Assignment 2

1. Find the elements of the Galois field of (2^4) Let's assume,

$$A(x) = x^3 + x^2 + 1$$
$$B(x) = x^2 + x + 1$$

   Calculate,
   a. A(x) + B(x)
   b. A(x) * B(x)

2. This question is about the Key
   Schedule of AES algorithm.
   Let's assume the initial key is: **4A C6 9E 45** and the Round constant is **00 01 10 11.**
   You need to use the S-box of AES.

   Find the key for the next round.

3. Knapsack Problem.
   Let {2, 3, 6, 13, 27, 52} be the SIK
   Choose m = 31 and n = 105
   Encrypt 100100
   Also, show the decryption part.

4. An RSA encryption scheme has the set-up parameters p = 31 and q = 37. The value of e = 17.
   Encrypt the plaintext M = 2 and show that after decryption you got the same value.