

Problem Set 4

Due: Thursday February 7, 2008, 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 $H: \{0,1\}^{64} \times \{0,1\}^{192} \rightarrow \{0,1\}^{128}$ 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 $|b| = 128$
 $y \leftarrow \text{AES}_{K\|a}(b)$ // Apply AES with 128-bit key $K\|a$ and input b to get output y
 return y

Show that H is not collision-resistant (meaning, not CR2-KK) by presenting a practical adversary A such that $\text{Adv}_H^{\text{cr2-kk}}(A)$ is close to one. (The better the attack, the more points you get.)

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