CS.202: Intro to Cryptography Thursday, 10/27/2016

Homework 4

Due Monday, 11/7/2016, at the beginning of the class

1 CCA insecurity of OFB and CBC modes

Show that OFB and CBC modes of block cipher operation are not *not* CCA-secure. In each case you can show a CCA attack which sends an encryption challenge pair (m_0, m_1) (note that $|m_0|$ and $|m_1$ must equal, but these messages are not limited to a single block of plaintext!), and then given $c = E(m_b)$ the attack can query the decryption oracle on a *single* ciphertext $c' \neq c$, and given the response it decides bit b. In both cases first show the attack, and then argue that your attack is succesful. (If your attack must ask more encryption and decryption queries, that's fine, but you can do it with a single decryption query...)

2 Encryption Scheme Attempts

Let $\{F_k\}$ be a PRF family with $K = X = Y = \{0,1\}^n$ for security parameter n. Let G be a PRG s.t. $|G(x)| = 2|x|$ for all x. For each encryption scheme below, state whether it is (a) Indistinguishable, (b) CPA-secure, and (c) CCA-secure, and briefly (but convincingly!) justify your answers. In each case the encryption key space is $\{0,1\}^n$. Assume that a_L, a_R refer to the left half or the right half, respectively, of a bitstring a of even length.

(a) Let $M = \{0,1\}^{4(n+1)}$, and let $E(k,m) = (G([k|0]) \oplus m_L, G([k|1]) \oplus m_R)$.

(b) Let $M = \{0,1\}^n$, and let $E(k,m) = F(k,k) \oplus m$.

(c) Let $M = \{0,1\}^{2n}$, and let $E(k,m) = (r, G(F(k,r)) \oplus m)$ for $r \leftarrow \{0,1\}^n$.

(d) Let $M = \{0,1\}^n$. Let $E(k,m) = (r,v,t)$ where $r \leftarrow \{0,1\}^n$, $v \leftarrow F(k_L, r) \oplus m$, $t \leftarrow F(k_R, v)$, and $(k_L|k_R) \leftarrow G(k)$, and let $D(k,c)$ parse c as a tuple (r,v,t), compute $(k_L|k_R) \leftarrow G(k)$, and output $m = F(k_L, r) \oplus v$ if $t = F(k_R, v)$ and $\perp$ otherwise.

3 CBC MAC

Consider the fixed-length *"raw CBC"* MAC construction on page 125 of [KL].

(a) Show that this construction is insecure on messages of length ln for any *variable* l.

(b) Show that if in this construction the IV vector t_0 is chosen at random and attached to the tag, instead of being fixed as $t_0 = 0^n$, i.e. if $Tag(k, [m_1|...|m_l]) = (t_0, t_1)$ for $t_0 \leftarrow \{0,1\}^n$ and $t_i = F(k, m_i \oplus t_{i-1})$ for $i > 0$, then the resulting MAC sheme would be insecure on messages of length ln for any *fixed* l.

(c) Show that if we include the intermediary block cipher outputs in the tag, i.e. if $Tag(k, [m_1|...|m_l]) = [t_1|...|t_l]$ for $t_0 = 0^n$ and $t_i = F(k, m_i \oplus t_{i-1})$ for $i > 0$, then the resulting MAC scheme would be insecure on messages of length ln for any *fixed* l.

4 HMAC Alternative

Before HMAC was invented, it was common practice to define MAC on variable-sized messages using a Hash Function H as $S(k, m) = H(k|m)$. Show that this is not a secure MAC if H is implemented from a compression function h using a Merkle-Damgard construction (see Figure 5.1, page 158).

5 Merkle-Damgard Transform

Do exercise 5.6 from the textbook, parts (a)-(d). If your answer is yes, *sketch* the proof. If no, demonstrate an attack.