Practice Problems-2: Foundations of Cryptography (Course No: CS60088)

Attempt All Questions

1. Let R, S and B are jointly distributed random variables with values in $\{0, 1\}$. Assume that B and S are independent, and that B is uniformly distributed. Prove that:

$$Pr[R = S] = \frac{1}{2} + Pr[R = B|S = B) - Pr[R = B]$$

2. Show that the existence of one-way functions implies $\mathcal{P} \neq \mathcal{NP}$.

3. Assume that $\mathcal{P} \neq \mathcal{NP}$. Show that there exists a function f that is computable in polynomial time, hard to invert in the *worst case*, but is not one-way.

4. Show that if a one-one function has a hard-core predicate, then it is a one-way function.