Feedback on Topic 6 Ex

Exercise Question – E6.1(i)

(i) Discuss, at the generic level, what are the factors that impact on the security of a digital signature.

Exercise Question – E6.1(i) - A

- Discuss, at the generic level, what are the factors that impact on the security of a digital signature.

Factors	Justifications
Security of the signature algorithm	If not, signature keys may be inferred.
Whether the signature signing key is secret	Otherwise, the origin of a signature may not be assured.
Whether the signature verification key is trust-worthy	Otherwise, the origin of a signature may not be assured.
The security of the hash function used	If a hash function is not weak-collision resistant, then the signature is vulnerable to selective forgery; if a hash function is not strong-collision resistant, then the signature is vulnerable to existential forgery.
Whether the source of time is tamper-proof and multiple sources are synchronised	If not, the integrity of the signature cannot be assured.

Exercise Question – E6.1(ii)

(ii) Assuming that the RSA algorithm is used for signature signing, identify all possible ways of forging a signature.

Exercise Question – E6.1(ii) - A

- **Use a signature signing key (private key) with a decent length.**
- **Use a secure/strong hash function.**
- **Timing sources tamper-proof and synchronised, or include a random number (nonce) contributed by the verifier in the signature.**
- **Obtain someone else's private signature key**
  - In a digital signature scheme "you are your private key".
- **Persuade others that someone else's public verification key belongs to you.**

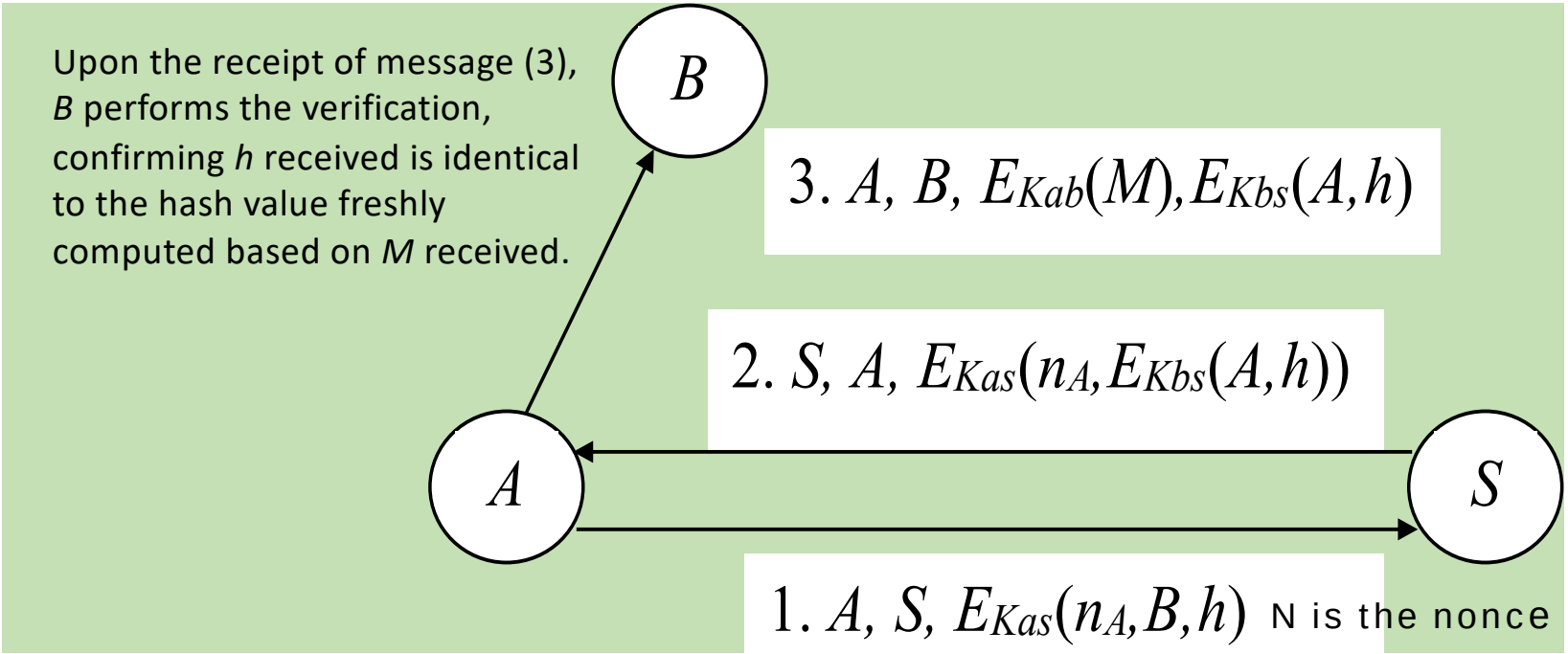
Exercise Question – E6.2(i)

A digital signature scheme may also be implemented using a symmetric-key cipher, but with the assistance of a trusted third party, an Arbitrator.

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

Exercise Question – E6.2(i) - A

Assuming that a party *A* wants to send a message *M*, signed by *A* through an arbitrator *S*, to another party *B*, and that *A* and *B* share a key k_{AB}. It is also assumed that the message M is timestamped (i.e. dated). One variant of the protocol is shown below where *h* is a hash value of *M* computed by *A*, i.e. *h* = H(*M*).



Exercise Question – E6.2(ii)

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

Exercise Question – E6.2(ii) - A

The main difference 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.
- 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.
- With the RSA scheme, the signer experiences more computational cost, but less communicational costs, than the symmetric scheme.