Assignment 9

The due date for submitting this assignment has passed. As per our records you have not submitted this assignment.

1) Given the following input (4322, 1334, 1417, 9679, 1989, 6171, 6173, 4199) and the hash function \( x \mod 10 \), which of the following statement(s) is(are) true?
   i. 9679, 1989, 4199 hash to the same value
   ii. 1417, 6171 has to the same value
   iii. All elements hash to the same value
   iv. Each element hashes to a different value

   A. i only
   B. ii only
   C. iii or iv
   D. i and ii only

2) Consider a hash table with 100 slots. Collisions are resolved using chaining. Assuming simple uniform hashing, what is the probability that the first 3 slots are unfilled after the first 3 insertions?
   A. \( (97 \times 97 \times 97)/100^3 \)
   B. \( (99 \times 98 \times 97)/100^3 \)
   C. \( (97 \times 96 \times 95)/100^3 \)
   D. \( (97 \times 96 \times 95)/(3! \times 100^3) \)

3) Which one of the following hash functions on integers will distribute keys most uniformly over 10 numbers from 0 to 9 for \( i \) ranging from 0 to 2020?
   A. \( h(i) = i^2 \mod 10 \)
   B. \( h(i) = (11 \times i^2) \mod 10 \)
   C. \( h(i) = i^3 \mod 10 \)
   D. \( h(i) = (12 \times i) \mod 10 \)

   A
Given a hash table \( T \) with 25 slots that stores 2000 elements, the load factor \( \alpha \) for \( T \) is ______.

- A. 0.0125
- B. 80
- C. 8000
- D. 1.25

No, the answer is incorrect.
Score: 0
Accepted Answers: 

Let \( h \) be a cryptographic hash function. Which of the following is not a property of \( h \)?

- A. Given hash \( y \), it should be computationally infeasible to find \( x \) such that \( y = h(x) \).
- B. Given hash \( y \) and a message \( x \) such that \( y = h(x) \), it should be computationally infeasible to find \( x' \neq x \) such that \( h(x') = h(x) = y \).
- C. Given hash \( y \), it should be easy to find \( x \) such that \( y = h(x) \).
- D. It should be computationally infeasible to find \( x', x \) such that \( h(x') = h(x) \).

No, the answer is incorrect.
Score: 0
Accepted Answers: 

Both MD4 and MD5 produce a ______ bit message digest whereas SHA-1 produces a ______ bit digest.

- A. 128, 160
- B. 128, 256
- C. 164, 160
- D. 164, 256

No, the answer is incorrect.
Score: 0
Accepted Answers: 

Let \( h \) be a hash chosen uniformly at random from a universal set \( \mathbb{H} \) of hash functions. Suppose hashing \( n \) keys into \( m \) slots in table \( T \). Then for a given key \( x \), \( E(\text{Number of collision with } x) \) (where \( E(X) \) denotes the expectation of \( X \)).

- A. \( \geq \frac{n}{m} \)
- B. \( = \frac{n}{m} \)
- C. \( < \frac{n}{m} \)
- D. \( < \frac{m}{n} \)

No, the answer is incorrect.
Score: 0
Accepted Answers: 

2 of 4 Friday 21 June 2019 10:56 AM
8) No, the answer is incorrect.
Score: 0
Accepted Answers:
C

In Digital Signature Standard Algorithm suppose $p = 283, q = 47, g = 60$. Let user’s private key 24 and random value chosen be $k = 15$. Consider a message $M$ with message digest $h = \text{Hash}(M)$ Then the signature $(r, s) =$ _______.

A. (19, 31)
B. (15, 20)
C. (19, 30)
D. (29, 40)

9) No, the answer is incorrect.
Score: 0
Accepted Answers:
C

Suppose that $(G, +)$ and $(H, \cdot)$ are abelian groups. A pairing is a _______ mapping $e : G \times G \rightarrow H$ that $e(a_1, b_2) =$ _______ for all $g_1, g_2 \in G$ and for all integers $a, b$.

A. degenerate, $e(g_1, g_2)^{a+b}$
B. non-degenerate, $e(g_1, g_2)^{a+b}$
C. degenerate, $e(g_1, g_2)^{ab}$
D. non-degenerate, $e(g_1, g_2)^{ab}$

10) No, the answer is incorrect.
Score: 0
Accepted Answers:
D

Input block size of SHA-1 is

A. 512
B. 160
C. 128
D. 256

