Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

Message authentication codes

Self-assessment test

Select the correct answer.

1. What is difference between a message authentication code and a hash function?
   - The message length (they can be longer in hash functions).
   - The use of a secret key.
   - Nothing, they are the same.
   - The randomness of the output (message authentication codes are more random)

2. What are the similarities between message authentication codes (MAC) and hash functions?
   - Hash functions are non-invertible and MAC can be invertible.
   - Collisions may appear in both cases.
   - The probability of finding a pair of messages with the same output is of 2^{-n} in both cases.
   - All of the above are correct.

3. What is the security property that can be verified through message authentication codes?
   - Confidentiality.
   - Access control.
   - Availability.
   - Non-repudiation.

4. The complexity of a brute force attack in a MAC function is determined by:
   - The minimum between the size of the key space and that of the messages.
   - The maximum between the size of the key space and that of the messages.
   - The size of the output of the MAC function.
   - The size of the message space, exclusively.

5. To design a MAC function, you can:
    - Use a hash function as the basis, adding bits to messages according to the key.
    - Use a symmetric cipher.
    - Make a new design, regardless of any other cryptographic mechanism.
    - All of the above are correct.