Practice Final Exam

Name: ____________________

Winter 2017, CS 485/585 Crypto
Portland State University

March 14, 2017
Prof. Fang Song

Instructions

- This exam contains 7 pages (including this cover page) and 5 questions. Total of points is 90.
- You will 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.
- You may refer to facts and theorems proved in class and textbook without proving them. But you need to write the statements clearly.
- 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	18	
3	15	
4	13	
5	14	
Total:	90	

1. *Short answers.*

   (a) (4 points) A research team at Letni recently built a special-purpose machine that can crack a 56-bit DES key in 6 hours, by exhaustive search. Using similar hardware, what is the time to break a block cipher with

   i. a 96-bit key?

   ii. a 128-bit key?

   (You may assume that the time needed to evaluate the block cipher is the same in all three cases.)

   (b) (5 points) Assume that there is a pseudorandom generator (PRG) that expands by 1 bit $G : \{0,1\}^n \to \{0,1\}^{n+1}$, does exists a PRG that expands n^2 bits? Answer (Yes, No, or Unknown) and justify your answer.

   (c) (6 points) Let $P_k : \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation. Under CBC mode, how to encrypt and authenticate a message $m = m_0 \| m_1, m_i \in \{0,1\}^n$?

   - CBC-ENC:

   - CBC-MAC:

   (d) (5 points) Consider the DDH (Decisional Diffie-Hellman) and Discrete Logarithm (DL) assumptions relative to some group sampling algorithm $\mathcal{G}$. If the DDH assumption is false, is the DL assumption necessarily false? Answer (yes, no, or unknown) and justify your answer.

   (e) (5 points) Use Euclidean algorithm to find $52^{-1} \bmod 225$.

   (f) (5 points) If $P = NP$, is *public-key* encryption possible? If so, what definition covered in class can be achieved? Justify your answer briefly.

2. *Private-key primitives.*

   (a) (6 points) $G(1^n)$: pick random $k \leftarrow \{0,1\}^n$. $E_k(m \in \{0,1\}^{3n})$: choose random $r \leftarrow \{0,1\}^n$ and output ciphertext $c = (r, (G(r)\|k) \oplus m)$, where G is a PRG with stretch $\ell(n) = 2n$. What's the strongest security definition that this encryption scheme meets? Justify your answer.

   (b) (6 points) $G(1^n)$: pick random $k \leftarrow \{0,1\}^n$. $E_k(m \in \{0,1\}^n)$: let $p\|k' = G(k)$ for $p, k' \in \{0,1\}^n$ where G is a PRG with stretch $\ell(n) = 2n$, output ciphertext $c = m \oplus p$, and replaces k with k' for the next call (so E is stateful). Is it CPA-secure? Justify your answer.

   (c) (6 points) Let (G, S, V) be a secure MAC for messages $\mathcal{M}$. Construct $\Pi' = (G' = G, S', V')$ that signs messages in $\mathcal{M}^\ell$, for $\ell > 1$, by signing each component independently, using the same signing key for each component. That is, for $\ell = 3$, we have $S'_k(m_0, m_1, m_2) = S_k(m_0)\|S_k(m_1)\|S_k(m_2)$. Show that Π' NOT a secure MAC. Your attack should make use of a single message query.

3. *Public-key cryptography.*

   (a) (5 points) Consider encryption scheme $E_{pk}(m) = r^e \| (m \cdot r)$, where $pk = (N, e)$ is generated by the standard RSA key generator on input 1^n , $r \leftarrow \mathbb{Z}_N^*$ and the message space is Z_N^*. Is it CPA-secure? Justify your answer.

   (b) (10 points) Let (G, S, V) be a secure signature scheme (existentially unforgeable under chosen-message-attacks) with message space $\{0, 1\}^*$. Generate two signing/verification key pairs $(pk_0, sk_0) \leftarrow G(1^n)$ and $(pk_1, sk_1) \leftarrow G(1^n)$. Which of the following are secure signature schemes? Show an attack or explain why the scheme is secure, that is, explain why an attack on the scheme leads to an attack on (G, S, V).

      i. Accept one valid: $S^{(1)}_{sk_0,sk_1}(m) := S_{sk_0}(m) \| S_{sk_1}(m)$. Verify: $V^{(1)}_{pk_0,pk_1}(m, (\sigma_0, \sigma_1)) =$ accept iff. $V_{pk_0}(m, \sigma_0) =$ accept OR or $V_{pk_1}(m, \sigma_1) =$ accept.

      ii. Sign with appendage: $S^{(2)}_{sk_1}(m) := S_{sk_1}(m\|1010)$; $V^{(2)}_{pk_1}(m, \sigma) := V_{pk_1}(m\|1010, \sigma)$.

4. *Collision resistant hash from Discrete logarithm.* Let $\mathcal{G}$ be group sampling algorithm that on input 1^n generates a group G of prime order q with generator $g \in G$. Let h be a random element in G.

   (a) (8 points) Show that the hash function $H(x, y) := g^x h^y$ from $\mathbb{Z}_q \times \mathbb{Z}_q \to G$ is collision resistant, assuming the discrete-log problem in G is difficult.

   (b) (5 points) Show that one who knows the discrete-log of h base g can easily find collisions for H.

5. *Double encryption*. Let $E = (G, E, D)$ be an encryption scheme. Construct a *double encryption* scheme $E' = (G' = G, E', D')$, where $E'_k(m) = E_k(E_k(m))$.

   (a) (6 points) Show that there is a computationally secret E such that E' is not computationally secret.

   (b) (8 points) Prove that for every CPA-secure E, E' is also CPA-secure. That is, show that for every CPA adversary A attacking E' there is a CPA adversary B attacking E with about the same success probability advantage and running time.

Scrap paper – no exam questions here.