Foundations of Cryptography

Homework Set No. 4

Date Due: Dec 4th 2003

1. Based on what we have seen in class, suggest the best one-time authentication scheme. That is given ε and n, what is the number of shared secret bits bits needed to authenticate an n-bit message where the adversary has probability of at most ε of cheating.

2. Many-time probabilistic authentication: a) Suggest a definition to the k-time authentication problem b)Suggest a solution to the problem.

3. Bonus question: Can making the solution to the one-time authentication problem interactive help? Can the number of shared secret bits be smaller than in a unidirectional scheme? Can the number of shared bits depend on ε only?