COS 433 — Cryptography — Homework 4.

Boaz Barak

Total of 130 points. Due March 3rd, 2010.

Exercise 1 (20+10 points)**.** Recall that in class we gave a construction of a *probabilistic* CPA-secure encryption scheme (i.e., the function E used extra randomness in computing the encryption). A *deterministic* encryption scheme, is a pair (E, D) such that E is a function of the key and message only and uses no additional randomness. It of course must satisfy as well that $D_k(E_k(x)) = x$ for every key k and message x.

1. Prove that a deterministic encryption scheme cannot be CPA secure.

2. Say that an encryption (E,D) is *unique message CPA secure* if it satisfies the following relaxed variant of CPA security— we make the same definition as CPA security except we say that Eve cannot uss for the two challenge messages x_1, x_2 of the challenge phase any of the messages she asked for encryptions to in the attack phase. Give a construction based on the tools we learned in class (PRG's, PRF's, PRP's) of a unique messages CPA secure *deterministic* encryption scheme.

3. Suppose you a broker wants to encrypt his communication, and all of his messages are either "buy" or "sell". He wants to ensure that an adversary monitoring on the line, even if it found out by observing the marker what were the first i messages, will have no non-trivial advantage in predicting the next message given the ciphertext. Would you recommend the Broker must use a CPA secure encryption or will a unique message CPA secure scheme suffice?

   For 10 extra points, *prove* that given an encryption scheme with appropriate security, assuming that the broker chooses "sell" with probability p and "buy" with probability $1-p$, such an adversary will not be able to guess the right message with probability better than $\max\{p, 1-p\} + \epsilon(n)$ where ϵ is a negligible function.

Exercise 2 (25 points)**.** Let $\{p_k\}_{k\in\{0,1\}^*}$ be a pseudorandom permutation collection, where for $k \in \{0,1\}^n$, p_k is a permutation over $\{0,1\}^m$.

1. Consider the following encryption scheme (E, D): $\mathsf{E}_k(x) = p_k(x)$, $\mathsf{D}_k(y) = p_k^{-1}(y)$. Prove that this scheme is *not* a CPA-secure encryption.

2. Consider the following scheme (E, D) that encrypts $m/2$-bit messages in the following way: on input $x \in \{0,1\}^{m/2}$, E_k chooses $r \leftarrow_{\mathrm{R}} \{0,1\}^{m/2}$ and outputs $p_k(x, r)$ (where comma denotes concatenation), on input $y \in \{0,1\}^{m/2}$, D_k computes $(x, r) = p_k^{-1}(y)$ and outputs x. Prove that (E, D) *is* a CPA-secure encryption scheme. See footnote for hint[1]

[1] **Hint:** Try proving first for partial credit that this scheme satisfies the weaker notion of *multiple message security*. That is, for every polynomial $p = p(n)$ and $x_1, \ldots, x_p, x'_1, \ldots, x'_p \in \{0,1\}^{m/2}$ the two sequences of random variables $\langle Enc_K(x_1), \ldots, \mathsf{E}_K(x_p)\rangle$ and $\langle \mathsf{E}'_K(x'_1), \ldots, \mathsf{E}'_K(x'_p)\rangle$ are computationally indistinguishable (where K and K' are two independent random variables distributed uniformly over $\{0,1\}^n$).

Exercise 3 (25 points)**.** The CBC construction is often used to get an encryption for larger message size. If $p : \{0,1\}^m \to \{0,1\}^m$ is a permutation, then $\mathsf{CBC}_\ell\langle p\rangle$ is a permutation from $\{0,1\}^{\ell\cdot m}$ to $\{0,1\}^{\ell\cdot m}$ defined in the following way: for $x_1,\ldots,x_\ell \in \{0,1\}^m$, let $y_0 = 0^n$ and define $y_i = p(y_{i-1} \oplus x_i)$. Then, $\mathsf{CBC}_\ell\langle p\rangle(x_1,\ldots,x_\ell) = (y_1,\ldots,y_\ell)$.[2] Note that the inverse of $\mathsf{CBC}_\ell\langle p\rangle$ can be computed in a similar way using the inverse of $p(\cdot)$.

Let $\{p_k\}$ be a pseudorandom permutation collection. Determine the CPA-security of the following two encryption schemes which are based on the CBC construction. That is, for each scheme either prove that it is CPA-secure or give an attack showing that it is not. For simplicity, we consider only the 3-block variant of the scheme (i.e. $\ell = 3$).

1. *(Padding in the end)* Given $p_k : \{0,1\}^m \to \{0,1\}^m$ and a message $x = x_1, x_2 \in \{0,1\}^{2m}$, E_k chooses $r \leftarrow_{\mathrm{R}} \{0,1\}^m$ and outputs $\mathsf{CBC}_3\langle p_k\rangle(x_1, x_2, r)$. Decrypting done in the obvious way.
2. *(Padding in the start)* Given $p_k : \{0,1\}^m \to \{0,1\}^m$ and a message $x = x_1, x_2 \in \{0,1\}^{2m}$, E_k chooses $r \leftarrow_{\mathrm{R}} \{0,1\}^m$ and outputs $\mathsf{CBC}_3\langle p_k\rangle(r, x_1, x_2)$. Decrypting done in the obvious way.

Exercise 4 (25 points)**.** Prove that the following encryption scheme is CCA secure. Let $\{p_k\}$ be a collection of pseudorandom permutations mapping $\{0,1\}^{3n}$ to $\{0,1\}^{3n}$.

- To encrypt $x \in \{0,1\}^n$ with key k do the following: choose $r \leftarrow_{\mathrm{R}} \{0,1\}^n$, and send $p_k(x\|r\|0^n)$ (were $\|$ denotes concatenation).
- To decrypt $y \in \{0,1\}^{3n}$, compute $x\|r\|w = p_k^{-1}(y)$. if $w \neq 0^n$ then output $\perp$. Otherwise, output x.

Exercise 5 (25 points)**.** Let (E, D) be a CPA secure scheme with key-size=message-size=n, and let $\{f_k\}$ be a collection of PRFs such that for every $k \in \{0,1\}^n$, $f_k : \{0,1\}^n \to \{0,1\}^n$. Consider the following scheme (E', D'):

Key k, k' each chosen uniformly and independently from $\{0,1\}^n$.

Encrypt $E'_{k,k'}(x) = (y, t)$ where $y = E_k(x)$ and $t = f_{k'}(y)$.

Decrypt $D_{k,k'}(y, t) = \perp$ if $f_{k'}(y) \neq t$ and $D_k(y)$ otherwise.

1. Prove that the scheme (E', D') is CCA secure.
2. Let (E'', D'') be the same scheme except that we reuse the key for the PRFs and encryption. That is, we set $k = k'$ to be the same string chosen at random in $\{0,1\}^n$. Prove that this scheme is not necessarily even CPA secure! That is, show that there exists a CPA secure (E, D) and a PRF collection $\{f_k\}$ such that if we build (E'', D'') using these components then the resulting scheme is not CPA secure. (For partial credit, show that it's not CCA secure only.)

   This example shows that "reusing" or "recycling" keys in cryptography is a very dangerous practice.

[2] The string y_0 is called the initialization vector or IV, and in practice is often chosen to be different than 0^m. However, as long as it's a fixed public value this doesn't make any security difference. Note that the KL book considers a different variant of CBC where the IV is chosen independently at random for each encryption.