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 $n = \{4, \ldots, 16\}$

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

Algorithm to find linear complexity of a finite sequence and feedback polynomial of LFSR of minimal length which generates this sequence. It also states an important result that the LFSR of length L which generates the sequence is unique iff $n \geq 2L$. I have also read about the algorithm and its proof from here.

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

The feedback bit is computed from a non-linear function of previous bits. An algorithm is known to generate the shortest (NL)FSR in linear time. Its application is in COS(vd) ciphers.