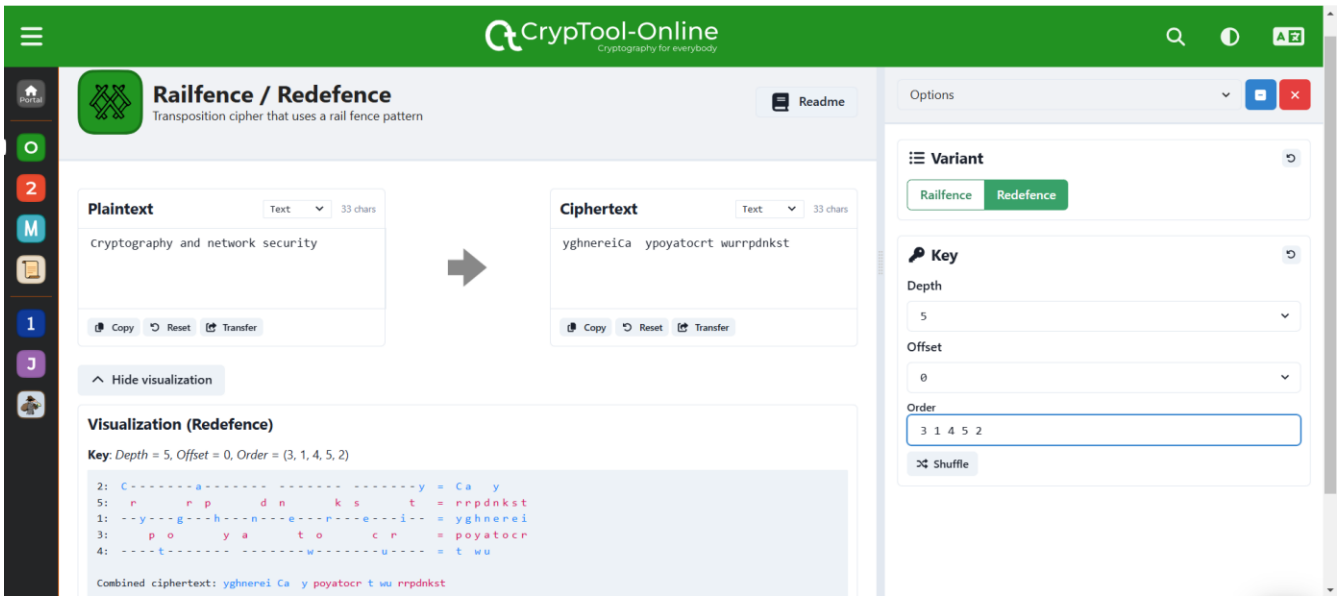

Figure 7:Encrypt the plaintext using key:34152 in transposition cipher

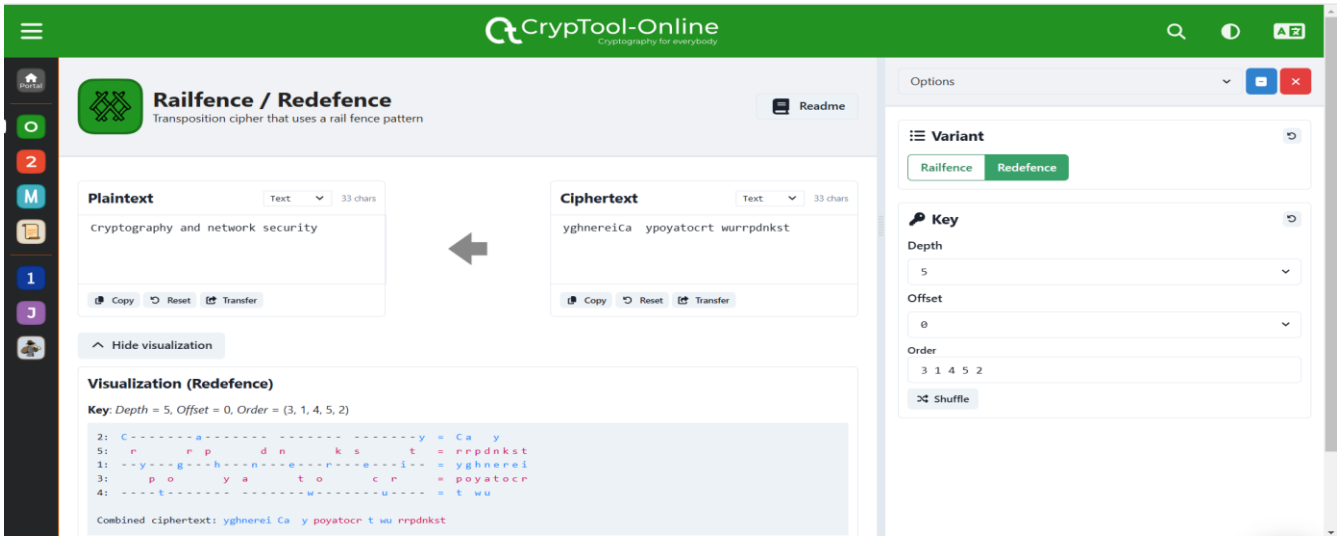

Figure 8:Decrtpt the Ciphertext using key:25134 in transposition cipher

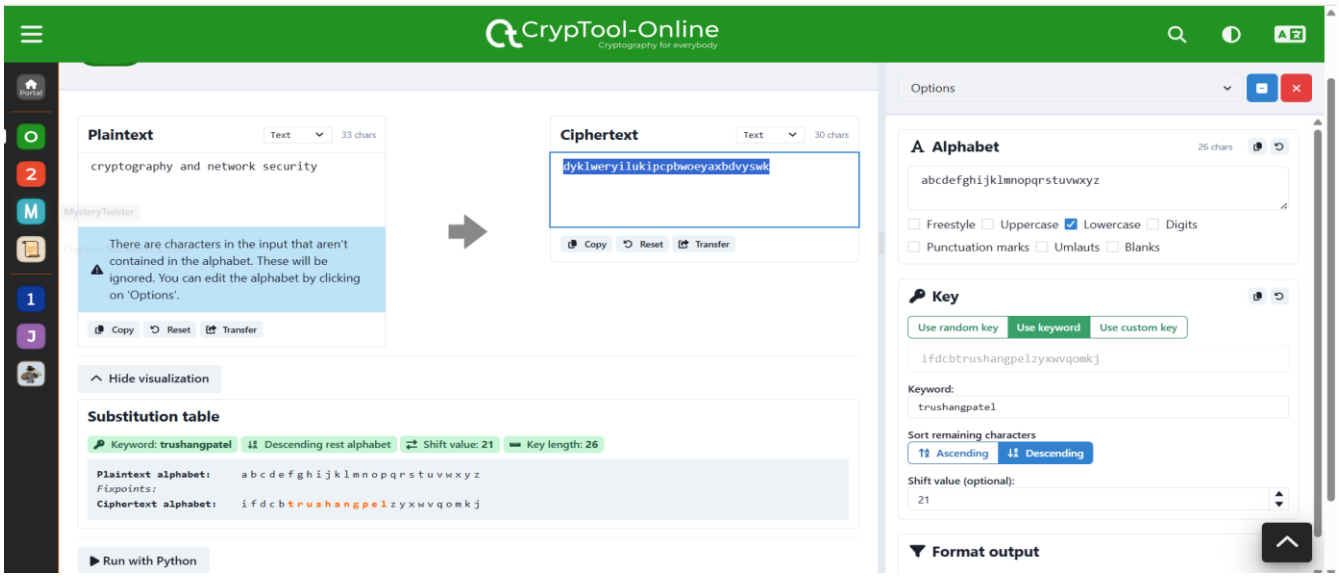

Figure 9:Encrypt the message using Monoalphabetic and key= trushangpatel

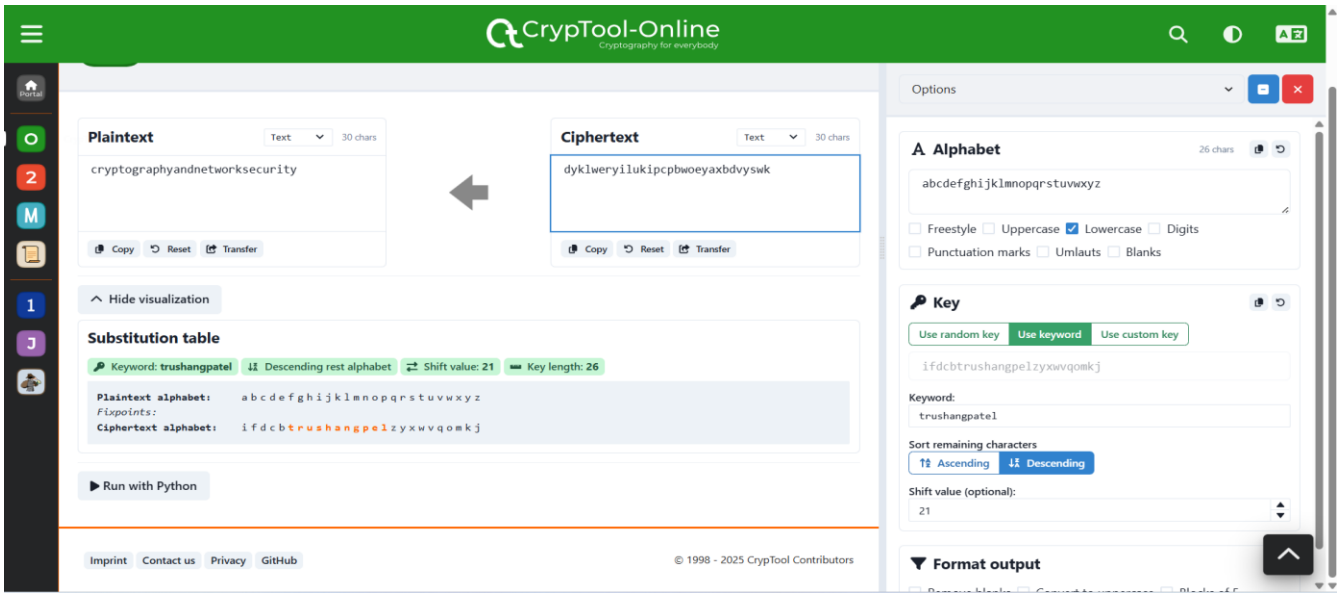

Figure 10:Decrypt the message using Monoalphabetic and key= trushangpatel

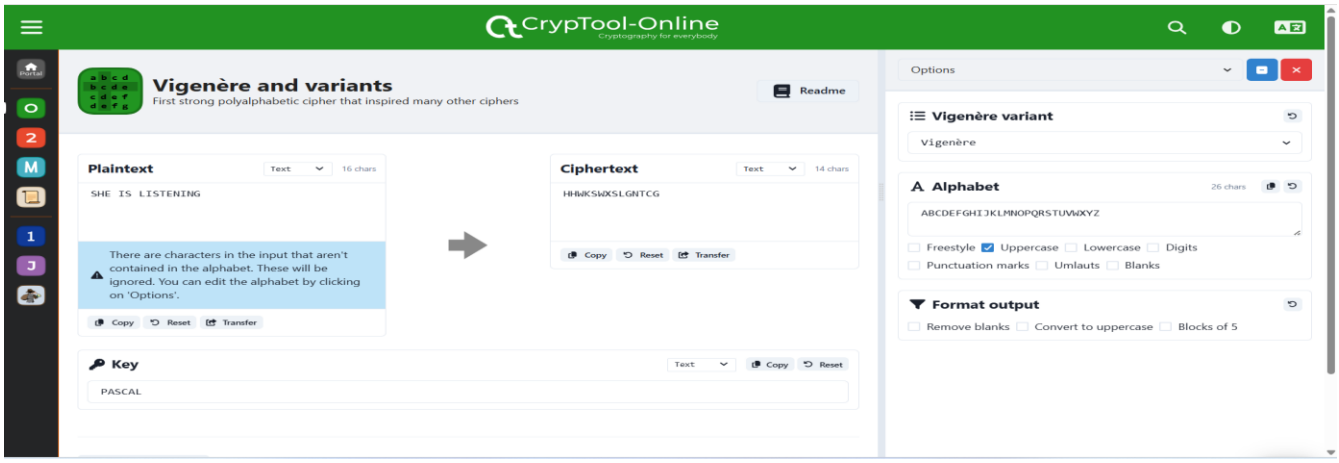

Figure 11:Encryption the message using Vigenère with key=PASCAL

