CSE 484 In-Class Worksheet #16 – Autumn 2010

Name: _____ UWNetID: _____ Date: _____

Email address: _____

Partner names for this activity: _____

Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: Suppose you are creating a new website, and you expect millions of users. How will you store those user's usernames and passwords, so that users can authenticate later but an adversary who breaks into your computers and steals all your data can't easily figure out everyone's password?

Q2: What problem, if any, do you see with the "Encrypt-and-MAC" approach for authenticated encryption?