Homework 2

Applied Cryptography
CS 598 : Fall 2013

Released: Thu Sep 18
Due: Thu Oct 09

Exercises on Encryption [Total 100 pts]

1. **Optimality of one-time pad.** For a one-time encryption scheme $\mathsf{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ to be perfectly secret and correct, show that we require $|\mathcal{K}| \geq |\mathcal{M}|$. [10 pts]

2. **Statistical Indistinguishability.** Recall that for two distributions X and Y over n-bit strings, the *statistical difference* (a.k.a. variational distance) between them is denoted by

$$\Delta(X, Y) = \max_{S \subseteq \{0,1\}^n} | \Pr_{x \leftarrow X}[x \in S] - \Pr_{x \leftarrow Y}[x \in S]|.$$

   (Alternately, this can be phrased in terms of a statistical test T, which checks if $x \in S$ for some subset S.) [10 pts]

   (a) Suppose $G : \{0,1\}^k \to \{0,1\}^n$ is a deterministic function, where $n > k$. Let X be the distribution of the output of $G(s)$ when $s \leftarrow \{0,1\}^k$ is chosen uniformly at random. Let Y be the uniform distribution over $\{0,1\}^n$. Show that $\Delta(X, Y) \geq \frac{1}{2}$. Conclude that the output of a psuedorandom random generator is quite distinguishable from a truly random distribution, if computationally unbounded distinguishers are considered.

   (b) Suppose X_k and Y_k are distributions over 2-bit strings (for all values of k). Further suppose that for all values of k, $\Delta(X_k, Y_k) \geq 0.1$. Show that X_k and Y_k are computationally distinguishable. (You may use *non-uniform* PPT distinguishers. For extra-credit, show that X_k and Y_k are significantly distinguishable by *uniform* PPT distinguishers.)

3. **One-way, but every single bit of the preimage is predictable:** For any function $f : \{0,1\}^* \to \{0,1\}^*$, define a function g_f as follows $g_f(x, S) = (f(x|_S), S, x|_{\bar{S}})$, where S is a subset of $\{1, 2, \ldots, |x|\}$ (represented as a bit vector of length $|x|$). Here $x|_S$ denotes a string obtained by choosing only those bits from x as specified by S and $x|_{\bar{S}}$ contains the remaining bits. [15 pts]

   (a) Show that if f is a one-way function, then so is g_f. You may assume that f is length-preserving (i.e., $|f(x)| = |x|$ for all x).

   (b) Show that no single bit of the input is a hard-core bit for g_f.

4. True or False (give reasons): [10 pts]

   (a) If $G : \{0,1\}^k \to \{0,1\}^n$ is a PRG, then so is $G' : \{0,1\}^{k+\ell} \to \{0,1\}^{n+\ell}$ defined as $G'(x \circ x') = G(x) \circ x'$ where $x \in \{0,1\}^k$, $x' \in \{0,1\}^\ell$, and $\circ$ denotes concatenation.

   (b) If $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^n$ is a PRF, then so is

      i. $F' : \{0,1\}^k \times \{0,1\}^{m+\ell} \to \{0,1\}^{n+\ell}$ defined as $F'(s; x \circ x') = F(s; x) \circ x'$ where $s \in \{0,1\}^k$, $x \in \{0,1\}^m$, $x' \in \{0,1\}^\ell$.

      ii. $F' : \{0,1\}^{k+\ell} \times \{0,1\}^m \to \{0,1\}^{n+\ell}$ defined as $F'(s \circ s'; x) = F(s; x) \circ s'$ where $s \in \{0,1\}^k$, $x \in \{0,1\}^m$, $s' \in \{0,1\}^\ell$.

5. Consider a "two-message encryption scheme" $\mathsf{Enc}^2 : \mathcal{K} \times \mathcal{M} \times \mathcal{M} \to \mathcal{C} \times \mathcal{C}$. [10 pts]

   (a) Define perfect secrecy for such an encryption.