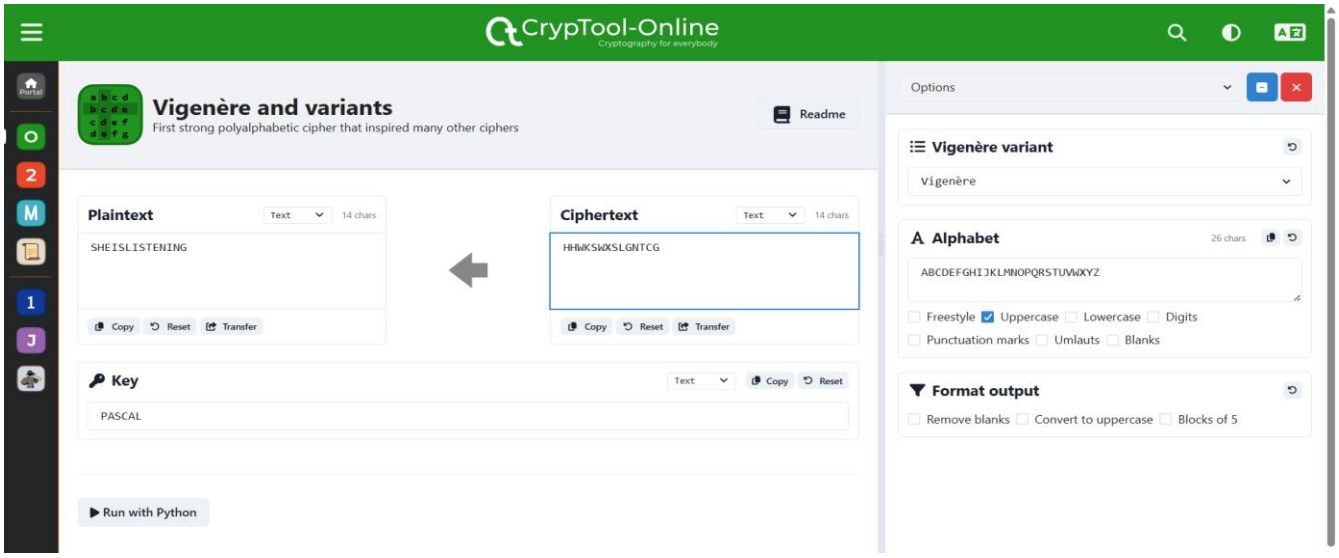

Figure 12: Decryption the message using Vigenère with key=PASCAL

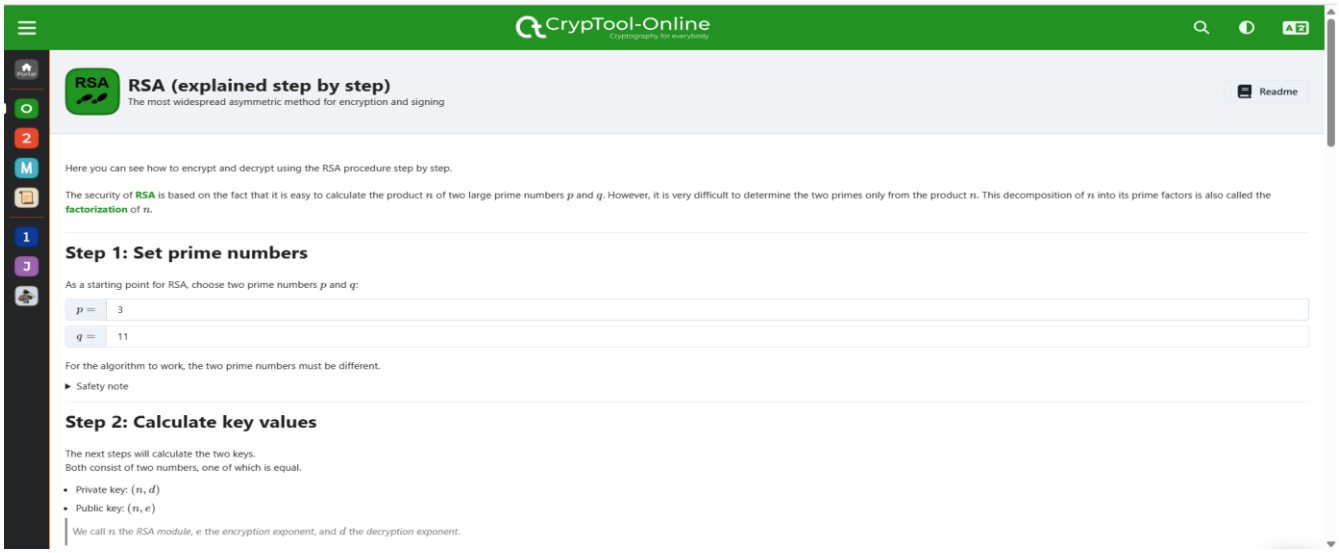

Figure 13:Pick two prime number

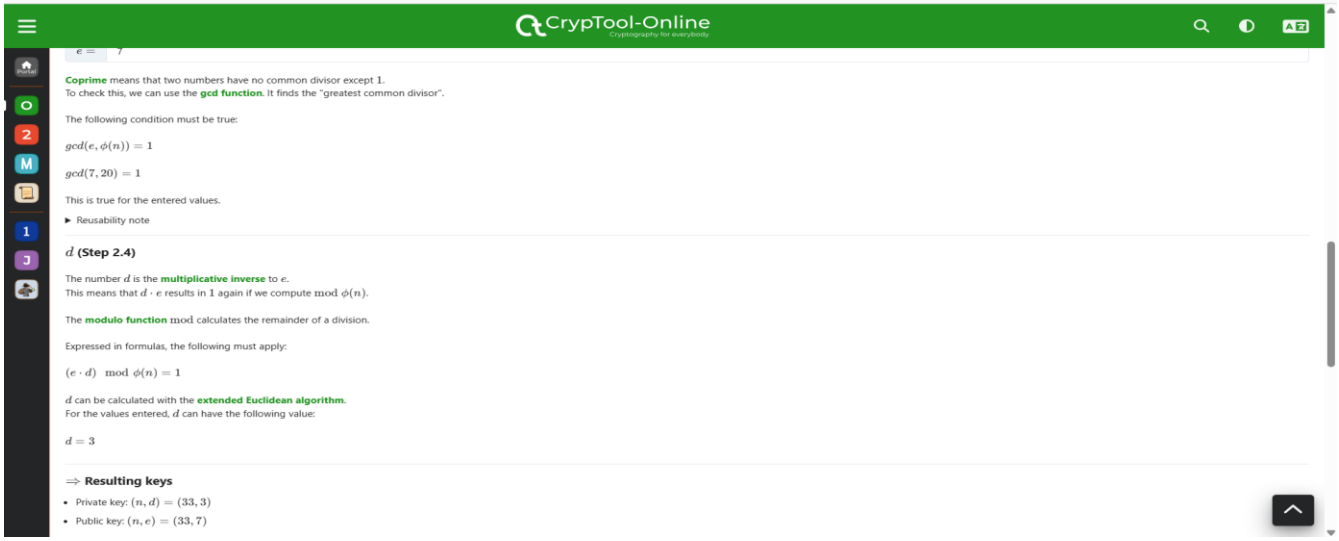

Figure 14:Generate the keys

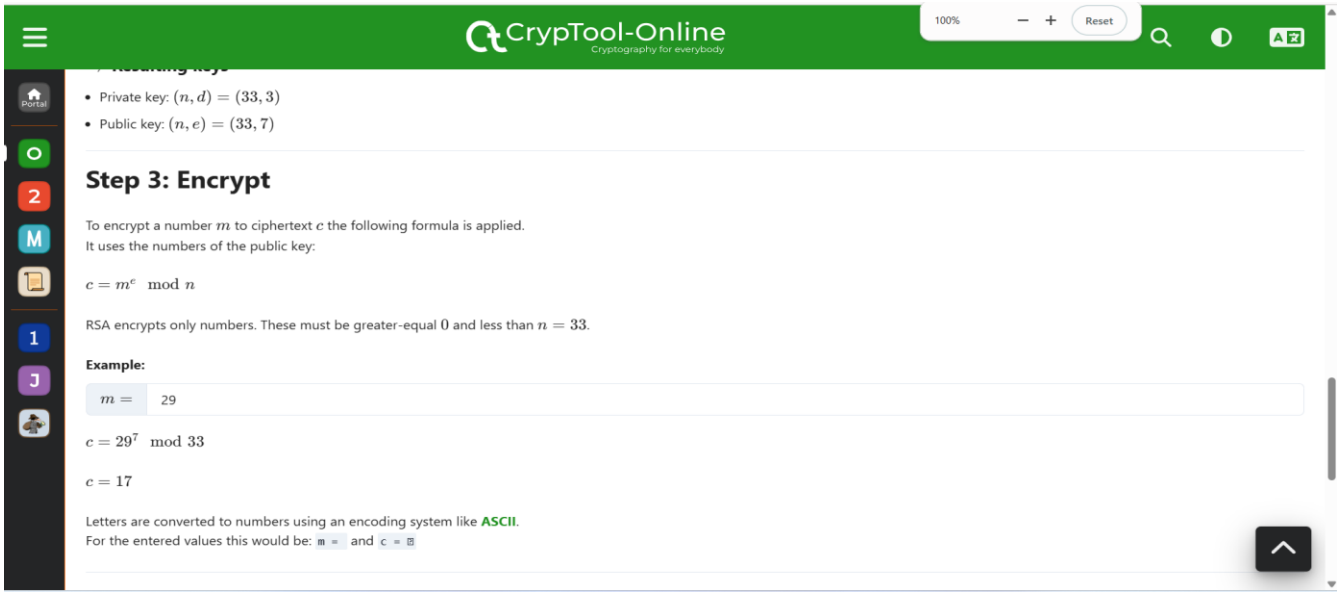

Figure 15:Encrypt the message

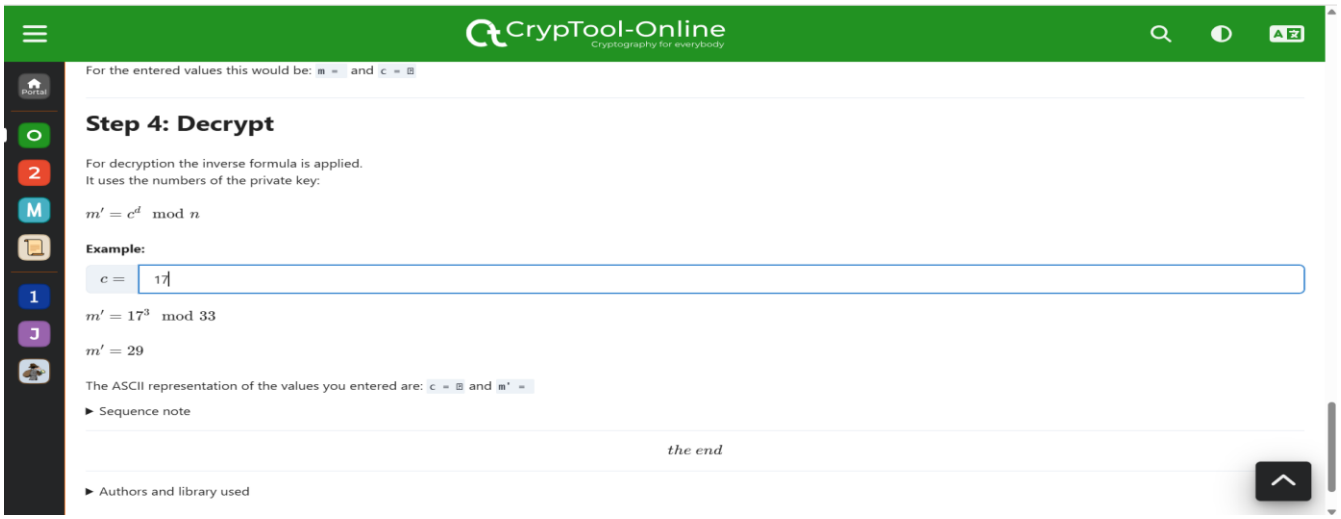

Figure 16:Decrypt the message

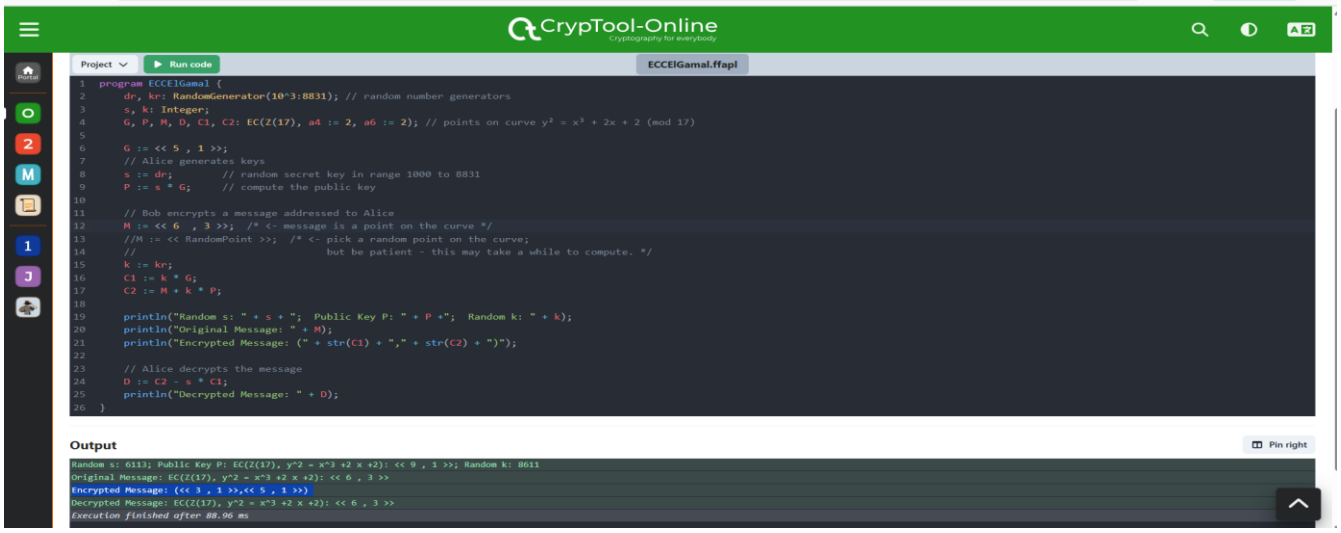

Figure 17:Use of Elgamal Cryptosystem

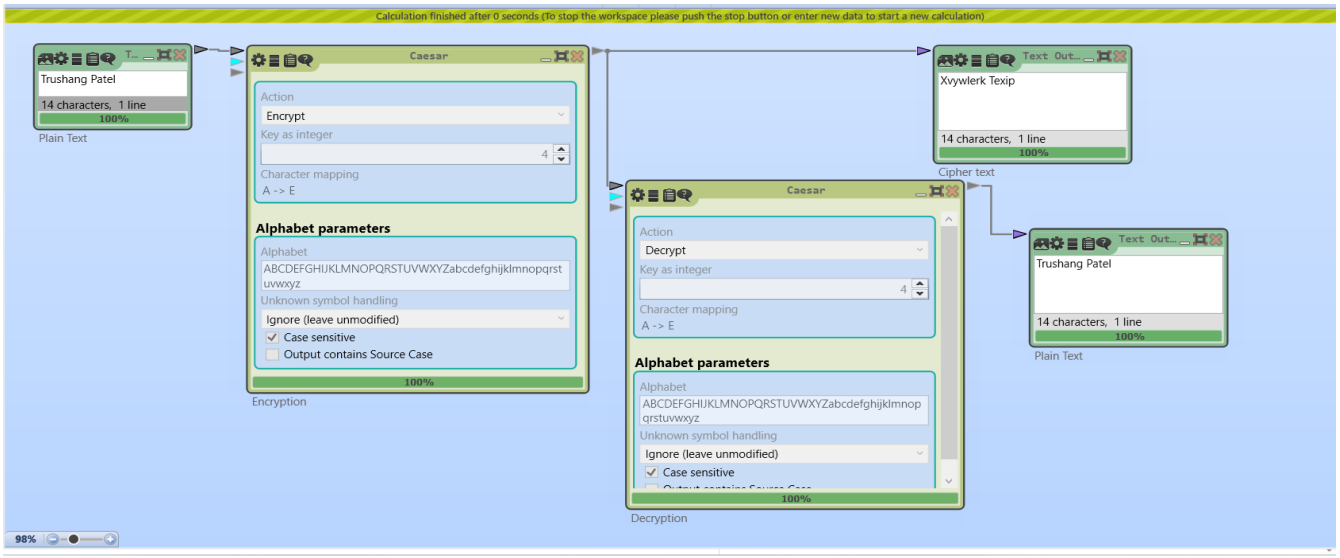

Figure 18:Encrypt and Decrypt the message using Caesar

