Practical No. 3

Rail Fence Cipher

**Q.1]** Write Python for encryption and decryption of Rail Fence cipher.

**Rail Fence Cipher:**

The Rail Fence Cipher is a form of transposition cipher where the plaintext is written in a zigzag pattern across multiple "rails" (rows) and then read off row by row to create the ciphertext. The number of rails acts as the key to the cipher. This method creates a jumbled version of the text that obscures its original order.

**Formula:**

There is no straightforward formula

**Strengths:**

* **Simplicity**: Easy to understand and implement with straightforward encryption and decryption processes.
* **Fast Operation**: Efficient for short and simple messages, requiring minimal computational resources.

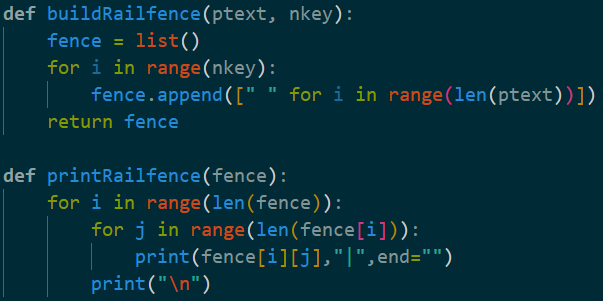
**Weakness:**

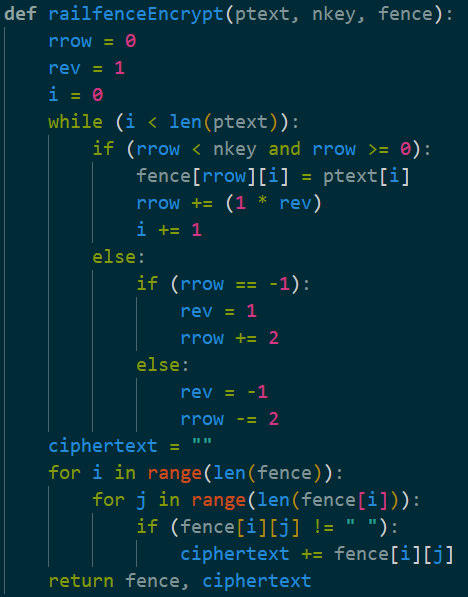
* **Low Security**: Provides minimal obfuscation and is easily broken with enough ciphertext.
* **Pattern Vulnerability**: Preserves the order of characters in a predictable pattern, making it susceptible to pattern analysis.

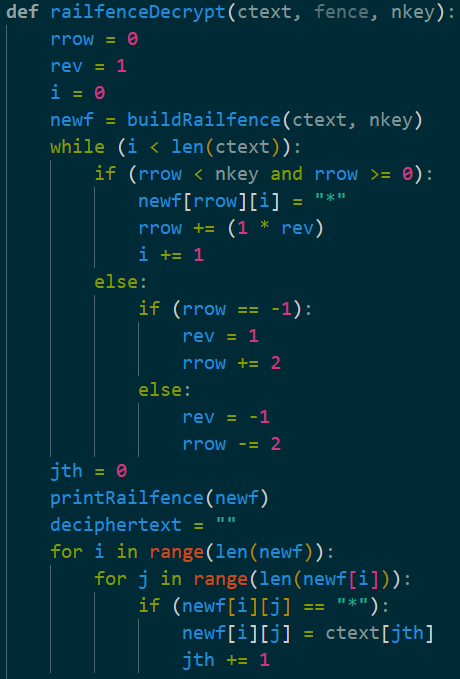
**Attacks:**

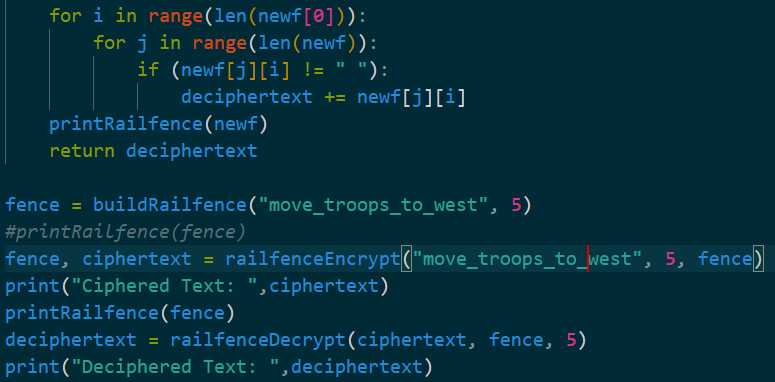
* **Simple Reconstruction**: By trying different rail numbers, the zigzag pattern can be reconstructed, and the plaintext revealed.
* **Frequency Analysis**: Not effective in transposition ciphers, but known plaintext attacks could help reconstruct the zigzag pattern.
* **Brute Force Attack**: Trying all possible numbers of rails (especially feasible with a small number of rails) to find the correct pattern for the ciphertext.

**Code:**

****

****

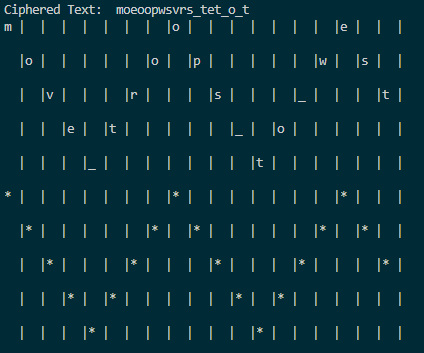
****

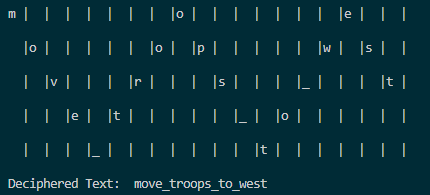
****

**Output:**

**Test Cases:**

**1]** Here the plaintext was “move to troops to west” and the key was 5 (“\_” was used as a replacement for space “ “)

****

****

**2]** Here the plantext was “cold weather is coming” and the key was 9.

