**NIRMA UNIVERSITY**

**Institute of Technology**

**B.Tech. Computer Science and Engineering**

**2CSDE54 Information and Network Security**

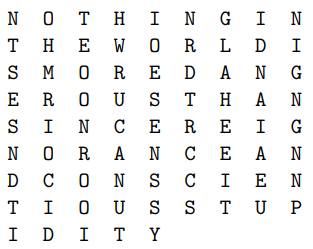
Perform encryption and decryption using the following transposition techniques

1. Rail fence - Row & Column Transformation
2. One time pad

A **rail fence cipher** is one in which plaintext symbols are rearranged (i.e., transposed or permuted) to produce ciphertext. The method of transposition may be either mathematical or typographical in nature

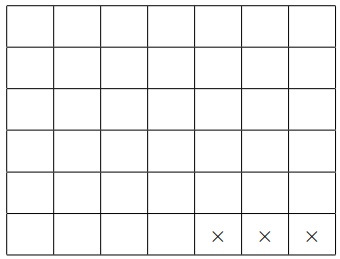
**Columnar Transposition:** The number of columns is the key information.

**To encipher :** Plaintext is written horizontally in k columns, and is then transcribed vertically columnby-column,

**To decipher :** Suppose that the length of the ciphertext is n and the key is k. Then the letters will fill n DIV k full rows, and there will be one partial row at the end with n MOD k letters. Transcribing row-by-row will then yield the plaintext.Example: Encrypt NOTHING IN THE WORLD IS MORE DANGEROUS THAN SINCERE IGNORANCE AND CONSCIENTIOUS STUPIDITY with a key of k = 9 columns. Solution: We write the plaintext horizontally in 9 columns as follows:

The cipher text is therefore: **NTSESNDTIOHMRIOCIDTEOONROOIHWRUCANUTIOESENSSYNRDTRCCSGLAHEEITIDNAIAEUNIGNGNNP**.

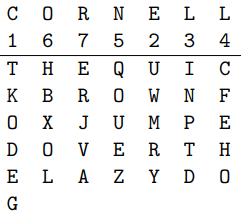
Example: Suppose the ciphertext is: GPSDO AILTI VRVAA WETEC NITHM EDLHE TALEA ONME. If it is known that the key is k = 7, find the plaintext. Solution: There are 39 letters in the ciphertext which means that there are 39 DIV 7 = 5 full rows and one partial row with 39 MOD 7 = 4 letters

****

**Keyword Columnar Transposition**

The order of transcription of the columns is determined by the alphabetical order of letters in the keyword. If there are repeated letters in the keyword, the columns corresponding to those letters are transcribed in order left-to-right

Example: Encrypt THE QUICK BROWN FOX JUMPED OVER THE LAZY DOG if the keyword is CORNELL.



Ciphertext: TKODE GUWMR YINPT DCFEH OQOUE ZHBXO LERJV A

**One time pad**

* The message is represented as a binary string (a sequence of 0’s and 1’s using a coding mechanism such as ASCII coding.
* The key is a truly random sequence of 0’s and 1’s of the same length as the message.
* message =‘IF’
* then its ASCII code =(1001001 1000110)
* key = (1010110 0110001)
* *Encryption:*
* 1001001 1000110 plaintext
* 1010110 0110001 key
* 0011111 1110110 ciphertext