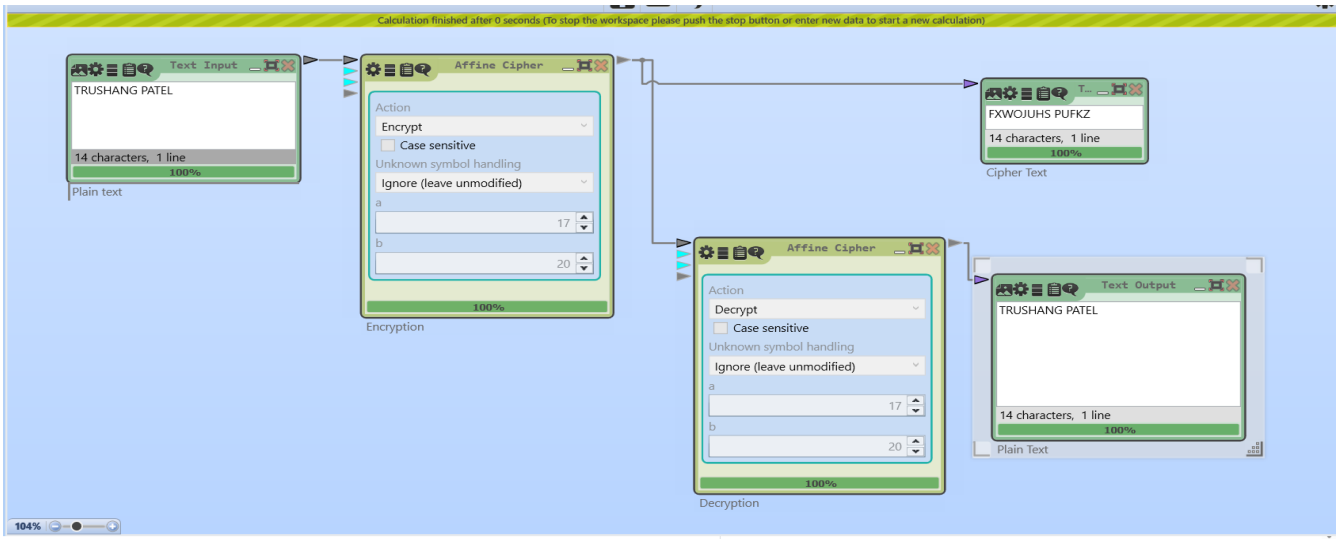

Figure 19:Encrypt and Decrypt the message using Affine Cipher

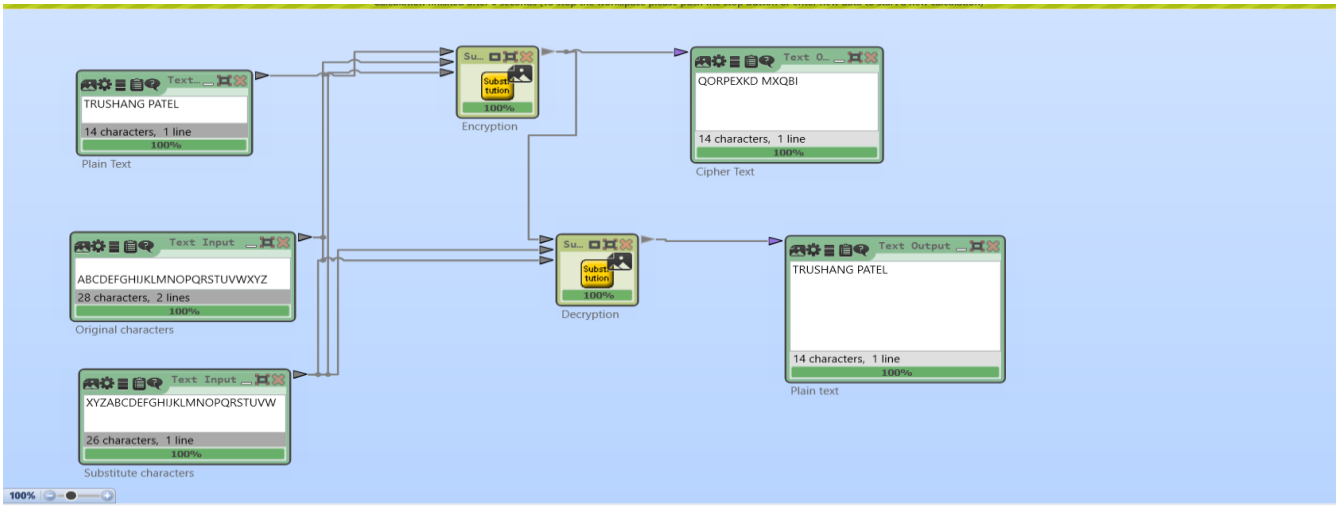

Figure 20:Encryption and decryption using substitution

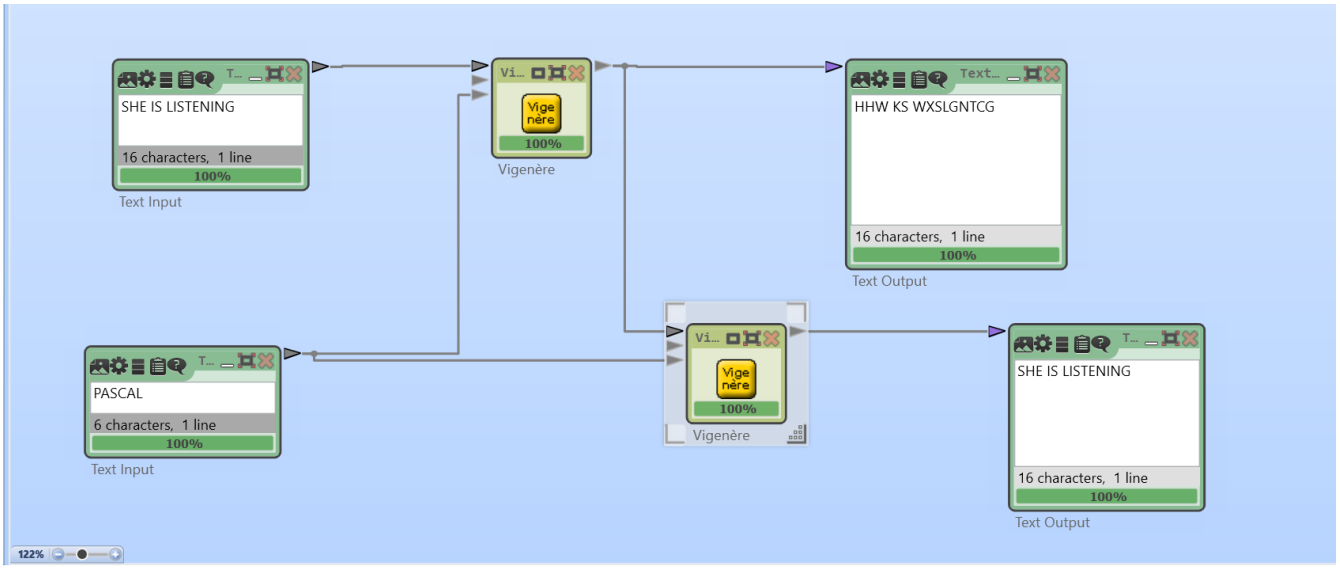

Figure 21:Encryption and Decryption using Vigenère cipher

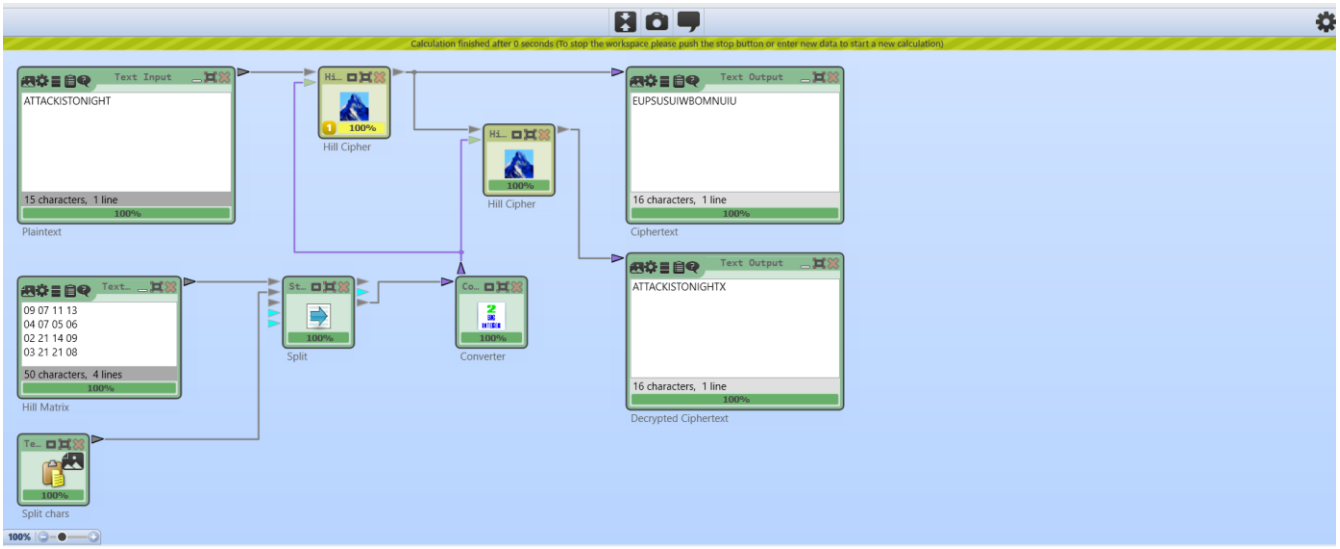

Figure 22:Encryption and Decryption using Hill cipher where=ATTACKISTONIGHT

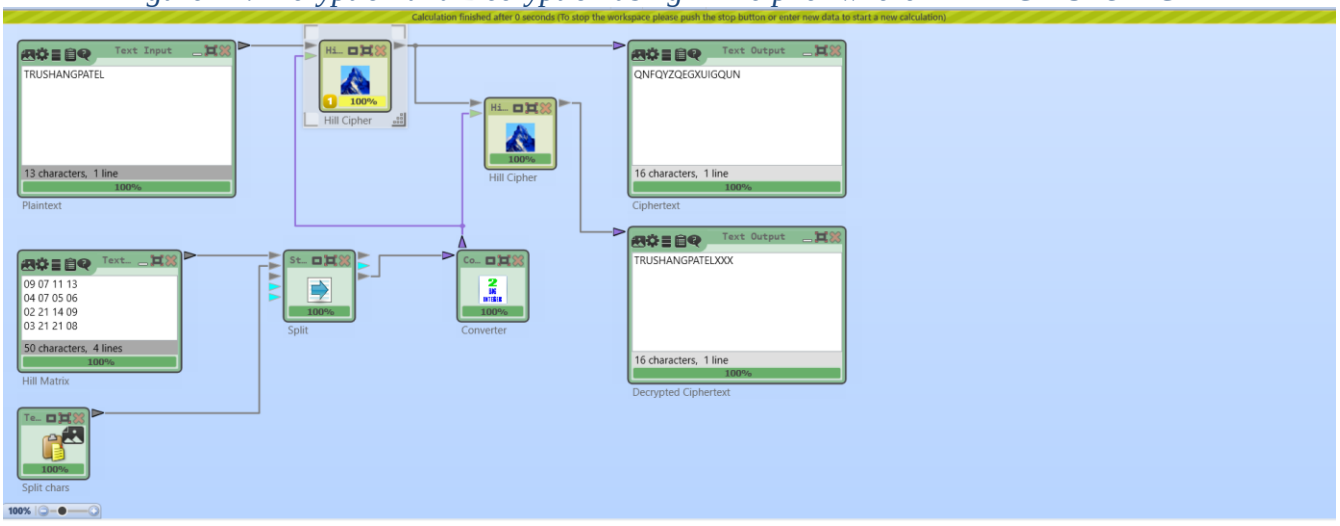

Figure 23:Encryption and Decryption using Hill cipher where plaintext = TRUSHANGPATEL

