Problem Set 3

Problem 1.

For every PPT Algorithmthere exists a probabilistic polynomial-time algorithmsuch that for all efficiently sampleable distributions  and all polynomial time computable functions and there exists a negligible function that accepts a security parameter*.*





Where is chosen according to the distribution of  and the probability is computed over the message space and the key space , and any random coins used by *,* and *.*

Problem 2.

Let  be a private-key encryption scheme that has computationally indistinguishable encryptions in the presence of eavesdropper such that for all probabilistic polynomial-time adversaries there exists a negligible function such that:



Whereis chosen uniformly from, and the probability is taken over the random coins ofrandom by the adversary selects two messages of different lengths.

**Proof:** The idea behind the proof of this claim is that if it is possible to guess the *i*th bit of *m* given , then it is also possible to distinguish between encryptions of plaintext messages  and 