CS 411-507 Cryptography

Homework #3

Yigit Kaan Tonkaz

29154

1)

2)

3)

Nonlinearity degree: Due to the XOR operations, we can say that function is highly nonlinear. The highest order of the terms in the function is 4. Therefore, we can say that nonlinearity degree is equal to 4.

Balance:

X1 = 0000000011111111

X2 = 0000111100001111

X3 = 0011001100110011

X4 = 0101010101010101

F(x1,x2,x3,x4) = 0100010101010100

Number of 0s = 10

Number of 1s = 6

Therefore, it is not balanced because the number of 0s and 1s is not equal.

Correlation:

For correlation -> number of times F and xi are equal/ number of 0s^1/2 \*number of 1s^1/2

For x1 = 8/ √10 \* √6 = 1.03

For x2 = 8/ √10 \* √6 = 1.03

For x3 = 6/ √10 \* √6 = 0.77

For x4 = 14/ √10 \* √6 = 1.8

Therefore, x4 has strong correlation compared to others and x3 weaker. But they all correlated to the output of function.

4)Yes we can, to find the plaintext from ciphertext C, we can use factorize to find prime factors of n. We do not know the private key so we cannot factoring directly in an easy way. We need to try for it and it takes some time. I could not find the prime factors of N without using of online tools but when it is found, plaintext could be find easily.

5)Since p(x) = x8+x7+x6+x+1, its bit sequence is 111000011

N = 8

I write the code for this question in q5.py

6)