Winter 2018 CS 485/585 Introduction to Cryptography

Homework 2

Portland State University — *Jan. 18, 2018, Update: 01/25/18*

Student: your name — *Due: Feb. 1, 2018*

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. Problems marked with "[**G**]" are required for graduate students. Undergraduate students will get bonus points for solving them. The .tex source is provided on course webpage as a template if you want to typeset your solutions in Latex.

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. (Pseudorandom Generators) Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. Let F be a length preserving pseudorandom function. In each of the following cases, decide whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample. Note: identify integers $\{0, 1, \ldots, 2^n - 1\}$ with binary strings $\{0,1\}^n$, e.g., $1 = 00\ldots01$.
   (a) (6 points) $G'(s) := G(s_1, \ldots, s_{\lfloor n/2 \rfloor}, s_{\lceil n/2 \rceil})$, where $s = s_1, \ldots, s_n$.
   (b) (6 points) $G'(s) := G(0^{|s|} \| s)$.
   (c) (6 points) $G'(s) := F_s(0) \| F_s(1)$.
   (d) (Bonus 5pts) $G'(s) := F_s(G(0)) \| F_s(G(1))$.

2. (Pseudorandom functions and pseudorandom permutations)
   (a) (15 points) [KL: Exercise 3.10] Let F be a length-preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{cn}$, $c = 1$ or 2, decide if F' is a pseudorandom function. If yes, prove it; if not, show an attack.
      i. $F'_k(x) := F_k(0\|x)$.
      ii. $F'_k(x) := F_k(0\|x) \| F_k(1\|x)$.
      iii. $F'_k(x) := F_k(0\|x) \| F_k(x\|1)$.
   (b) (5 points) [KL: Exercise 3.16] Prove that a pseudorandom permutaiton is also a pseudorandom function when the block length $\ell(n) \geq n$.

3. (Encryption against chosen-plaintext attacks)
   (a) (10 points) Read [KL: Section 3.6.2] on CBC-mode and work out the following.

i. Consider a stateful variant of CBC-mode where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing it at random each time). Is this scheme CPA-secure? If yes, prove it; if not, describe an attack.

ii. Describe the effect of a single-bit error in the ciphertext when using CBC mode.

(b) (15 points) Let F be a pseudorandom permutation on of block length n, and G be a pseudorandom generator with 1-bit expansion $\ell(n) = n + 1$. For each of the following encryption schemes, decide whether it is computationally secret or CPA-secure.

i. To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \leftarrow \{0,1\}^n$, and output $(r, G(r) \oplus m)$.

ii. To encrypt $m \in \{0,1\}^n$, output $m \oplus F_k(0^n)$.

iii. To encryption $m \in \{0,1\}^n$, output $F_k(m)$.

(c) (5 points) **[G]** [KL: Exercise 3.29]

4. (Message authentication)

(a) (12 points) Consider the definitions of a secure MAC (i.e., existentially unforgeable under adpative chosen-message attacks [KL: Def.4.2]) and a strongly-secure MAC ([KL: Def.4.3]).

i. [KL: Exercise 4.4] Prove that for canonical MAC schemes, a secure MAC is also strongly secure.

ii. [KL: Exercise 4.5] Assume secure MACs exist. Prove that there is a secure MAC, which is NOT strongly secure.

(b) (5 points) [KL: Exercise 4.6]