Practice Exam

Name: ____________________

Winter 2018, CS 485/585 Crypto
Portland State University

March 14, 2018
Prof. Fang Song

Instructions

- This exam contains 8 pages (including this cover page) and 5 questions. Total of points is 90.
- You have 100 minutes. Be strategic and allocate your time wisely.
- You may use two double-sided letter size (8.5-by-11) study sheet. Calculator is allowed. Any other resources and electrical devices (e.g. laptops, phones) are NOT permitted.
- Your work will be graded on correctness and clarity. Please write legibly.
- Don't forget to write your name on top!

Grade Table (for instructor use only)

Question	Points	Score
1	30	
2	17	
3	12	
4	15	
5	16	
Total:	90	

1. *Short answers*.

   (a) (5 points) Suppose Alice wants to encrypt a 1000-bit message. She is considering using the one-time pad, or the shift cipher over an alphabet of size 2^{1000} (instead of 26). What is key space size in each scheme?

   - One-time pad:
   - Shift cipher:

   (b) (5 points) For a uniformly random function $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$, does it always hold that $\mathcal{O}(x) \neq \mathcal{O}(x')$ when $x \neq x'$? Answer (yes, no, or unknown) and justify your answer.

   (c) (5 points) A secure MAC (i.e., unforgeable under chosen-message attack) cannot have a deterministic signing algorithm $S_k(\cdot)$. Is this statement True or False? Justify your answer.

   (d) (5 points) Let $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a secure PRF with $\mathcal{Y} = \{0,1\}^n$. Is $F_0(k,x) := F(k,x)[0,\ldots,\ell]$ also a secure PRF for every $0 \leq \ell \leq n$? Here $F_0(k,x)$ outputs the first ℓ bits of the output of $F(k,x)$.

   (e) (5 points) When using RSA-FDH (Full-Domain-Hash) to sign messages, how many valid signatures are there for a given message m for a fixed verification key? (the hash function used in RSA-FDH is fixed). Justify your answer.

   (f) (5 points) Recall the complexity classes P and NP. Suppose that $P = NP$. Is secure *symmetric-key* encryption possible? Justify your answer.

2. Iron man recently opened a startup company "WealthyCoin", and designed a few *symmetric-key cryptography* schemes.

   (a) (5 points) Let G be a PRG, construct $G'(s) = G(s) \oplus G(\bar{s})$. Is G' necessarily a PRG? Give a sketch proof or counterexample. (Here $\bar{s} = s \oplus 1^{|s|}$ denotes the bitwise complement of s, which sends each 0 to 1 and each 1 to 0.)

   (b) (6 points) Let P_k be a pseudorandom permutation with uniformly random key $k \in \{0,1\}^n$. To encrypt a message $m \in \{0,1\}^{n/2}$, choose uniformly random $r \in \{0,1\}^{n/2}$ and output ciphertext $c = P_k(r \| m)$. Iron man claims this is a CCA-secure scheme. Do you agree? If so, give a proof; otherwise, give an attack and determine what security definition it achieves.

   (c) (6 points) Let $H : \{0,1\}^* \to \{0,1\}^{128}$ be a collision resistant hash function known to the adversary. Define a MAC $S_k(m) := H(m) \oplus k$. Is this a secure MAC? If so, explain why. If not, describe an attack.

3. Wonder woman becomes excited about the brave new world of *public-key* cryptography, and she has proposed some constructions.

   (a) (6 points) $E'_{pk}(m) = E_{pk}(k) \| P_k(m)$, where E is a CPA-secure public-key encryption algorithm, pk is generated according to the key generator of E on input 1^n. $P_k(\cdot)$ is a pseudorandom permutation. Is E' necessarily CPA secure? Give a sketch proof or show an attack.

   (b) (6 points) Double sign. Let $\Pi = (G, S, V)$ be a secure signature scheme. Construct $\Pi' = (G' = G, S', V')$ such that: $S'_{sk}(m) := S_{sk}(m\|m)$; and Verify: $V'_{pk}(m, \sigma) := V_{pk}(m\|m, \sigma)$. Is Π' secure? Give a sketch proof or show an attack.

   (c) (Bonus 2pts) Based on above, who has a better sense in cryptography (i.e., higher rate of constructing secure schemes), Iron man or Wonder woman?

4. Expanding the message space of a cipher.

   (a) (8 points) Let (E, D) be a CPA-secure encryption scheme that encrypts messages in some space $\mathcal{M}$. Let (E_0, D_0) encrypt messages in $\mathcal{M}^\ell$, for some $\ell > 1$, by encrypting each component independently, but using the same secret key. That is, for $\ell = 3$, $E_0(k, (m_0, m_1, m_2)) = (E(k, m_0), E(k, m_1), E(k, m_2))$. Is (E_0, D_0) CPA secure? If so, explain why. If not, describe an attack.

   (b) (7 points) Suppose that (E, D) provides authenticated encryption. Does (E_0, D_0) provide authenticated encryption? If so, explain why. If not, describe an attack.

5. (Collision resistant hash function from the RSA problem) Let n be a random RSA modulus, e a prime and relatively prime to $\phi(n)$, and u random in $\mathbb{Z}_n^*$. Show that the function

$$H_{n,u,e} : \mathbb{Z}_n^* \otimes \{0, \dots, e-1\} \to \mathbb{Z}_n^*$$
$$(x, y) \mapsto x^e u^y \in \mathbb{Z}_n ,$$

is collision resistant assuming that the RSA problem (i.e., taking eth roots modulo n) is hard. Suppose A is an algorithm that takes n, u as input and outputs a collision for $H_{n,u,e}(\cdot)$. Your goal is to construct an algorithm B for computing eth roots modulo n.

(a) (5 points) Your algorithm B takes random n, u as input and should output $u^{1/e}$. First, show how to use A to construct $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}$ such that $a^e = u^b$ and $0 \neq |b| < e$.

(b) (6 points) Clearly $a^{1/b}$ is an eth root of u (since $(a^{1/b})^e = u$), but unfortunately for B, it cannot compute roots in $\mathbb{Z}_n$. Nevertheless, show how B can compute the eth root of u from a, u, e, b. This will complete your description of algorithm B. Hint: since e is prime and $0 \neq |b| < e$ we know that b and e are relatively prime. Hence, there are integers s, t so that $bs + et = 1$. Use a, u, s, t to find the eth root of u in $\mathbb{Z}_n$.

(c) (5 points) Show that if the factorization of n becomes public, then the function is not even a one-way function.

Scrap paper – no exam questions here.