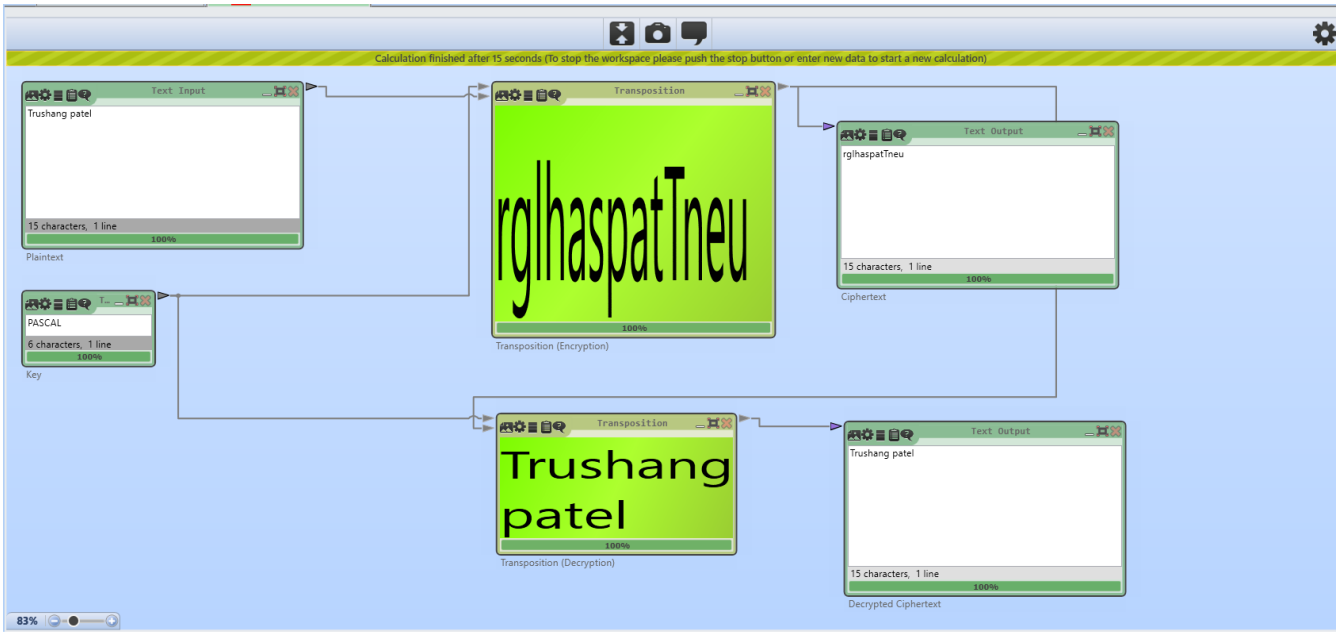

Figure 24:Encryption and Decryption using transposition cipher where plaintext = Trushang patel

