Objective:
Design a protocol to solve an e-commerce problem.

What to do:
The IRS is relying more and more heavily on electronic filing of taxes. Consider the following hypothetical situation:

Imagine that everyone in the US files their taxes electronically. This puts an enormous load on the upload sites on the tax deadline day, April 14. Millions of users are trying to upload their returns to the same set of servers at the same time. The rest of the year, the servers are barely used, representing a huge wasted resource.

To solve this problem, the IRS needs a protocol for delayed uploading of tax returns. This will spread the peak load out over a longer period and allow them to get by with fewer upload servers. This protocol must satisfy the following criteria:

- A fixed time is set after which returns must be generated. Returns filed more than a week before the deadline are not a problem.
- Returns need not be uploaded by the deadline: they can be uploaded over a period of several weeks afterward.
- Users should not be able to modify their return after the deadline, even if it has not yet been uploaded. This is the key requirement.
- Returns are large documents, on the order of 10 MB, as tax laws get more complicated.
- You may assume that the IRS and all taxpayer have public key certificates.

Describe a protocol that would solve this problem. Make sure that your answer describes all cryptographic operations to be used, the kinds of services that need to be available, and the steps involved.

What to turn in:
Write a description of your protocol as a Word document and submit it to the COL site.