PRIYADARSHINI COLLEGE OF ENGINEERING
(Recognised by A.I.C.T.E., New Delhi & Govt. of Maharashtra, Affiliated to R.T.M.Nagpur University)Near CRPF Campus, Hingna Road, Nagpur-440 019, Maharashtra (India)
Phone : 07104 - 236381, 237307, Fax : 07104 - 237681,

Practical No. 4

Aim: - To implement Rail Fence Cipher of transposition Techniques.

Theory :

The **rail fence cipher** (sometimes called zigzag cipher) is a **transposition cipher** that jumbles up the order of the letters of a message using a basic algorithm.

The rail fence cipher works by writing your message on **alternate lines** across the page, and then reading off each line in turn.

For example, let's consider the **plaintext** "This is a secret message".

Plaintext T H I S I S A S E C R E T M E S S A G E

To encode this message we will first write over two lines (the "rails of the fence") as follows:

Rail Fence Encoding

T		I		I		A		E		R		T		E		S		G	
	H		S		S		S		C		E		M		S		A		E

Note that all white spaces have been removed from the plain text.

The **ciphertext** is then read off by writing the top row first, followed by the bottom row:

Ciphertext T I I A E R T E S G H S S S C E M S A E

Conclusion:

The concept of trasposition stream ciphers , Rail Fence Cipher has been studied successfully.

Viva Questions:

Q. 1 What is Trasposition Technique?

Q. 2 Exaplain How Rail Fence Works?

Q. 3 What is disadvantage of Rail Fence ?