Assignment-1

Rachit Parikh (CRS-2101)

Cryptology

Disclaimer : I declare that all the work presented in this assignment is my own work and I have only consulted the internet when it was absolutely necessary.

Q-1 : Watch "The Imitation Game"

I have already seen this movie twice.

Q-2 : Write C program to find primitive polynomials over $GF(2)$ for $n = \{4, \ldots, 12\}$

Click here to get the code.

Q-3 : Write C program to implement Stream Cipher

Click here to get the code.

Q-4 : Understand Berlekamp-Massey algorithm

Q-5 : Understand more about Non-linear feedback shift registers