Selin Eyupoglu 21090

CS 411 HOMEWORK 3

1. Period is 7. Since it does not visit all states and thus give the maximum period which is 2^6-1=63, this polynomial can't be primitive.

Here is the first period with the given seed:
seed = 100000
1. 010000
2. 001000
3. 000100
4. 000010
5. 000001
6. 100000

2. Length of the shortest LFSR is 11.
Connection polynomial is : [1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1]
So, $1+x^3+x^5+x^7+x^{11}$ is the connection polynomial that generates the binary sequence.

3. Decrypted message is the following text:

Dear Student,
You have just earned 40 points. Congrats!
Best,
Erkay Savas

Connection polynomial = [1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1] which correspond to $x^{11} + x^9 + 1$

4. a. I performed the necessary multiplication and reduced it in GF(2^8) (divided by p(x)) to $x^7 + x^6 + x^4 + x^3 +1$.

b. When the necessary multiplication is done and the resulting polynomial is reduced in GF(2^8)), the remainder is 1. Which means that their multiplication results in 1 in GF(2^8), thus the polynomials are inverse of each other.

5.
If ShiftRow is removed, then attacker can treat input block(128 bits) as 4 independent 32 bits block. Hence attacker can attack these 4 blocks one by one to recover the key. If MixColumn is removed, then attacker can treat input block(128 bits) as 16 independent 8 bits. If both of the layers are removed, bytes become independent of each other, in other words, every byte of the ciphertext would not depend on every other byte of the plaintext, but only on the one byte at the same position. Hence, attacker can attack these 16 blocks seperately.
Now in order to attack the cipher, one should find a way to figure out the key schedule. Since key addition layer is becomes a trivial operation, we should focus on Byte Substitution layer. If we give the plaintext as aaaaaa.. or bbbbbb… then the key schedule would be observable from the patterns in the ciphertext. Also, by looking at the elements in the ciphertext in one pattern, one can observe

the the elements of the lookup table which has 256 entries (which is used in the byte substitution layer).

*Corresponding python codes are named such as question_no.py.