Paxson Spring 2017 — CS 161 Computer Security — Midterm 2

PRINT your name: _____, _____
(last) (first)

I am aware of the Berkeley Campus Code of Student Conduct and acknowledge that any academic misconduct will be reported to the Center for Student Conduct, and may result in partial or complete loss of credit.

SIGN your name: _____

PRINT your class account login: `cs161-`_____ and SID: _____

Your TA's name: _____

Your section time: _____

Exam # for person sitting to your left: _____

Exam # for person sitting to your right: _____

You may consult one sheet of paper (double-sided) of notes. You may not consult other notes, textbooks, etc. Calculators, computers, and other electronic devices are not permitted.

You have 80 minutes. There are 5 questions, of varying credit (300 points total). The questions are of varying difficulty, so avoid spending too long on any one question. Parts of the exam will be graded automatically by scanning the **bubbles you fill in**, so please do your best to fill them in somewhat completely. Don't worry—if something goes wrong with the scanning, you'll have a chance to correct it during the regrade period.

If you have a question, raise your hand, and when an instructor motions to you, come to them to ask the question.

Do not turn this page until your instructor tells you to do so.

Question:	1	2	3	4	5	Total
Points:	80	60	40	60	60	300
Score:						

Problem 1 ***True/False*** **(80 points)**

For each of the following, FILL IN THE BUBBLE next to **True** if the statement is correct, or next to **False** if it is not. Each correct answer is worth 4 points. Incorrect answers are worth 0 points. Answers left blank are worth 1 point.

(a) Public key encryption is usually slower and has more overhead than symmetric key encryption.

True **False**

(b) If Alice comes up with a new idea that she wants to patent, to prove that she was the one who came up with the idea she can generate a digital signature of a description of the idea.

True **False**

(c) A cryptographic hash function is deterministic: given the same input, it always produces the same output.

True **False**

(d) A block cipher is deterministic: given the same input and key, it always produces the same output.

True **False**

(e) Alice and Bob share a symmetric key K, known to nobody else. Alice sends Bob a message $m =$ "I owe you \$100" and attaches a MAC tag t computed using K and m. Bob can use m and t to prove to a third party that Alice sent m.

True **False**

(f) A Diffie–Hellman exchange is secure against a passive attacker (Eve) but not against an active attacker (Mallory).

True **False**

(g) Suppose Alice has two secret keys, k_1 and k_2. If she encrypts messages using AES-CBC encryption with k_1, then she can generate secure IV's by computing $IV_i = \text{HMAC}(m_i, k_2)$, i.e., the IV is the HMAC of the message (m_i) using secret key k_2.

True **False**

(h) For AES encryption, Alice should not use the same symmetric key to encrypt more than one message.

○ **True** ○ **False**

(i) Given a random key, Alice can use AES-ECB to create a PRNG.

○ **True** ○ **False**

(j) To communicate confidentially in the presence of an eavesdropper, Alice and Bob can use the Diffie-Hellman protocol to exchange RSA public keys that they then use for public key encryption.

○ **True** ○ **False**

(k) ISPs are obligated to verify the IP source address on any traffic entering their network.

○ **True** ○ **False**

(l) A useful property of fiber optic cables is that the technology fundamentally eliminates the possibility of eavesdropping.

○ **True** ○ **False**

(m) It's difficult for an off-path attacker sending IP packets with a spoofed source to view the responses to those packets.

○ **True** ○ **False**

(n) In the event where the domain-name-to-IP-address binding changes, the DNS server responsible for the given domain name sends invalidation messages to clients in order to flush their mappings.

○ **True** ○ **False**

(o) Randomizing the DNS query identifier prevents an on-path attacker from spoofing DNS responses.

○ **True** ○ **False**

(p) If a laptop joining a WiFi network uses both DHCP and DNS, it will first use DHCP before using DNS.

O True **O False**

(q) When establishing a TCP connection, the client and the server engage in a three-way handshake to determine the shared Initial Sequence Number they will both use for that connection.

O True **O False**

(r) Hosts that use DHCP on a wired networking technology such as Ethernet are protected against possible DHCP spoofing attacks.

O True **O False**

(s) Source port randomization helps defend against an off-path attacker performing the Kaminsky DNS cache poisoning attack.

O True **O False**

(t) "Bailiwick" checks in modern DNS resolvers will prevent a malicious name server responsible for `foo.com` from using the Additional fields in its DNS responses to poison cache entries for `bar.com`.

O True **O False**

(u) If a WiFi network `MyCoolWifi` uses WPA2-Personal, and the administrator of the network chooses the network's password carefully so that it cannot be guessed, that will prevent an attacker who does not know the `MyCoolWifi` password from successfully eavesdropping on messages sent by users who know the password and have joined `MyCoolWifi`.

