Computer Science and Engineering, UCSD — Winter 09
CSE 107: Introduction to Modern Cryptography — **Instructor:** Mihir Bellare
Problem Set 4 — February 9, 2009

Problem Set 4

Due: Wednesday February 18, 2009, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in.

Problem 1. [**30 points**] Define the family of functions $H\colon \{0,1\}^{64} \times \{0,1\}^{192} \to \{0,1\}^{128}$ as follows:

function $H_K(x)$ // $|K| = 64$ and $|x| = 192$
  Let a be the first 64 bits of x and b the rest // $|a| = 64$ and $|b| = 128$
  $y \leftarrow \mathsf{AES}_{K \,\|\, a}(b)$ // Apply AES with 128-bit key $K \,\|\, a$ and input b to get output y
  return y

Show that H is not collision-resistant by presenting a practical adversary A such that $\mathbf{Adv}_H^{\text{cr2-kk}}(A)$ is close to one. (The better the attack, the more points you get.)

Problem 2. [**40 points**] Let $h\colon \mathcal{K} \times \{0,1\}^{2b} \to \{0,1\}^b$ be a compression function. Define $H\colon \mathcal{K} \times \{0,1\}^{4b} \to \{0,1\}^b$ as follows:

function $H(K, M)$
  Break M into $2b$-bit blocks, $M = M_1 \,\|\, M_2$
  $V_1 \leftarrow h(K, M_1)$; $V_2 \leftarrow h(K, M_2)$
  $V \leftarrow h(K, V_1 \,\|\, V_2)$
  return V

Show that if h is collision-resistant then so is H. Do this by stating and proving an analogue of Theorem 6.8 in the course notes.

Problem 3. [**50 points**] Let $\mathsf{sha1}\colon \{0,1\}^{672} \to \{0,1\}^{160}$ be the compression function underlying the $\mathsf{SHA1}$ hash function. We define a message authentication scheme $\Pi = (\mathcal{K}, \mathrm{MAC}, \mathrm{VF})$ as follows. The key generation algorithm returns a random 160 bit string as the key K, and the tagging and verifying algorithms are:

Algorithm $\mathrm{MAC}_K(M)$
    Divide M into 512 bit blocks, $M = M[1] \ldots M[n]$
    $C[0] \leftarrow K$
    For $i = 1, \ldots, n$ do
        $C[i] \leftarrow \mathsf{sha1}(C[i-1] \,\|\, M[i])$
    EndFor
    Return $C[n]$
	Algorithm $\mathrm{VF}_K(M, \sigma)$
	    If $\sigma = \mathrm{MAC}_K(M)$ then return 1
	    Else return 0

The message space is the set of all strings whose length is a positive multiple of 512.

Present a practical chosen-message attack that succeeds in forgery using one query to the tagging oracle.
