HIT — Cryptography — Homework 2

September 4, 2014

Problem 1. Prove that the indistinguishable encryptions in the presence of an eavesdropper cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is not restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$.

Problem 2. Assuming the existence of a pseudorandom function, prove that there exists an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper, but is not CPA-secure. Hint: You will need to use the fact that in a CPA the adversary can choose its queries to the encryption oracle adaptively (i.e., new query may be constructed from previous queries).

Problem 3. Present a construction of a variable output-length pseudorandom generator from any pseudorandom function. Prove that your construction is PRG.

Problem 4. Present formulas for decryption of all the different modes of operation for encryption: ECB, CBC, OFB, CRT. For which modes can decryption be parallelized?

Problem 5. Show that the CBC, OFB and CRT modes do not yield CCA-secure encryption schemes (regardless of F).