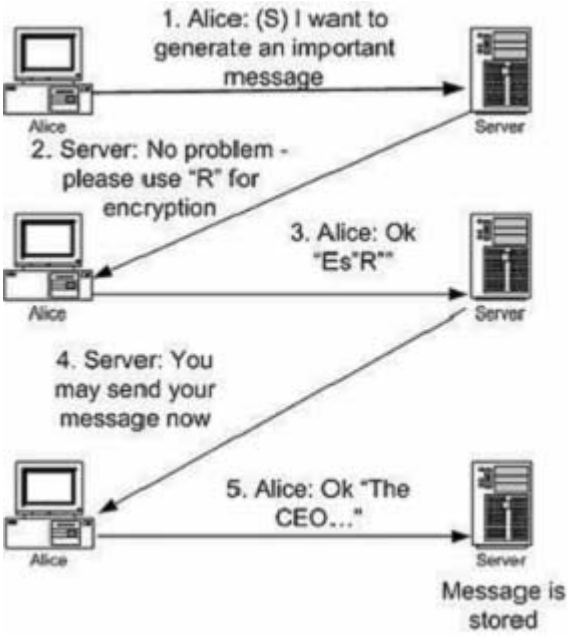
Assignment 1

Due Week 3 at the start of class

1) Why are timestamps used in the Kerberos protocol (see page 27)?

2) Assume that Alice shares a secret *s* with her company's server computer. When Alice is on a trip, she tries to store an important message in the CEO's account directory. This message needn't be encrypted since confidentiality is not important here, but the CEO needs to be guaranteed that the message really is from someone who knows the secret *s* (e.g. Alice) when the CEO opens his/her computer the next day. A naïve protocol to achieve this may look like this:

Alice-->Server: "This is Alice, I have an important message to forward to the CEO"
Server-->Alice: "OK, please encrypt R" (where R is a random nonce)
Alice-->Server: "Es(R)" (that is, R is encrypted with the secret *s*)
Server-->Alice: "Please send the message"
Alice-->Server: "The CEO needs to attend a meeting in Liverpool on May 1, 2003"



The server stores this message in the CEO's directory. Is this protocol secure? If not, how do you feel it could be modified to make it so?

3) Design an algorithm to achieve the Byzantine Agreement for the case that there are four processes, amongst which one is corrupted. You may use some of the on-line help programs available such as http://disappearing-inc.com/B/protocols/byzag1.html

4) An increasingly common mechanism is to ask for several pieces of security information rather than one. A call center might ask not just for your mother's maiden name, a password, and the amount of your last purchase, but also your dog's nickname and your favorite color. Such schemes need careful evaluation of their usability and effectiveness using the tools of applied psychology. Design such a password protocol and evaluate its usability and effectiveness. (A verbal text description is enough.)

5) Analyze one of the commonly used password management protocol (e.g., Microsoft Outlook password management), what is the weakness of this protocol?