Exercise 4 – Foundations of Cryptography 89-856

Due Date: 16th June 2019

Exercise 1: Formally prove that the zero-knowledge proof for Hamiltonicity (from the previous exercise) is a *proof of knowledge* with knowledge error 1/2. Prove that if you run the proof n times sequentially, then the result is a proof of knowledge with knowledge error 2^{-n}.

Exercise 2: Consider an experiment in which the adversary outputs two vectors of plaintexts of length $t(n)$. Then, $t(n)$ independently chosen keys are used to encrypt the challenge ciphertext; the i plaintext in the chosen vector is encrypted with the i key. Formally define security for an eavesdropping adversary (use the indistinguishability formalization). Does security for a single encryption imply security under this definition? Prove or refute in both the private-key and public-key settings.

Exercise 3: Prove that the existence of secure private-key encryption schemes (for eavesdropping adversaries) implies the existence of one-way functions. (Be careful, since the one-time pad is secure and yet does not imply one-way functions.)