Module:- Public Key Infrastructure Date:- 15/09/2022

Assignment :- 01

Cryptography:- Cryptography is the art and science of achieving security by encoding messages to make them non-readable.

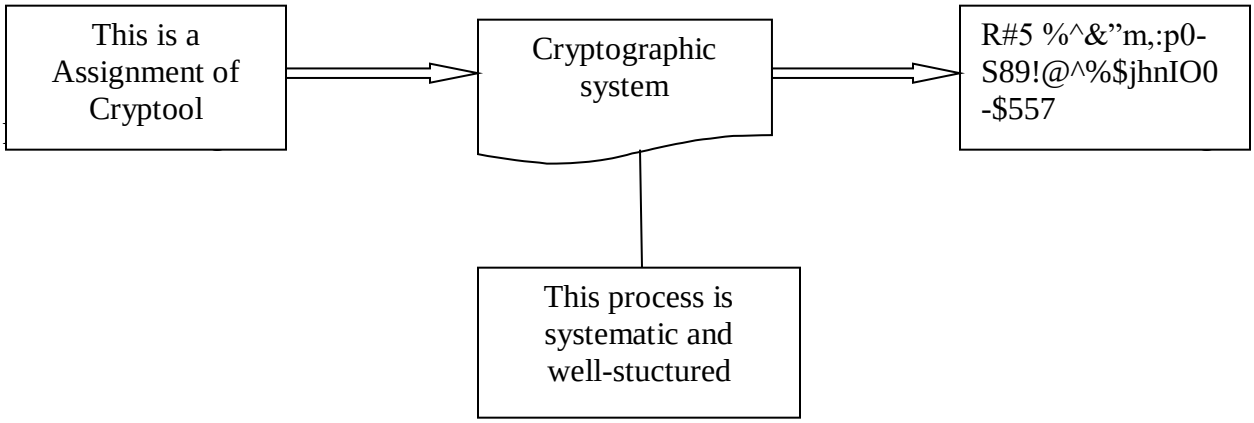
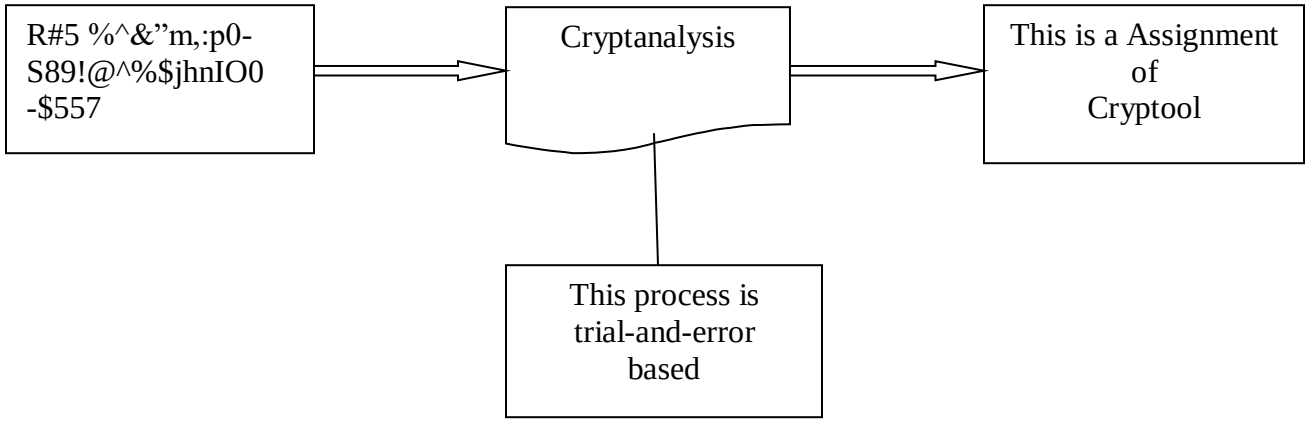


Fig. (a) Cryptographic system

Cryptanalysis:- Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.



Fig(b):- Cryptanalysis

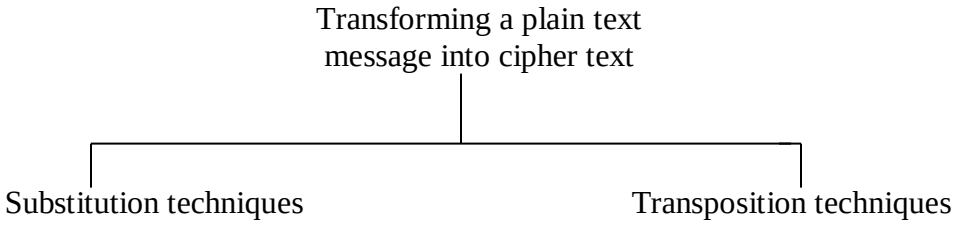
Cryptology :- Cryptology is a combination of cryptography and cryptanalysis.

Cryptography + Cryptanalysis = Cryptology

Plain Text :- Clear text or plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Cipher Text :- When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

❖ **Two Primary ways in which Conversion of Plain Text to Cipher text and vise-versa.**



Substitution Technique :- Here each Character Simply Replaced by another Character.

A	B	C	D	E	F	G	H	I	J	K	L	M
k	m	j	z	p	b	o	d	t	s	g	v	i
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
y	w	l	x	n	c	q	a	r	f	e	u	h

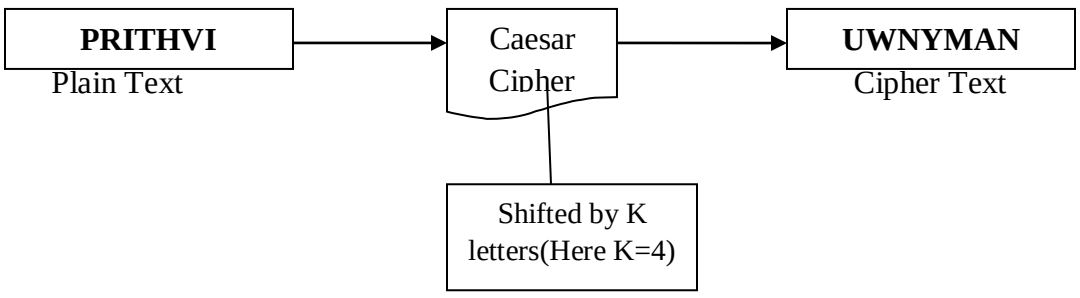
- Read each alphabet in the cipher text message, and search for it in the second row of the above table (i.e. the second row of the table).
- When a match is found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the above table (e.g. if the alphabet in cipher text is J, replace it with G).
- Repeat the process for all alphabets in the cipher text message.

Substitution Technique work following type :

A) Caesar Cipher :- In the substitution cipher technique, the characters of a plain text message are replaced by other characters, numbers or symbols.

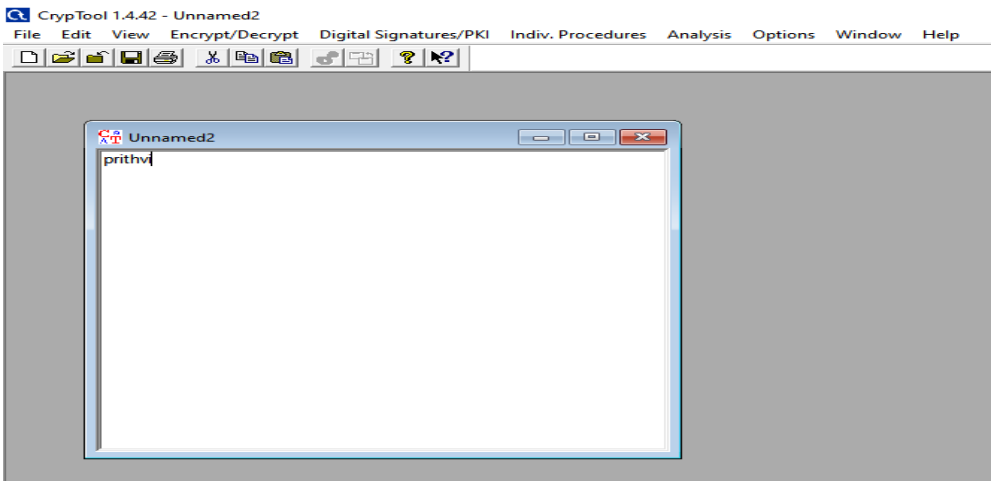
- A type of Substitution technique is Caesar Cipher is also called Shift Cipher.Where each Character is Shifted By **K** Letters.
- Caesar Cipher can be perform following steps.

