# Practice Question Solutions

Q1 Ans:- Given in class notes

Q2 Ans:- One attack is padding the encrypted message with p i.e, $(c = m \text{ XOR } k)$ XOR $p$, which will be encrypted to $m$ XOR $p$.

Thus the message is modified by the adversary.

Q3 Ans:- Since we are discussing perfect secrecy the best way to answer is to write in terms of the likelihood of ~~the~~ a message 'm' changing before seeing 'c' and after seeing 'c'.

Here we should say that basically seeing the ciphertext does not affect the likelihood of m, since it is only the first two bits that we recover which has nothing to do with 'm'.

Q4 Ans:- Since we are discussing perfect secrecy the best way to answer is to write in terms of the likelihood of a message m changing before seeing 'c' and after seeing 'c'. Here we should say that basically seeing 'c' affects the likelihood of the message.

More specifically, 'c' can only be the output of the ~~message~~ encryption of a message where the middle $(k+1)^{th}$ bit of c and the message are complements.

So for a mesage m, with $(k+1)^{th}$ bit same as c, probability before seeing 'c', $\Pr[M=m] > 0$ and after seeing c, $\Pr[M=m \mid C=c] = 0$. Hence not perfectly secure. OR (you can use Shannon's theorem and say key length is shorter than msg length.)