

Find the pdf file corresponding to your roll number in the directory <https://www.ee.iitb.ac.in/~sarva/courses/EE720/2018/assignments/assignment2/>. Upload the answers as a **pdf** file in Moodle. Use the tex file provided in the directory to fill in your answers. The **upload deadline** will be 11:00pm IST on Wednesday, January 31, 2018.

1. [5 points] Consider a variant of the one-time pad with message space  $=\{0,1\}^l$  and keyspace  $\mathcal{K}$  restricted to all  $l$ -bit strings with an even number of 1's. Is this scheme perfectly secret? Justify your answer either with a proof or a counterexample.

**Solution:** Write your answer here

2. [5 points] Let  $\text{negl}_1$  and  $\text{negl}_2$  be negligible functions. Prove that the function  $\text{negl}_3$  defined by  $\text{negl}_3(n) = \text{negl}_1(n) + \text{negl}_2(n)$  is negligible.

**Solution:** Write your answer here