O True **O False**

Problem 2 ***Short questions*** **(60 points)**

(a) (8 points) Let M be a message of size 64 bytes. Let $C = \text{AES-CBC}_K(M)$; C does not include the IV. For which of the following values can a one-bit error in the value the receiver has for it potentially cause EVERY BLOCK to be decrypted incorrectly? **Mark ALL that apply.**

○ C ○ IV ○ K ○ **None of these**

(b) (8 points) Let M be a message of size 64 bytes. Let $C = \text{AES-CTR}_K(M)$; C does not include the nonce. For which of the following values can a one-bit error in the value the receiver has for it potentially cause EVERY BLOCK to be decrypted incorrectly? **Mark ALL that apply.**

○ C ○ Nonce ○ K ○ **None of these**

(c) (12 points) Let $M = M_1||M_2$ be a message of size exactly 2 blocks (where M_i are the blocks of M). Assume that Alice shares a secret key k with Bob. Alice encrypts M using AES-ECB, and computes $C = C_1||C_2$. She then computes a tag $t = F_k(C)$, and sends (C, t) to Bob. Which of the following choices for F would allow Bob to detect if an attacker tampers with C? **Mark ALL that apply.**

○ $F_k(C) = \text{MAC}_k(C_1) \,||\, \text{MAC}_k(C_2)$

○ $F_k(C) = \text{MAC}_k(\text{MAC}_k(C_1))$

○ $F_k(C) = \text{MAC}_k(C_1 \,||\, C_2)$

○ $F_k(C) = \text{MAC}_k(C_1 \oplus C_2)$

○ $F_k(C) = \text{MAC}_k(C_2 \,||\, C_1)$

○ None of these

(d) (12 points) Alice wants to encrypt messages using the CTR mode of operation, but instead of using AES, she wants to use some other keyed function F. Which of the following properties must F *necessarily* have to allow Alice and Bob to exchange messages securely? **Mark ALL that apply.**

○ The size of the input and output strings must be equal

○ F must be deterministic, i.e., the same input must always map to the same output

○ Unless one has knowledge of the key, the output of F must appear indistinguishable from a random string of the same length

○ F must be invertible, i.e., given the output along with the key, it must be possible to obtain the corresponding input.

(e) (8 points) RANK the following types of attackers according to which is strongest (rank=1). An attacker of type A is stronger than an attacker of type B if A can succeed at any attacks that B can succeed at, plus A has additional attack capabilities that B does not. If two types of attackers have equal strength, then give them the same rank: either both as 1 (with the third, inferior type of attacker ranked as 2), or both as 2 (if the third type of attacker is superior to them, and thus ranked 1). If none of the attackers is strictly stronger than any of the others, give them all the same rank of 1.

1. Passive on-path attacker

   ○ 1 ○ 2 ○ 3

2. Off-path attacker

   ○ 1 ○ 2 ○ 3

3. MITM attacker

   ○ 1 ○ 2 ○ 3

(f) (12 points) Tyrion is trying to download the latest version of the Bearship web browser from its official website, caltopia.edu. However, the download from caltopia.edu is taking too long, so Tyrion logs onto FastTorrent, a file sharing service where anyone can upload files for others to download. He searches for Bearship on FastTorrent and downloads the first file that's returned in the search results. Which of the following could caltopia.edu publish on their website to help users like Tyrion efficiently verify that the file they downloaded from a file-sharing service really is the Bearship browser, and not some malicious program? Efficiency means that if the browser is n bytes, the user does not have to download more than $n + O(1)$ bytes. Assume that the caltopia.edu website is secure. **Mark ALL that apply.**

- ○ Publish a screenshot of Bearship's user interface
- ○ Publish a secure hash (e.g., SHA-256) of the Bearship binary
- ○ Publish a digital signature of the Bearship binary
- ○ Publish a MAC, along with an associated key, of the Bearship binary
- ○ Publish a version of the Bearship binary encrypted using caltopia.edu's public key
- ○ Publish a version of the Bearship binary encrypted using AES, along with an associated key.

Problem 3 ***Just How Brutal Does The Force Need To Be?*** **(40 points)**

Consider a secure hash function H that produces a 60-bit hash.

(a) Suppose that $H(1)$ happens to hash to 0 (i.e., 60 zero bits). If you don't know anything further about H other than that fact and that it's a secure hash function, what is the probability that $H(2)$ also hashes to 0?

(b) What is the probability that H has at least one collision? Explain in 1 sentence.

(c) Suppose that commodity hardware can compute a single computation of H in 10 nanoseconds ($= 10^{-8}$ sec). Within an order of magnitude, how many years will it take for an attacker using a single system to find an x such that $H(x) = y$ for a specific y? You can approximate one year as $3 \cdot 10^7$ sec.

(d) Suppose now that a sustained form of Moore's Law means that after every year, H can be computed twice as quickly as for the previous year. (For this problem, assume that this acceleration happens discretely year-by-year, rather than being spread across a given year, as is actually more realistic.) Given this change, now about how many years will it take the attacker to find such an x?

Problem 4 ***RST injection*** **(60 points)**

This problem concerns RST injection attacks.

(a) In ONE SENTENCE, explain the purpose of a RST injection attack: that is, what goal does an attacker try to accomplish by launching such an attack?