Ex:-

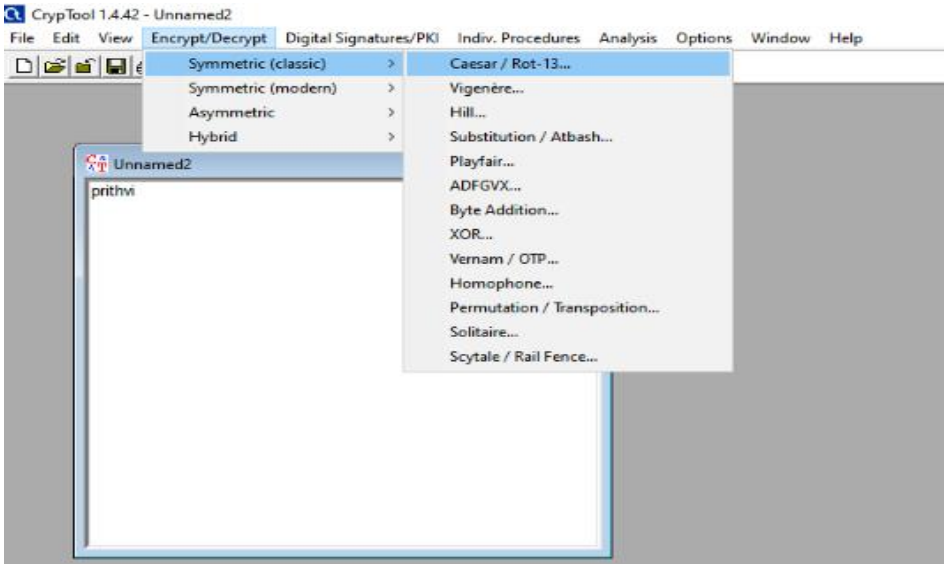


PRACTICAL:-

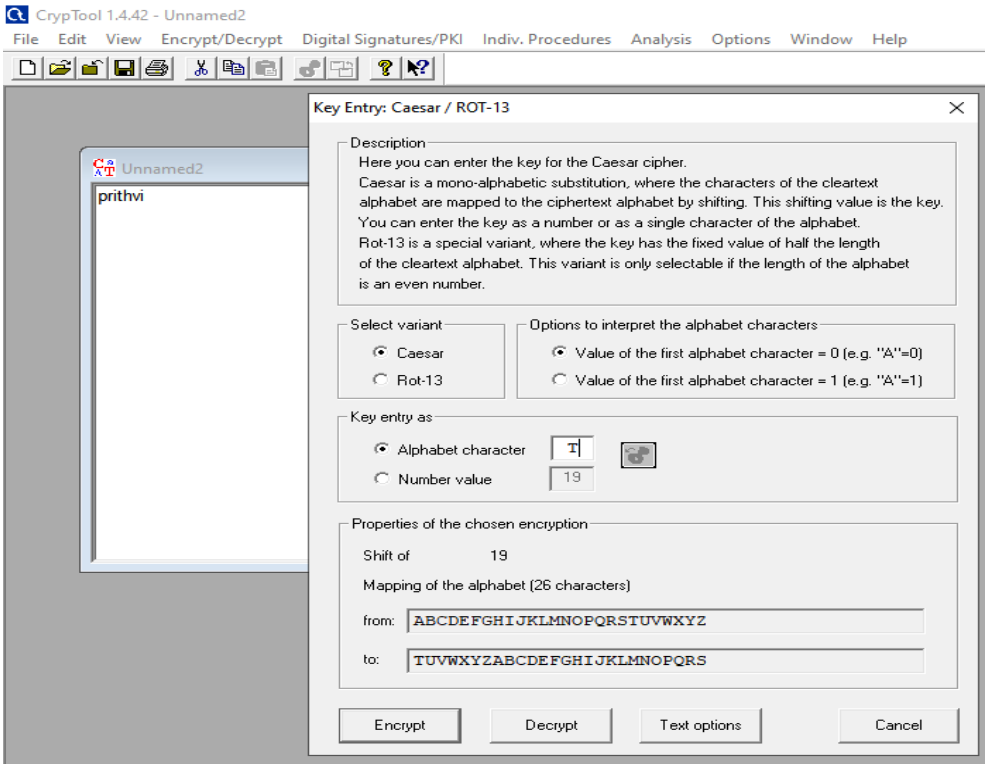
Step-1 : First of all we have to open cryptool. Then open new page and type some message or plain text such as " PRITHVI" .



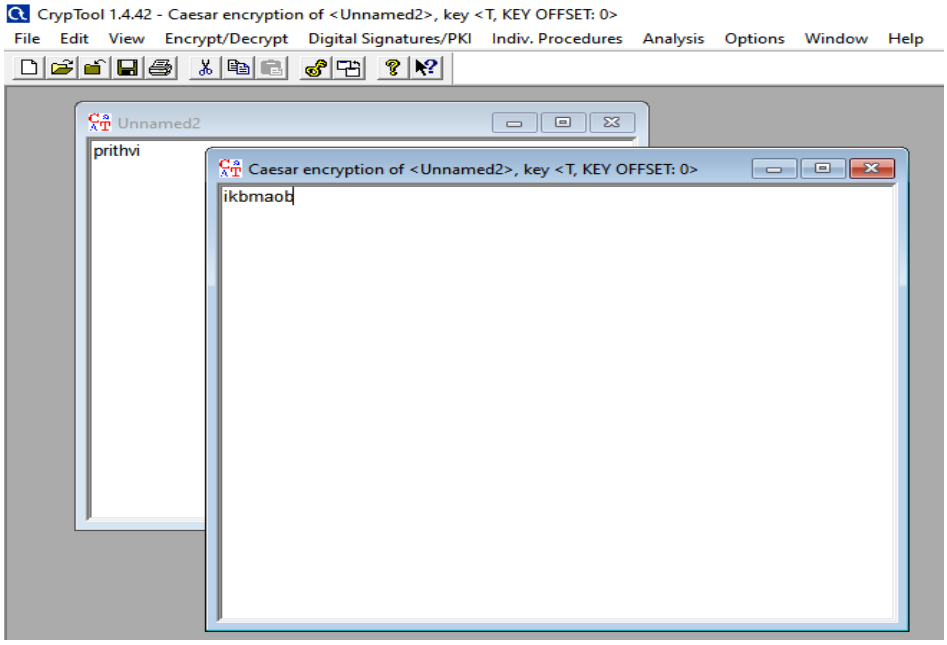
Step 2 : Then we will go Encrypt/Decrypt mode select Symmetric key(Classic) and again select Caesar /Rot-13.



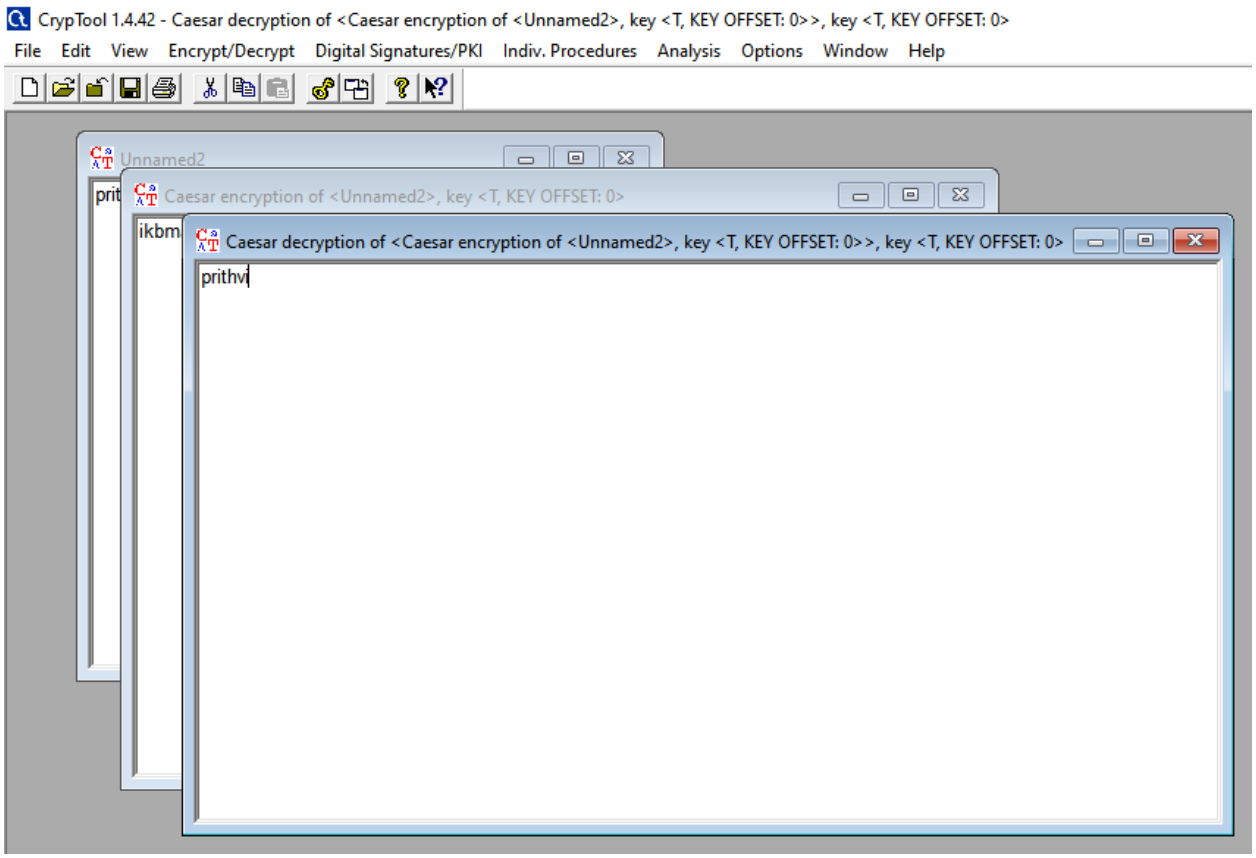
Step- 3 : Opening new pop that show two radio button one is Caesar and second is Root-13.Then we can select Caesar option. In parallel way is also show two radio button one is Alphabet character = 0(e.g A=0) and Alphabet character =1(e.g A=1) then we can select first button.Then we put Alphabet character "T" and T's alphabetical number is 20 but cryptool show's 19 because we have select Alphabet character =0. T to Z Alphabet replaced before of A ex: TUVWXYZABCDEFGHIJKLMNOPQRS.



Step-4 : Then we can select Encryption option showing above image and encrypted value is " "prithvi" to 'ikbmaot" using key K=19(Here shifted each alphabet by 19).



Step-5 :- We have select to Decryption option showing in step-3(image) and Decrypted value is " ikbmaot" to 'prithvi" using key K=19(Here shifted each alphabet by 19).



