14-741/18-631: Midterm exam
Tuesday, Sept. 29 2020, 90 minutes

Name:

Andrew ID:

Scores

Problem 1 (20 pts max):

Problem 2 (30 pts max):

Problem 3 (30 pts max):

Problem 4 (20 pts max):

Total (100 pts max):

Guidelines

- This exam contains 4 problems and is 5 pages long. Check you have all pages. To help us grade as anonymously as possible, please **do not write your name or any other identifying information on any page other than this cover page**.
- Be neat and concise in your explanations. You won't be penalized for using incorrect grammar, but you will get penalized if we can't understand what you are writing.
- Show your work clearly. If your reasoning (in other words, steps) is correct, but your final answer is wrong, you will receive most of the credit. On the other hand, answers without proof, explanation, or argumentation get no credit, *even if they are correct*.
- This exam is open-book. All reference books, class notes, dictionaries and calculators are allowed. **Searching the Internet during the exam constitutes an academic integrity violation and will be punished by failure of the class ("R") and other disciplinary measures at the discretion of the University.**
- Open-book does not mean open communications. Cheating on the exam (including accessing the Internet) automatically results in failure of the class and will be reported to the University administration. We do enforce university and departmental plagiarism policies strictly.
- It is advantageous to partially answer a question than not attempt it at all.
- Good luck!

1 DES (20 pts)

1. (10 pts) Bank A decided to enable offline pin verification by the ATM. To do so, the ATM card's magnetic stripe will store both the customer's account number and the encrypted PIN. The PIN is a 4 digit number selected by the customer. The PIN is encrypted using DES with an encryption key K. Bank A has one encryption key K for every customer and each ATM has K installed. That is the magnetic stripe stores $(\mathit{accnt\_number}, \mathsf{enc}_K(\mathit{PIN}))$. When the customer inserts the ATM card into the ATM machine, the ATM machine will prompt the user to enter a PIN (*pin*). The ATM then computes $c = \mathsf{enc}_K(\mathit{pin})$ and compares c with the encrypted PIN stored on the card. If they are the same, the ATM will allow the customer to withdraw money. Let's assume that an attacker can buy an ATM card reader/writer to read from and write to the magnetic stripe. How can an attacker withdraw money from the victim's account with a stolen ATM card without knowing the key K?

2. (10 pts) Bank A worries about DES being too weak and an attacker could obtain the key K by using brute force. Therefore, the bank proposes to replace DES with 2-DES using two keys K_1 and K_2 to improve security. That is, the encrypted PIN on the card is now $c = \mathsf{enc}_{K_2}(\mathsf{enc}_{K_1}(\mathit{PIN}))$. Is Bank A's proposal effective in making guessing the keys harder for the attacker? Explain why or why not.

2 Public Key Cryptography (30 pts)

Alice and Bob decide to use public key cryptography to secure their communication. Alice has a public, private key pair (K_A and K_A^{-1}). Bob has a public, private key pair (K_B and K_B^{-1}).

1. (10 pts) Bob wants his messages to Alice to have secrecy and message authentication properties. What scheme(s) that Bob should use and what is the message format that Bob should send to Alice (assuming the plaintext is m)? Please clearly state in your answer each of the functions (operations) that you are using.

2. (10 pts) Alice obtained the correct public key of Bob, but Bob mistook an attacker Mallory's public key K_M for Alice's key. Which one(s) of the properties among secrecy and message authentication of Bob's messages can Mallory violate and how?

3. (10 pts) Alice wants to check whether K_C is Charlie's public key. Alice obtained and validated Charlie's public key certificate CERT (for K_C). CERT is signed by CA1, whose public key is K_{CA1}. CA1's public key certificate (for K_{CA1}) is signed by CA2, and CA2 has a self-signed certificate. Alice learned that CA2's servers have recently been compromised, and its private key for signing certificates might have been leaked. However, CA1 has not been compromised. Should Alice trust that K_C is Charlie's key? Why or why not?

3 Birthday Paradox and Forged Signatures (30 pts)

1. (10 pts) CMU is hosting an alumni event and invited people who graduated between 1967 and 2019 (inclusive). How many people do you need to gather in the same room to have more than a **25%** chance that two of them gradated in the same year?

2. (10 pts) How many people do you need to gather in the same room to have more than a **25%** chance that one of them graduated in 2019?

3. (10pts) Alice wants to send an email saying "I have job openings." to Bob, with a digital signature of the hash of the message. The hash function that Alice uses is SHA-256, which generates a fixed size 256-bit (32-byte) hash. Alice uses her own private key for the signature. Bob has the corresponding public key. The key pair is a 2048-bit RSA key. Charlie is Alice's secretary, and is malicious. Charlie wants to change the message to "I do not have job openings" while fooling Bob into believing that's what Alice said.

   Alice writes an email and ask Charlie to edit it. Charlie sends the edited email to Alice for final approval. Alice then computes the hash of the approved email and signs the hash. Then Alice gives the signature to Charlie, and asks him to send the email with the signature to Bob. What does Charlie need to do to have more than a 50% chance of succeeding in fooling Bob into believing that Alice's message is that she does not have job openings? (you do not need to produce a concrete number).

4 Keys (20 pts)

Consider the following encryption system. Time is discretized into slots $t = 0, 1, \ldots, n$. A master key K_0, is selected at time $t = 0$ by Alice and is shared with Bob. You can assume that K_0 is shared securely. Alice and Bob have synchronized clocks. At any time n ($n > 0$) Alice (or Bob) wants to send a message $m(n)$ to the other party, they encrypt it with a time-dependent key $K(n) = H^{(n)}(K_0)$, where H is a cryptographically secure hash function, and for any x, $H^{(n)}(x)$ denotes the function H applied n times to x; that is $H^{(1)}(x) = H(x)$, $H^{(2)}(x) = H(H(x))$, $H^{(3)}(x) = H(H(H(x)))$, and so forth up to $n = 100$.

Alice and Bob decide to refresh their keys periodically, at every hundred's cycle. For example, at time $t = 100$, they will exchange a new key K_1 to generate the next 100 keys (i.e., $K(101) = H(K_1)$, $\cdots$, $K(199) = H^{99}(K_1)$, and $K(200) = H^{100}(K_1)$. Alice and Bob decide to use a variant of Diffie-Hellman key exchange protocol as follows.

STEP.i Alice selects g and p as required by Diffie-Hellman, sends $\mathsf{enc}_{K(100)}(g, p)$ to Bob.

STEP.ii Alice select a secret value A, and sends $\mathsf{enc}_{K(100)}(g^A \bmod p)$ to Bob.

STEP.iii Bob select a secret value B, and sends $\mathsf{enc}_{K(100)}(g^B \bmod p)$ to Alice.

STEP.iv Alice decrypts Bob's message and get b and computes $b^A \bmod p$, and sets K_1 to it

STEP.v Bob decrypts Alice's message and get a and computes $a^B \bmod p$ and sets K_1 to it

1. (10 pts) Bob argues that none of the encryptions in the above exchange is necessary. Do you agree? Why and why not?

2. (10 pts) Mallory is monitoring the communication between Alice and Bob and collecting all the ciphertext from time $t = 1$ and onward. Mallory somehow obtained $K(30)$. Mallory wants to maximize the number of messages between Alice and Bob that she can decrypt. How can Mallory do it and how many messages (and what are the messages) that Mallory can decrypt?