

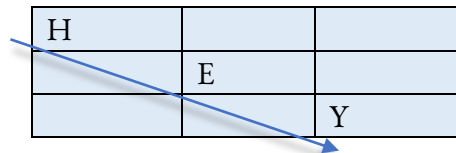
The Rail Fence is a graphically interesting take to encrypting and decrypting information and it emphasizes the various aspects of non-linear (multi-dimensional) ways to encrypt data.

The concept behind this cipher is –

- A graphical interface is imagined (rail matrix).
- The entered text is input into the table in a diagonal and down manner.

To look like this

Example input: HEY



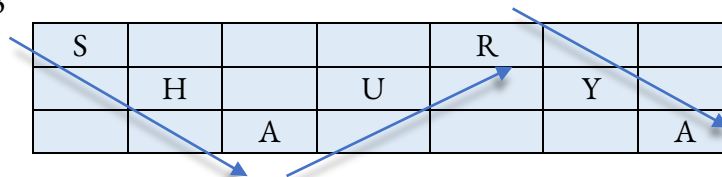
H		
	E	
		Y

- The number of columns is the characters present in the input string.
- The number of rows is the number of rails provided.

Now, number of rails acts as the security key to define the cipher's functioning.

For example, Sample input: SHAURYA

Number of rails: 3



S				R		
	H		U		Y	
		A				A

Once we reach the bottom rail, we traverse upwards and so the input is written in a zig-zag manner.

- In this case the output encrypted text would be
 - SRHUYAA

Note: The encrypted text would be the provided graph and the system reads through it line by line.
So,

Rail1	S				R			SR	+
Rail2		H		U		Y		HUY	+
Rail3			A				A	AA	=
Output								SRHUYAA	

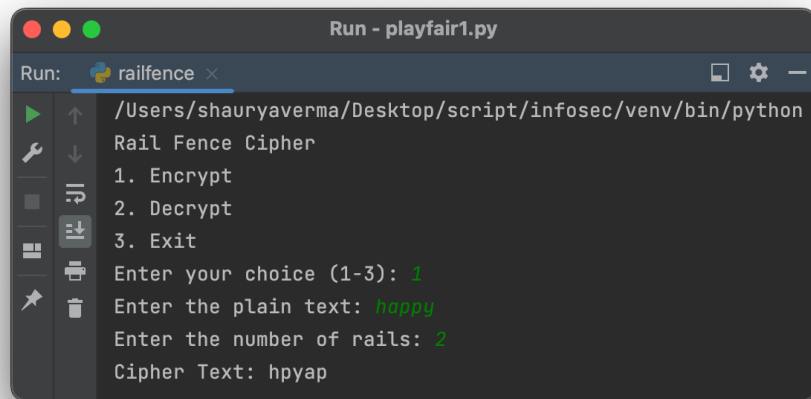
For Decryption:

- The rail matrix is constructed first using the data (number of characters, number of rails)
- Then the encrypted data is input into the matrix row-wise.
- After filling the matrix, we traverse it in a zig-zag manner to obtain the original text.

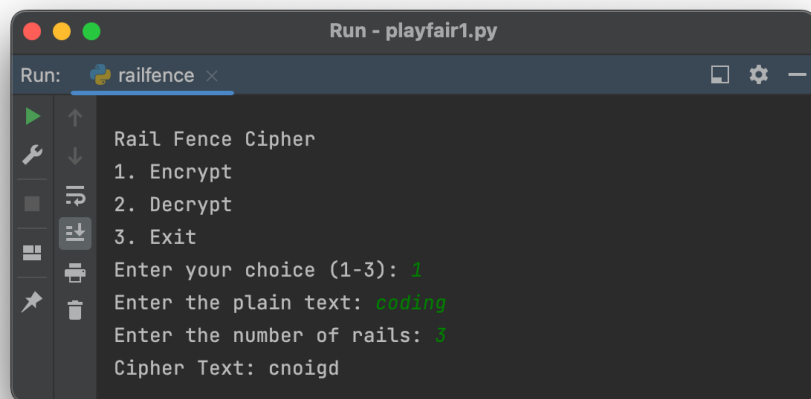
Provided code and output covers both encryption and decryption.

(for GitHub mobile swipe right)

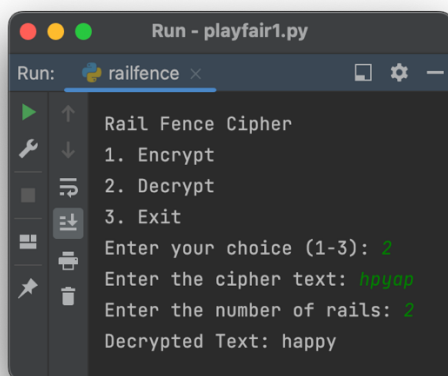
Output and verification of decryption -



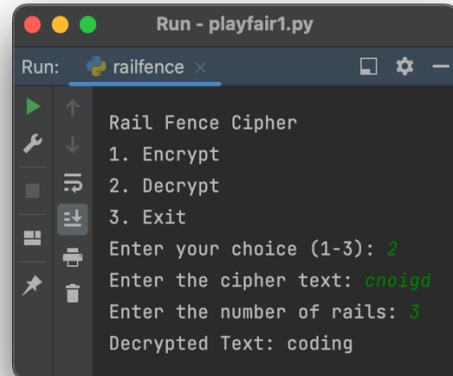
```
Run - playfair1.py
Run: railfence x
/Users/shauryaverma/Desktop/script/infosec/venv/bin/python
Rail Fence Cipher
1. Encrypt
2. Decrypt
3. Exit
Enter your choice (1-3): 1
Enter the plain text: happy
Enter the number of rails: 2
Cipher Text: hpyap
```



```
Run - playfair1.py
Run: railfence x
Rail Fence Cipher
1. Encrypt
2. Decrypt
3. Exit
Enter your choice (1-3): 1
Enter the plain text: coding
Enter the number of rails: 3
Cipher Text: cnoigd
```



```
Run - playfair1.py
Run: railfence x
Rail Fence Cipher
1. Encrypt
2. Decrypt
3. Exit
Enter your choice (1-3): 2
Enter the cipher text: hpyap
Enter the number of rails: 2
Decrypted Text: happy
```



```
Run - playfair1.py
Run: railfence x
Rail Fence Cipher
1. Encrypt
2. Decrypt
3. Exit
Enter your choice (1-3): 2
Enter the cipher text: cnoigd
Enter the number of rails: 3
Decrypted Text: coding
```

Happy Coding!