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 of, the choice of , and the key , and any random coins used in the encryption process.

**Proof:** If there exists an adversary  that can guess the *i’th* bit of given  with probability at least  for some function , then there exists an adversary that succeeds in the indistinguishability experiment for  with probability . If has indistinguishable encryptions, then  must be negligible.

Let be a probabilistic polynomial-time adversary and define  as follows:



Where *m* is chosen uniformly from. Assume input of  to . Take , let  be the set of all strings of length *n* whose *i’th* bit is 0, and let  be the set of all strings of length *n* whose bit is 1. It follows that:



Where *m* is chosen uniformly from  and  is chose uniformly from . (The above holds because  and  each contains exactly half of . Therefore, the probability that *m* lies in each set is exactly ½.)

An adversary A is given input  and outputs a pair of messages 