Homework 3- CPA and CCA security

Total of 125 points.

1. (60 points) In the following questions, $\{p_k\}$ denotes a pseudorandom permutation collection where for every $k \in \{0,1\}^n$, p_k is a permutation on n bits. For each one of the following schemes for encrypting $2n$ bits, say whether it is *necessarily* CPA secure, *necessarily* not CPA secure, or the answer depends on the particular choice of $\{p_k\}$. Prove your assertions.

   a. (ECB Mode, 15 points): $E(m_1, m_2) = p_k(m_1) \| p_k(m_2)$ (as usual $\|$ denotes concatenation[1])

   b. (CTR Mode, 15 points): $E(m_1, m_2) = IV \| y_1 \| y_2$ where IV is chosen at random in $\{0,1\}^n$, and $y_i = p_k(IV + i) \oplus m_i$ where addition is done modulo 2^n.

   c. (CTR' Mode, 15 points): $E(m_1, m_2) = IV \| y_1 \| y_2$ where IV is chosen at random in $\{0,1\}^n$, and $y_i = p_k(IV + i + m_i)$ where addition is done modulo 2^n.

   d. (CBC Mode with random IV, 15 points): $E(m_1, m_2) = IV \| y_1 \| y_2$ where IV is chosen at random in $\{0,1\}^n$, $y_1 = p_k(m_1 \oplus IV)$ and $y_2 = p_k(m_2 \oplus y_1)$.

2. (40 points) In the following questions, (S, V) is a secure MAC with n bit keys and messages in $\{0,1\}^*$, (E, D) is a CPA-secure encryption scheme with n bit keys and messages in $\{0,1\}^*$. For each one of the following schemes (E', D') for encrypting an n bit message m, say whether it is *necessarily* CCA secure, *necessarily* not CCA secure, or the answer depends on the particular choice of the primitives. Prove your assertions.

   a. (10 points) $E'_{k_1,k_2}(m) = E_{k_1}(m \| S_{k_2}(m))$. $D'_{k_1,k_2}(c)$ is obtained by letting $m \| \sigma = D_{k_1}(c)$ and outputting m if $V(m, \sigma) = 1$ and `error` otherwise.

   b. (10 points) $E'_{k_1,k_2}(m) = E_{k_1}(m) \| S_{k_2}(m)$. $D'_{k_1,k_2}(c \| \sigma)$ is obtained by letting $m = D_{k_1}(c)$ and outputting m if $V_(m, \sigma) = 1$ and `error` otherwise.

   c. (10 points) $E'_{k_1,k_2,k_3}(m) = c \| \sigma \| \sigma'$ where $c = E_{k_1}(m)$, $\sigma = S_{k_2}(c)$, $\sigma' = S_{k_3}(c)$. $D'_{k_1,k_2,k_3}(c \| \sigma \| \sigma') = D_{k_1}(m)$ if either $V_{k_2}(c) = \sigma$ or $V_{k_3}(c) = \sigma'$; otherwise $D'_{k_1,k_2,k_3}(c \| \sigma \| \sigma') =$`error`.

   d. (10 points) $E'_{k_1,k_2,k_3}(m) = c \| \sigma \| \sigma'$ where $c = E_{k_1}(m)$, $\sigma = S_{k_2}(c)$, $\sigma' = S_{k_3}(c)$. $D'_{k_1,k_2,k_3}(c \| \sigma \| \sigma') = D_{k_1}(m)$ if both $V_{k_2}(c) = \sigma$ and $V_{k_3}(c) = \sigma'$; otherwise $D'_{k_1,k_2,k_3}(c \| \sigma \| \sigma') =$`error`.

[1] Throughout this homework assignment we'll assume that if the lengths of the different parts are not known then we use some encoding to mark the point of concatenation so it's possible to parse the different parts.

3. (25 points) Prove the security of the simplified GCM mode described in the lecture notes for two blocks. That is, let H be a collection of functions from $\{0,1\}^{3n}$ to $\{0,1\}^n$ such that for every $x \neq x' \in \{0,1\}^{3n}$ and $y, y' \in \{0,1\}^n$, $\Pr_{h \leftarrow_R H}[h(x) = y \wedge h(x') = y'] = 2^{-2n}$. Let $\{p_k\}$ be a pseudorandom permutation collection on n bits. Prove that the following encryption on $2n$ bits is CCA secure:

   - $E_{k,h}(m_1, m_2) = (IV, y_1, y_2, y_3)$ where IV is chosen at random in $[2^n]$, $y_1 = p_k(IV + 1) \oplus m_1$, $y_2 = p_k(IV + 2) \oplus m_2$ and $y_3 = p_k(IV + 3) \oplus h(IV \| y_1 \| y_2)$. (Addition is done modulo 2^n as usual.)
   - $D_{k,h}(IV \| y_1 \| y_2 \| y_3)$ is obtained by outputting "'error"' if $m_3 \neq h(IV \| y_1 \| y_2) \oplus p_k(IV + 3)$ and otherwise outputting (m_1, m_2).