B)Vigenere Cipher:- The Vigenere cipher is a type of polyalphabetic Substitution cipher. The Encryption Process combines one character of plain text and Corresponding character of key to get character of cipher text using Vigenere Square matrix. That matrix is Alphabetical type, Numeral type and Symbolic type.

For Ex:- **Plain text** = NIKAM

Key = HITFSGF // used only 5 alphabet because plaint text used only 5 word

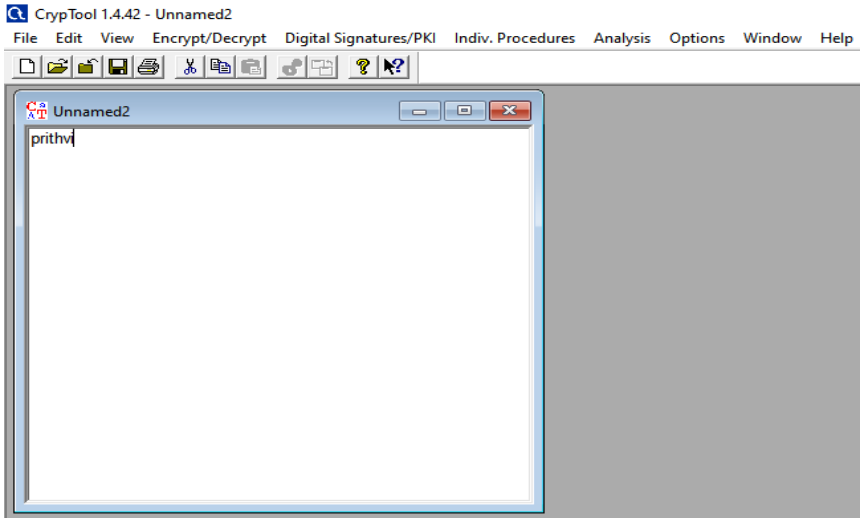
Cipher text = UQDFE

- The Vigenere Table Consist of 26 alphabet in row and column. In this row not repeated same alphabet and column work same as.
- Character of Plain text and character of key corresponding to each other at that meeting point between character plain text and key produce character of cipher text
- The Vigenere Matrix apply each character of Plain text using key.

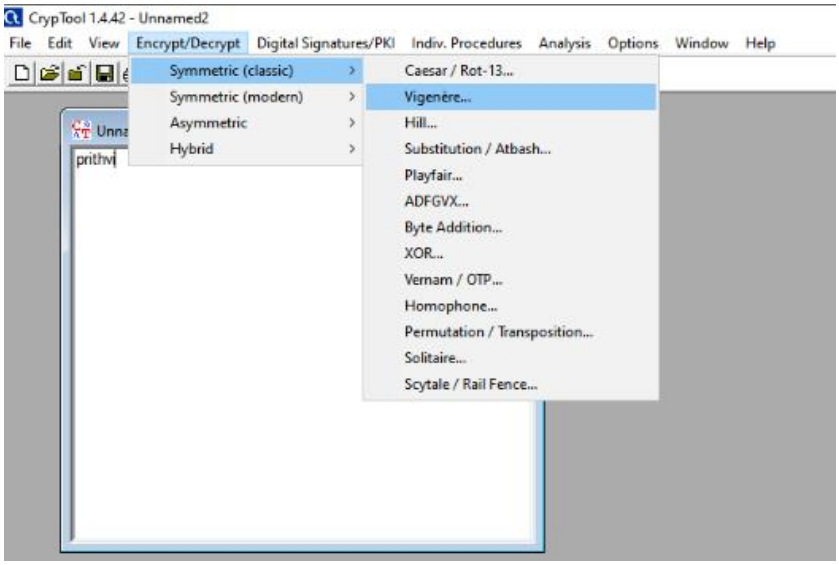
	a	b	c	d	e	f	g	h	i	j	k	L	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	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

PRACTICAL :-

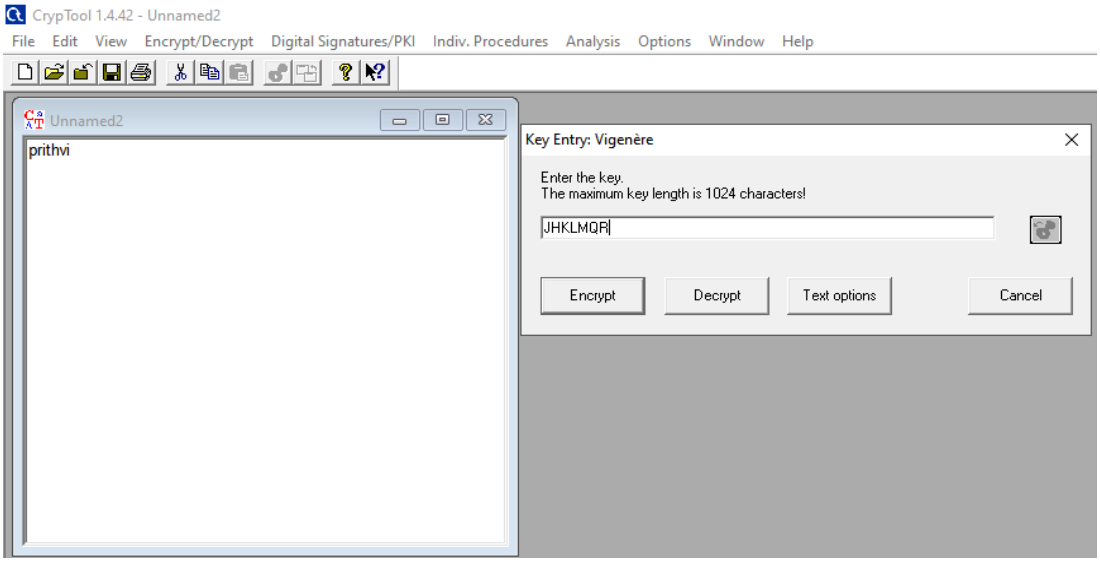
Step-1:- First of all we have to open cryptool. Then open new page and type some message or plain text such as " PRITHVI" .



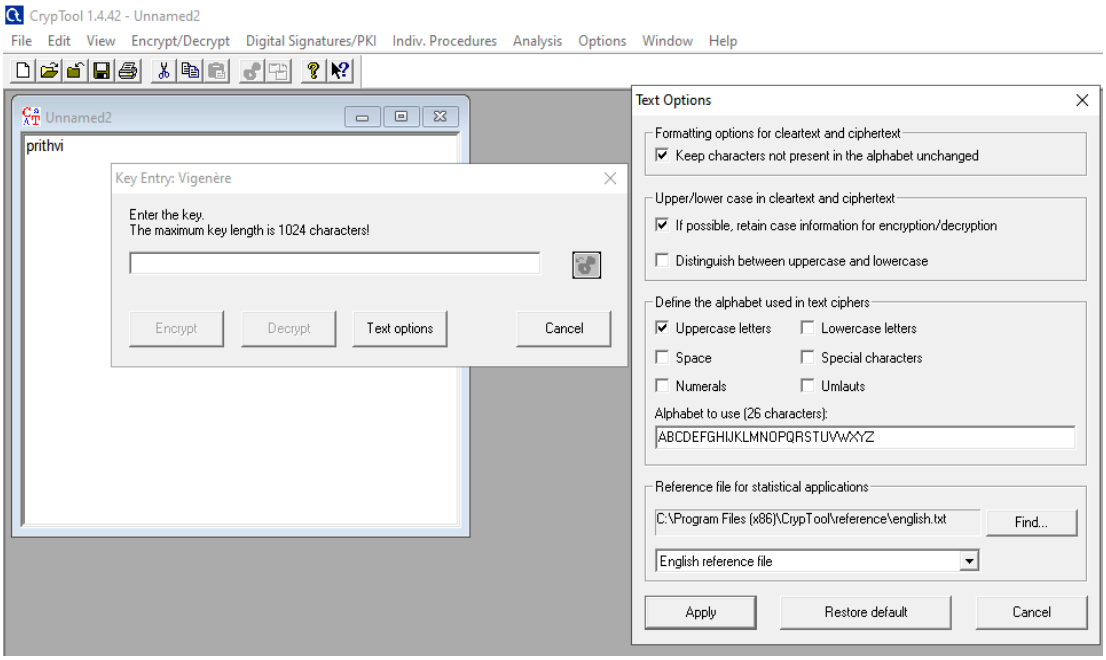
Step- 2 :- We will go Encrypt/Decrypt mode select Symmetric key(Classic) and in same way we can select Vigenere option.



