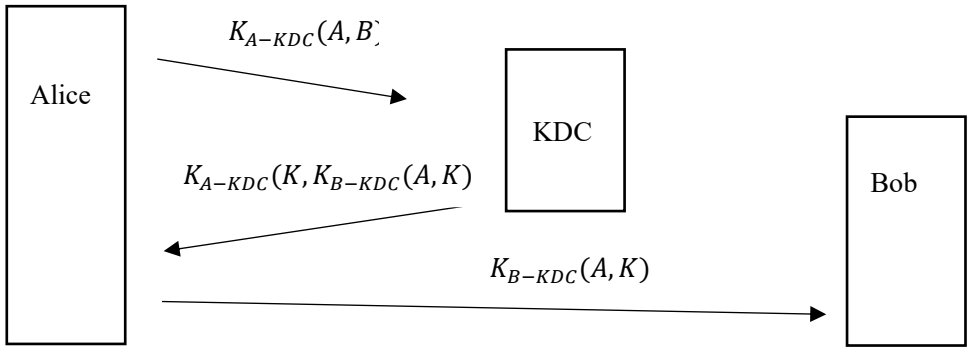
Rusu Wu
11694764
Assignment 8
CptS455

1.



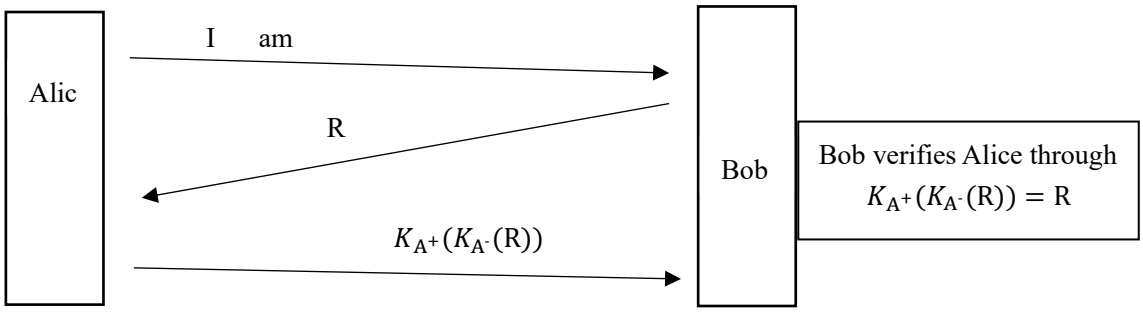
a) The second message is $K_{A-KDC}(K, K_{B-KDC}(A, K)$

b) The third message is $K_{B-KDC}(A, K)$

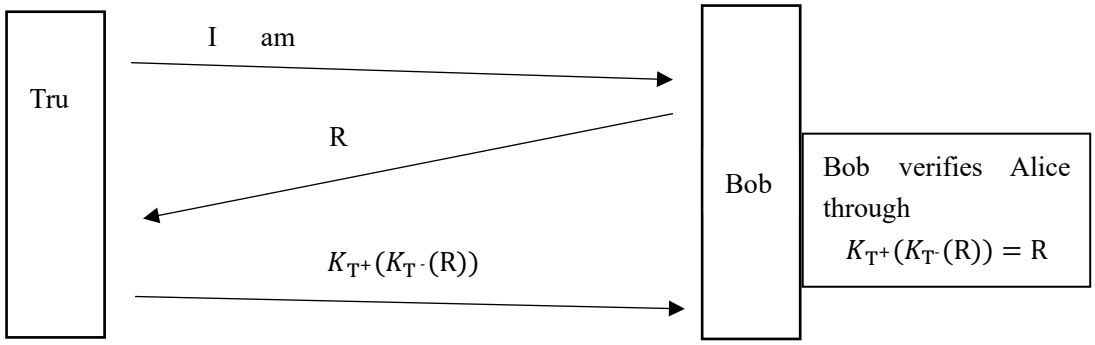
2. Using digital signatures means that it needs to have an authorized Public Key Infrastructure. However, since all the routers for OSPF are in the same address domain, OSPF can easily distribute symmetric key to each router without using Public Key Infrastructure. Therefore, a MAC enough, and it is unnecessary to apply digital signatures.

3.

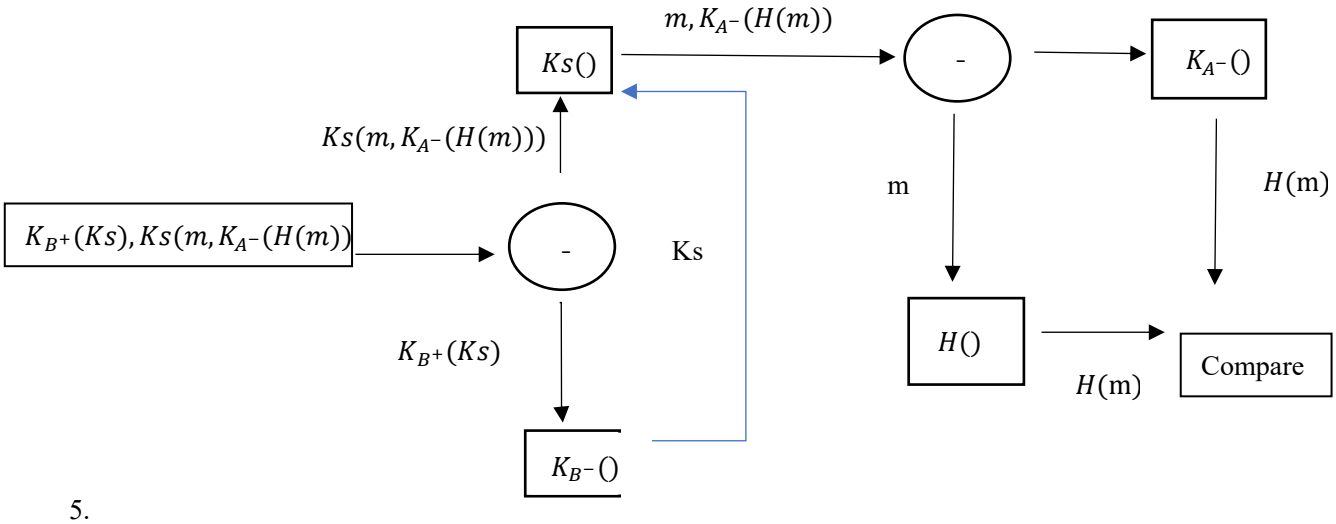
(a)



b)



4.



5.

a) No, if Alice do not have a public key, Bob can not verify that the message is created by Alice. Hence, it is not possible to design that scheme.

b) Yes, although Bob can not verify that the message is from Alice, Alice can still send a message that only can be identify by Bob; Alice can encrypt the message with Bob's Public key and send it to Bob.