Homework 2

Cryptography & Network Security
CS 406/CS 649 : Spring 2017

Released: Mon March 6
Due: Thu March 16

OWF, Trapdoor OWP, PKE, CRHF [Total 100 pts]

1. **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 $\{1,2,\ldots,|x|\}$ of size $\lfloor |x|/2 \rfloor$. Here $x|_S$ denotes the string obtained by choosing only those bits from x whose indices are in S and $x|_{\bar{S}}$ is the string containing the remaining bits.

   (a) Suppose f is a one-way function when $x \leftarrow \{0,1\}^k$. Then show that so is g_f when $x \leftarrow \{0,1\}^k$ and S is uniformly randomly chosen from subsets of $\{0,1\}^k$ of size $k/2$. You may assume that f is length-preserving (i.e., $|f(x)| = |x|$ for all x). [15 pts]

   (b) Show that no single bit of the input is a hard-core bit for g_f. [5 pts]

2. **Hash Functions.** In this problem we consider hash functions on a finite domain (from $\{0,1\}^{n(k)}$ to $\{0,1\}^{m(k)}$).

   (a) **Preimage collision resistance $\not\Rightarrow$ Second-preimage collision resistance.** Suppose $\mathcal{H}$ is preimage collision resistant. Modify $\mathcal{H}$ to $\mathcal{H}'$ (possibly with a different domain), so that the latter remains preimage collision resistant, but is not second-preimage collision resistant. (Prove these properties of $\mathcal{H}'$.) [6 pts]

   (b) **Second-preimage collision resistance $\not\Rightarrow$ Preimage collision resistance.** Given a CRHF $\mathcal{H}$ which compresses by two bits (say from n bits to $n-2$ bits), construct a CRHF $\mathcal{H}'$ that compresses by one bit (say from $n+1$ bits to n bits), such that the function $f(h',x) = (h', h'(x))$ (where $h' \in \mathcal{H}'$) is **not** a OWF. (In both $\mathcal{H}$ and $\mathcal{H}'$, collision-resistance holds when the hash function is drawn uniformly at random from the family.) [8 pts]

   (c) **(Sufficiently Shrinking) CRHF implies OWF.** Show that if $\mathcal{H}$ is a CRHF from n bits to $n/2$ bits, then the function $f(h,x) = (h, h(x))$ is a OWF. [16 pts]

   Hint: You may use the following intermediate steps. Below we say that "x has a collision under f" if there exists an $x' \neq x$ such that $f(x) = f(x')$.

   i. Let $\mathcal{H}$ be a CRHF and suppose that for every $h \in \mathcal{H}$ and every x, x has a collision under h. Show that the function $f(h,x) = (h, h(x))$ is a OWF.

   ii. Now, suppose that for each $h \in \mathcal{H}$, all but a negligible fraction of x's have a collision under h. Show that the function $f(h,x) = (h, h(x))$ is a OWF.

   iii. Finally, apply the above to the case of $f : \{0,1\}^n \to \{0,1\}^{n/2}$.

3. **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) *(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 $C \leftarrow \mathsf{Enc}_{PK}(M)$.

   Note that the LHS above is the amount of information related to M that Eve receives, and the RHS is the amount of information that Bob receives. [Extra Credit]

4. **Square Root modulo $N = PQ$ as hard as factorizing.** Consider sampling two random k-bit prime numbers $P \neq Q$, and setting $N = PQ$. Suppose we are given an algorithm A which, on being given N and a random $x \in \mathbb{QR}_N$, returns $y \in \mathbb{Z}_N$ such that with probability ϵ, $y^2 \equiv x \pmod{N}$. (The probability is over the choice of P, Q, x and the randomness used by the algorithm A.) Give an algorithm B which, on being given N as above, outputs the factors P, Q with probability at least $\epsilon/2$ (the probability being over the choice of P, Q and the randomness of B). [20 pts]

   Hint: First, reduce the problem of factorizing N to finding two non-zero elements $a, b \in \mathbb{Z}_N$ such that $ab \equiv 0 \pmod{N}$. Use the square-root finding algorithm A to find "collisions" for the squaring function, and try to turn the collisions to a, b as above. In showing how to get collisions from square-root, use the Chinese Remainder Theorem.

5. **Pitfalls in fiddling with CCA secure schemes.** To protect against packet corruptions while transmission, suppose one uses an "enhanced" PKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$, derived from a PKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ 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 $(\mathsf{KeyGen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is IND-CPA secure, if $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is. [15 pts]

   Hint: Consider a series of a hybrid experiments, with the first corresponding to using $\mathsf{Enc}^*(m_0)$ in the CCA security experiment, the last one to using $\mathsf{Enc}^*(m_1)$, and any two adjacent hybrids differing by an encryption of the form $\mathsf{Enc}(m_b)$.

   (b) Show that $(\mathsf{KeyGen}, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is *not* IND-CCA secure, even if $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is. [5 pts]