密碼工程Quiz4

學號:112550090 姓名:曾士珍

Problem1

1. Is a primitive polynomial?

能在GF(2)可以生成最大週期序列的多項式為primitive polynomial

用以下程式碼來實作該多項式的LFSR：

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

|  |
| --- |
|  |
| 由結果可以看出週期為255(為8個位元時可以產生的最大週期數)，在第256組時回到跟第1組一樣的狀況 |

由執行結果可以得出為primitive polynomial

1. What is the maximum cycle length generated by ?

多項式的最高次方項係數是8(代表LFSR 的寄存器有8個位元)且是primitive polynomial，因此可以生成的序列的最大週期長度為

1. Are all irreducible polynomials primitive polynomials?

不是，所有的primitive polynomials都是不可約的，但反之不一定成立。

反例：不可被因式分解

|  |  |
| --- | --- |
|  |  |
| LFSR過程程式碼 | 週期僅為21 |

5個位元時可以產生的最大週期數應為，故irreducible polynomials不一定是primitive polynomials

Problem2

1. Please use as a characteristic polynomial to write a Python program to encrypt the following plaintext message with the initial key 00000001, then decrypt it to see if your encryption is correct.

|  |
| --- |
| Encrypted text: 0100000001010110010010100101000101010011011101010001011111000101010111000110100000110001101110111001100111010101010110100111000000000101110101100110101000001110111110110011011110101111100010001100100001010001010000110100110101001100011001010010111010001001110010110110001000011100110011110110110000011110110011010110000100100010100101011110000100100011101111001000000011010001011100000000010111001001010010110100111001000111011011000001100111110011000111101111001100111001100111101111000000100001100111111111001100000110111110100010100010010100110100000110101100011011111011110011000110000101110110100100000001010010011010100011110110100100101101011010001010011010111101010010100010000100111101000011111010101101101010001001000111100100000101111110111100110010101011011001010011111111000011111100001101001001011100100001011011000111010011110101011001110001001001011000001111101001001011111000111111010101010010110111011000111001101011111010001010010101110111110111111100110000101011011000011011010010011000000011000110001001110100100101111001100010000100001111101100100010100101001111110100000110110100000111010000000111110100000101101001101000000100011110111100011000110100110110110100010111111000000001011111110011000111011101101001111100001110111010000010010000111101100010011110101110100100001110101100110100100000111101001001111110001100001011110110100110100111111111101000111110101000001011010010101100101011001001011011101110000111111101111001111000001011001000001111011000011000100010110110010100111000100000010111101011000000001101011001011100011000000011000010000111110010100100001001011010010101000111110100100010101101001001010111100110000111011111000100010100111000010001100011111100001100001011110010111101101001101001010111010010011011110000001111101101000010011100011001010000010100110110001000011100110101010110111100111011101110001011100110100011101110111011101010111111100111001100101001011000010000100110010000011101111110010011100110111111101010001001101111001011010110100110001000100000100111011110100100010011110000010101010101001010010000010100101101000010011001010000000111010100010101000111010100111010101001111000101111001000010001100111010000011001110101100110010000001100111100010010011110111001100000001101101101011010010011110100001001001100011110000010010110000110110101000111010100011101110010000111010100000110110101010111011000101111 |
| Decrypted text: ATNYCUWEARESTRIVINGTOBEAGREATUNIVERSITYTHATTRANSCENDSDISCIPLINARYDIVIDESTOSOLVETHEINCREASINGLYCOMPLEXPROBLEMSTHATTHEWORLDFACESWEWILLCONTINUETOBEGUIDEDBYTHEIDEATHATWECANACHIEVESOMETHINGMUCHGREATERTOGETHERTHANWECANINDIVIDUALLYAFTERALLTHATWASTHEIDEATHATLEDTOTHECREATIONOFOURUNIVERSITYINTHEFIRSTPLACE |

1. Due to the property of ASCII coding the ASCII A to Z, the MSB of each byte will be zero (left most bit); therefore, every 8 bits will reveal 1 bit of random number (i.e. keystream); if it is possible to find out the characteristic polynomial of a system by solving of linear equations?

可以，以4-stage的LFSR，我們可以列出以下等式：

一張含有 文字, 字型, 白色, 書法 的圖片

自動產生的描述

若可以知道一組的值，便可以計算出的值

更一般化的來說，若能知到2n個output bits的值，就可以解出n-stage的LFSR

1. **Extra credit:** Write a linear equations program solving program to find the charac teristic polynomial for this encryption with initial 00000001.

枚舉所有可能的，再將已知的代入b)的方程組確認，程式碼如下圖：

|  |  |
| --- | --- |
| 程式碼 | output |
| 一張含有 文字, 螢幕擷取畫面, 字型 的圖片  自動產生的描述 |  |

Problem3

1. Please write a Python program to simulate two algorithms with a set of 4 cards, shuffling each a million times. Collect the count of all combinations and output.

|  |  |
| --- | --- |
| 一張含有 文字, 螢幕擷取畫面, 功能表, 字型 的圖片  自動產生的描述 |  |

1. Based on your analysis, which one is better, why?

Fisher-Yates Shuffle Algorithm較好。

1. 由standard deviation可以看出，其相較於Naïve Shuffle Algorithm有更均匀分布的洗牌结果。
2. 由上圖程式跑1000000次的執行時間可以看出，其相較於Naïve Shuffle Algorithm更有執行效率較高。

c) What are the drawbacks of the other one, and what causes these drawbacks?

Naïve Shuffle Algorithm在選擇位置時沒有進行有效的隨機化，僅僅是在每次迭代中隨機選擇一個位置，而未考慮已經選擇過的位置或者已經移動過的元素，這可能導致某些元素被過度集中或遺漏，從而影響洗牌結果的均勻性和隨機性。