ECS 227 — Modern Cryptography — Spring 2010

Phillip Rogaway

Out: Tuesday, 4 May 2010.
Due: Wednesday, beginning of class, 12 May 2010

7. In our symbolic treatment of encryption we did not distinguish the length of undecryptable ciphertexts; all such expression parts were mapped to the pattern $\square$. To match this convention, our computational treatment of encryption had to assume that encryption was length-concealing. Describe an alternative method of mapping expressions to patterns such such that, at least plausibly, the computational treatment will correspond to the more customary assumption of length-revealing encryption.

8. Formalize and prove that authenticated encryption (our $\mathbf{Adv}^{\mathrm{ae}}_{\Pi}(A)$ notion of security) implies indistinguishability under an adaptive chosen ciphertext attack (our $\mathbf{Adv}^{\mathrm{cca}}_{\Pi}(A)$ notion).