CSS322 – Quiz 6 Answers

Name: ____

ID: ______________________________ Mark: __________ (out of 10)

Question 1 [2 marks]

a) What is the difference (in parameters) between a Hash function and a MAC function?

b) What algorithm can used to convert a Hash function into a MAC function?

c) Explain a benefit of converting a Hash function into a MAC function.

Answers

a. A MAC function takes the data and secret key as input, whereas a Hash function only takes data as input

b. HMAC

c. Can take advantage of the significant knowledge (including resistance to attacks) and software/hardware already developed for commonly used Hash functions

Question 2 [5 marks]

a) Assuming users must be allowed to choose any password they wish, describe two different approaches that can be used to make systems more secure against online password guessing attacks. [2 marks]

b) Assuming a user had an 10-character password. Which would you consider the strongest against a dictionary attack?
  i. Random characters
  ii. Combination of two English words
  iii. Pronounceable string (without dictionary words)
  iv. Combination of several names (in English), with mixed upper and lower case.

c) For practical purposes (e.g. efficiency, ease of use), hash functions have three desirable properties. Which of the following is NOT a desirable property of a has function:
  i. Produces fixed length output
  ii. Hard to compute for any input message
  iii. Works on variable sized input messages
  iv. None of the above

d) If you are developing a MySQL database to store customer information for a business, what is the best approach to store the password:
  i. Save it as plain text

ii. Encrypt the password with Triple-DES
iii. Hash the password with SHA-256
iv. Don't store the password in the database, store it as plain text in a separate file

Answer

a. Lock system (e.g. account) if too many guesses; Limit the speed that guesses can be made; Try to find the attacker (Record the attempts made and report to administrator or users)

b.Random characters.

c. Hard to compute for any input message (it should be easy to compute)

d. Hash the password.

Question 3 [3 marks]

An attacker C intercepts a message, and a signed hash of that message, that was sent from A to B. That is, C intercepts: M || E(PR_A,H(M)).

a) If the hash function H() does not have the weak collision resistance property, then can the attacker modify M without B detecting the modification (YES or NO). Explain your answer.

b) If the hash function H() has the weak collision resistance property, but does not have the strong collision resistance property, then can the attacker modify M without B detecting the modification (YES or NO). Explain your answer.

Answer

a. Yes. Without weak collision resistance, the attacker can find a value Y such that H(Y) = H(M). Therefore, C changes M to be Y, but sends the same signature E(PR_A,H(M)), and B will decrypted the signature and check the received H(M) and find it to be the same as the calculated H(Y).

b. No. With weak collision resistance, the above attack is not possible. Without strong collision resistance, the attacker can only choose to values X and Y with the same hash values. C cannot find another message with the same hash as M.