Homework 3

FEBRUARY 7

Due by the **start of class on TUESDAY, FEBRUARY 21**. Start early!

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea. For this problem set, a random subset of problems will be graded.

You may collaborate with others on this problem set. However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. Encryption and CPA.
   (a) (6 points) Let G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$ and let F be a pseudorandom function. For the following encryptions schemes, decide if it is 1) not even computationally secret; or 2) computationally secret but not CPA-secure; or 3) CPA-secure. Justify your answers.
      i) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$, and output ciphertext $(r, G(r) \oplus m)$.
      ii) To encrypt $m \in \{0,1\}^n$, output ciphertext $m \oplus F_k(0^n)$.
   (b) (6 points) Let F be a pseudorandom permutation (F_k and F_k^{-1} are both efficiently computable), and define a fixed-length encryption scheme (G, E, D) as follows: on message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, encryption algorithm E chooses a uniform string $r \in \{0,1\}^{n/2}$ and compute $c := F_k(r\|m)$.
      i) Show how to decrypt.
      ii) Is it CPA-secure for messages of length $n/2$? If so, give a proof; if not, describe an attack.
   (c) (6 points) ([KL: 3.20]) Consider a *stateful* variant of CBC-mode encryption where the sender simply increments IV by 1 each time a message is encrypted (rather than choosing a random IV each time). Is this variant CPA-secure? Prove or describe an attack for your answer.
   (d) (Bonus 5 points) [KL: Excercise 3.29] Let $\Pi_1 = (G_1, E_1, D_1)$ and $\Pi_2 = (G_2, E_2, D_2)$ be two encryption schemes for which at least one of them is CPA-secure, but we don't know which one. Show how to construct an encryption scheme from Π_1 and Π_2 that is guaranteed to be CPA-secure. Give a proof for your construction.
2. MAC
   (a) (6 points) [KL: Exercise 4.6] Consider the following MAC for messages of length $\ell(n) = 2n - 2$ using a pseudorandom function F: on input a message $m := m_0\|m_1$ ($|m_0| = |m_1| = n - 1$) and key $k \in \{0,1\}^n$, MAC algorithm S outputs $t = F_k(0\|m_0)\|F_k(1\|m_1)$.
      i) Describe a natural Verification algorithm V.
      ii) Is the MAC scheme secure? Prove your answer or describe an attack.

(b) (10 points) [KL: Exercise 4.14] Show that the following modificatons of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages).

i) S outputs all intermediate blocks $t_1, \ldots, t_\ell$ rather than just t_ℓ. (Verification only checks t_ℓ.)

ii) A random initial block is used each time a messge is authenticated.

3. Hash functions and Random Oracle model.

(a) (5 points) [KL: Exercise 5.3] Let (G, H) be a collision-resistant hash function. Is $(G, \hat{H})$ defined by $\hat{H}^s(x) := H^s(H^s(x))$ necessarily collision resistant? Justify you answer.

(b) (6 points) Consider the following construction of a MAC, using a hash function (G, H): run G to obtain a key k for H; to sign a message m, $S_k(m)$ outputs a `C program` P that on input (k, m) outputs the constant $H^k(m)$. The verification algorithm V on key k and message-tag pair (m, P) outputs 1 iff. $P(k, m) = H^k(m)$. Prove that (G, S, V) is secure in the random oracle model. Namely prove that if H is a random function and $H^k(m)$ is defined as $H(k\|m)$, then there is no adversary that succeeds in a chosen-message-attack against (G, S, V).

(c) (Bonus 5 points) Prove that (G, S, V) above is *insecure* no matter what hash function we use as long as $H^k(m)$ is efficiently computable[1].

4. One-way functions.

(a) (5 points) [KL: Exercise 7.2] Prove that if f is a one-way function, then the function g defined by $g(x_1, x_2) := (f(x_1), x_2)$, where $|x_1| = |x_2|$, is also a one-way function.

(b) (Bonus 5 points) Let f be a length-preserving one-way *function*, and let hc be a hard-core predicate of f. Define G as $G(x) = f(x)\|hc(x)$. Is G necessarily a pseudorandom generator? Justify your answer.

[1] This is an example of the potential danger of the random oracle heuristics. Read the CGH paper https://eprint.iacr.org/1998/011.pdf if interested