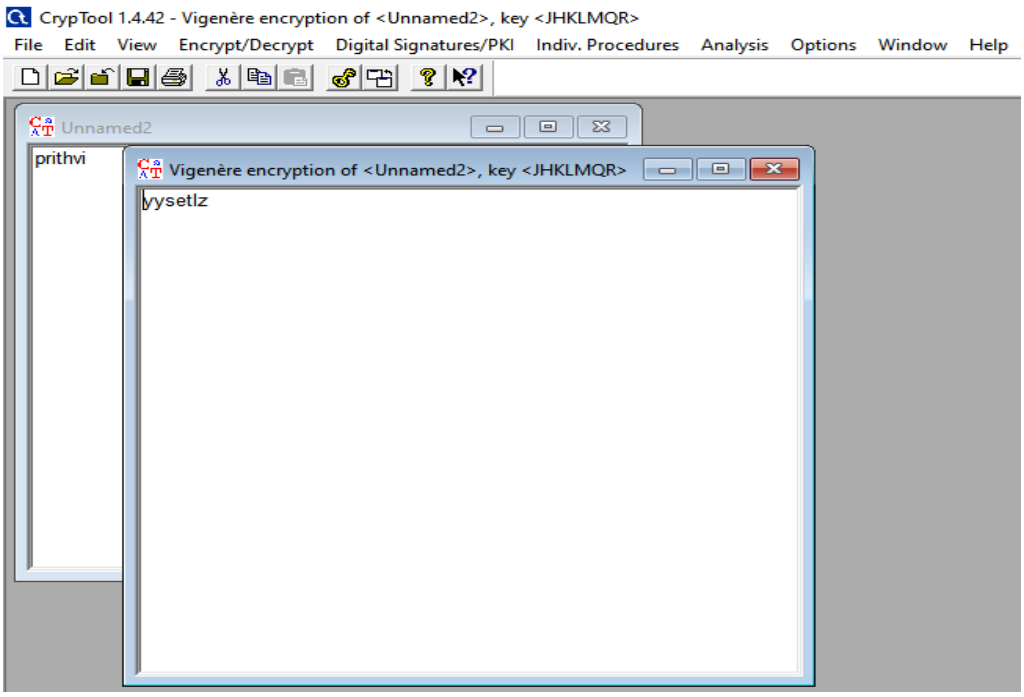
Step- 3:- After step -2 open new pop that show key entry text block then we can put key "JHKLMQR" Corresponding of Plain text "PRITHVI".



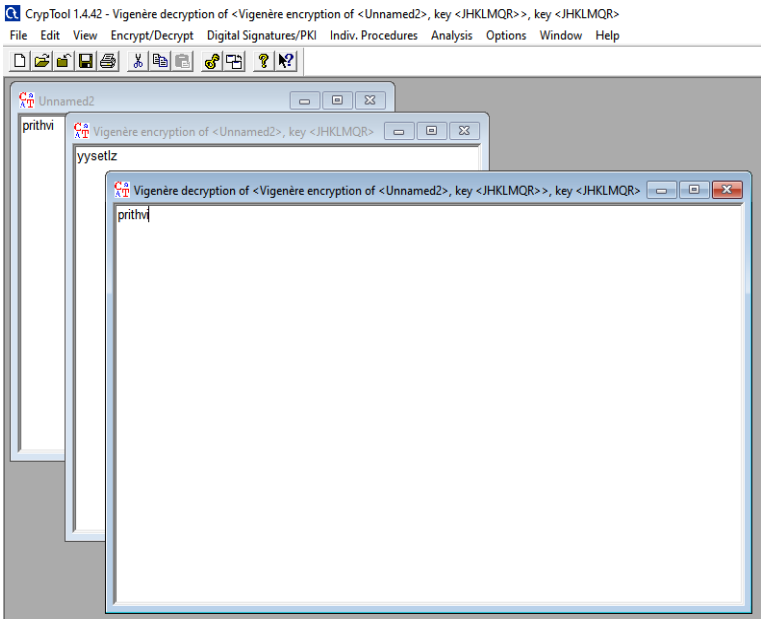
In pop box, text option shows various type of letters option in following image. Then we can choose alphabetical letters option and tool create 26* 26 alphabetical matrix.



Step -4:- We can select encrypt option after selection of text option. In encryption plain text "prithvi" and key "JHKLMQR" produce result Cipher text " yysetlz" using Vigenere Matrix Table.



Step – 5:- We have select to Decryption option showing in step-3(image) and Decrypted value is " yysetlz" to 'prithvi" using Vigenere matrix table.



C)Play Fair :- In Playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

1. Generate the key Square(5×5):
   - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
   - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.
2. Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. For example:

PlainText: "PRITHVINIKAM"

After Split: 'PR' 'IT' 'HV' 'IN' 'IK' 'AM'

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: "blood"

After Split: 'bl' 'ox' 'od'

Here **'x'** is the bogus letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “bloodi”
AfterSplit: ‘bl’ ‘ox’ ‘od’ ‘iz’
Here **‘z’** is the bogus letter.

Rules for Encryption:

- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
  For example:

Diagraph: "PE"
Encrypted Text: VM
Encryption:
P -> V
E -> M

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

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
  For example:

Diagraph: "FK"
Encrypted Text: GL
Encryption:
F -> G
K -> L

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

- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
  For example:

Diagraph: "IS"
Encrypted Text: OH
Encryption:
I -> O , S -> H

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

Plain Text: "NIKAM"
Encrypted Text: ORFCOU
Encryption:
N -> R
I -> O
K -> F
A -> C
M -> O
X -> U

NI

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

KA

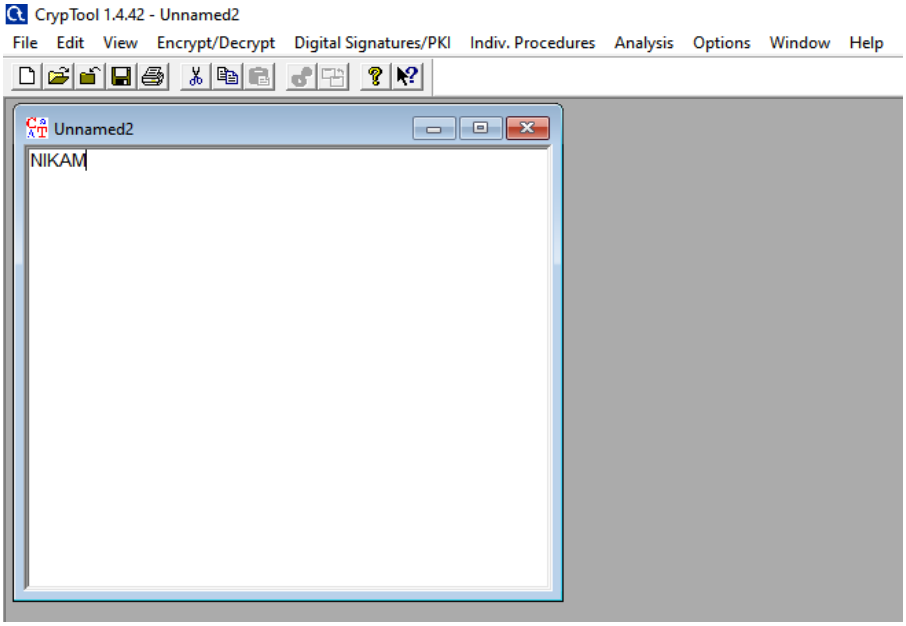
P	R	I	T	H
V	A	B	C	D
E	F	G	K	L
M	N	O	Q	S
U	W	X	Y	Z

MZ

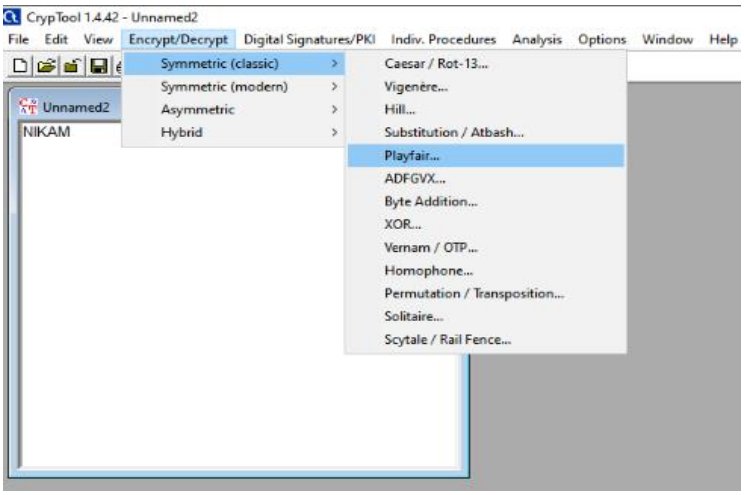
P	R	I	T	H
V	A	B	C	D
E	F	G	K	L
M	N	O	Q	S
U	W	X	Y	Z

PRACTICAL:-

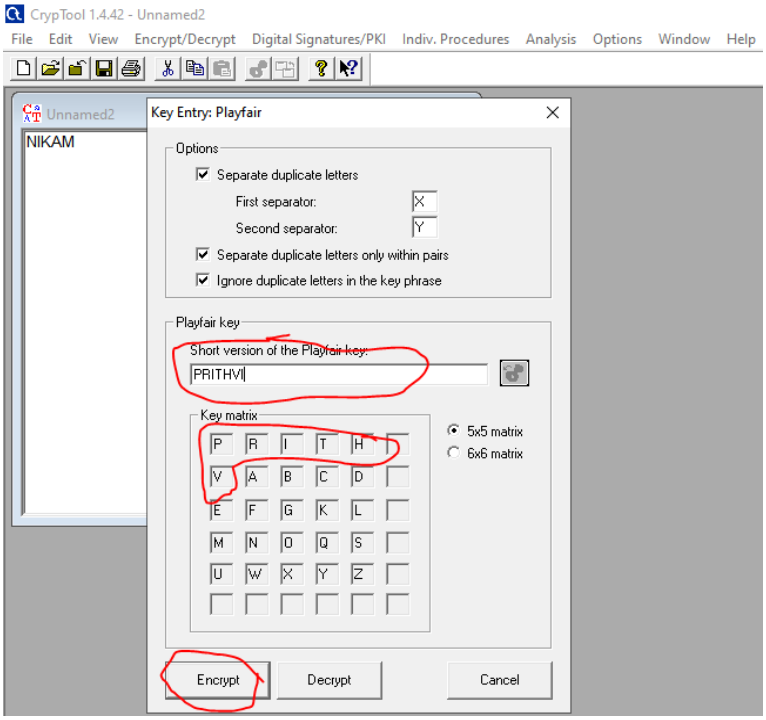
Step -1:- First of all we have to open cryptool. Then open new page and type some message or plain text such as " NIKAM" .



