Homework 2: Basic crypto.
Due at 11:59PM on March 1, 2013 as a PDF via websubmit.

February 19, 2013

Exercise 1. (The point of this question is to demonstrate that MACs need not preserve the confidentiality of the message!!) Let (Gen, MAC, Ver) be a secure MAC. Use a reduction to show that

$$MAC'(m) = (m, MAC(m))$$

is also a secure MAC.

Exercise 2. Consider a password file stored as shown below, where $r_i = h(password_i)$.

user	h(password)
u_1	r_1
...	...
u_q	r_q

1. If $h : \{0,1\}^n \to \{0,1\}^m$ is a one-way function, and all passwords are chosen **randomly** from $\{0,1\}^n$, then can an adversary that runs in time that is polynomial in n and m find (i, p_i) such that $h(p_i) = r_i$? If you answer is yes, provide a proof by reduction, as we did in class. If you answer is no, present the attack the adversary uses to find (i, p_i).

2. Repeat 1., now supposing that h is a collision resistant hash function.

3. Repeat 1., now supposing that passwords are chosen randomly from D, a dictionary of size n^{10}.

Exercise 3. Let f be a secure pseudorandom function.

1. Prove that the following MAC for messages of length n is secure: The shared key is a random $k \in \{0,1\}^n$. To authenticate a message m_1 compute the tag $f_k(m_1)$. You should prove this using a reduction; that is, show that if the pseudorandom function is secure, then the MAC is secure.

2. Show that the following MAC for messages of length $2n$ is insecure: The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ where $|m_1| = |m_2| = n$, compute the tag $f_k(m_1)||f_k(f_k(m_2))$.

Exercise 4. Let $\mathcal{PKE}$ be a public-key encryption scheme. For each property of $\mathcal{PKE}$ below, say whether it is enough, all by itself, to rule out chosen plaintext attack (CPA) security of $\mathcal{PKE}$. Briefly justify each answer.

1. The first bit of a message is equal to the last bit of its encryption.

2. Given a ciphertext, it is easy to tell which public key was used to produce it.

Exercise 5. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator. Is the following scheme a CPA secure encryption scheme? To encrypt message $m \in \{0,1\}^{2n}$ under key k send $(k, G(k) \oplus m)$. If yes, provide a proof by reduction. If no, provide an attack.

Exercise 6. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom function. Is the following scheme a CPA secure encryption scheme? To encrypt message $m \in \{0,1\}^{2n}$ under key k choose a random $r \in_r \{0,1\}^n$ and send $(r, f_k(r) \oplus m)$. If yes, provide a proof by reduction. If no, provide an attack.

Submission policy.

Every submitted assignment MUST include the following information:

1. List of collaborators
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)
3. Number of late days used on this assignment
4. Total number of late days used thus far in the entire semester

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism below.