Foundations of Cryptography

Homework Set No. 6

Date Due: Dec 25th 2003

1. Show how to construct from a signature scheme that is existentially unforgeable against *random* message attacks a signature scheme that is existentially unforgeable against *adaptively chosen* message attacks

Hint: use two schemes of the first type