Massachusetts Institute of Technology
6.857: Network and Computer Security
Professors Ronald L. Rivest and Yael Tauman Kalai

Handout 6
April 13, 2020
Due: April 27, 2020

Problem Set 5

- This problem set is due on *Monday, April 27, 2020* at **11:59 PM**.
- The number of points allocated for each problem is a rough estimate in minutes of how long the problem will take to solve.
- Please submit your problem set, in PDF format, on Gradescope. A LaTeX template of the problem set is provided. Include all problems in the same PDF file.
- You are to work on this problem set **individually**.
- This problem set is **open notes**. You may use the lecture notes posted to the course website, and any notes that you took yourself during class. You may also use any other resources online or otherwise, except for other students. Consulting office hours and private posts on Piazza is also allowed.
- Corrections, if any, will be announced on Piazza.

Name:	
Student ID:	

Problem 1. True or False [4 points each; 24 points total]

Circle true or false for the following statements, and **briefly justify your answer.**

True **False** Consider the following variation of RSA. Encrypt a message m as $(r^e, H(r) \cdot m^e)$ where r is a random element in $\mathbb{Z}_n^*$ and $H : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$. This scheme is CCA secure in the Random Oracle Model.

True **False** Differential cryptanalysis was the first published attack which was capable of breaking the full 16-round DES in less than 2^{55} complexity.

True **False** CBC mode with AES is CPA-secure when we use a fixed IV.

True **False** One-Time Pad Encryption Scheme is not CPA secure.

True **False** CCA security implies CPA security.

True **False** An algorithm that only releases aggregate statistics of its private data is differentially private.

Problem 2. Short Answer [8 points each; 88 points total]

Answer in no more than a couple of sentences.

(a) What is the order of $\mathbb{Z}_n^*$ when $n = 105$? What is the least t such that $13^t = 1 \mod 105$?

(b) Name three privacy guarantees you would want a digital contact tracing scheme to have.

(c) An interactive proof system extends classical ones in two ways: It allows interaction, and allows the verifier to toss coins and accept a false statement with very small probability. Suppose we only allowed interaction, without allowing randomness and false acceptance. Explain why such proofs are not more powerful than classical proofs.

(d) Let $\text{Enc}_K : \{0,1\}^n \to \{0,1\}^n$ be an ideal block cipher.

Alice and Bob want to use Enc to encrypt messages of length $2n$. Alice suggests encrypting a message $m = (m_1, m_2)$ by choosing a random $r \in \{0,1\}^n$, computing $c_1 = \text{Enc}(K, r) \oplus m_1$ and $c_2 = \text{Enc}(K, \text{Enc}(K, r)) \oplus m_2$, and outputting (r, c_1, c_2) as the ciphertext.

Is this scheme secure against adaptive chosen plaintext attacks (IND-CPA)? Is it secure against adaptive chosen ciphertext attacks (IND-CCA2)? Explain your answers.

(e) Consider a candidate commitment scheme $\text{Com}(M, K) = (h(K), \text{Enc}(K, M))$, where K is the randomness of Com, $h : \{0,1\}^n \rightarrow \{0,1\}^{\frac{n}{2}}$ is a hash function, and Enc is a CPA-secure encryption.

1. What can go wrong if h is not collision resistant?

2. Suppose h is collision resistant. Is the scheme necessarily hiding?

3. Suppose h is collision resistant. Is the scheme necessarily binding?

(f) Suppose Alice has a secret s and uses Shamir's secret sharing scheme over $\mathbb{Z}_p^*$ to share it with her friends. Alice has n friends and wants any k of them to be able to retrieve the message. After she distributes the shares, she understands that she has made a mistake and the shares reveal the secret $s' = 2s + 1$. Explain how should her friends change their shares to obtain the real secret s (assuming they know that the secret that was distributed was twice the intended secret plus 1).

(g) Consider a candidate commitment scheme $\mathrm{Com}(m, r) = (f(r), r \oplus m)$, where f is a one-way function. Is this commitment scheme hiding? Is it binding? Explain.

(h) Let M_n be a Merkle tree of depth n with 2^n leaves. You are given the root of M_n. Consider the problem of authenticating two different leaves at the same time.

1. What is the minimum number of values you need in the best case? Explain.

2. What is the minimum number of values you need in the worst case? Explain.

(i) Explain why a commitment scheme needs to be randomized.

(j) Recall that the Bitcoin protocol recommends that a payment is accepted, not as soon as it appears on the block-chain, but rather after 6 additional blocks are added? Why is any delay recommended?

(k) In order to pick a random sample of ballots to examine in an election audit, one should start with a random "seed" S. Nobody should be able to force S to take a particular value. S determines (via some pseudorandom number generator) which ballots are examined.

Two mutually suspicious parties A and B want to pick a value for S in an additive group G, in such a way that neither can unduly influence S. Consider the following approach:

1. A picks a value $a \in G$ and announces $\text{Com}(a)$ to B where Com is a commitment scheme.
2. Similarly B picks a value $b \in G$ and announces $\text{Com}(b)$ to A.
3. Both parties open their commitments to reveal a and b respectively.
4. S is selected to be $a + b$.

