Fundamentals of Cryptography

Homework 1

**Sepehr Ebadi 9933243**

|  |  |
| --- | --- |
|  |  |

**Question 1**

1. What is the multiplicative inverse of 7 in Z9, Z10, and Z11?

Z9 :

Z10 :

Z11 :

1. What is the multiplicative inverse of 9, 10, and 11 in Z7?

9 :

10 :

11 :

**Question 2**



**Question 3**

In the **affine cipher**, given two pairs of **plaintext-ciphertext**:

By subtracting the two ciphertexts, we have:

This is how **a** is calculated. Then for **b**, we have:

The condition for selecting ​ and ​ ​ is that the inverse of ​ must exist in mod m:

**Question 4**



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | output |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |  |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |  |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |  |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |  |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |  |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |  |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |  |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |  |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |  |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |  |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |  |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |  |

the first 16-bit output based on the table :

**Question 5**

1. What is the initialization vector?

Given that the degree of the LFSR is 3, therfore 3 first bit of key is equal to initial value of LFSR(3 initial bits go out of the LFSR without changing).

**LFSR Initialization Vector = 001**

1. Determine the feedback coefficients of the LFSR.

𝑠2𝑝2+𝑠1𝑝1+𝑠0𝑝0=𝑠3

𝑠3𝑝2+𝑠2𝑝1+𝑠1𝑝0=𝑠4

𝑠4𝑝2+𝑠3𝑝1+𝑠2𝑝0=𝑠5

Now, by substituting the key value (0010111), we find the feedback coefficients:

𝑠0=0 , 𝑠1=0 , 𝑠2=1 ⇒ 1𝑝2+0𝑝1+0𝑝0=0 (𝑠3)

𝑠1=0 , 𝑠2=1 , 𝑠3=0 ⇒ 0𝑝2+1𝑝1+0𝑝0=1 (𝑠4)

𝑠2=1 , 𝑠3=0 , 𝑠4=1 ⇒ 1𝑝2+0𝑝1+1𝑝0=1 (𝑠5)

By solving these 3 equations and 3 unknowns, the feedback coefficients are obtained as:

𝑝0=1 , 𝑝1=1 , 𝑝2=0

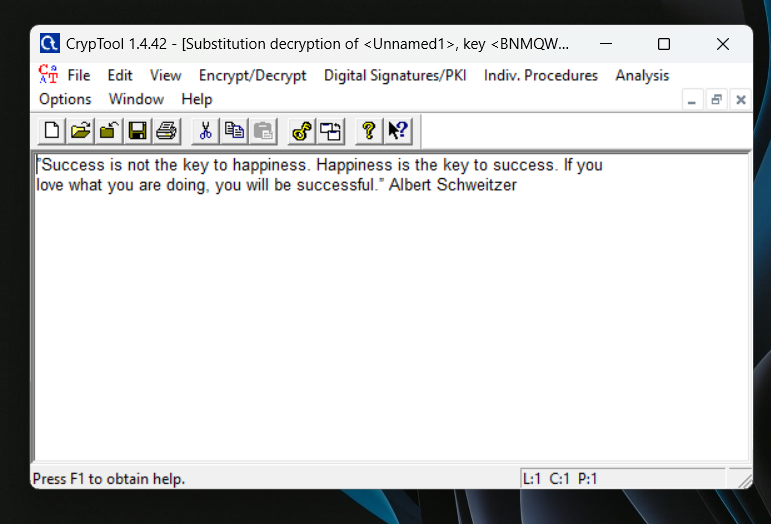
Thus, the LFSR's characteristic polynomial is as follows:

1. Draw a circuit diagram and verify the output sequence of the LFSR.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | output |
| 1 | 0 | 0 |  |
| 0 | 1 | 0 |  |
| 1 | 0 | 1 |  |
| 1 | 1 | 0 |  |
| 1 | 1 | 1 |  |
| 0 | 1 | 1 |  |
| 0 | 0 | 1 |  |

**“CrypTool”**

**Question 6**



**Question 7**

