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)

Hash functions

Self-assessment test

Select the correct answer.

1. What is a hash function?
   - It is a process that, given a message, generates an output which is always smaller.
   - It is a process that, given a pair of messages, generates a pair of outputs always different.
   - It is a process that, given any input message, generates an output with the same size always.
   - It is a process that encrypts a message in an irrecoverable way.

2. What is the linked between hash functions and collisions?
   - "Bad" hash functions generate collisions.
   - All hash functions generate collisions.
   - Hash functions whose output is short generate collisions.
   - Hash functions, as they are irreversible, generate collisions, but it is computationally impossible to find them.

3. A hash function cryptographically secure…
   - It can only be applied to messages whose length is bigger than that of the output.
   - It should generate a pseudorandom output.
   - They cannot generate collusions.
   - It is typically a slow process in comparison with encryption.

4. If one bit of the message is modified, and a 56-bits hash function is applied, the hash of the original and modified version of the message will differ, on average, in:
   - 1 bit, in the same position where the message was modified.
   - 1 bit, in any part of the hash.
   - 56 bits.
   - 28 bits.

5. A good hash function…
   - Applied over the same message, it should generate the same output.
   - Applied over the same message, it could generate different results.
   - It must have a hardware implementation.
   - It must be developed based on secret design.

6. Given a message M, how hard is to find other message such that both hashes are the same, if the hash function is cryptographically secure?
   - Mathematically impossible.
   - Computationally impossible.
   - Probabilistically impossible.
   - Technically improbable.

7. The one-way property states that…
   - It is not technically feasible find a message that generates a chosen hash.
   - It is not easy to find a pair of messages with the same hash.
   - It is impossible to get a message from its hash.
   - A hash function cannot be applied over 2 messages at a time.

8. When can we say that a hash function is “broken”?
   - When a collision in a message can be found.
   - When collisions are found easier than applying brute force.
   - When there is a technically feasible procedure (algorithm) within a short period of time.
   - When the collusion attack involves less than 2^{121} operations.

9. The birthday paradox shows the probability of a collision attack, modeling…
   - People (identities) as messages, and the birthday date (day and month) as the hash.
   - Birthday date (day and month) as message, and the person (identity) as the hash.
   - People (identities) as messages and the birthday date (day, month, and year) as the hash.
   - The birthday day as message, and the person (identity) as the hash.

10. Choose the correct sentence concerning MD5:
    - It is considered technically robust.
    - It generates a 256-bits output.
    - It cannot work with messages smaller than 512 bits.
    - It is based on a compressed function that is iteratively applied.

11. Concerning SHA-x, family:
    - They correspond to iterative improvements of the same design.
    - SHA-1 is considered insecure since 2005.
    - SHA-256 does not belong to the family SHA-2.
    - SHA-2 was compromised, as well as SHA-3.