

CSE 651 Homework 6

Due: Wednesday, June 3 by class time

1. As indicated in the class notes, a common way to construct a MAC is to incorporate a secret key k into a hash function h . For instance, let $\text{MAC}_k(m) = h(m)$ with $\text{IV} = k$.

Show that this particular MAC is insecure. (Hint: Given a legitimate $(m, \text{MAC}_k(m))$, construct a pair (x, y) such that $y = \text{MAC}_k(x)$, where x is modified from m . Note: h and the underlying compression function f are public information.)

2.

Consider a hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$. Let $N = 2^n$.

The birthday attack's success probability p is known to satisfy $k \geq \sqrt{2pN}$.

Suppose the attacker can generate a quadrillion (10^{15}) messages per second.

Suppose $n = 160$. How long will it take to generate sufficient messages to have a success probability of $p \geq 2^{-30}$?