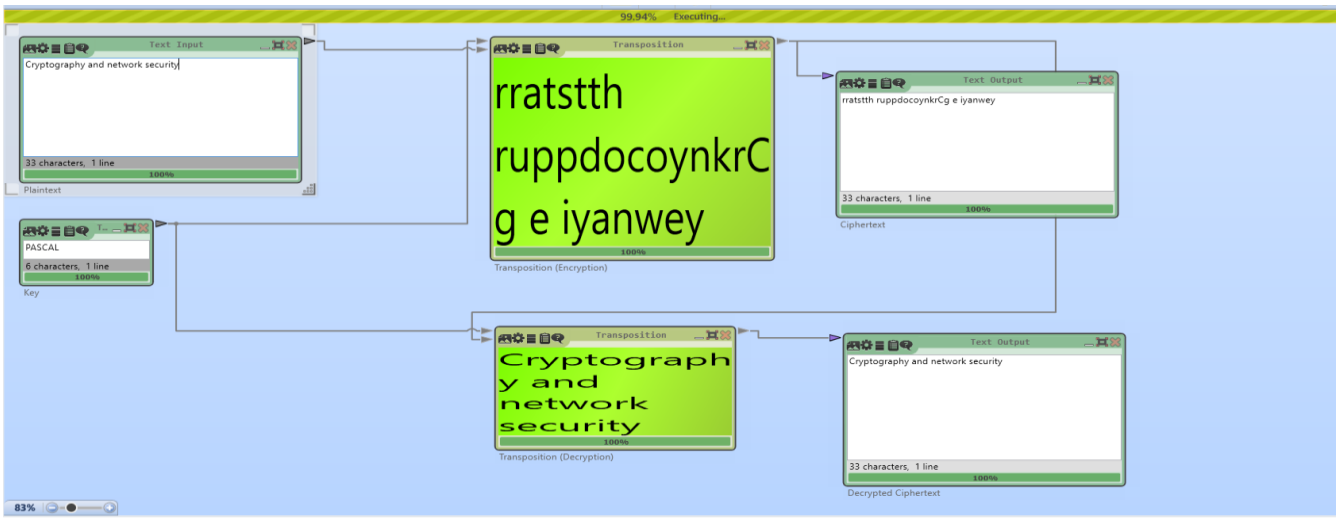

Figure 25Encryption and Decryption using transposition cipher where key = PASCAL

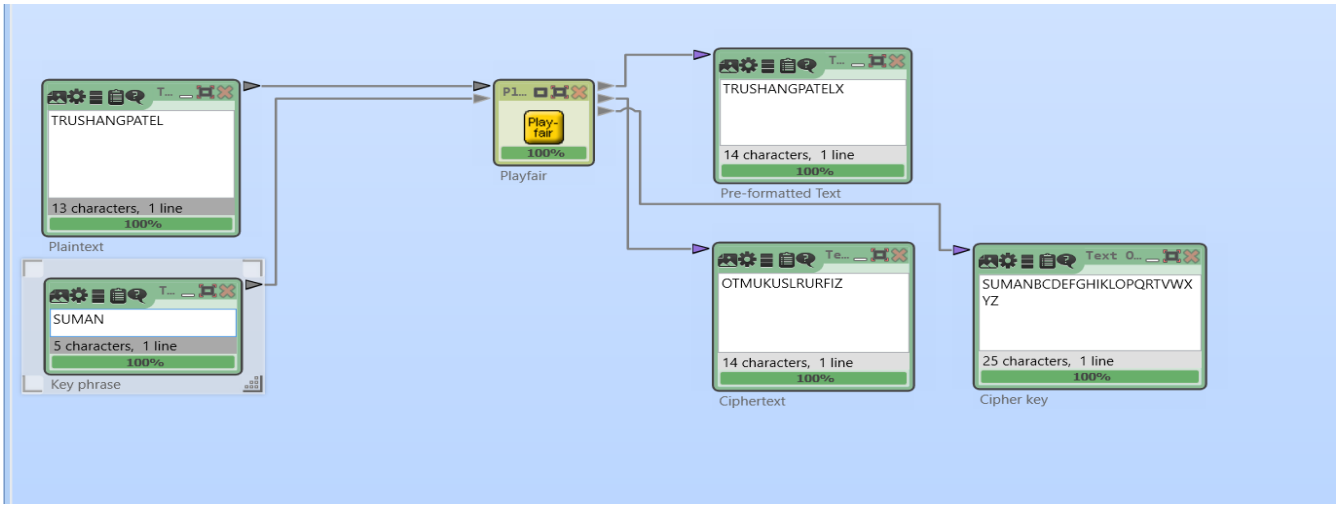

Figure 26:Example of Playfair where key = SUMAN

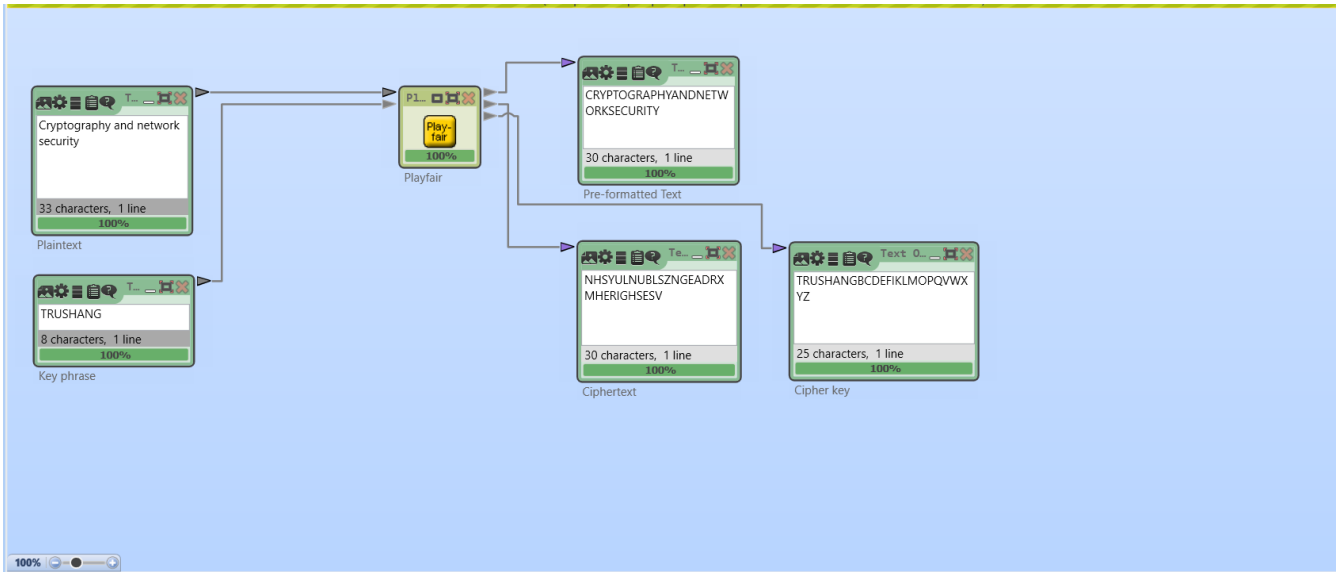

Figure 27:Exmaple of Playfair where key=TRUSHANG

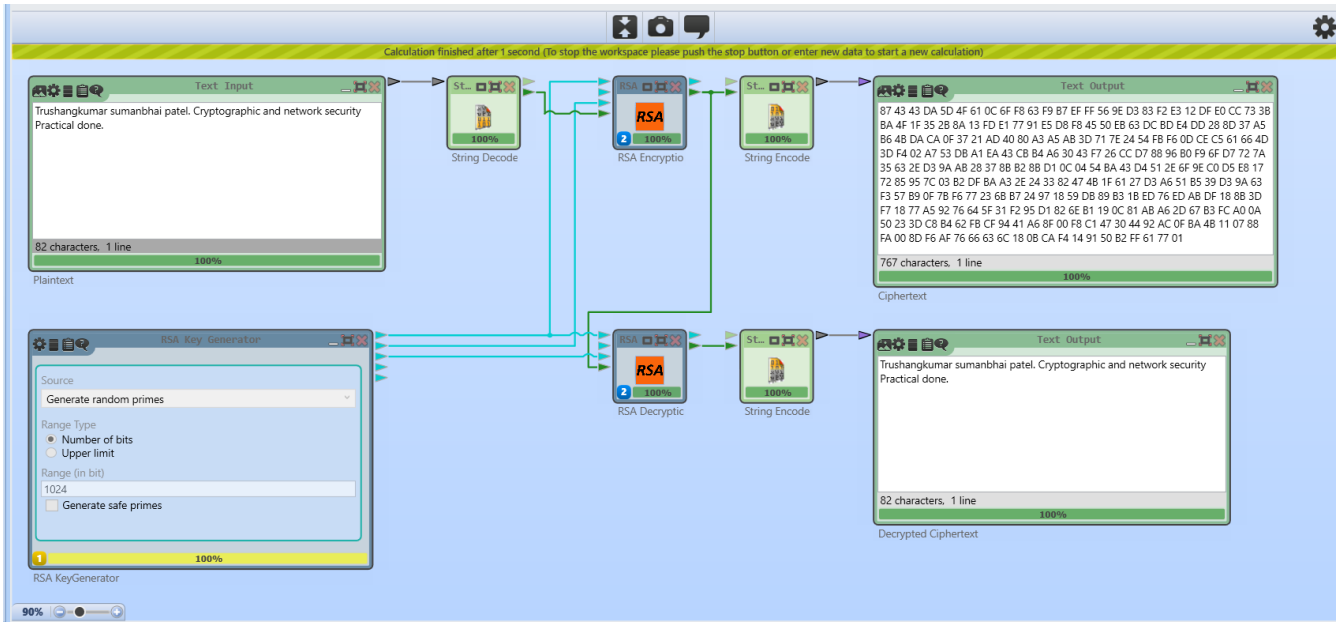

Figure 28:Encryption and Decryption using RSA algorithm

Figure 29:Plaintext of JavaCrypTool practical

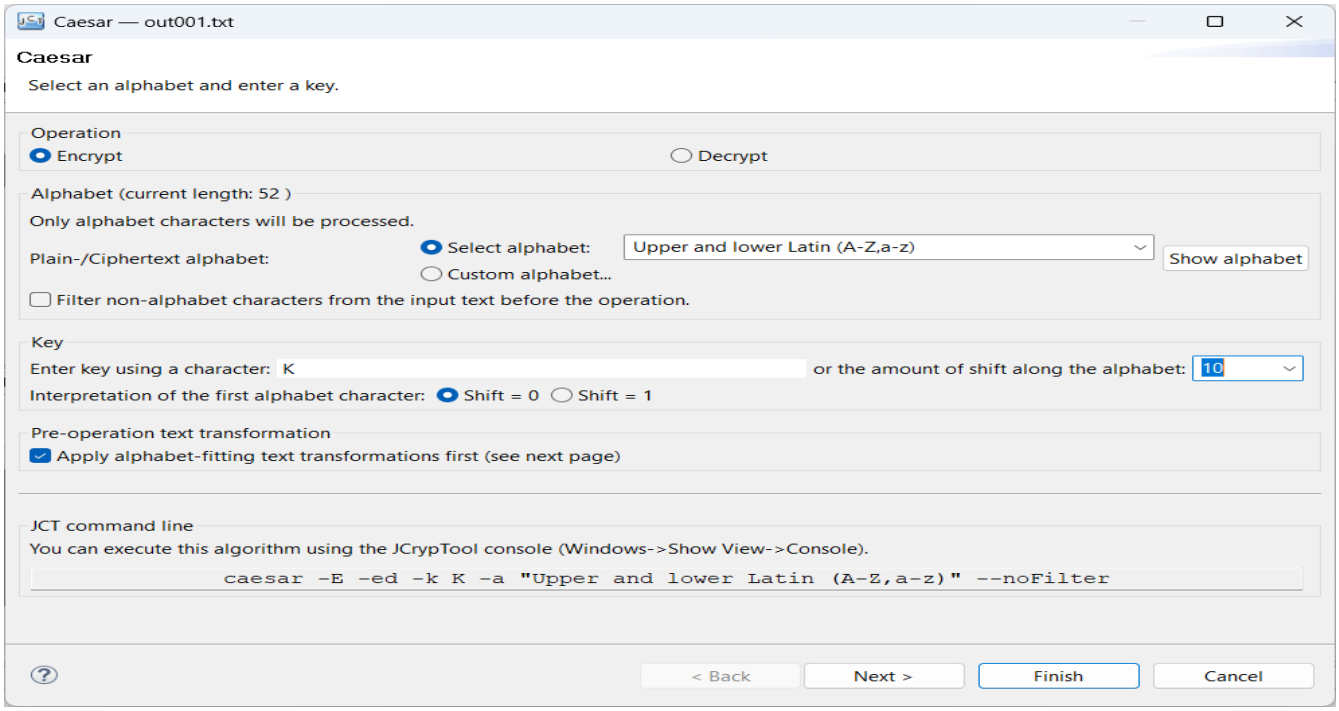

Figure 30:Encrypt Using Caser cipher

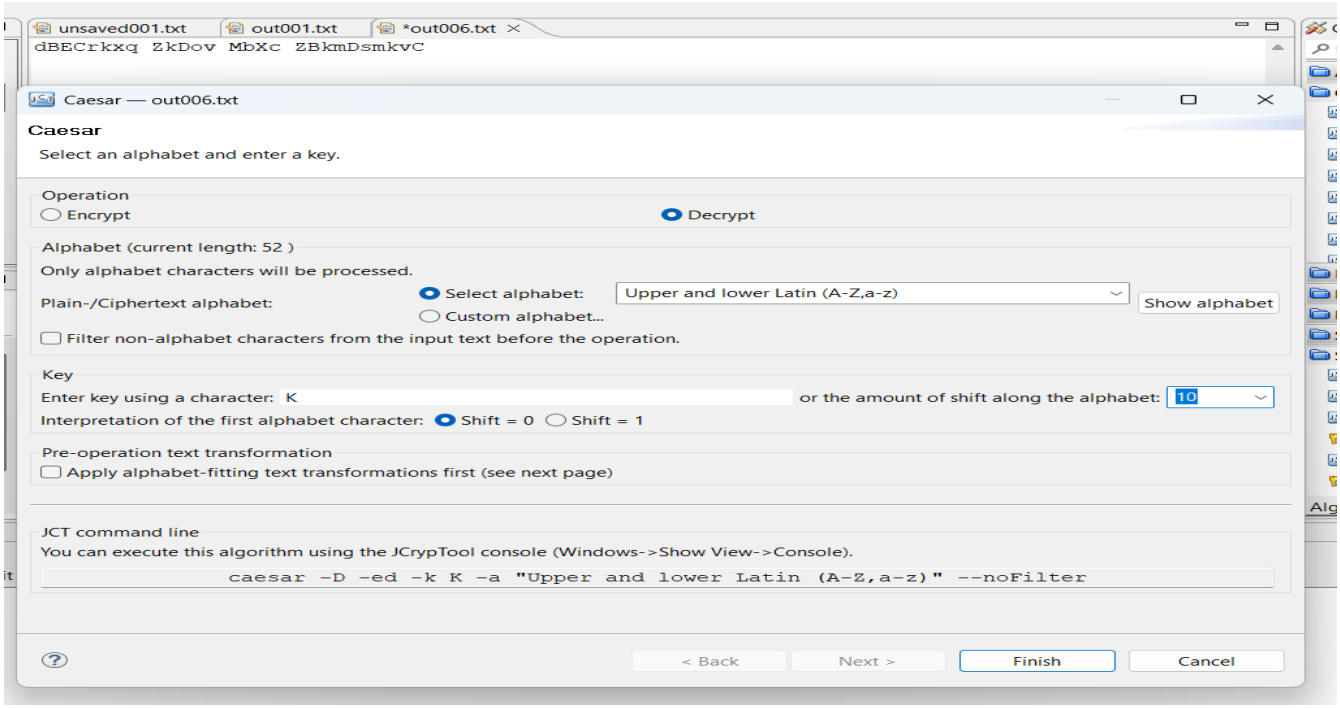

Figure 31:Decrypt using caser cipher

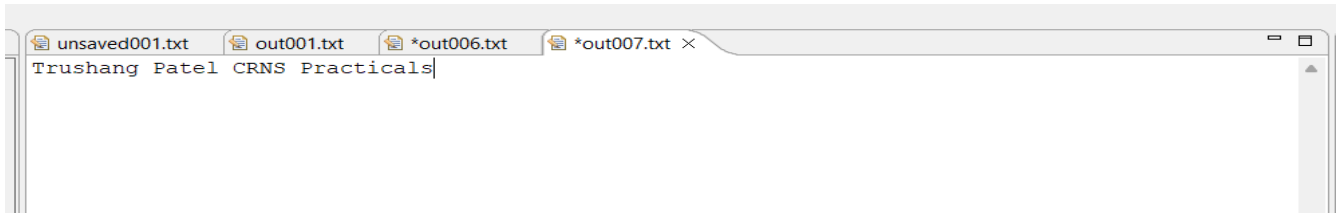

Figure 32:After Decrypting output

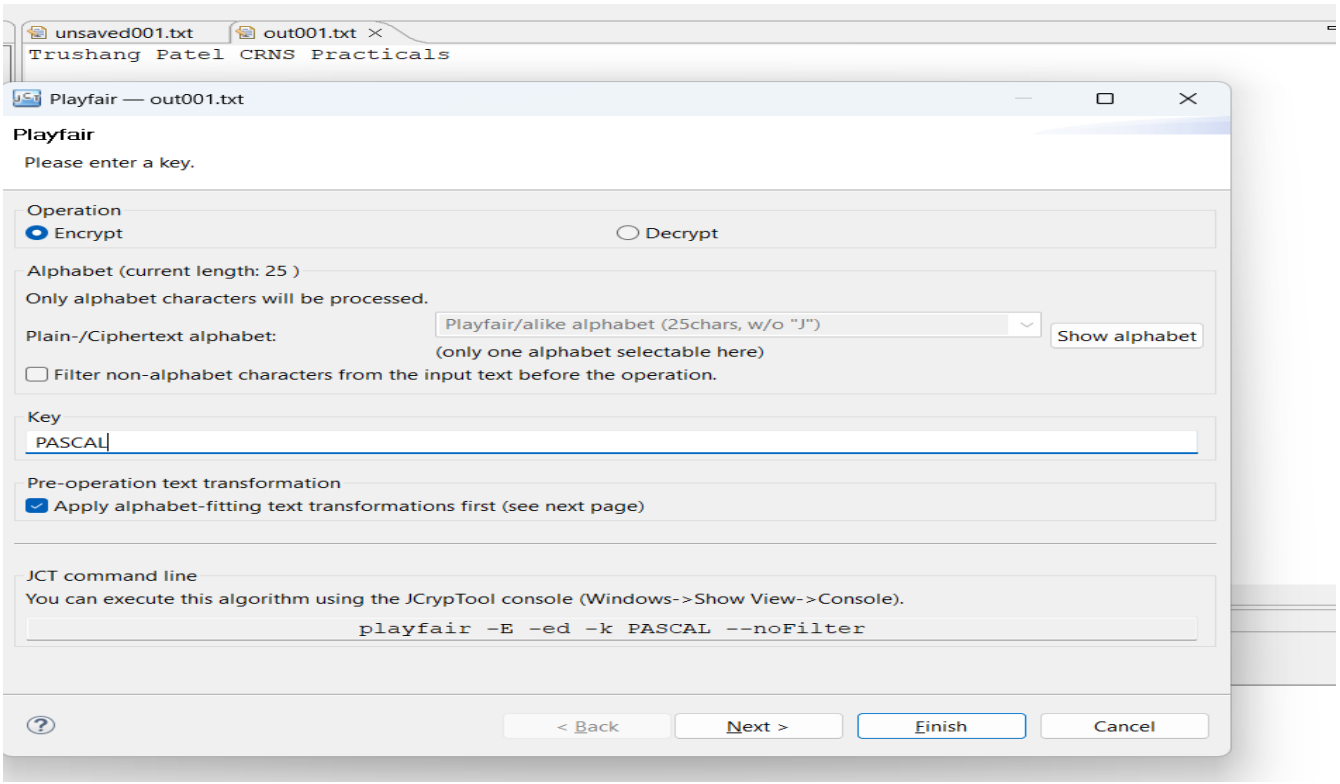

