



Note that  $K_{AB}$  is a shared symmetric key used only for mutual authentication.

1. Find 2 attacks Trudy can use to convince Bob that she is really Alice.
2. Fix this protocol so that it is secure.