COS 433 — Cryptography — Homework 3.

Boaz Barak

Total of 120 points. Due October 11th, 2007.

Exercise 0 (0 points). 1. Read the analysis of the construction of CPA-secure encryption from PRFs in the Katz-Lindell book (proof of Theorem 3.25, pages 90–93) and compare it to the proof sketch given in class.

2. Read the analysis of the constructions of PRF's from PRG's in Goldreich's book (see excerpt on the web page under Lecture 5) and compare it to the proof given in class.

Exercise 1 (20 points). The RSA SecureID card (see Figure 1) is a credit-card sized device that displays 6 digits that change every minute. The idea is that when you log into your account remotely (say when you want to log into your UNIX account in Princeton from an Internet Cafe) then you have to type the numbers that appear in the card in addition to your PIN or password.

1. What is the security advantage of such a card over traditional password? That is, what sort of attack can this card resist which cannot be resisted using a standard password mechanism? (When making this comparison, assume that it's possible for users to remember a 6-digits PIN or a password with similar security.)
2. Describe how you would implement such a scheme using pseudorandom functions.

   Assume that the PRF family takes a seed of size n to map n bits to n bits, and that the number of possible devices is M (for $M < 2^n$). How many bits of storage does your implementation use at the server and each of the devices? (there is an implementation that uses at most $O(n)$ bits in each place).
3. Try to *define* what it means that such a scheme is *secure* and sketch a proof that your construction satisfies it (you don't have to formally define and prove if you don't want to—you can use English but try to be precise). Say how the security depends on n - the number of bits that the device stores in memory (where its running time is polynomial in n) and on k - the number of digits that it displays to the user. You'll get **10 extra points** for a fully rigorous definition and proof. (Remember that rigorous does *not* equal formal and tedious—it just means precise and without logical gaps.)

Exercise 2 (20 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).

1. Show that there is no *deterministic* encryption scheme satisfying the CPA security definition we gave in class.

Figure 1: RSA SecurID Device.

2. Give a variant of the CPA security definition for *stateful* encryption schemes, where E and D can keep state between each encryption and decryption they perform. Prove that there exists a deterministic stateful encryption scheme that is CPA secure under your definition.

Exercise 3 (25 points)**.** In these two questions you'll show that if we have a pseudorandom function family with particular input and output sizes, we can easily obtain a family that handles larger inputs and outputs. (It's easy to handle smaller outputs and inputs by truncation and padding.)

1. *(Changing PRFs output size)* Prove that if there exists a collection $\{f_s\}$ of pseudorandom functions with $f_s : \{0,1\}^{|s|} \to \{0,1\}$ (i.e., one-bit output) then there exists a collection $\{f'_s\}$ with $f'_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}$. See footnote for hint.[1]

2. *(Changing PRFs input size)* Prove that if there exists a collection $\{f_s\}$ of pseudorandom functions with $f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}$ then there exists a collection $\{f'_s\}$ with $f'_s : \{0,1\}^* \to \{0,1\}^{|s|}$ (i.e., f'_s for a random $s \in \{0,1\}^n$ is indistinguishable from a random function from $\{0,1\}^*$ to $\{0,1\}^n$. See footnote for hint[2]

The following exercises use the definition of *pseudorandom permutations* as in given in class; see also Section 3.6.3 (page 94) of Katz-Lindell.

Exercise 4 (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

[1] **Hint:** First come up with a pseudorandom family with output longer than 1 but shorter than $|s|$. For example, if $s \in \{0,1\}^{n^2}$ then the output can be n. Then show that existence of PRF implies existence of pseudorandom generators and use that to expand your output.

[2] **Hint:** (This is definitely not the only approach to do this.) First note that such a PRF family implies immediately a family where $f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|/2}$. Then try to use this to get a function f'_s that works only for inputs whose size is a multiple of $|s|/2$. Then try to get a function that works for every finite length string.

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[3]

Exercise 5 (20 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, $\mathsf{CBC}_\ell\langle p\rangle(x_1, \ldots, x_\ell) = (y_1, \ldots, y_\ell)$.[4] 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 6 (0 points)**.** Consider the following scenario: Alice is a customer and Bob is an online merchant, and Alice wants to send her credit card number to Bob over the web, at which point Bob will verify the number against some database and decide whether to continue with the transaction. Assume that they are able to share a random secret key. Think whether you can implement a way to do this using a CPA secure encryption scheme.

Think whether your protocol is secure against an eavesdropper Eve that listens on the line of communication. Then, think whether it's secure even if Eve can be *active*— modify the messages sent between Alice and Bob.

[3] **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 $\{0,1\}^n$).

[4] 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.