CISC 367 – Spring 2016

Homework Assignment – Secure Email

1. Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K_B^+, K_B^-), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H($\cdot$).

   (a) In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, diagram your design to show how.

   (b) Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, diagram your design to show how.