U4 Starred

Friday, November 26, 2021 17:26

★1. What is MAC? What are the requirements of MAC?

1. A message authentication code (MAC) is an algorithm that requires the use of a secret key.
2. A MAC takes a variable-length message and a secret key as input and produces an authentication code

Variable length code + secret key --->>	MAC ---> >	authentication code

3. A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message
4. How to create a MAC
   a. Combine a cryptographic hash function in some fashion with a secret key
   b. use a symmetric block cipher in such a way that it produces a fixed length output for a variable length input

- Requirements of MAC

- Considering the types of attacks, MAC needs to satisfy the following

1. **knowing a message and MAC, is infeasible to find another message with same MAC**

   MAC(K, M') = MAC(K, M)

2. **MACs should be uniformly distributed in the sense that for randomly chosen Messages M and M'**

   MAC MAC(K, M') = MAC(K, M) is 2^{-n} where n is the number of bits in the tag

3. Let be equal to some known transformation on. That is M' = f(M). For example, f may involve inverting one or more specific bits. In

that case, Pr [MAC(K, M) = MAC(K, M')] = 2^{-n}

MAC should depend equally on all bits of the message

★2. What is digital signature and its types

1. Digital Signature

a. A digital signature is an authentication mechanism that enables the **creator of a message to attach a code that acts as a signature**.

b. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key.

c. The signature guarantees the source and integrity of the message.

d. The digital signature standard (DSS) is an NIST standard that uses the secure hash algorithm (SHA)

e. Digital signatures provide the ability to:

   i. verify author, date & time of signature

   ii. authenticate message contents

   iii. be verified by third parties to resolve disputes

f. hence include authentication function with additional capabilities

g. In situations where no complete trust between sender and receiver, more than authentication is needed. The solution is Digital Signatures

2. Digital Signature Properties

a. It must verify the author and the date and time of the signature.

b. It must authenticate the contents at the time of the signature.

c. It must be verifiable by third parties, to resolve disputes

d. Digital signature function includes the authentication function

3. Direct Digital Signatures

a. It involves only sender and receiver

b. It is assumed receiver has sender's public-key

c. The digital signature iS made by sender signing entire message or hash with private key

d. It can also encrypt using receivers public-key

e. It is important that sign first then encrypt message & signature

f. The security depends on sender’s private-key

★3. Explain general structure of secure hash function.