   (b) Let $\mathcal{M} = \mathcal{K} = \mathcal{C}$ be the set of n-bit strings. Let $\mathsf{Enc}^2(K, m_1, m_2) = (K \oplus m_1, K \oplus m_2)$, where $\oplus$ is bit-wise xor-ing. Prove that this is **not** perfectly secret, according to your definition.

6. The NCSA has a PetaFLOPS computer on campus that can execute over 10^{15} floating point operations per second. Suppose that a single evaluation of a block-cipher (DES or AES) takes 10 FLOPs. How long would it take for the NCSA computer to recover a DES key, using a brute-force search? (Clearly state what your brute-force search involves.) How about a 128-bit AES key? [5 pts]

7. **[Extra]** The triple-DES (3DES) is a block-cipher that uses the DES block-cipher three times, with three different keys. The output ("ciphertext") of 3DES with key (K_1, K_2, K_3), on input ("plaintext") P is defined as $C = \mathrm{DES}_{K_1}(\mathrm{DES}^{-1}_{K_2}(\mathrm{DES}_{K_3}(P)))$ where DES_K and DES^{-1}_K stand for the application of the DES block-cipher in the forward ("encryption") and reverse ("decryption") directions. Suppose you are given oracle access to 3DES with a fixed key (K_1, K_2, K_3). Describe an algorithm for recovering the keys. Your algorithm can use the DES block-cipher as a black-box (in either forward or reverse directions: i.e., feed it a (key,plaintext) pair and obtain a ciphertext, or feed it a (key,ciphertext) pair and obtain a plaintext). Can you devise an algorithm which calls the DES block-cipher "only" about 2^{112} times (instead of 2^{168} times, which is what enumerating over all triples of 56-bit keys entails). How much memory does your algorithm use?

8. **Impossibility of deterministic CPA-secure encryption.** Suppose a symmetric key encryption scheme has a deterministic encryption algorithm. Give an adversary in the IND-CPA experiment for SKE to show that this scheme cannot be CPA-secure. [10 pts]

9. **Impossibility of information-theoretic public-key encryption.**

   (a) Show that no public-key encryption scheme can be secure against computationally unbounded adversaries. More concretely, show that if $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is a public-key encryption scheme with perfect correctness (i.e., $\mathsf{Dec}_{SK}(\mathsf{Enc}_{PK}(M)) = M$, for all messages M and valid key-pairs (PK, SK)) then there is a function Eve such that for all messages M and valid public-keys PK, $\mathsf{Eve}_{PK}(\mathsf{Enc}_{PK}(M)) = M$ (i.e., EVe can recover the message using only the public-key and not the secret-key). [10 pts]

   (b) **[Extra]** *(This problem uses information theoretic terminology. $I(X;Y)$ denotes the mutual information between the random variables X and Y.)* Show an information theoretic statement that if Alice and Bob do not share private information, then whatever information Alice can convey to Bob using a public-key encryption scheme (which may or may not be perfectly correct), Eve gets the entire information. More precisely, show that for any probabilistic algorithms KeyGen and Enc, $I(PK, C; M) = I(PK, SK, C; M)$ where M comes from an arbitrary distribution, $(PK, SK) \leftarrow \mathsf{KeyGen}$ and $C \leftarrow \mathsf{Enc}_{PK}(M)$.

10. **Pitfalls in fiddling with CCA secure schemes.** To protect against packet corruptions while transmission, suppose one uses an "enhanced" PKE scheme $(\mathsf{Gen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$, derived from a PKE scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows. The ciphertext in the enhanced scheme consists of three ciphertexts independently generated as encryptions of the plaintext under the original scheme. i.e., $\mathsf{Enc}^*(m) = (c_1, c_2, c_3)$, where $c_i \leftarrow \mathsf{Enc}(m)$. For decryption, the three ciphertexts are decrypted. If at least two of the ciphertexts decrypt to the same message, that message is output as the decryption. Otherwise an error message is produced.

    (a) Show that $(\mathsf{Gen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is IND-CPA secure, if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is. [10 pts]

    (b) Show that $(\mathsf{Gen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is *not* IND-CCA secure, even if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is. [10 pts]