CSE, MNIT Jaipur
Advanced Cryptography(CST-701)
Time:60 Min (20/12/2020)

2020-21
M-Tech, I Sem
Total Marks:60

End Term Examination, Part-II

1 **[10+10 points]**

(a) Assume a 6-degree LFSR with c0 = c5 = 1 and c1 = c2 = c3 = c4 = 0. Identify whether the given LFSR is a maximal PFSR or not?

(b) Prove or disprove that Vigeneere cipher is a perfect cipher.

2 **[8+8 points]** Answer the followings:-

(a) Assume we have a PRG, G(s) such that s belongs to set $\{0,1\}^n$. Then identify whether $G(s') = G(s)||s$ will be a secure PRG or not.

(b) Given a secure PRF $F_k(x)$, the construction $G(k1;k2)(x) = F_{k1}(x) \oplus F_{k2}(x)$ is a secure PRF.

3 **[10+10 points]** Write the followings:-

(a) Difference between confusion and diffusion

(b) Difference between the indistinguishablity based definition of COA and CPA based security

4 **[2+2 points]** Write about any topic of the course which you liked and the one which you did not find interesting.