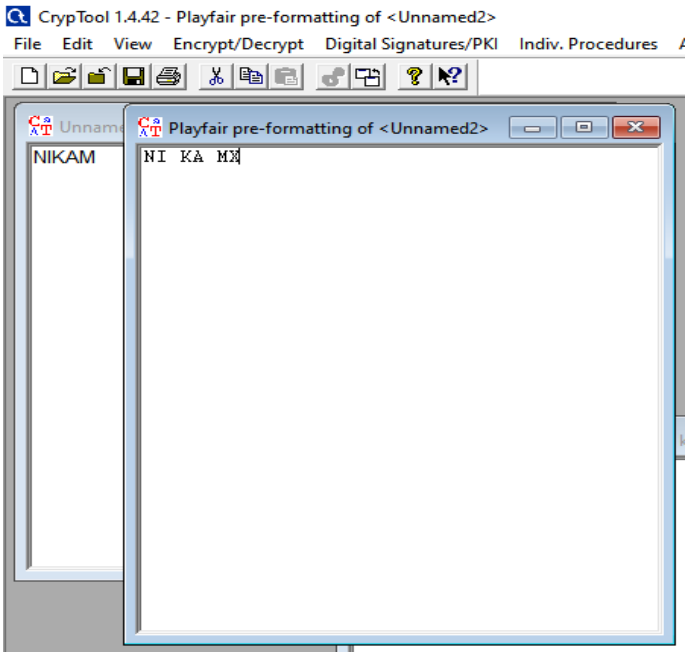
Step – 2:- We will go Encrypt/Decrypt mode select Symmetric key(Classic) and in same way we can select Plalyfair option.



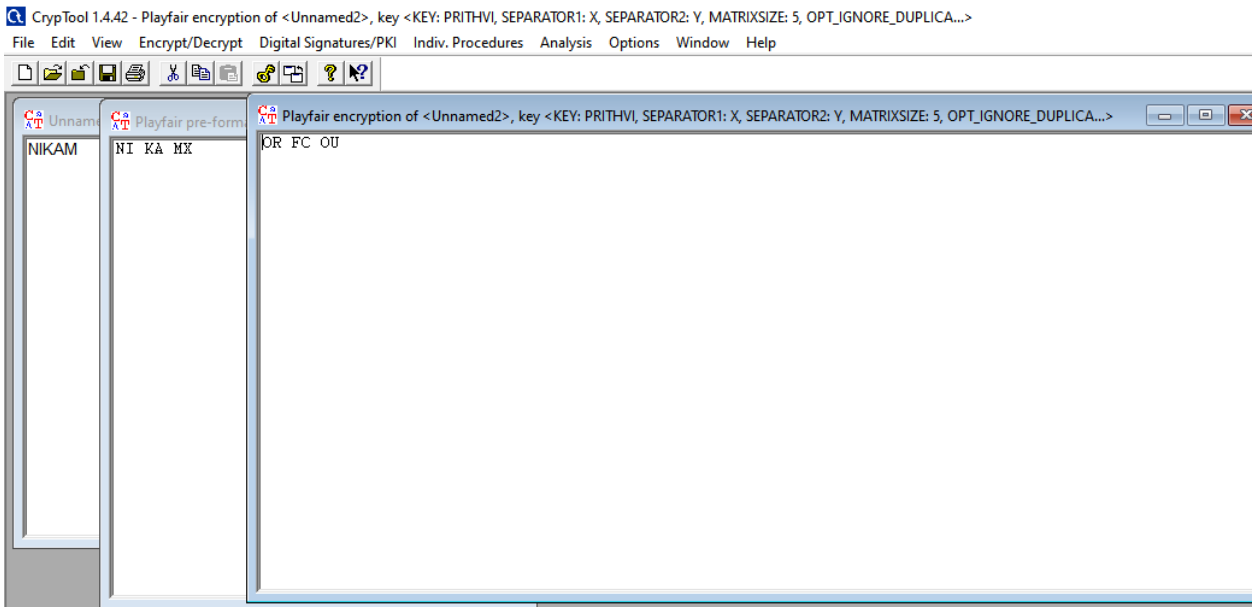
Step- 3:- Open new popup window that show Playfair key and 5x5 or 6x6 key matrix. We can put playfair key "PRITHVI" than select 5x5 matrix .In matrix remove repeated alphabet in key and result is placed before A to Z(except PRITHVI).then select Encrypt option



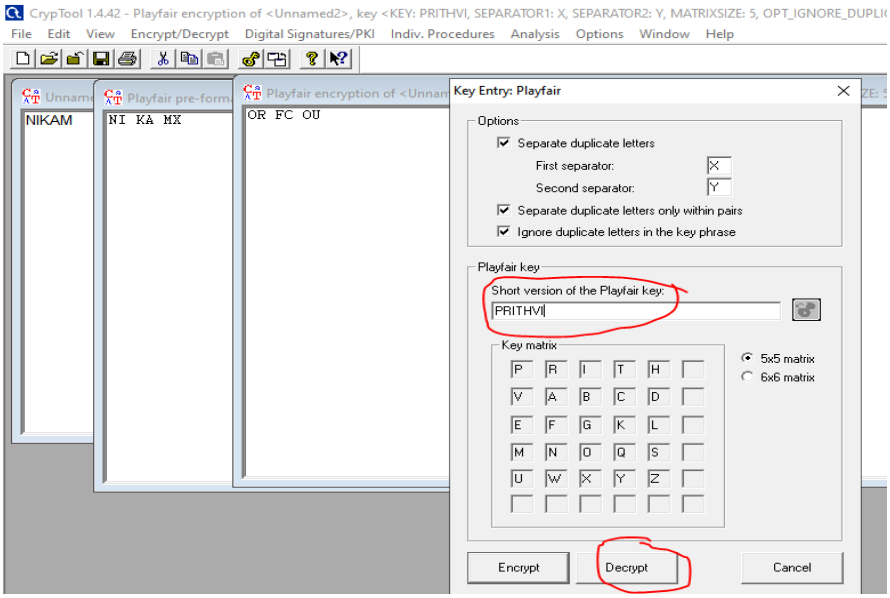
Step-4:- Before encryption Playfair creates two –two pair of alphabet. For ex:- "NIKAM" is convert in two-two pair or digraph such as "NI" "KA" "MX". X is a padding or bogus word.



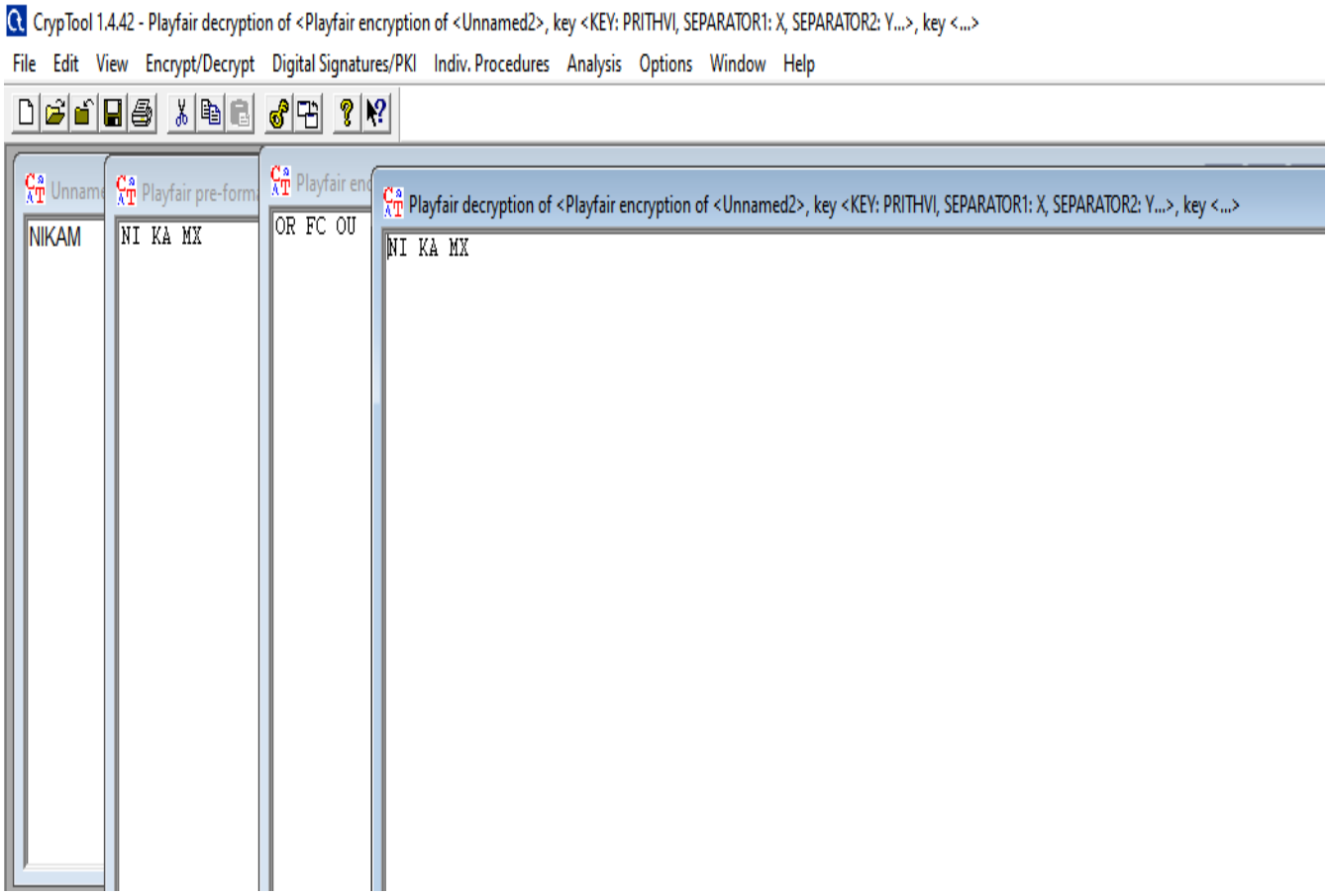
After encryption “NI” “KA” “MX” is converted into “OR” “FC” “OU” using playfair key “PRITHVI”



Step-5:- Again we can follow step-2.open new window and we can enter playfair key “PRITHVI” using 5x5 matrix.and also select decrypt option.



