UCL Department of Computer Science
CS M038/GZ06: Mobile and Cloud Computing
Spring 2014
Kyle Jamieson and Brad Karp

One-pager: Mylar (Popa *et al.*, 2010) **Due: Start of lecture, 19th March 2014**

Instructions: ***in your own words,*** *answer the following questions as* ***succinctly*** *as possible (in 200–500 words total, but shorter answers within this range are encouraged). Quoting figures or text from the assigned reading or from any other source is specifically prohibited.*

Suppose that Alice uses a web application built with Mylar, and wishes to make an encrypted document available to ten other users. At some point she decides that she no longer trusts just one of those ten other users, and wishes to remove that one user from the list of users able to obtain the cleartext for that encrypted document. What steps in the Mylar system must Alice take in order to achieve this change in the access control to the encrypted document? Is there a way for Alice to keep the document encrypted with the same private key as before, but be certain that the one user she no longer trusts will thereafter no longer be able to access that document's contents? If so, how? If not, what must Alice do instead to achieve this result?