Tutorial -7

SOEN-321

Problem-3 –Ex5

Determine the problems in the following protocol in which A wants to establish a shared session key with B using the help of a trusted authority S

A→S: A, B

S→A: KAB

A→B: A, KAB

The key (KAB) is sent in the clear. Therefore, the attacker can also see the key and decrypt the corresponding ciphertexts.

Problem-4 –Ex5

Consider the following authentication protocol

A → B: TA, SigA(TA,B)

(i) What is the objective of the time stamp TA?

The timestamp ensures the freshness of the signature and prevents replay attacks. If there is no timestamp in the signature, the attacker can use a previously signed message and try to impersonate A.

Problem-4 –Ex5

Consider the following authentication protocol

A → B: TA, SigA(TA,B)

(ii)After this protocols is executed

(a) B is authenticated to A

(b) A is authenticated to B

(c) Both A and B are authenticated to each other

Authentication is the result of

1- proof of knowledge

2- freshness

proof of knowledge is the result of signature (only A has the private key for A and thus would be able to sign as A)

freshness is from the timestamp

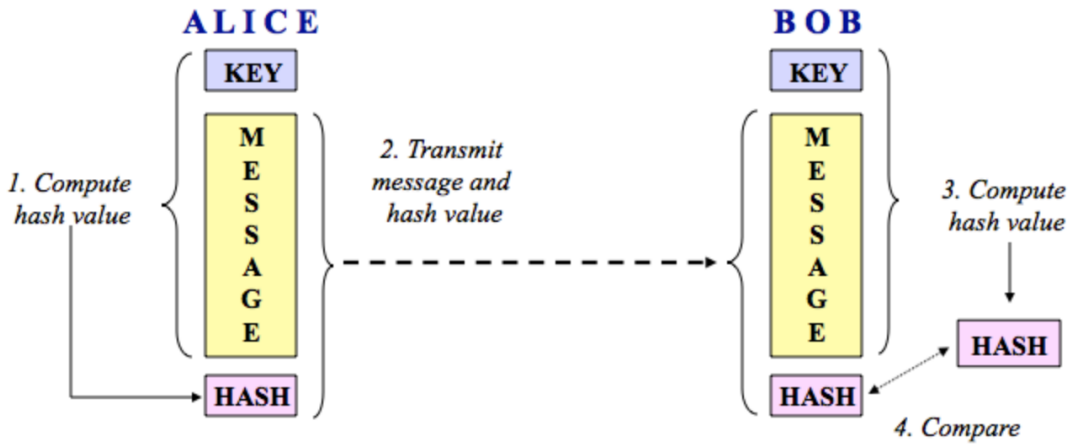
“A” is authenticated to B.

MAC

A message authentication code (MAC)

- To confirm that the message came from the stated sender (its authenticity)
- Has not been changed in transit (its integrity).

One way to build a MAC algorithm is through the use of a keyed hash function.



- Input: a secret key and an arbitrary-length message to be authenticated
- Output: a MAC.

Verifier can verify message integrity and authentication since the verifier also knows the secret key. [1]

[1] Gary C. Kessler, Ph.D. *An Overview of Cryptography*, www.garykessler.net/library/crypto.html.

Problem-1 –Ex6

Alice and Bob share a symmetric key k. Alice sends Bob a message stating, “I owe you $100", and also sends a message authentication code (MAC) on this message computed using the key k. Assuming the MAC algorithm is secure, can Bob go to his bank and prove to the bank teller that Alice does indeed owe him $100 by showing M and MAC(M) to the teller?

No. Bob cannot do so because the MAC key has to be known by **both Alice and Bob**. Thus Bob could have produced this message M and MAC(M) by himself. In other words, unlike digital signature, a MAC scheme does not provide non-repudiation; it only ensure message integrity and authentication