Quiz 5

- To break an ASCII code plaintext phase encrypted by a 8 bit LSFR with XOR operation.
- **Cue:**
- Since standard ASCII represent 128 characters. It uses 7 bits to represent each character, therefore, the first bit of each byte (8bit) is always 0.
- For instance, a capital "T" is represented by 84, or 01010100 in binary. A lowercase "t" is represented by 116 or 01110100 in binary.
- And so a random bit of LSFR will comprised every at the first bit of each encrypted bytes.
- Use these compromised random bits to construct linear equations to break this encrypted messages and then you can see the plaintext.

1. The sequence was generated by $x^8 + x + 1$ or $x^8 + x^4 + x^3 + x^2 + 1$
2. Find the initial fill 8 bit seed key.
3. Does this LFSR produce a maximal length linear recursive sequence?

Encrypted bit streams as below:

11000111 11001110 11000110 11010100 11001001
11001111 11101111 10110000 01010100 01010001
01000010 01011101 01010000 01110000 00011100
10110001 01010111 01010101 01011011 01001011
01100111 00100011 11100101

Please recovery to a ASCII phase!