Unit 5 - Week 4

Week4_Assignment1

The due date for submitting this assignment has passed. Due on 2017-08-23, 23:59 IST.
As per our records you have not submitted this assignment.

1) Let (X,Y,K,H) be the hash family with $|X|= 2^{256}$ and $|Y|= 2^{32}$. Then the number of all possible hash functions in this family is *1 point*

- $2^{2^{40}}$
- $2^{2^{261}}$
- 2^{261}
- 2^{40}

No, the answer is incorrect.
Score: 0

Accepted Answers:
$2^{2^{261}}$

2) Assume random oracle model. Suppose that $h \in F^{(X,Y)}$ is chosen randomly, and let $X_0 \subseteq X$. Suppose that the values h(x) have been determined (by querying the oracle for h) if and only if $x \in X_0$ Let |X|=N and |Y|=M , N ≥ 2M. Then chose the correct statement. *1 point*

- Pr[h(x)=y]=1/M for all $x \in X \setminus X_0$ and all $y \in Y$.
- Pr[h(x)=y]=1/N for all $x \in X \setminus X0$ and all $y \in Y$.
- Pr[h(x)=y]=1/M-$|X_0|$ for all $x \in X \setminus X_0$ and all $y \in Y$.
- Pr[h(x)=y]=1/N-|X0| for all $x \in X \setminus X0$ and all $y \in Y$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
Pr[h(x)=y]=1/M for all $x \in X \setminus X_0$ and all $y \in Y$.

3) Let (X,Y,K,H) be a hash family with $|Y|= 4096$ and $X_0 \subset X$ such that $|X_0|= 32$. Suppose that ϵ be the average-case success probability for finding preimage. Then the best estimate of ϵ is *1 point*

- 2^{-12}
- 2^{-17}
- 2^{-5}
- 2^{-7}

No, the answer is incorrect.
Score: 0

Accepted Answers:
2^{-7}

4) Let a compression hash function be collision resistant. Then the hash function constructed by Merkle-Damdård algorithm **1 point**

- is collision resistant.
- is not collision resistant.
- may or may not be collision resistant.
- none of them.

No, the answer is incorrect.
Score: 0

Accepted Answers:
is collision resistant.

5) Suppose that $n = m > 1$ and $h : Z_2^m \rightarrow Z_2^m$ is defined by $h(x)=x^2 + ax + b \mod 2^m$. Then second preimage **1 point**

- can be found only by solving a quadratic equation.
- cannot be found.
- can be found by without solving a quadratic equation.
- Sometimes can be found by solving a linear equation but not always.

No, the answer is incorrect.
Score: 0

Accepted Answers:
can be found by without solving a quadratic equation.

6) Suppose that $h: X \rightarrow Y$ is a hash function such that it is possible to find $x, x' \in X$ with $x \neq x'$ such that $h(x)= h(x')$. Then **1 point**

- h is not preimage resistant.
- h is not second preimage resistant.
- h is not collision resistant but may or may not be second preimage resistant.
- h is not collision resistant and not second preimage resistant.

No, the answer is incorrect.
Score: 0

Accepted Answers:
h is not collision resistant but may or may not be second preimage resistant.

7) Find the correct statement among the following. **1 point**

- If a hash function is collision resistant then it is preimage resistant.
- If a hash function is second preimage resistant then it is collision resistant.
- If a hash function is collision resistant then it is second preimage resistant.
- If a hash function is preimage resistant then it is second preimage resistant.

No, the answer is incorrect.
Score: 0

Accepted Answers:
If a hash function is collision resistant then it is second preimage resistant.

8) Suppose that $h: X \rightarrow Y$ is a hash function considered in random oracle model. Suppose that Q queries are allowed and Q is small compared to $M= |Y|$. Then the best estimate of the average case success probability of find-second-preimage algorithm is **1 point**

- Q / M
- $Q / (M-1)$
- $(Q-1) / (M-1)$
- $(Q-1) / M$

No, the answer is incorrect.
Score: 0

Accepted Answers:
(Q-1) / M

9) Let B= {0,1}. Suppose that f: $B^{100} \rightarrow B^{50}$ is a collision resistant hash function. Define h: $B^{200} \rightarrow B^{50}$ such that $h(x) = f(f(x') \,||\, f(x''))$ for all $x \in B^{200}$, where $x = x' \,||\, x''$, $x', x'' \in B^{100}$. Then *1 point*

- h is not collision resistant.
- h may or may not be collision resistant.
- h is collision resistant.
- none of them.

No, the answer is incorrect.
Score: 0

Accepted Answers:
h is collision resistant.

10) Suppose you have a 40-bit message digest. Q is the smallest number of valid pairs required to obtain collision with probability 0.5. Which one of the following with the best estimate of Q? *1 point*

- 2^{20}
- 2^{40}
- 2^{80}
- 2^{10}

No, the answer is incorrect.
Score: 0

Accepted Answers:
2^{20}

Previous Page End