Computer Science and Engineering, UCSD | Fall 10
CSE 107: Introduction to Modern Cryptography | **Instructor:** Mihir Bellare
Problem Set 4 | October 25, 2010

Problem Set 4

Due: Monday November 1, 2010, 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. [20 points] Define the family of functions $H\colon \{0,1\}^{64} \times \{0,1\}^{192} \to \{0,1\}^{128}$ as follows:

function $H_K(x)$
  $a \,\|\, b \leftarrow x$
  $y \leftarrow \mathsf{AES}_{K \,\|\, a}(b)$
  return y

Here, $a \,\|\, b \leftarrow x$ means we split x as $x = a \,\|\, b$ with $|a| = 64$ and $|b| = 128$. Show that H is not collision-resistant by presenting a practical adversary A such that $\mathbf{Adv}^{\mathrm{cr}}_{H}(A)$ is close to one. (The better the attack, the more points you get.)

Problem 2. [30 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 $H(K, M)$
  $M_1 \,\|\, M_2 \leftarrow M$
  $V_1 \leftarrow h(K, M_1)$; $V_2 \leftarrow h(K, M_2)$
  $V \leftarrow h(K, V_1 \,\|\, V_2)$
  return V

Here, $M_1 \,\|\, M_2 \leftarrow M$ means we split M as $M = M_1 \,\|\, M_2$ with $|M_1| = |M_2| = 2b$. Show that if h is collision-resistant then so is H. Do this by stating and proving an analogue of the Theorem in class, which also appears as Theorem 6.8 in the course notes.

Problem 3. [20 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 $\mathcal{MA} = (\mathcal{K}, \mathcal{T}, \mathcal{V})$ as follows. The key generation algorithm returns a random 160 bit string as the key K, and the tagging and verifying algorithms are:

Algorithm $\mathcal{T}_K(M)$	Algorithm $\mathcal{V}_K(M, \sigma)$
$M[1] \ldots M[n] \leftarrow M$	If $\sigma = \mathcal{T}_K(M)$ then return 1
$C[0] \leftarrow K$	Else return 0
For $i = 1, \ldots, n$ do	
$\quad C[i] \leftarrow \mathsf{sha1}(C[i-1] \parallel M[i])$	
Return $C[n]$	

Above, $M[1] \ldots M[n] \leftarrow M$ means we break $M = M[1] \ldots M[n]$ into 512-bit blocks. 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.
