IS309: Network Security Technology
Tutorial 3, Week 3 (March 9)
Due Date: March 16

Chunyu Xue 518021910698

1 Problem 1

(50 points) Prove the theorem: Any hash function that is collision resistant is second preimage resistant.

Proof. We prove this theorem by proving the converse-negative proposition that:

Any hash function that is not second preimage resistant is not collision resistant.

Suppose H to be any hash function that is not second preimage resistant, then we can know that given a uniform $x \in \{0,1\}^*$, it is possible (large enough) for a PPT adversary to find $x' \in \{0,1\}^*$ such that $x' \neq x$ and $H(x') = H(x)$.

Thus, it's possible (large enough) for a PPT adversary to find a pair of distinct inputs (x', x) having the same hash value $H(x') = H(x)$, which means that hash function H is not collision resistant.

Proof complete.

□

2 Problem 2

(50 points) Prove the theorem: Any hash function that is second preimage resistant is preimage resistant.

Proof. We prove this theorem by proving the converse-negative proposition that:

Any hash function that is not preimage resistant is not second preimage resistant.

Suppose H to be any hash function that is not preimage resistant, then we can know that given a uniform $y \in \{0,1,\}^{l(n)}$, it is possible (large enough) for a PPT adversary to find a value $x \in \{0,1\}^*$ such that $H(x) = y$.

Thus, when given a uniform $x \in \{0,1\}^*$, we can also get the corresponding uniform $y = H(x) \in \{0,1\}^{l(n)}$, and from above we can know that it is possible (large enough) for a PPT adversary to find a value $x' \in \{0,1\}^* \neq x$ such that $H(x') = y = H(x)$ (since the input space of H is much larger than output space H), which means that hash function H is not second preimage resistant.

Proof complete.

□