(b) What information is needed for an attacker to carry out a successful RST injection attack?

(c) Explain under what circumstances an off-path attacker can conduct a successful RST injection attack. If it is impossible for them to do so, explain why they cannot.

(d) Suppose an attacker launches a RST injection attack against Alice. Are there situations in which Alice can detect that the attack has occurred? If **YES**, explain how she might do so. If **NO**, explain why it's not possible for her to do so.

(e) If Alice connects to a WPA2-Enterprise WiFi network, can an attacker successfully launch a RST injection attack against her? Explain why or why not.

Problem 5 ***How do you keep a secret?*** **(60 points)**

Frodo is trying to send a series of secret messages to Galadriel. For this question, we will refer to Galadriel as G and Frodo as F.

(a) (30 points) Assume that G and F share a secret key k. Let The-All-Seeing-Eye be a passive attacker who sees all messages sent by F to G.

For each encryption scheme below, select whether the encryption scheme is **Secure** or **Insecure**, and justify your answer in one or two sentences. A scheme is secure if, after observing all of the ciphertexts sent by F, The-All-Seeing-Eye learns nothing about the contents of any plaintext message beyond the message's length.

i. Encryption scheme:

1. F sets $IV = H(\text{the current timestamp})$, where H is a cryptographically strong hash function, and the timestamp is produced with enough precision such that two separate encryptions will not use the same timestamp value.
2. To send a new message m, F encrypts m using AES-CTR mode with IV and sends the resulting ciphertext.

Is this protocol secure against The-All-Seeing-Eye?

○ **Secure** ○ **Insecure**

Explanation:

ii. Encryption scheme:

1. F computes $p = H(k)$, where H is a cryptographically strong hash function
2. F stores a long-term counter x, which starts at 0 (assume no risk of overflow)
3. Let n be the number of bits in k, and assume that for this question, all messages are exactly n bits long and p is also n bits long. To send a new message m, F increments x by one and computes $s = \text{PRNG}(x)[1 : n]$, where s is the first n bits of a secure PRNG with a seed of x.
4. F then computes $k_x = p \oplus s$ and sends the ciphertext: $c = m \oplus k_x$.

Is this protocol secure against The-All-Seeing-Eye?

○ **Secure** ○ **Insecure**

Explanation:

(b) (30 points) Now assume that instead of sharing a secret key, G and F have shared their public keys, K_G and K_F. They use these keys to exchange a new symmetric key using the following protocol:

1. $F \longrightarrow G \ : \ \{F, N_1\}_{K_G}$
2. $G \longrightarrow F \ : \ \{N_1, N_2\}_{K_F}$
3. $F \longrightarrow G \ : \ \{N_2\}_{K_G}$

In step 1, F generates a random nonce N_1 and sends it to G along with his identity F (to identify himself to G), after encrypting these with her public key. G responds in step 2 by generating a random nonce N_2, and sends it to F along with N_1 (to prove that she possesses the private key K_G^{-1}) after encrypting these with F's public key. F finally returns N_2 encrypted with G's public key, to prove that he possesses the private key K_F^{-1}.

F and G now compute a new symmetric key as $K = N_1 \oplus N_2$, and encrypt all subsequent messages using K.

Frodo meets Mallory, and unfortunately doesn't know that Mallory is evil. Frodo decides to start a conversation with Mallory after obtaining her public key K_M. Mallory realizes that if Frodo initiates the same key exchange protocol with her, then she can do so with Galadriel while pretending to be Frodo. (Assume Mallory has obtained Galadriel's public key.)

i. **Fill in the blanks** such that at the end of these steps, Galadriel thinks that she's exchanged a symmetric key K' with Frodo. Write down the value of K'.

(i) $F \longrightarrow M \ : \ \{F, N_1\}_{K_M}$ (ii) $M \longrightarrow G \ :$ _____

(iii) $G \longrightarrow M \ :$ _____ (iv) $M \longrightarrow F \ :$ _____

(v) $F \longrightarrow M \ :$ _____ (vi) $M \longrightarrow G \ :$ _____

$K' =$ _____

ii. Which of the following changes to **step 1** ("$F \longrightarrow G \ :\{F, N_1\}_{K_G}$") would prevent Mallory from impersonating Frodo? **Mark ALL that apply.**
The notation $[M]_{K^{-1}}$ represents a signature over M using a private key K^{-1}.

- ○ $F \longrightarrow G \ : \ (C, [C]_{K_F^{-1}})$, where $C = \{F, N_1\}_{K_G}$ (i.e., include a signature computed over the ciphertext)
- ○ $F \longrightarrow G \ : \ (\{F, N_1\}_{K_G}, [F, N_1]_{K_F^{-1}})$ (i.e., include a signature computed over the plaintext)
- ○ $F \longrightarrow G \ : \ (C, [C]_{K_F^{-1}})$, where $C = (F, \{N_1\}_{K_G})$ (i.e., only encrypt the nonce in the ciphertext; include a signature computed over this ciphertext)
- ○ None of these