

CSE 651 Homework 6

Due: Wednesday, June 2 by class time

1. Do problem 12.3 on the 5th edition (or 12.10 on the 4th) of Stallings. (This problem shows that CBC-MAC is not secure.)

2.

Consider $\text{CMAC}(m, k, k')$:

$m = m_1 || m_2 || \dots || m_l$, where $|m_i| = n$.

$c_0 \leftarrow \text{IV}$ (typically 0^n)

for $i \leftarrow 1$ to $l-1$ do

$c_i \leftarrow E_k(c_{i-1} \oplus m_i)$

$c_l \leftarrow E_k(c_{l-1} \oplus m_l \oplus k')$

return (c_l)

Now suppose we use a random IV (rather than a fixed one) for each message, and let the tag be $\langle \text{IV}, c_l \rangle$. Show that this variant of CMAC is not secure.

(For simplicity, assume no padding.)

(Hint: Given a legitimate $(m, \text{CMAC}_{k,k'}(m))$, construct a pair (x, y) such that $y = \text{CMAC}_{k,k'}(x)$ without using k and k' , where x is modified from m .)

3.

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 $p \geq 2^{-30}$?

4. Do problem 10.1 of Stallings.