Figure 33:Encrypt using Playfair cipher

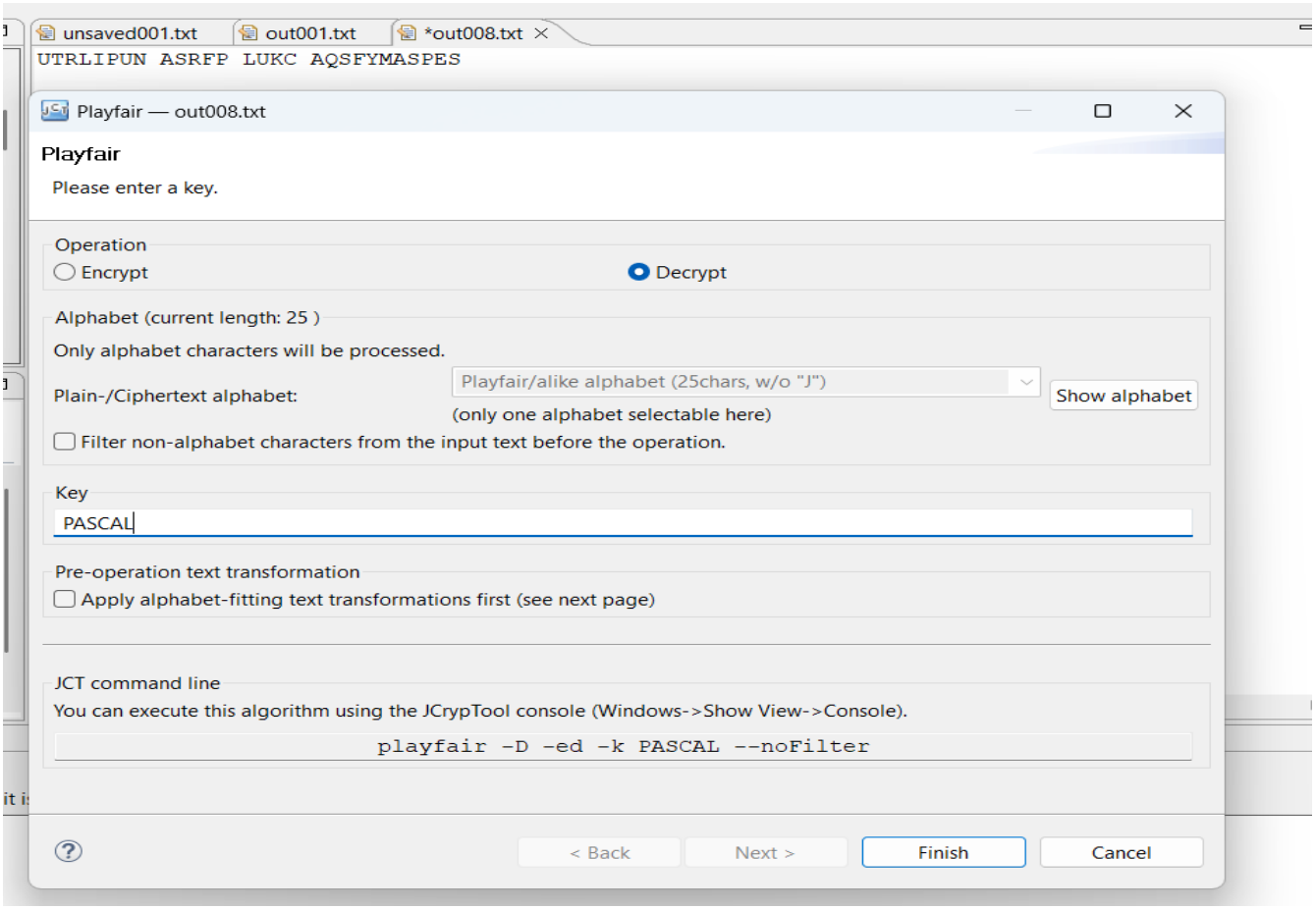

Figure 34:Decrypt using Playfair cipher

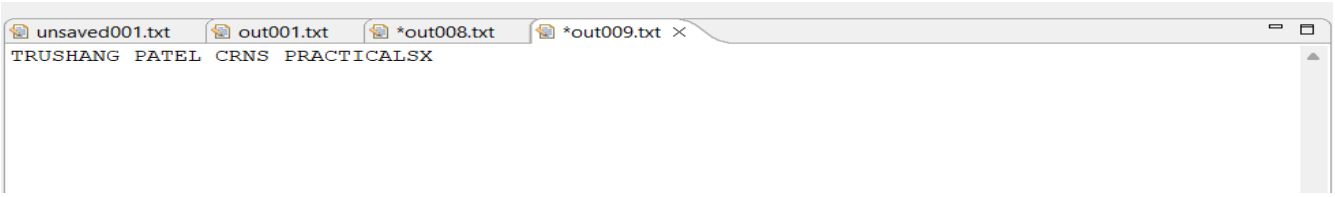

Figure 35:Output of Playfair cipher

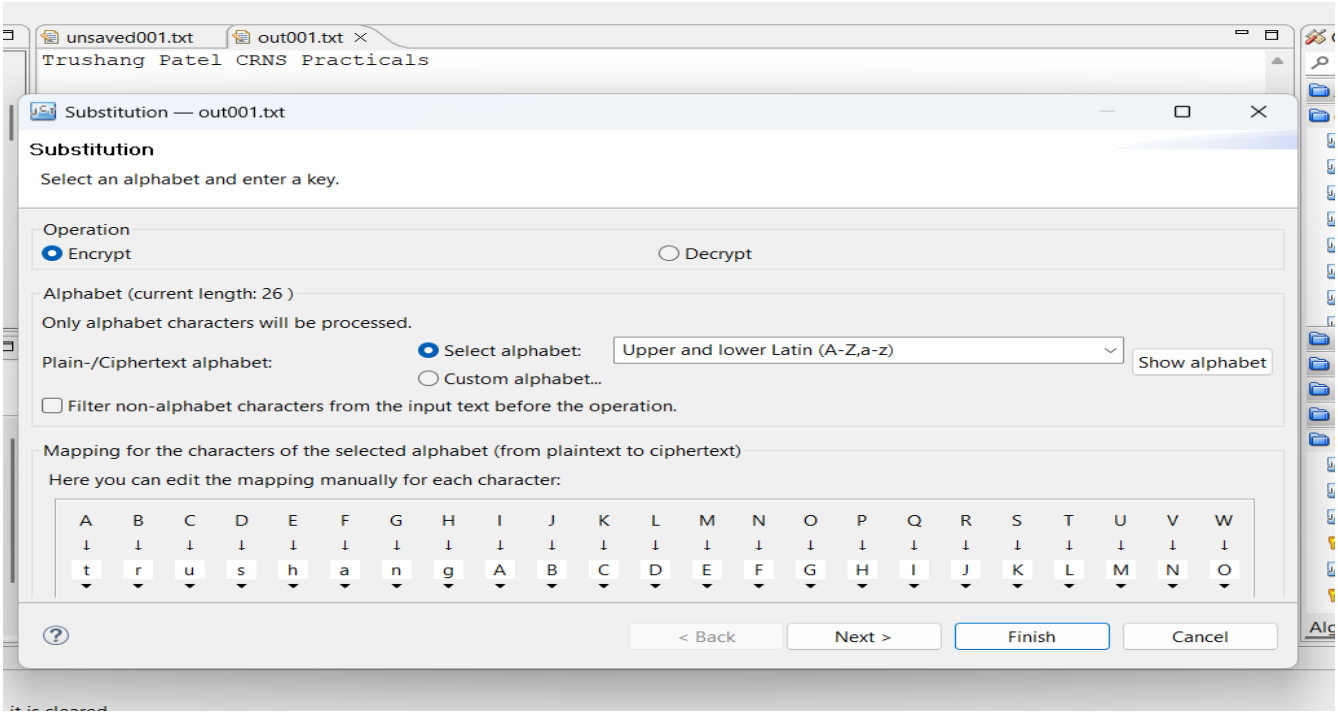

Figure 36:Encryption using substitution cipher

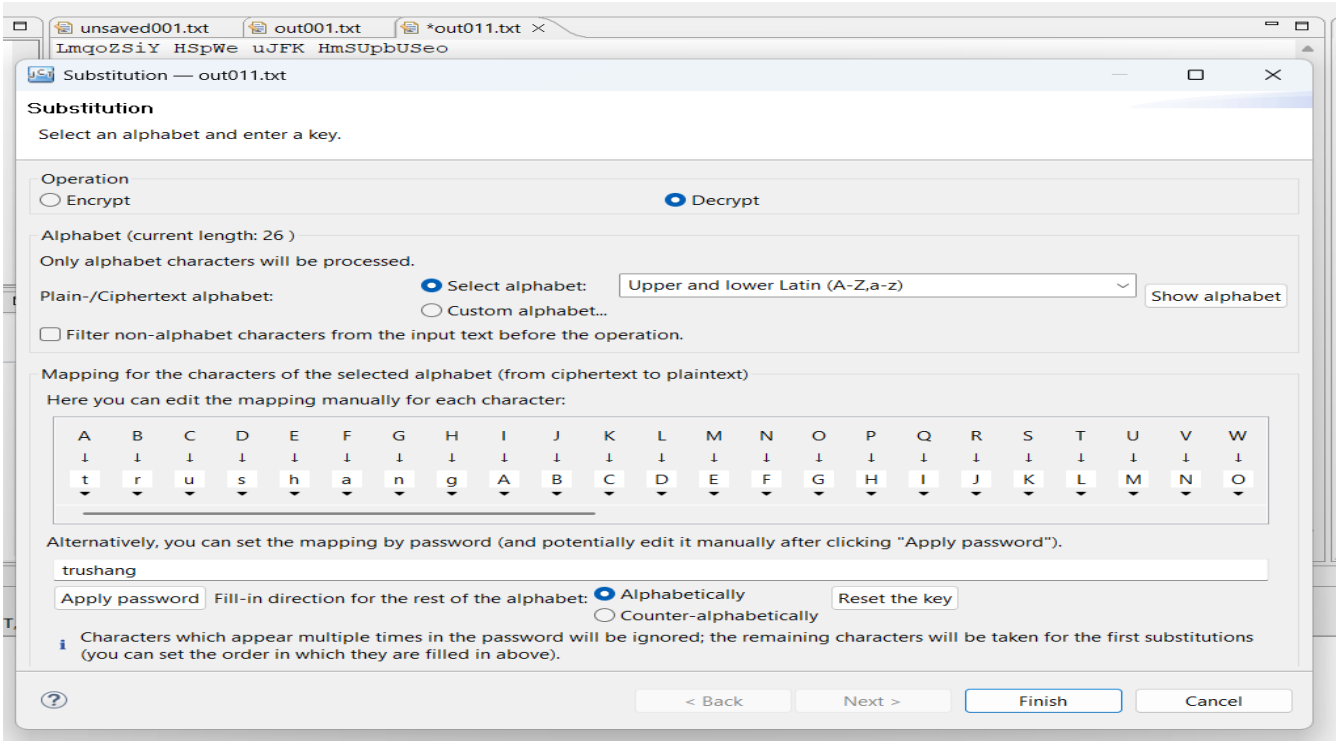

Figure 37:Decrypt using Substitution cipher

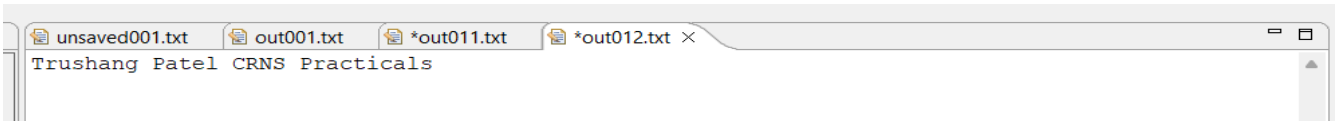

Figure 38: Output of the Substitution

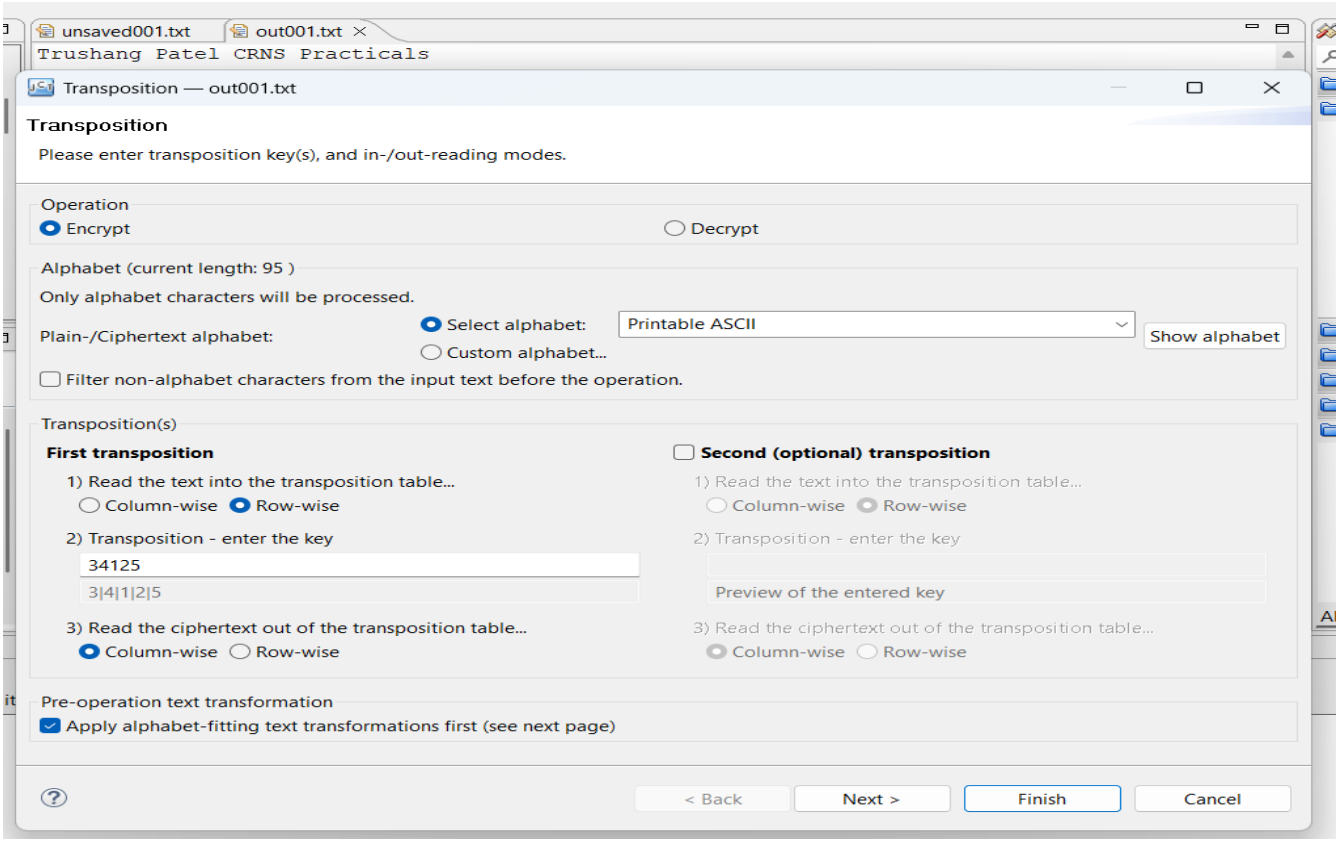

Figure 39: Encryption using Transposition cipher

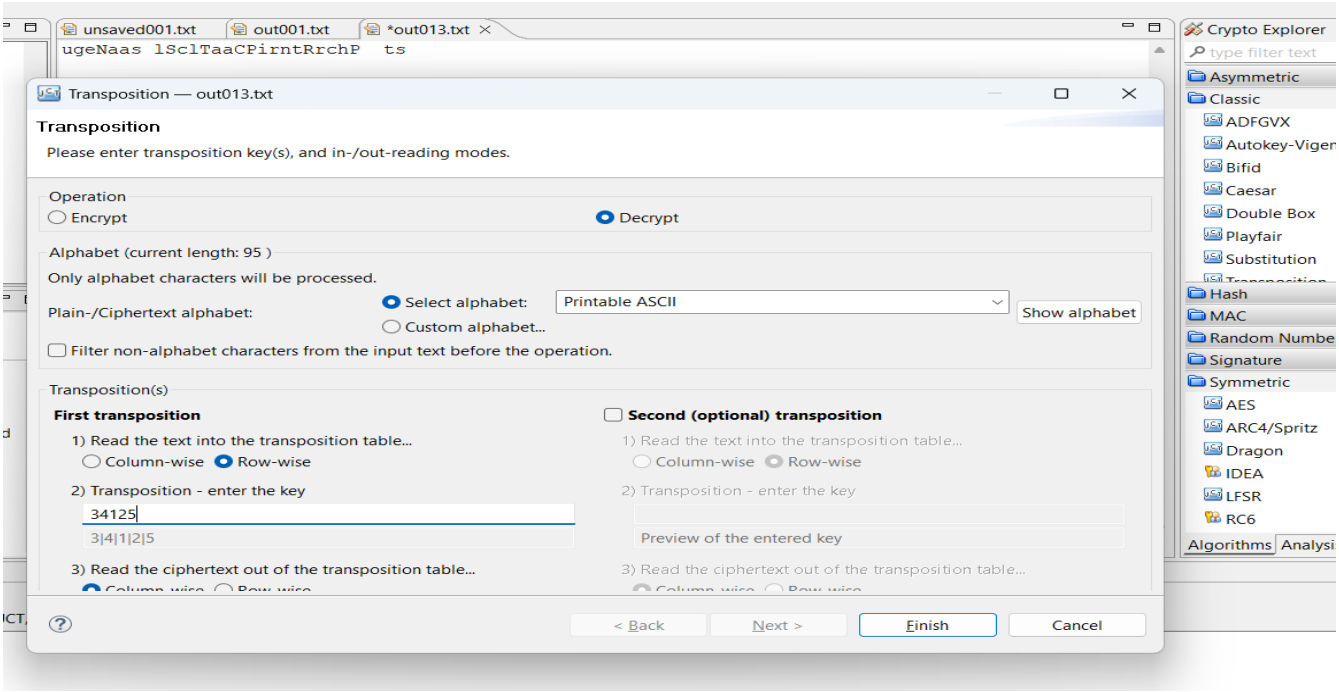

Figure 40:Decryption using Transposition cipher

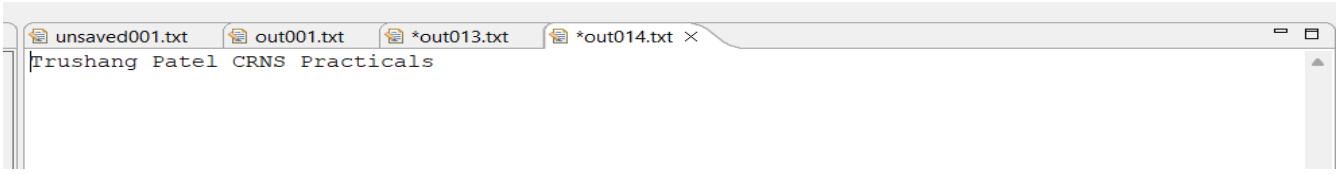

Figure 41:Output of the transposition cipher

