**Question 1. *Understanding and Using “cryptool” :***

**Task 1: Download and install Cryptool 2 software**

**Cryptool 2:** [**https://www.cryptool.org/en/**](https://www.cryptool.org/en/)

**Task 2: Use Cryptool 2 to answer the following questions “***Use screenshots and description to document your successful result*s”**:**

**a. Perform Hill cipher using the key =**$\left(\begin{matrix}9&14\\13&3\end{matrix}\right)$ **on the text below and write the ciphered text below:**

***“Waiting is painful. Forgetting is painful. But not knowing which to do is the worst kind of suffering”***

***(*“***Use screenshots and description to document your successful result*s”**:*)***

***[Marks: 2]***

**b.** **The following text was encrypted using the Vigenere cipher *with Key=”this”*. Find the plain-text.**

***“Mom kxjzwm vn dbmm, lavcya, pa lh mide zmnxu bafla sgk bg zlb mi lqyaa bafla”***

***(*“***Use screenshots and description to document your successful result*s”**:*)***

***[Marks: 2]***

**Question 2.**

Create a linear feedback shift register with 4 cells in which b4 = b1⊕b0. Show the value of output for 20 transitions (shifts) if the seed is (0001)2



Fill the following table for the 20 states. Initial and first state given for your understanding.

***[Marks: 2]***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| States | b4 | b3 | b2 | b1 | b0 | ki |
| Initial | 1 | 0 | 0 | 0 | 1 |  |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |
| 18 |  |  |  |  |  |  |
| 19 |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |

**Question 3.**

Perform just one round operation of the S-DES for the following 8-bit input.

**Input 🡪 00111001**

Find the output which becomes the input for the next round using the following figure. Show all the steps involved in the diagram.

***[Marks: 2]***