After decryption the result is “OR” “FC” “OU” to “NI” “KA” “MX”using playfair key”PRITHVI”.



Transposition Technique :-Transposition techniques differ from substitution techniques in the way that they do not simply replace one alphabet with another: they also perform some permutation over the plain text alphabets.
Transposition Technique type following us:

A)Rail fence cipher:-The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher.It derives its name from the way in which it is encoded. Rail fence technique involves writing plain text as sequence of diagonals and then reading it row-by row to produce cipher text.

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

For example:- **Plain text** = PRITHVI ROW = 2

Rail fence

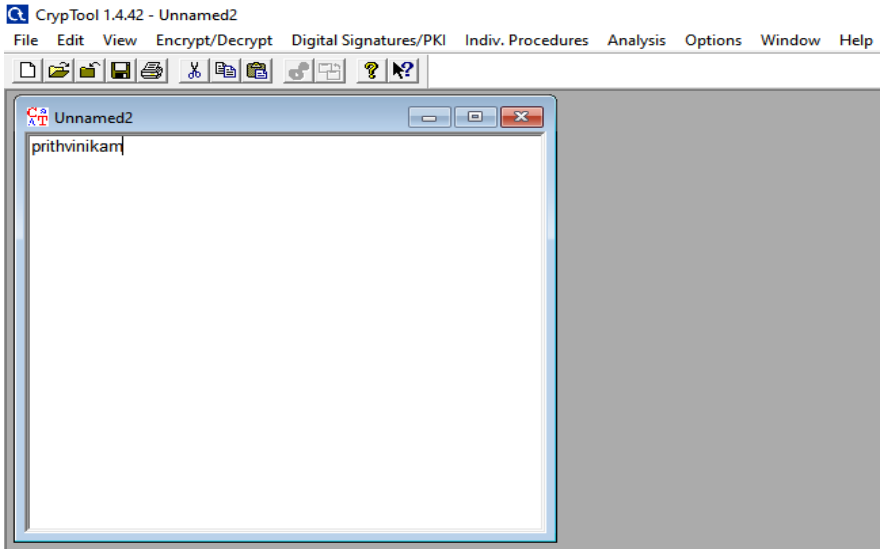
Row 1 ⟶ P I H I

. Row 2 ⟶ R T V

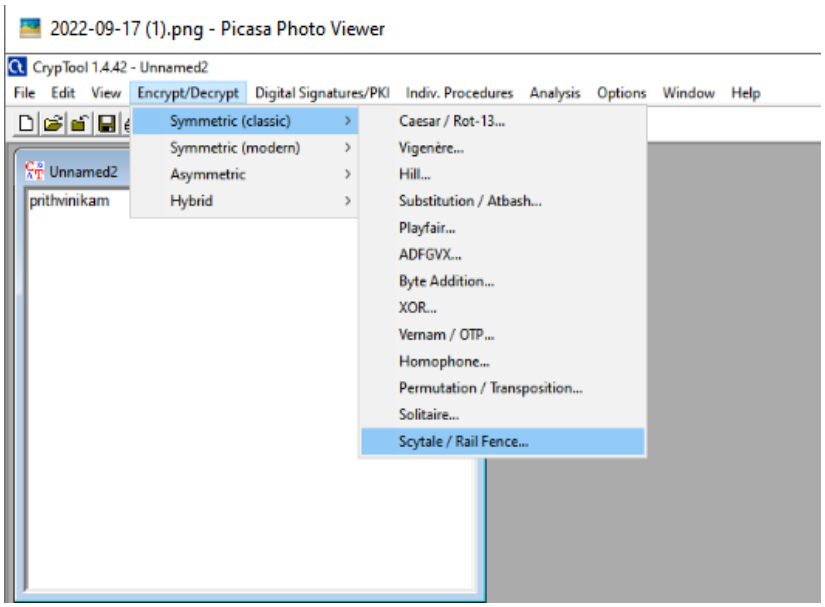
Cipher Text = PITHVIRTV

PRACTICAL:-

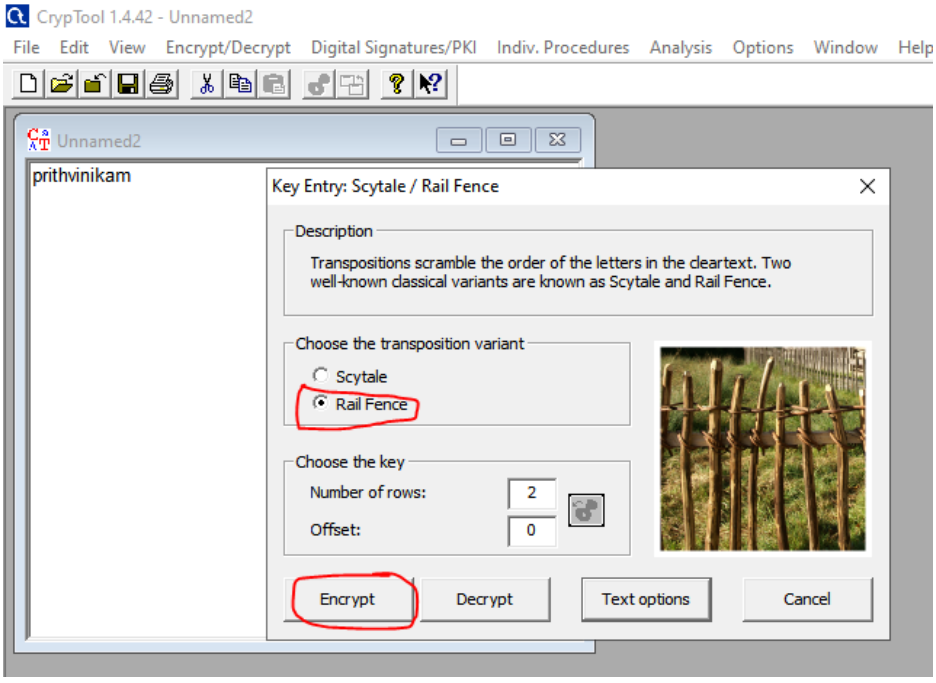
Step -1:- First of all we have to open cryptool. Then open new page and type some message or plain text such as " PRITHVINIKAM" .



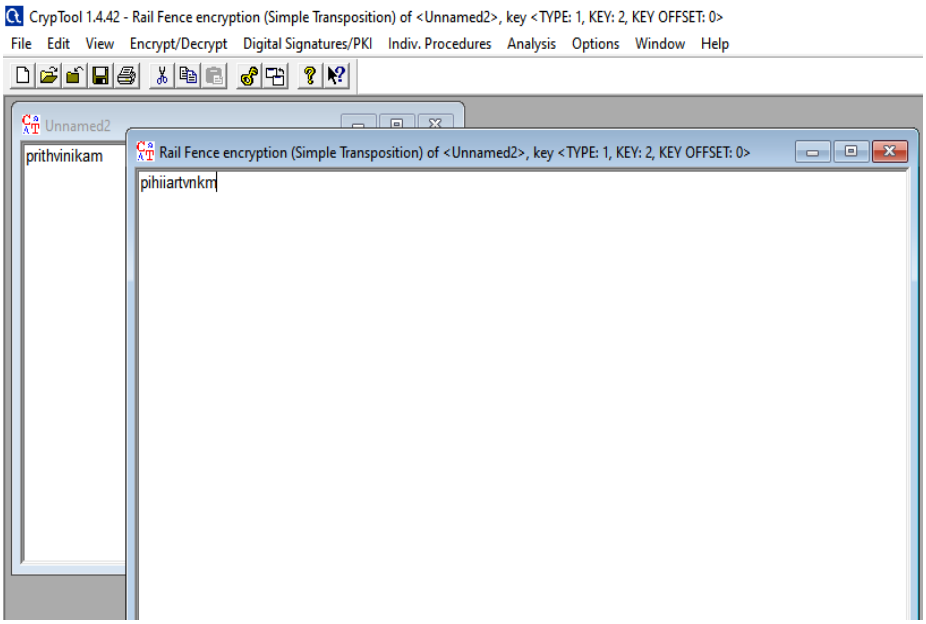
Step -2:- We will go Encrypt/Decrypt mode select Symmetric key(Classic) and in same way we can select Scytale / Rail Fence option.