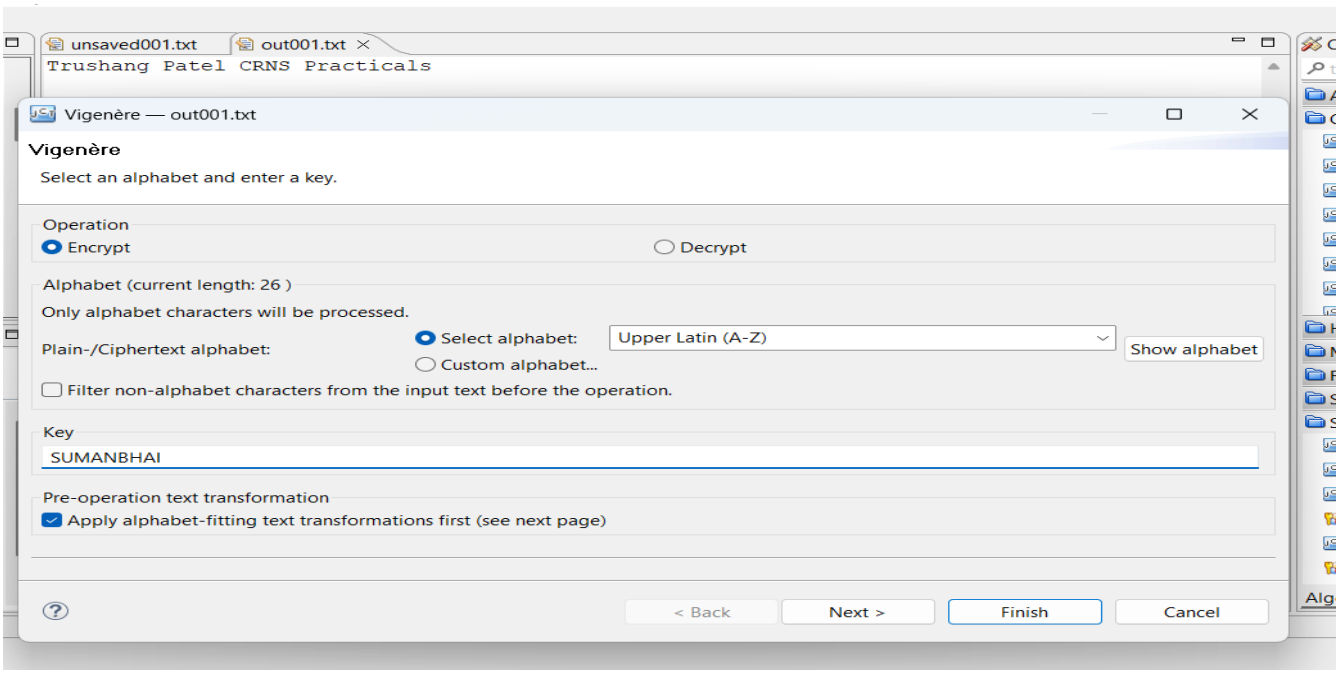

Figure 42:Encryption using Vigenère cipher

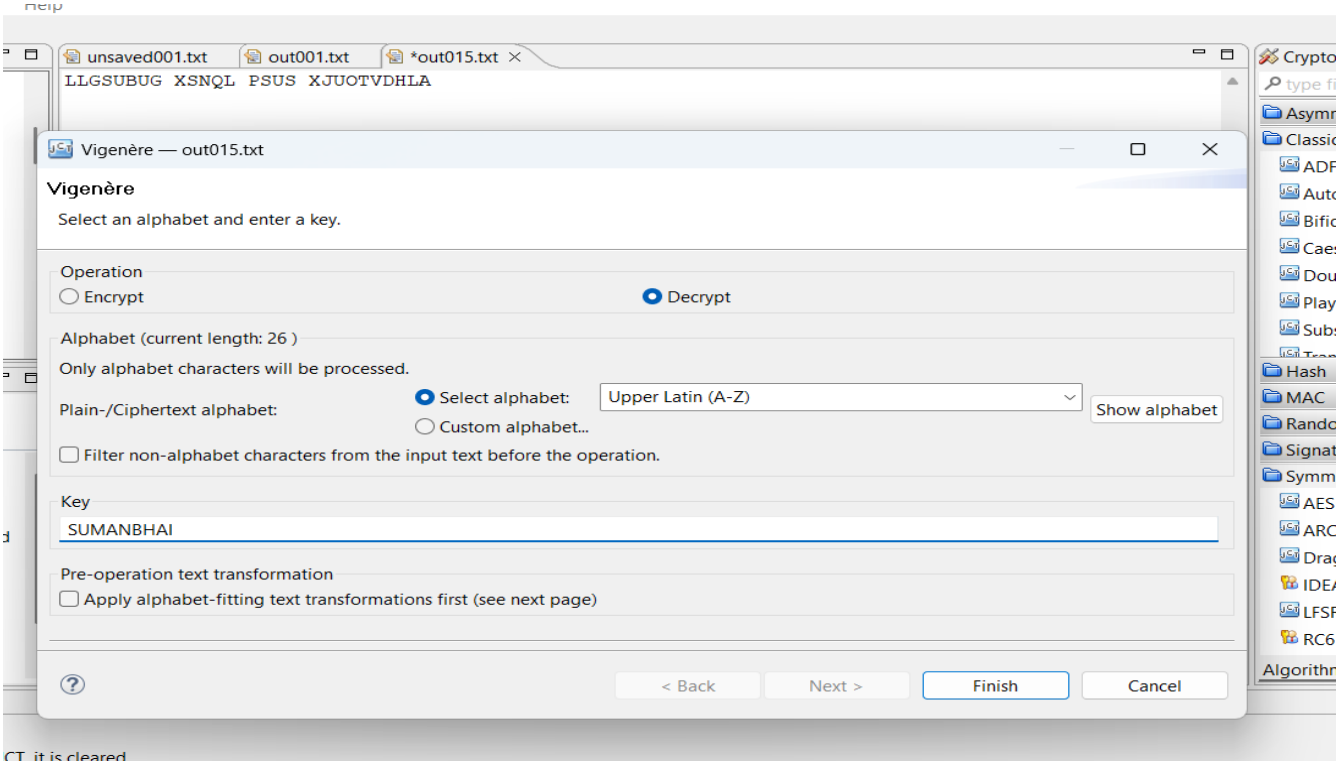

Figure 43:Decryption using Vigenère cipher

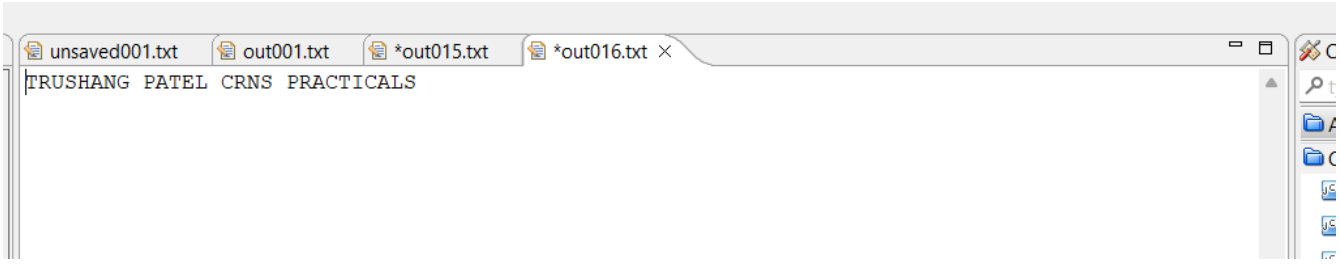

Figure 44:Output of Vigenère cipher

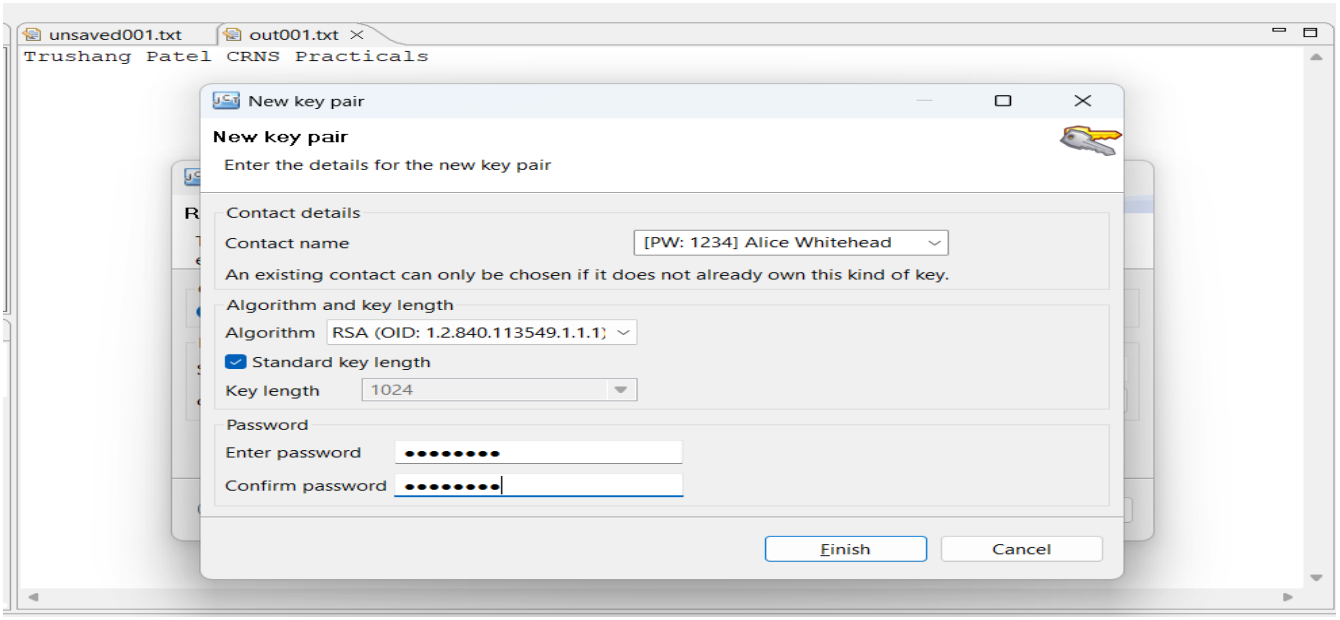

Figure 45:Generate key for RSA

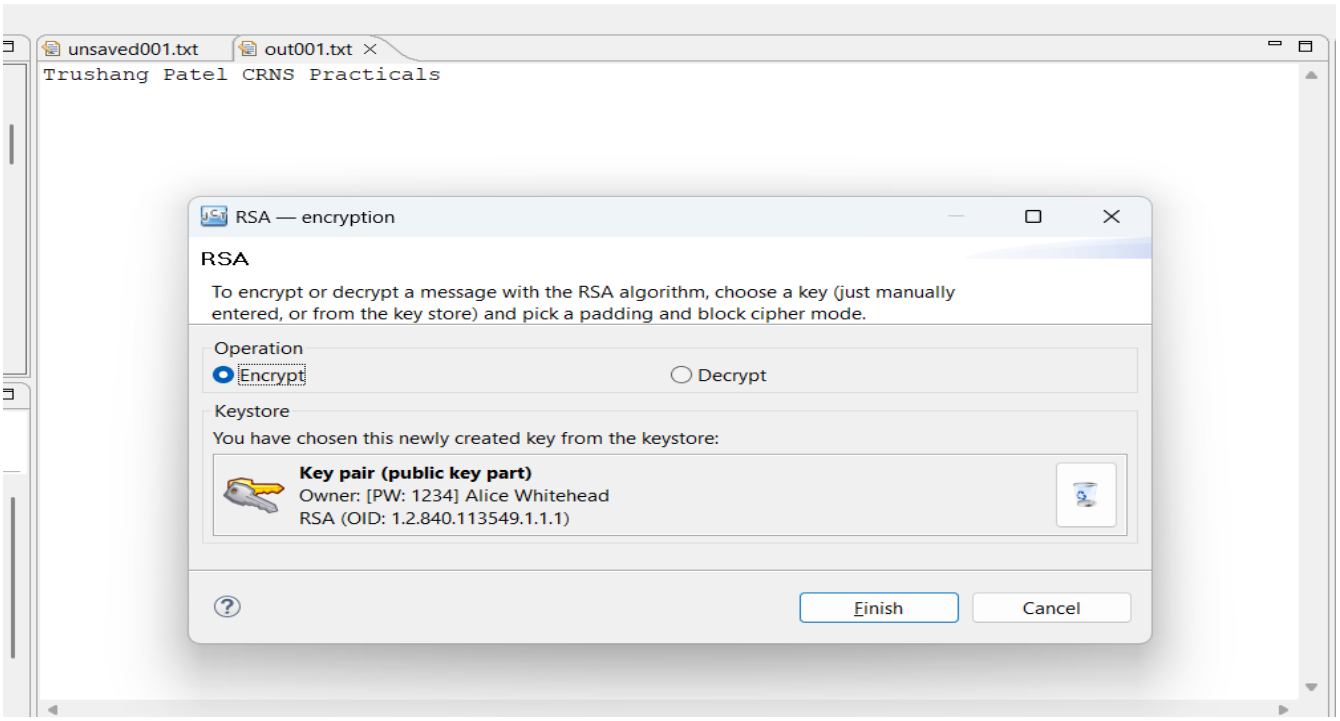

Figure 46:Encryption using RSA

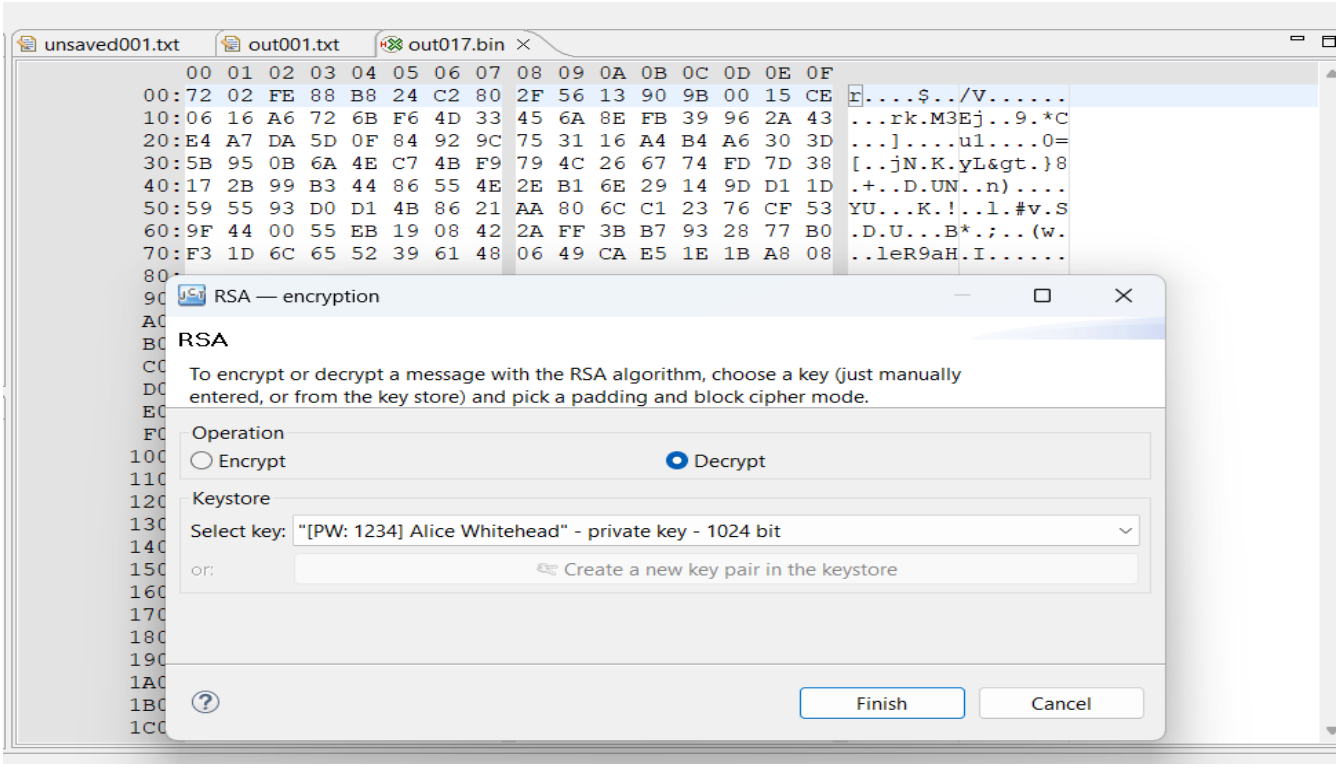

Figure 47:Decryption of the RSA

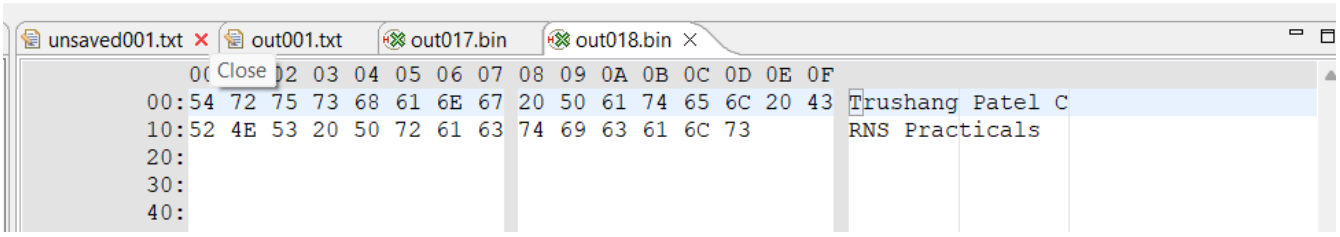

Figure 48:Output of the RSA

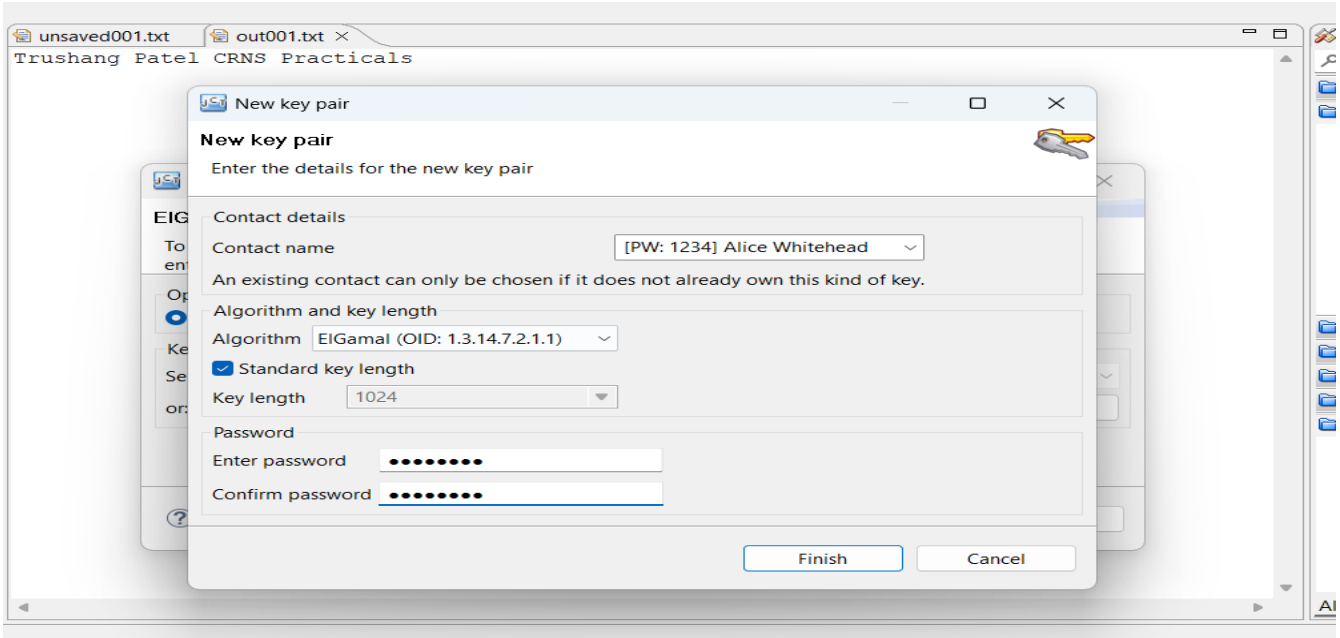

Figure 49:Key Generation using ElGamal

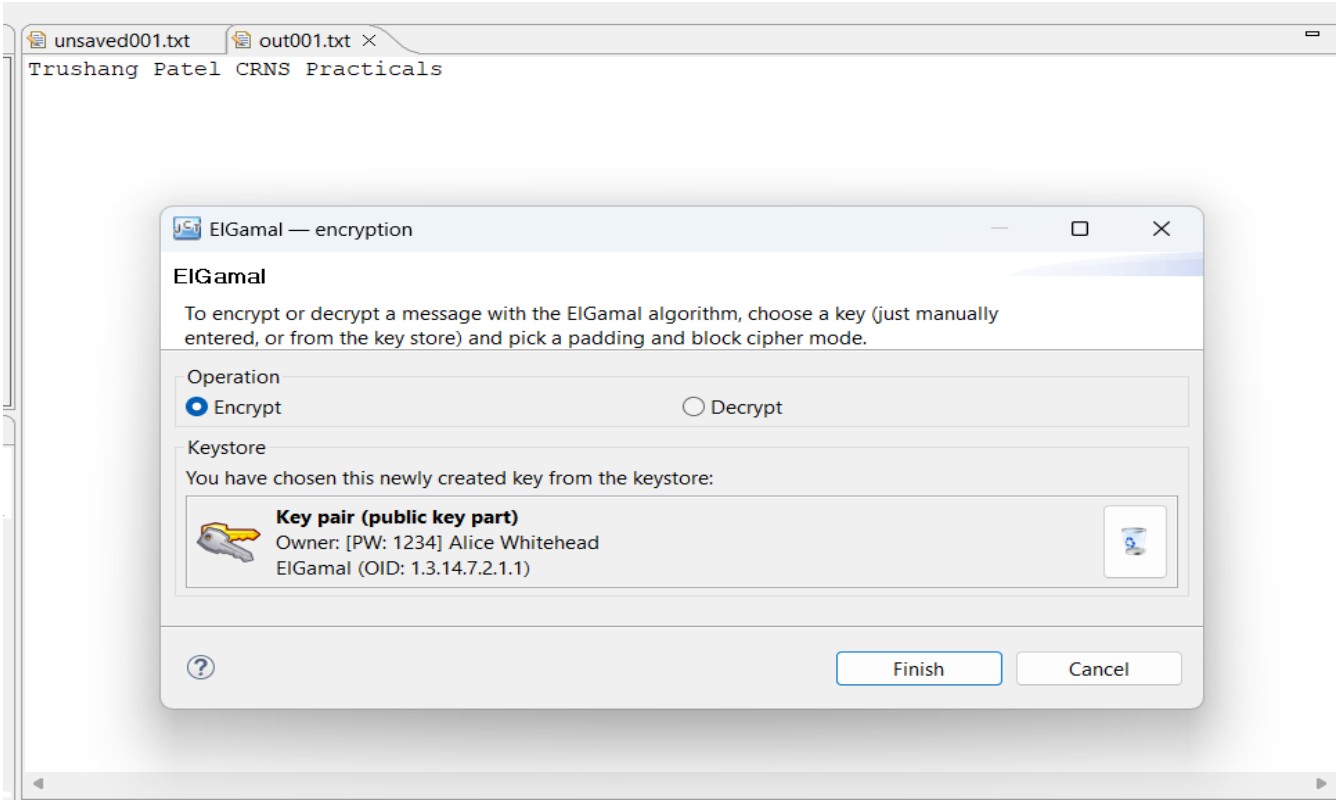

Figure 50:Encryption using ElGamal

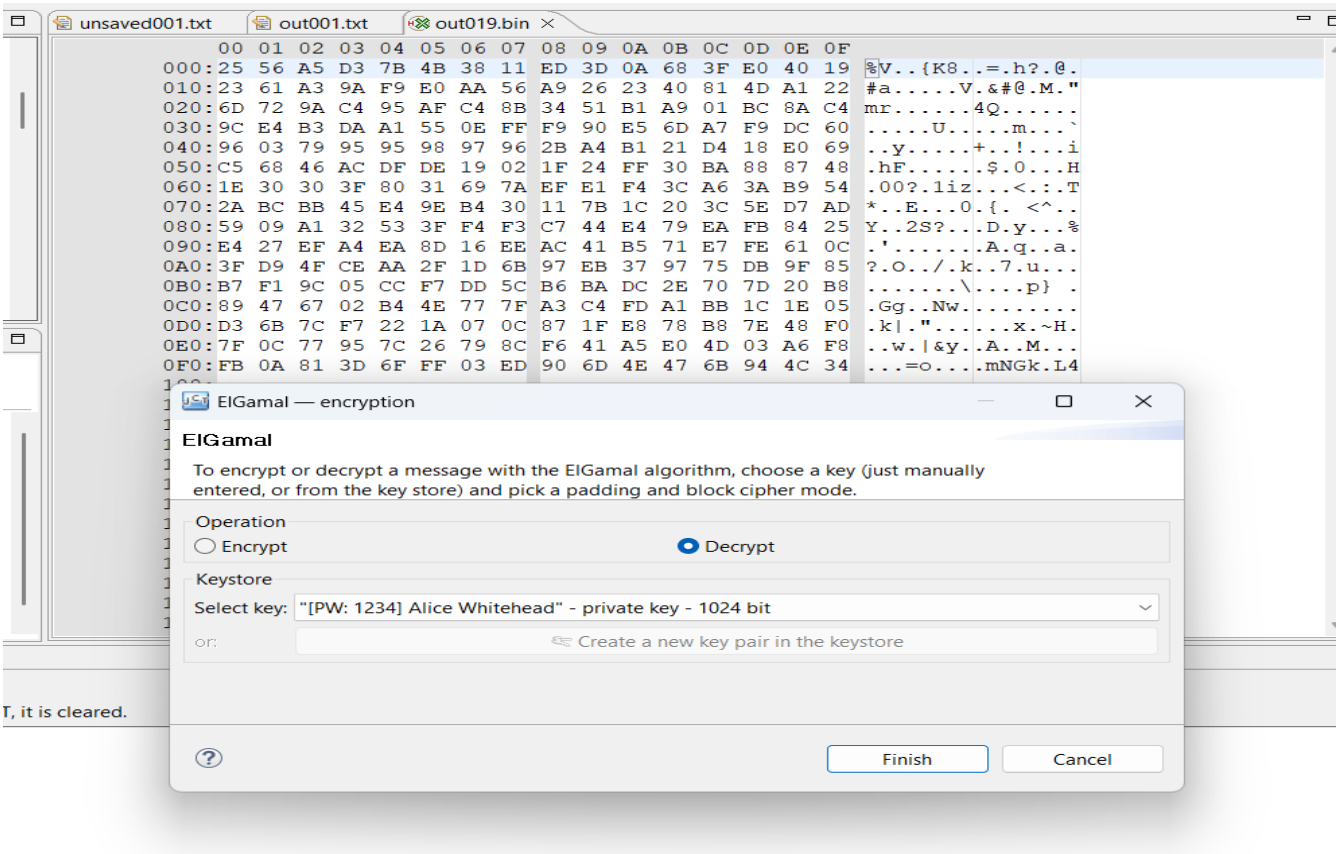

