Experiment No.8

Rail-fence Technique

Theoretical Background

The rail fence cipher is a very old encryption scheme, pre-dating the Middle Ages. It was used as a field cipher by both sides in the US Civil War. The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

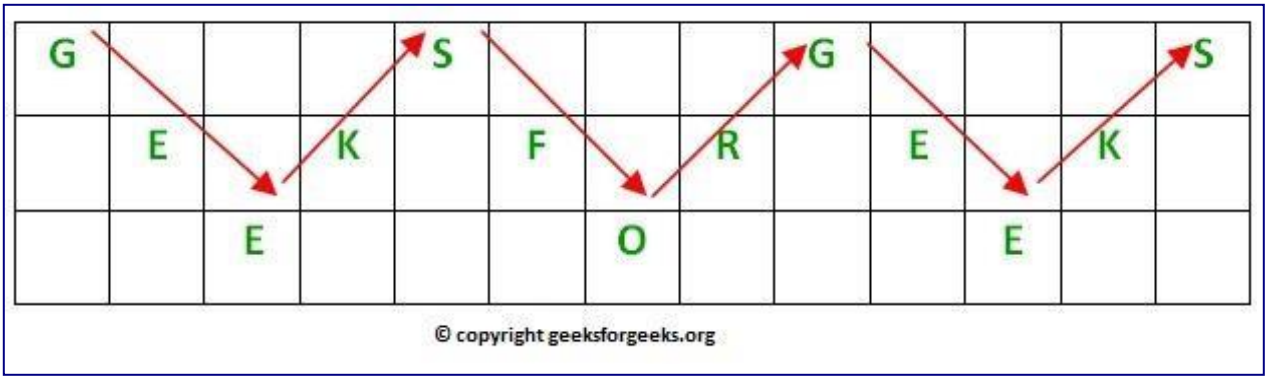
The number of rails used to break up the message serves as the cryptographic key. The rail fence cipher is not very strong, the number of practical keys (the number of rails) is small enough that a cryptanalyst can try them all by hand. Thus, these days you can meet it in games, geocaches, riddles or puzzles. Below you can find two calculators, first can be used to encrypt message with the rail fence cipher, second can be used to crack message encrypted with the rail fence cipher by brute force - it simply outputs decoded message for different number of "rails".

Encryption:

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-szag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

For example, if the message is “GeeksforGeeks” and the number of rails = 3 then cipher is prepared as:



Decryption:

As we’ve seen earlier, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

- Hence, rail matrix can be constructed accordingly. Once we’ve got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.

Implementation:
Let cipher-text = “GsGsekfrek eoe” , and Key = 3

- Number of columns in matrix = len(cipher-text) = 12
- Number of rows = key = 3

The rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached. When the top rail is reached, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows. For example,

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm.

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

Rail Fence Encoding key = 3																			
	T				I				E				T				S			
		H		S		S		S		C		E		M		S		A		E
			I				A				R				E				G	

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

Program Code:

```
#include<stdio.h>
int main()
{
  char str[20]="HelloStudent", str1[10]="", str2[10]="";
  int i, cnt1=0, cnt2=0;
  printf("Rail Fence - Encryption\n\n");
  printf("Plain Text: HelloStudent\n\n");

  for(i=0; i<strlen(str); i++)
  {
    if( i%2 == 0)
    {
      str1[cnt1++]=str[i];
    }
    else
      str2[cnt2++]=str[i];
  }
  printf("Cipher Text: %s%s",str1,str2);
```

```
  return 0;
  getch();
}
```

Output:

Rail Fence - Encryption

Plain Text: HelloStudent

Cipher Text: HlotdnelSuet

Conclusion

We have conclude that how should we perform Encryption and Decryption on Plain Text data using Rail-fence Technique.

Exercise

1. What is Rail-fence Technique?
2. What is Encryption and Decryption?
3. What is purpose of Rail-fence Technique?
4. Write Advantages and Disadvantages of Rail-fence Technique.

Answers

……
……
……
……
……
……
……
……
……
……
……
……
……
……

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Marks obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total(25)**	

Network and Information Security(22620)