DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 19CS3041S
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

4. Transposition and Columnar Techniques

Date of the Session: 16/08/2021

Time of the Session: 9 to 10:40 am

Learning Outcomes:

- **To understand the concept of Encryption and Decryption.**
- **To understand the applications of Transposition techniques**
- **To understand the applications of Columnar techniques**

Pre-Lab Task:

1. **What is transposition cipher?**

   Transposition cipher is an encryption technique used in cryptography in which the letters or characters of the plain text are rearranged according to a regular system so that the cipher text consists of permutations of the plaintext

2. **What are the applications of rail-fence cipher?**

   As Rail-fence cipher is a difficult-to-decrypt encryption technique it can be used in various high security organisations in encrypting highly confidential data.

3. **Brief description of columnar transposition cipher.**

   Columnar transposition cipher is a type of transposition cipher in cryptography where the plain text is written in rows in a n*n matrix according to some set of rules bound by the given key and then it is read off in columns as the ciphertext.

4. **Columnar transposition cipher is also known as _____.**
   transposition cipher

5. **How to break a rail-fence cipher?**

   The rail fence cipher is a simple type of transposition cipher. It's also aptly named the zigzag cipher due to the way the encryption occurs—plaintext characters are mixed up in a zigzag manner.This cipher has little to no security as the resultant ciphertext is an anagram. Thus, someone with a piece of paper and a pencil could easily break the cipher.

In-Lab Task:

1. Write a program to implement Rail-Fence Cipher (encryption/decryption) for any given plain text.

Sample input: S21atlocation56 No of Rails: 3

Sample output: - Stan2alcto5loi6

```
import java.util.*;
class RailFenceBasic{
 int depth;
 String Encryption(String plainText,int depth)throws Exception
 {
  int r=depth,len=plainText.length();
  int c=len/depth;
  char mat[][]=new char[r][c];
  int k=0;

  String cipherText="";

  for(int i=0;i< c;i++)
  {
   for(int j=0;j< r;j++)
   {
    if(k!=len)
     mat[j][i]=plainText.charAt(k++);
    else
     mat[j][i]='X';
   }
  }
  for(int i=0;i< r;i++)
  {
   for(int j=0;j< c;j++)
   {
    cipherText+=mat[i][j];
```

```
  }
 }
 return cipherText;
}


String Decryption(String cipherText,int depth)throws Exception
{
 int r=depth,len=cipherText.length();
 int c=len/depth;
 char mat[][]=new char[r][c];
 int k=0;

 String plainText="";


 for(int i=0;i< r;i++)
 {
  for(int j=0;j< c;j++)
  {
   mat[i][j]=cipherText.charAt(k++);
  }
 }
 for(int i=0;i< c;i++)
 {
  for(int j=0;j< r;j++)
  {
   plainText+=mat[j][i];
  }
 }

 return plainText;
}
}
```

```
class RailFence{
 public static void main(String args[])throws Exception
 {
  RailFenceBasic rf=new RailFenceBasic();
            Scanner scn=new Scanner(System.in);
            int depth;

            String plainText,cipherText,decryptedText;

            System.out.println("Enter plain text:");
            plainText=scn.nextLine();

            System.out.println("Enter depth for Encryption:");
            depth=scn.nextInt();

  cipherText=rf.Encryption(plainText,depth);
  System.out.println("Encrypted text is:\n"+cipherText);

            decryptedText=rf.Decryption(cipherText, depth);

  System.out.println("Decrypted text is:\n"+decryptedText);

 }
}
```

Post Lab Task:

1. **Write a pseudo code for encryption and decryption using Rail Fence Cipher.**

Encryption:

1. First the plain text is written in a matrix that has n rows where n=length of key
2. Key is the main asset of this technique
3. The plain text is written in the n rowed matrix in a diagonal manner such that the first character of the key starts at the first row first column next one in the second row second column and 3rd one in the 3rd row 3rd column and later it traverses back the same path such that the next character is written in the 2nd row 4th column and goes on
4. Later the cipher text is read off in rows

Decryption:

1. As we know that the number of rows in the matrix is equal to the length of the key and the number of columns is the length of the plaintext
2. The rail matrix can be constructed with these two known values and the we can figure out where the text should be placed.
3. Then we will fill the cipher text row wise and later we traverse the cipher text in a zig zag manner to get the original plain text.

(For Evaluator's use only)

Comment of the Evaluator (if Any)	**Evaluator's Observation**
	Marks Secured: _____out of _____ **Full Name of the Evaluator:** **Signature of the Evaluator Date of Evaluation**