Figure 51:Decryption using ElGamal

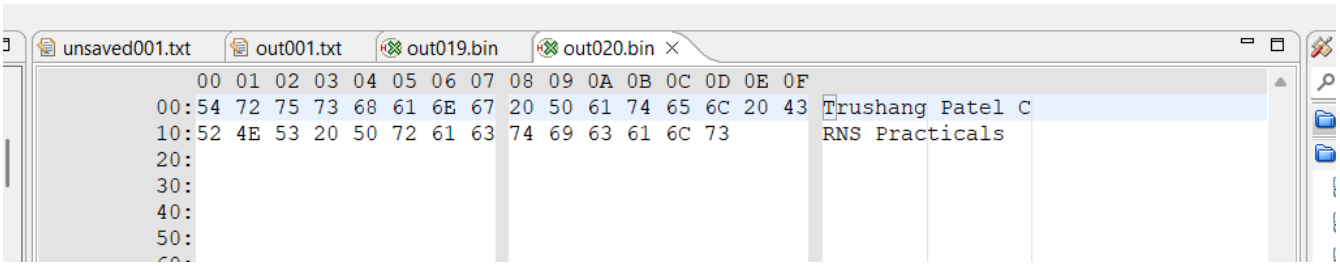

Figure 52:Output of ElGamal

LATEST APPLICATIONS:

- Post-Quantum Cryptography Standards
- Integration of PQC in Messaging Platforms
- Quantum-Resistant Encryption in VPN Services
- Development of Mix Networks for Anonymity

LEARNING OUTCOME:

In this practical, I learned how encryption and decryption work within a cryptosystem and tested their application using various cryptographic algorithms.

REFERENCES:

1. Crypto Tool : https://www.cryptool.org/en/cto/
2. Britannica : https://www.britannica.com/topic/Caesar-cipher
3. GeeksforGeeks : geeksforgeeks.org/transposition-cipher-techniques-in-cryptography/
4. ChatGPT: https://chatgpt.com/