School of Computing Science and Engineering

Course Code : BCAS3010

Course Name: Network Security

UNIT I

Introduction: Basic Terminology

GALGOTIAS
UNIVERSITY

Name of the Faculty: Dr. S.Vijayalakshmi

Program Name: BCAS3010

CLASSICAL ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques: substitution and transposition.

Transposition Cipher

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

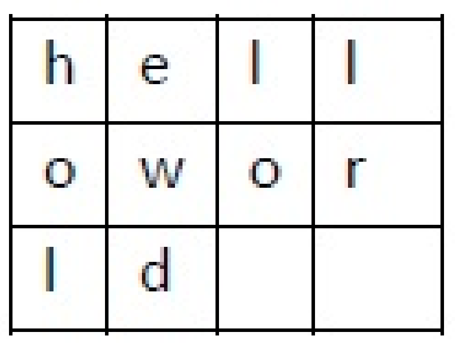
GALGOTIAS UNIVERSITY

Example

A simple example for a transposition cipher is **columnar transposition cipher** where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below

The plain text characters are placed horizontally and the cipher text is created with vertical format as **: holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.



h	e	l	l
o	w	o	r
l	d		

Example

Rail Fence Cipher – Encryption and Decryption

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

Examples:

Encryption

Input : "GeeksforGeeks “ Key = 3 Output : GsGsekfrek eoe

Decryption

Input : GsGsekfrek eoe Key = 3 Output : "GeeksforGeeks “

Encryption

Input : "defend the east wall“ Key = 3 Output : dnhaweedtees alf tl

Decryption

Input : dnhaweedtees alf tl Key = 3 Output : defend the east wall

Encryption

Input : "attack at once“ Key = 2 Output : atc toctaka ne

Decryption

Input : "atc toctaka ne" Key = 2 Output : attack at once

GALGOTIAS UNIVERSITY

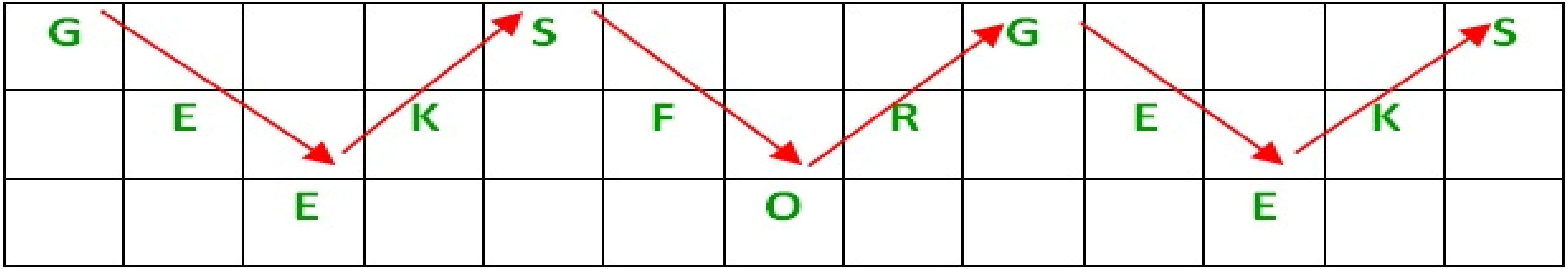
Encryption

- ❑ 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-zag manner
- ❑ After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

GALGOTIAS UNIVERSITY

Example

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



G				S				G				S
	E		K		F		R		E		K	
		E				O				E		

UNIVERSITY

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

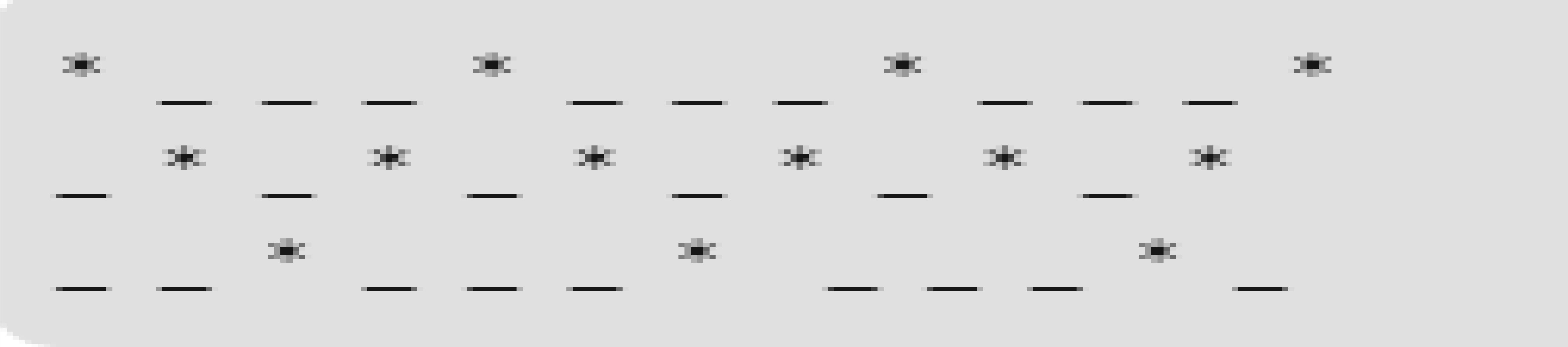
Number of columns in matrix = len(cipher-text) = 12

Number of rows = key = 3

GALGOTIAS UNIVERSITY

Example

- Hence original matrix will be of 3*12 , now marking places with text as ‘*’ we get



*	_	_	_	*	_	_	_	*	_	_	_	*
_	*	_	*	_	*	_	*	_	*	_	*	
_	_	*	_	_	_	*	_	_	_	*	_	

Feistel Cipher model

- ❑ structure or a design used to develop many block ciphers such as DES. Feistel cipher may have invertible, non-invertible and self invertible components in its design. Same encryption as well as decryption algorithm is used. A separate key is used for each round. However same round keys are used for encryption as well as decryption.
- ❑ **Feistel cipher algorithm**

Create a list of all the Plain Text characters.

