Problem Set 4

Due: Monday October 26, 2009, in class.

Collaboration is *not* allowed on this problem set. See the course information sheet for more information and details about rules.

Problem 1. [30 points] Let $E\colon \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a block cipher. Let D be the set of all strings whose length is a positive multiple of l.

1. **[10 points]** Define the hash function $H_1\colon \{0,1\}^k \times D \to \{0,1\}^l$ via the CBC construction, as follows:

algorithm $H_1(K, M)$
  $M[1]M[2]\ldots M[n] \leftarrow M$
  $C[0] \leftarrow 0^l$
  For $i = 1, \ldots, n$ do $C[i] \leftarrow E(K, C[i-1] \oplus M[i])$
  Return $C[n]$

Show that H_1 is not collision-resistant.

2. **[20 points]** Define the hash function $H_2\colon \{0,1\}^k \times D \to \{0,1\}^l$ as follows:

algorithm $H_2(K, M)$
  $M[1]M[2]\ldots M[n] \leftarrow M$
  $C[0] \leftarrow 0^l$
  For $i = 1, \ldots, n$ do $B[i] \leftarrow E(K, C[i-1] \oplus M[i])$; $C[i] \leftarrow E(K, B[i] \oplus M[i])$
  Return $C[n]$

Is H_2 collision-resistant? If you say NO, present an attack. If YES, explain your answer, or, better yet, prove it.

Above, $M[1]M[2]\ldots M[n] \leftarrow M$ means we break M into l-bit blocks, with $M[i]$ denoting the i-th block. For any attack (adversary) you provide, state its time-complexity. (The amount of credit you get depends on how low this is.)

Problem 2. [35 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:

algorithm $H(K, M)$

$M_1 \| M_2 \leftarrow M$
$V_1 \leftarrow h(K, M_1)$; $V_2 \leftarrow h(K, M_2)$
$V \leftarrow h(K, V_1 \| V_2)$
return V

Above, by $M_1 \| M_2 \leftarrow M$, we mean that M_1 is the first $2b$ bit of M and M_2 is the rest, so that $|M_1| = |M_2| = 2b$.

1. **[25 points]** Show that if h is collision-resistant then so is H. Do this by stating and proving an analogue of the Theorem on MD from class. (It also appears as Theorem 6.5.2 in the chapter on Hash Functions. Here by collision-resistant we mean what the notes call CR2-KK).

2. **[10 points]** What possible benefits does this construction have over MD? How would you extend it to hash arbitrary length messages while retaining these benefits and security?
