

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] Prove that the Vigenère cipher using period  $t$  is perfectly indistinguishable when used to encrypt messages of length  $t$ . Prove this directly without proving the perfect secrecy of the scheme and then using the equivalence of perfect secrecy and perfect indistinguishability.

**Solution:** Write your answer here

2. [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