

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] When the one-time pad is used with the all-zeros key, i.e. $k = 0^l$, we have $\text{Enc}_k(m) = m \oplus k = m$. This means that the plaintext will be sent as it is. To prevent this, suppose we modify the one-time pad to use only non-zero keys, $k \neq 0^l$. The key generation algorithm **Gen** picks key k uniformly from the set $\{0,1\}^l \setminus \{0^l\}$ which has cardinality $2^l - 1$. Is this modified scheme still perfectly secret? Justify your answer either with a proof or a counterexample.

Solution: Write your answer here