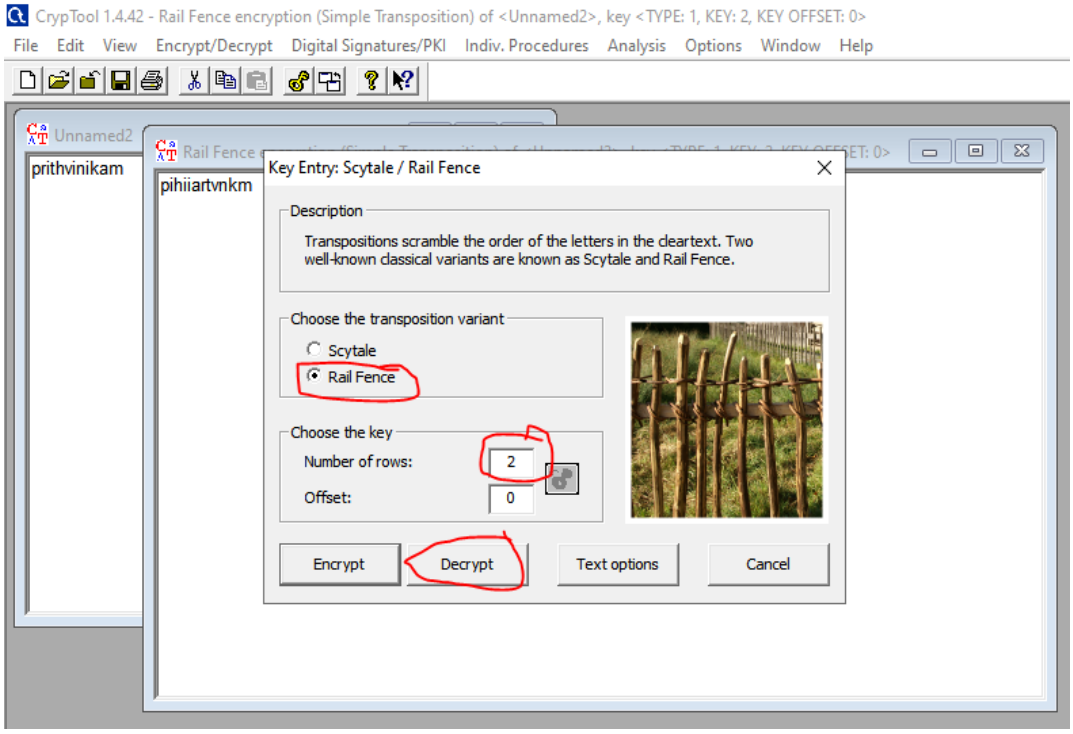
Step – 3:- Now open popup window that show two radio button one is Scytal and another is Rail fence.Then we can select Rail Fence button.Put Number of row = 2 with offset =0 then select encrypt option.



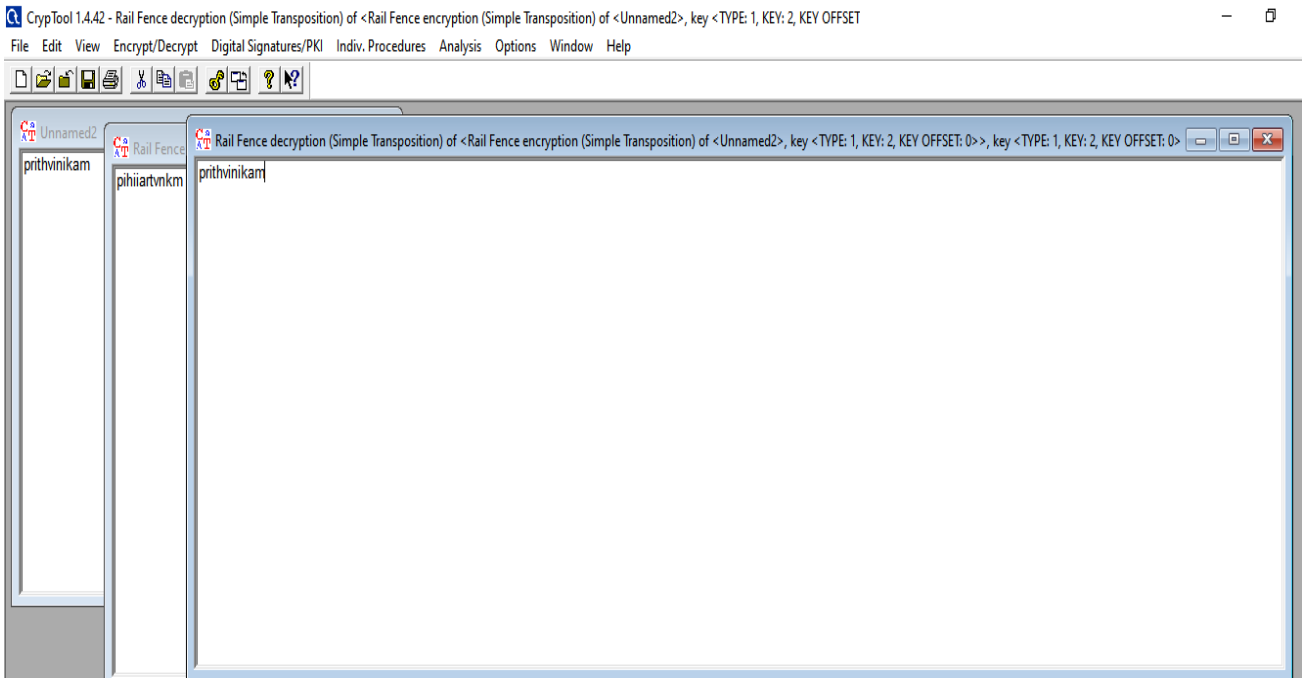
Step-4:- After Encryption the plaintext " prithvinikam" to cipher text "pihiiartvnkm".



Step-5:- follow step -2 opening new popup and we can select Railfence button number of rows =2 with offset =0.and then select decrypt option.

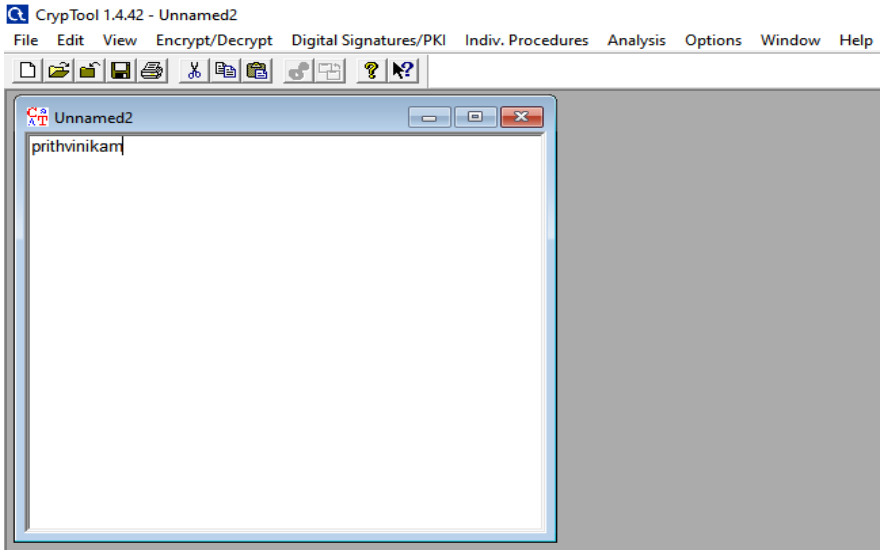


After decryption result is cipher text “pihiiartvnkm” to palin text” prithvinikam”

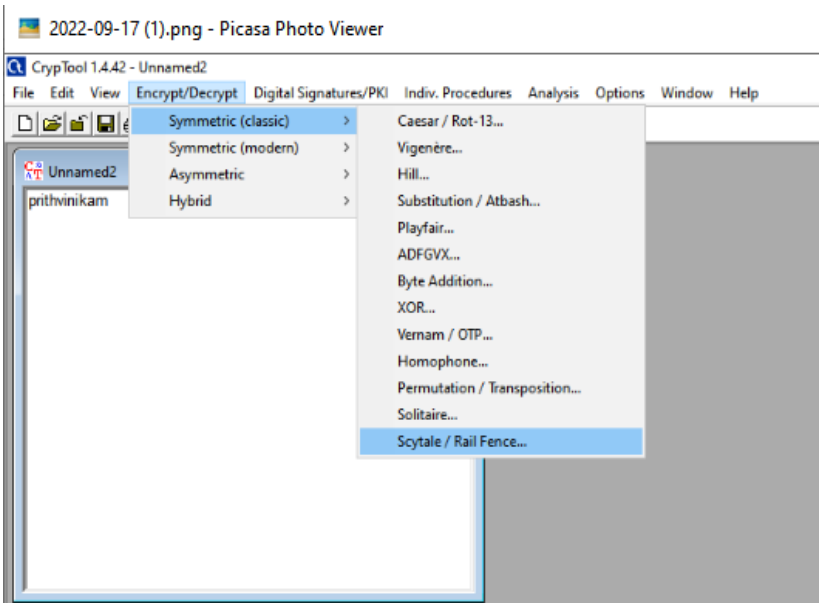


B)Scytal cipher :- A scytale is a stick, a piece of wood around which a ribbon (leather) is wrapped and on which a message is written, when the ribbon is unrolled an encrypted message appears (the order of the letters having changed)

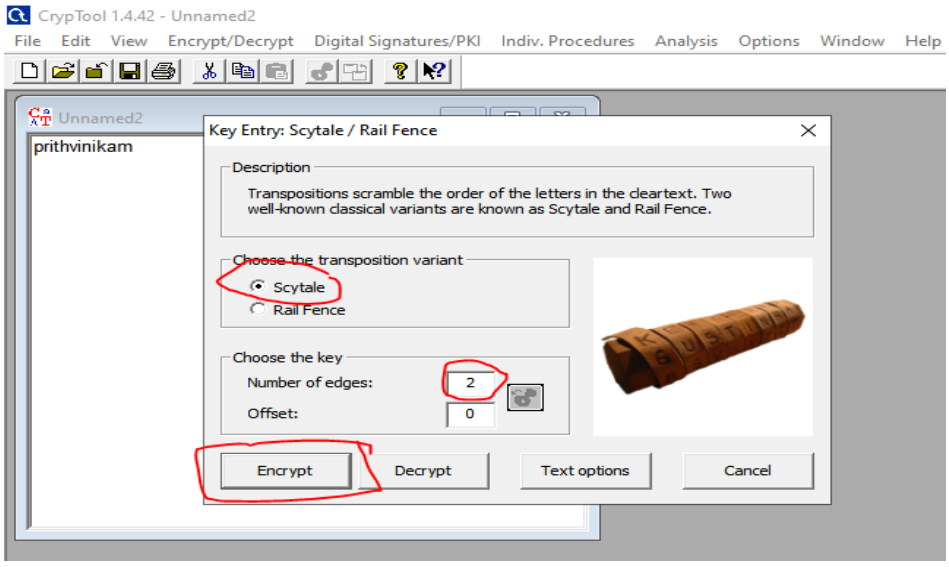
Step-1:- First of all we have to open cryptool. Then open new page and type some message or plain text such as " PRITHVINIKAM" .



