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

Attempt All Questions

1. Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space M, every $m, m' \in M$, and every $c \in C$:

$$Pr[M = m|C = c] = Pr[M = m'|C = c]$$

2. When using the one-time pad (Vernam's cipher) with the key $k = 0^l$, it follows that $Enc_k(m) = k \oplus m = m$, and the message is transferred in the clear! A suggestion to improve the situation is encrypt using only the nonzero keys, ie. $k \neq 0^l$. Thus the Gen function chooses k uniformly at random from the set of non-zero keys of length l. Argue for or against the suggestion, in the context of perfect secrecy.
3. Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is uniformly chosen from the key space, is perfectly secret.
4. Consider an encryption scheme which is the set of all permutations on M, denoted by K. Let the key generation algorithm Gen choose a random permutation from K. Enc is performed by computing the chosen permutation on the plaintext, while Dec is performed by performing the inverse permutation. For all distributions over M, all $m, m' \in M$ with $m \neq m'$, and all $c, c' \in C$ with $c \neq c'$ and $Pr[C = c \wedge C' = c'$, compute the following for the cipher:
   (a) $Pr[C = c \wedge C' = c'|M = m \wedge M' = m']$
   (b) Compute $Pr[C = c \wedge C' = c']$
   Hence prove that for this encryption scheme the following holds:

$$Pr[M = m \wedge M' = m'|C = c \wedge C' = c'] = Pr[M = m \wedge M' = m'|M \neq M']$$