网络安全技术课堂作业

Homework 2

网络空间安全学院 信息安全专业

2112492 刘修铭 1027

1 设 $H(m)$ 是一个抗碰撞的 $Hash$ 函数，将任意长消息映射为定长的 n 位 $Hash$ 值。对于所有的消息 x, x', $x \neq x'$，都有 $H(x) \neq H(x')$。上述结论是否正确？说明原因。

不正确。由于任意长消息均映射到定长为 n 位的 hash 值。故而 hash 的空间仅为 n 位。而对于任意长的明文空间，总会存在 x 与 x'，满足 $x \neq x'$，但二者被映射到同一个长度为 n 的 hash 值上，即 $H(x) = H(x')$。而哈希函数的抗碰撞性是指在合理的时间内难以找到两个不同的输入有相同的哈希值，但并不意味着足够长的时间下，无法找到。综上，题目中的结论是错误的。