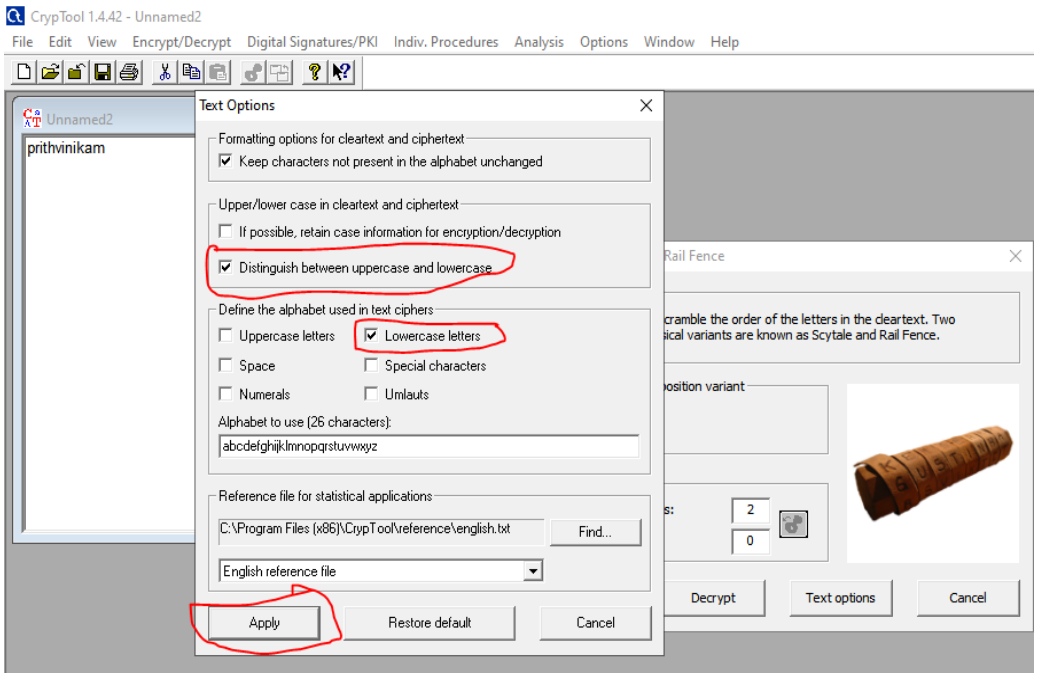
Step -2:- We will go Encrypt/Decrypt mode select Symmetric key(Classic) and in same way we can select Scytale / Rail Fence option.



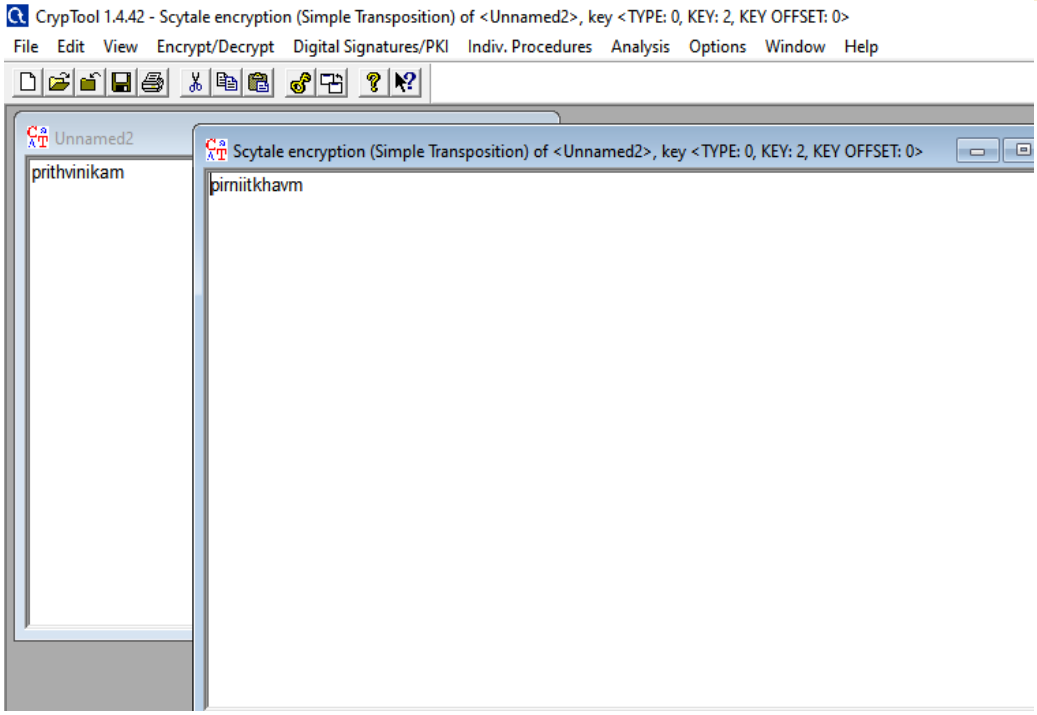
Step- 3:- Now open popup window that show two radio button one is Scytal and another is Rail fence.Then we can select Scytal button. Put Number of row = 2 with offset =0 then select encrypt option.



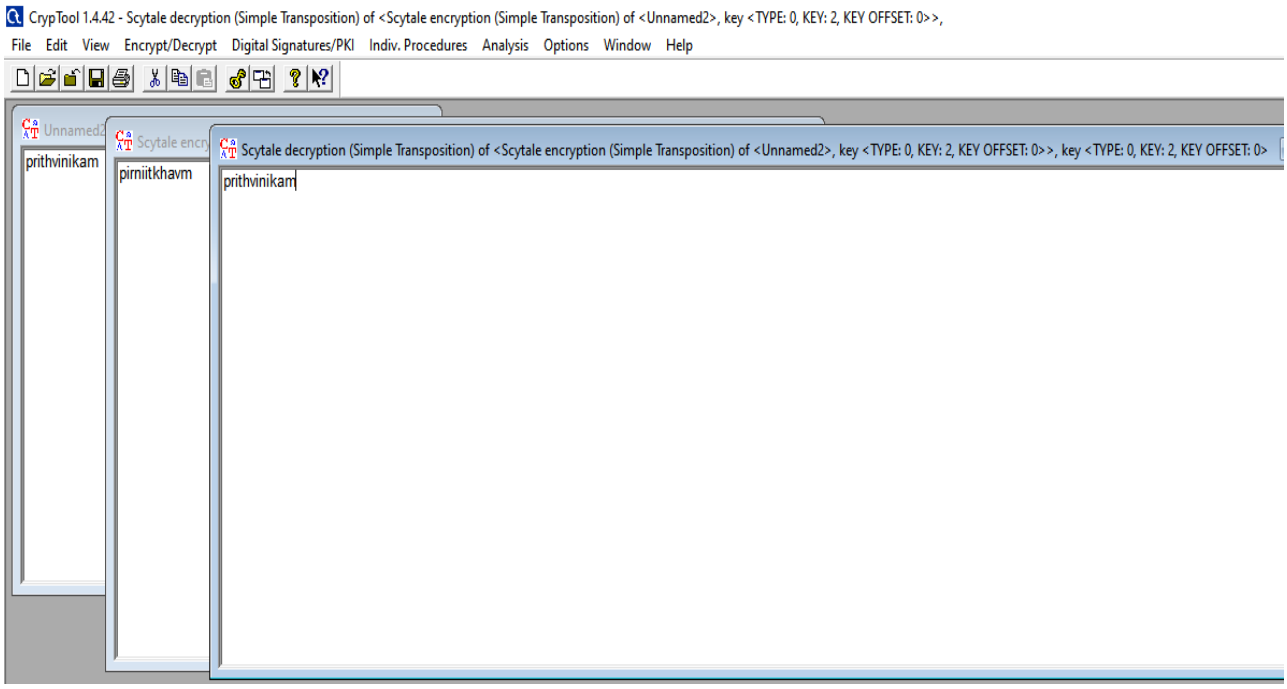
Before encryption we can select text option and choose uppercase and lowercase checkbox and then apply.



Step-4:-After encryption the Plain text "prithvinikam" converted to cipher text "pirniitkhavm".



Step-5:- follow step -2 opening new popup and we can select Scytale button number of rows =2 with offset =0.and then select decrypt option. After decryption result is cipher text"pirniitkhavm" to palin text" prithvinikam"


CrypTool 1.4.42 - Scytale decryption (Simple Transposition) of <Scytale encryption (Simple Transposition) of <Unnamed2>, key <TYPE: 0, KEY: 2, KEY OFFSET: 0>>,
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
prithvinikam
pirniitkhavm
Scytale decryption (Simple Transposition) of <Scytale encryption (Simple Transposition) of <Unnamed2>, key <TYPE: 0, KEY: 2, KEY OFFSET: 0>>, key <TYPE: 0, KEY: 2, KEY OFFSET: 0>
prithvinikam