Exercise 6 Feedback

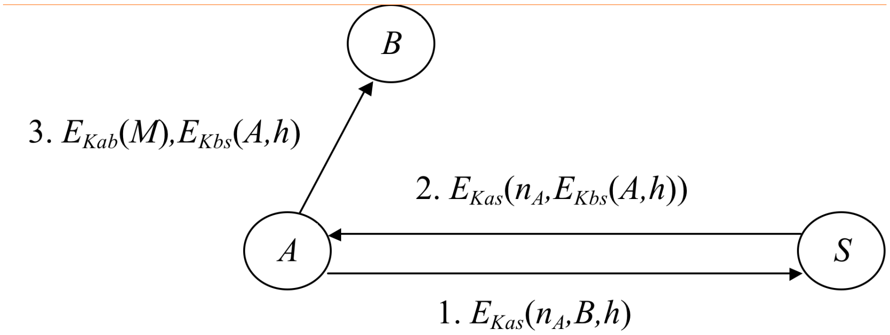
Q6(b):

(i) Design a digital signature protocol using symmetric encryption and an arbiter, but do not expose the content of a message to be signed to the arbiter.

(ii) Compare the signature protocol designed in (i) with the RSA based signature scheme.

Answers to 6(b):

(i) Suppose that a party *A* wants to send a message *M*, signed by *A* through an arbiter *S*, to another party *B*, and that *A* and *B* share a key k_{AB}. A protocol design is shown below where *h* is a hash value of *M* computed by *A*, i.e. *h* = H(*M*); it is assumed that M is timestamped (or dated).


B
3. $E_{Kab}(M), E_{Kbs}(A,h)$
2. $E_{Kas}(n_A, E_{Kbs}(A,h))$
A
S
1. $E_{Kas}(n_A, B, h)$

(ii) The main differences between the two schemes are:

- The RSA signature scheme only requires an off-line trusted third party (TTP), whereas this one requires an on-line TTP;
- With the RSA scheme, the signer experiences more computational cost, but less communicational costs, than the symmetric scheme.
- The RSA scheme does not require a shared secret, rather the signer needs to have a key pair, and the signature verification key must be certified by a trustworthy CA, whereas the above signature protocol requires a method for symmetric key distribution.