Show that this scheme is not necessarily secure, even if Com is a hiding and binding commitment function.

Problem 3. Medium Answer [20 points each; 40 points total]

(a) Let $(\mathrm{Gen}_1, \mathrm{Enc}, \mathrm{Dec})$ be any CPA secure encryption scheme, and let $(\mathrm{Gen}_2, \mathrm{MAC}, \mathrm{Ver})$ be any MAC scheme that is existentially unforgeable under Chosen Message Attacks. Consider the encryption scheme $(\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$, where Gen' generates K_1 according to Gen_1, and K_2 according to Gen_2, and where Enc' is one of the following encryption algorithms:

1. $\mathrm{Enc}'((K_1, K_2), M) = M \parallel \mathrm{MAC}(K_2, \mathrm{Enc}(K_1, M))$
2. $\mathrm{Enc}'((K_1, K_2), M) = \mathrm{Enc}(K_1, M) \parallel \mathrm{MAC}(K_2, \mathrm{Enc}(K_1, M))$
   (both values of $\mathrm{Enc}(K_1, M)$ are the same)
3. $\mathrm{Enc}'((K_1, K_2), M) = \mathrm{Enc}(K_1, M) \parallel \mathrm{MAC}(K_2, M)$
4. $\mathrm{Enc}'((K_1, K_2), M) = \mathrm{Enc}(K_1, M \parallel \mathrm{MAC}(K_2, M))$

where $\parallel$ denotes concatenation.

For each of these encryption schemes, briefly explain why or why not the scheme is guaranteed to be CCA secure.

(b) Consider the digital signature scheme $(\text{Gen}, \text{Sign}, \text{Ver})$ for signing messages $m \in \{1, \ldots, p-1\}$, defined as follows:

- $\text{Gen}(1^n)$: Choose an n-bit prime p, a generator g for $\mathbb{Z}_p^*$, and a random element $x \in \{1, 2, \ldots, p-2\}$. Let x be the private key and $y = g^x \mod p$ be the public key. (We think of p, g as fixed and known to all users.)
- $\text{Sign}(x, m)$: Choose a random element $k \in \{2, \ldots, p-2\}$ such that $\gcd(k, p-1) = 1$. Let $r = g^k \mod p$. Let the signature be (r, s) where $s = (m - x \cdot r) \cdot k^{-1} \mod p-1$.
- $\text{Ver}(y, m, (r, s))$: Outputs 1 (i.e., accepts) if and only if $g^m = y^r \cdot r^s \mod p$.

Show that this scheme is correct, i.e., a validly produced signature will always be accepted.

Suppose that the random number generator is broken and this results in k being fixed. Would this scheme be existentially unforgeable under chosen message attack? Briefly explain why if it is, or provide an example of an attack if not.

Problem 4. Long Answer [40 points total]

Let $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be any public key encryption scheme with message space $\{0,1\}^n$, where n is the security parameter.

(a) Suppose that this scheme is secure against random message attacks; Namely,

$$(\mathrm{pk}, r, \mathrm{Enc}(\mathrm{pk}, r)) \approx (\mathrm{pk}, r, \mathrm{Enc}(\mathrm{pk}, r'))$$

for $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}(1^n)$, and uniformly and independently chosen messages $r, r' \leftarrow \{0,1\}^n$.

Consider the modified encryption scheme $(\mathrm{Gen}, \mathrm{Enc}', \mathrm{Dec}')$, where

- $\mathrm{Enc}'(\mathrm{pk}, m)$ chooses a random $r \leftarrow \{0,1\}^n$ and outputs $\mathrm{Enc}(\mathrm{pk}, r)$ along with $r \oplus m$.
- $\mathrm{Dec}'(\mathrm{sk}, (c, s))$ first computes $r = \mathrm{Dec}(\mathrm{sk}, c)$ and outputs $m = r \oplus s$.

Is $(\mathrm{Gen}, \mathrm{Enc}', \mathrm{Dec}')$ semantically secure? Explain your answer.

(b) Suppose that $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is only one-way secure; namely for every PPT algorithm A there exists a negligible function μ such that for every $n \in \mathbb{N}$,

$$\Pr[A(\mathrm{pk}, \mathrm{Enc}(\mathrm{pk}, r)) = r] \leq \mu(n)]$$

for $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}(1^n)$, and uniformly chosen message $r \leftarrow \{0,1\}^n$. (Note that textbook RSA is one-way secure.)

Demonstrate that $(\mathrm{Gen}, \mathrm{Enc}', \mathrm{Dec}')$, described above, is not necessarily semantically secure, by giving a counter example.

(c) Give a construction for converting any public key encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ that is one-way secure into one that is semantically secure in the Random Oracle Model. No need to prove the security of your construction.