Cryptography, homework sheet 4

Due for 2MMC10: 06 October 2016, 10:45
and for Mastermath: 03 November 2016, 10:45 by email to `crypto.course@tue.nl`

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. Do not email Tanja your homework or put homework in mailboxes.

1. A message of length 64 bytes is encrypted with AES and sent via a network. During the transmission one bit in the second block is flipped. Explain for ECB, CBC, CFB, OFB, and CTR mode

   (a) how many bits are potentially different in the deciphered text compared to the initial plaintext;

   (b) how many bits are definitely different in the deciphered text compared to the initial plaintext.

2. In this exercise you should argue about the formal security properties of hash functions and find security reductions.

   (a) Let h be a hash function. Let $H = h \circ h$ be the hash function resulting from applying h twice, i.e., $H(m) = h(h(m)$. Show that H is preimage resistant if h is preimage resistant. To prove this, assume you are given A that breaks PRE for H. Show that it breaks PRE for h.

   (b) Let $h_1 : \{0,1\}^* \to \{0,1\}^{n_1}$ and $h_2 : \{0,1\}^* \to \{0,1\}^{n_2}$ be hash functions. Show that the combined hash function $H : \{0,1\}^* \to \{0,1\}^{n_1+n_2}, m \mapsto h_1(m)||h_2(m)$ is collision resistant if at least one of h_1 and h_2 is collision resistant.

   (c) Let $h_1 : \{0,1\}^* \to \{0,1\}^{n_1}$ and $h_2 : \{0,1\}^* \to \{0,1\}^{n_2}$ be hash functions. Show that collision resistance of h_1 does not imply collision resistance of the combined hash function $H : \{0,1\}^* \to \{0,1\}^{n_1}, m \mapsto h_1(h_2(m))$. Also show that preimage resistance of h_1 is sufficient to guarantee preimage resistance of H.

3. Sometimes an attacker gets to attack multiple targets at once and is satisfied breaking any *one* of them. For hash functions multi-target preimage attacks are interesting. We speak of a k-target preimage attack if the attacker is given the outputs $h(m_1), h(m_2), \ldots, h(m_k)$ but not the inputs $m_1, m_2, \ldots, m_k$ of a hash function $h : \{0,1\}^* \to \{0,1\}^n$ and has the goal of finding some (i, x) so that $h(x) = h(m_i)$.

   (a) Find an attack that takes time $2^n/k$ to succeed in finding such an (i, x) with high probability.

   (b) Show that a k-target preimage attack A succeeding with probability p can be turned into a 1-target preimage attack, i.e., a regular preimage attack, taking the same time as A and succeeding with probability p/k.