Quiz 5: Cryptographic Hash Functions

Started: Feb 15 at 4:10pm

Quiz Instructions

Question 1 — 2 pts

Which of the following statements are **false** for hash functions?

- [ ] The output size is fixed.
- [ ] The input size can vary.
- [x] Given an input, a hash function can produce multiple outputs
- [ ] Across varying inputs, the output of the hash function needs to be uniformly distributed.

Question 2 — 1 pts

Which of the following terms are used to describe the output of the hash function?

- [x] Fingerprint
- [x] Hash value
- [ ] Cache
- [ ] Message
- [x] Digest

Question 3 — 1 pts

Which of the following states that for any given input, it is computationally infeasible to find another input that produces the same hash as the given input?

- (•) Second preimage resistance
- ( ) Preimage resistance
- ( ) One-way property
- ( ) Collision resistance

Question 4 — 2 pts

Which of the following statements are true for cryptographic hash function requirements?

- [ ] All practical hash functions need to fulfill the same set of requirements.
- [ ] Any hash function that is strong collision resistant is also pre-image resistant.
- [x] Any hash function that is collision resistance is second preimage resistance.

- [ ] Any hash function that is preimage resistant is second preimage resistance.
- [x] Avalanche effect is a desirable property of hash function because it prevents attacks that compare the outputs to infer the relations between the corresponding inputs.

Question 5

2 pts

If the hash value is represented by two bytes, how many computations (i.e. distinct inputs) **in the worst case** are needed to break collision resistance?

256

(2x8)^2

Question 6

1 pts

Consider SHA-512. What is the number of padding bits if the length of the original message is 2580 bits?

364

1024-1024/8-2580mod1024

Question 7

1 pts

Consider the hash function $h : \{0,1\}^n \to \{0,1\}$ which takes input $m = m_1 m_2 \ldots m_n$ and outputs $m_1 \oplus m_2 \oplus \cdots \oplus m_n$, i.e., the XOR of the input bits of m. Is it true that h is preimage resistant?

- ○ True
- ◉ False

Question 8

2 pts

There are 7 people in a room. What is the probability that two of them have birthdays in the same month? (Assume the birthday of each person is uniformly distributed in the 12 months and independent of each other.)

- ○ 39%
- ○ 61%
- ◉ 89%

1-nPr/n^r

- ○ 11%

Question 9

2 pts

Let $f : \{0,1\}^n \to \{0,1\}^m$ be a cryptographic hash function that is preimage resistant and second preimage resistant. Note that its input is an n-bit string. To allow hashing a string of $2n$ bits, the function $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is constructed from f by $g(x,y) = f(x \oplus y)$, where $\oplus$ denotes bitwise XOR. Which of the following statement is correct?

- (●) g is preimage resistance. g is not second preimage resistance.
- ( ) g is not preimage resistance. g is not second preimage resistance.
- ( ) g is preimage resistance. g is second preimage resistance.
- ( ) g is not preimage resistance. g is second preimage resistance.

Quiz saved at 11:44pm

Submit Quiz