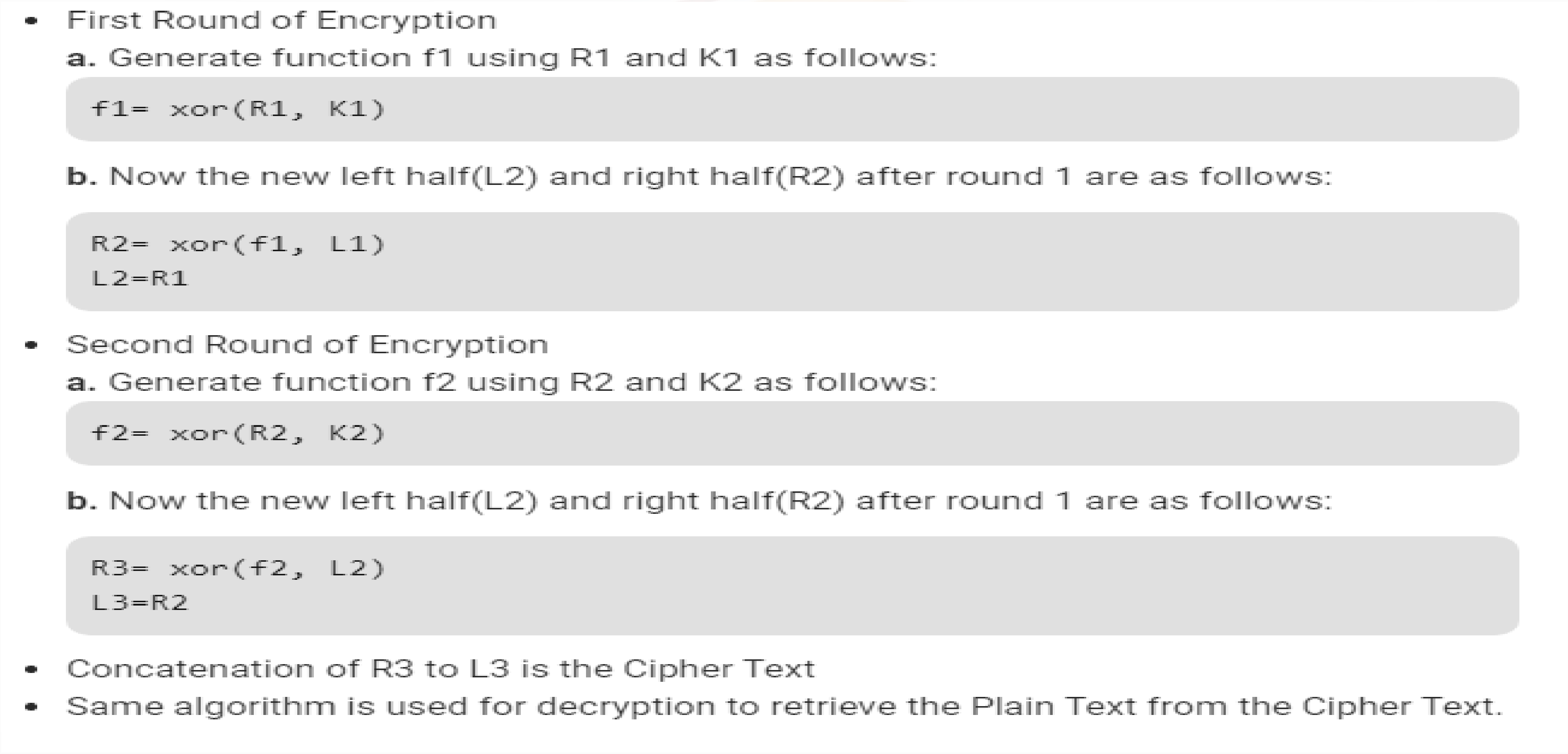
Convert the Plain Text to Ascii and then 8-bit binary format.

Divide the binary Plain Text string into two halves: left half (L1)and right half (R1)

Generate a random binary keys (K1 and K2) of length equal to the half the length of the Plain Text for the two rounds.

GALGOTIAS UNIVERSITY

Algorithm



- First Round of Encryption

  a. Generate function f1 using R1 and K1 as follows:

  ```
  f1= xor(R1, K1)
  ```

  b. Now the new left half(L2) and right half(R2) after round 1 are as follows:

  ```
  R2= xor(f1, L1)
  L2=R1
  ```

- Second Round of Encryption

  a. Generate function f2 using R2 and K2 as follows:

  ```
  f2= xor(R2, K2)
  ```

  b. Now the new left half(L2) and right half(R2) after round 1 are as follows:

  ```
  R3= xor(f2, L2)
  L3=R2
  ```

- Concatenation of R3 to L3 is the Cipher Text
- Same algorithm is used for decryption to retrieve the Plain Text from the Cipher Text.

Example

Examples:

- Plain Text is: Hello
- Cipher Text: E1!w(
- Retrieved Plain Text is: b'Hello’
- Plain Text is: Geeks
- Cipher Text: O;Q
- Retrieved Plain Text is: b'Geeks'

GALGOTIAS UNIVERSITY

Thank You