Fall 2019
CS134: Computer and Network Security
Homework 3
Due: 12/04/19: 11:59pm

Full Name:
UCI ID Number:
Sources:

Guidelines:

- Use any word processor (or handwrite and scan your answers). Upload your solutions **in PDF** to Gradescope.
- No collaboration is allowed. The only people you may consult are the TA-s and the instructor.
- Looking up, paraphrasing or copying answers from the Internet or other sources is not allowed; doing so is a violation of academic honesty. You must cite any sources you use, e.g., reference books, Wikipedia, etc.

Warning: any submissions not following the above guidelines will receive a score of zero.

P1	P2	P3	Total
/40	/30	/30	/100

Problem 1: Certificate Revocation Trees

Suppose a certificate authority (CA) uses a Certificate Revocation Tree (CRT) to represent revoked certificates. The CA has issued a total of 500,000 certificates. Of those, 127 have been revoked. Assume that the ID of all revoked certificates are not continuous.

Each time a CRT is issued or updated, the CA hands the CRT to an online server CRT-SRV. CRT-SRV is responsible for storing and answering queries about the most up-to-date CRT. Answer to the following questions.

(a) What is the height of the CRT?

(b) If another 128 certificates get revoked, how many hash computations does the CA have to do to update the CRL? Assume that: (1) All 128 revoked certificates' IDs are not continuous; and (2) The additional 128 certificates' IDs are larger than the 127 certificates that are already revoked.

Suppose that Alice wants to check whether Bob's certificate is revoked. She queries CRT-SRV with Bob's certificate ID 43. Assume that Bob's certificate is not being revoked. Answer to the following questions.

(c) How many elements are there in the co-path of the answer to the query?

(d) How does Alice determine whether Bob's certificate is revoked? **Limit your answer to 3 lines.**

Solution:

Problem 2: Dining Cryptographers
Recall the *Super-posed Sending* protocol described in the lecture slides. Answer the following questions:

(a) Given n as the number of users in the network and m as the length of the message being announced, what is the time complexity of the Super-posed sending algorithm for one user in terms of m and n? (Assume the cost of communication between users is zero)

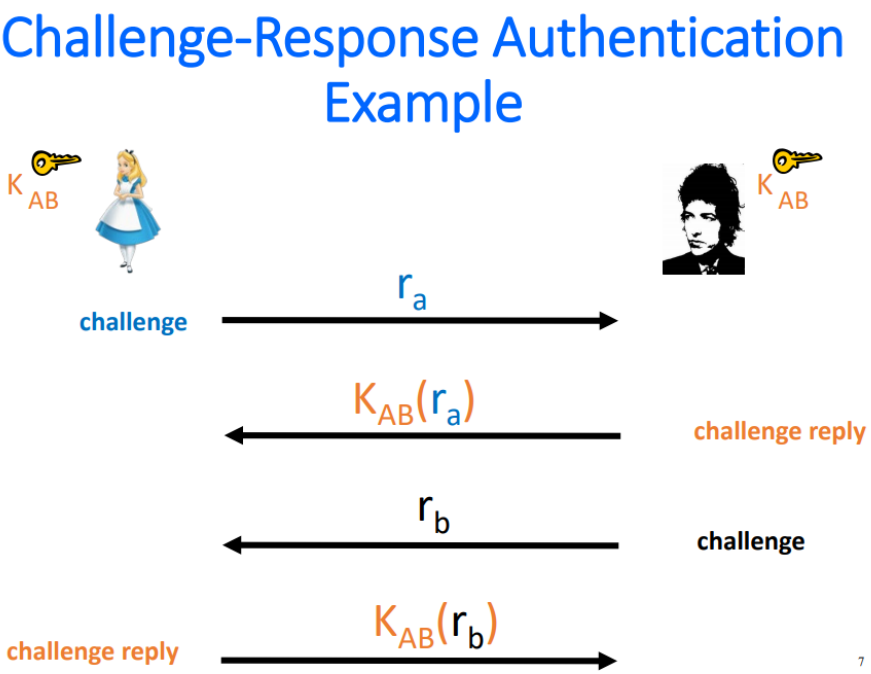
(b) Assume Eve and Charlie are Alice's neighbors. Eve and Charlie are able to collude off-line. How could they determine if Alice is the anonymous sender of the message? Assume the message is a one-bit '1' for simplicity.

(c) Consider a user Eve who is participating in the network, and is not the anonymous sender. How could she prevent everyone else from seeing the message, while still being able to see the message herself? Assume everyone else in the network is honest.

NOTE: You **must** justify all of your answers. **Limit your answers to 6 lines each.**

Solution:

Problem 3: Authentication Protocol
Recall the authentication protocol in the lecture:



(a) Explain how an adversary (Eve) can perform a reflection attack to bypass this authentication protocol without knowing K_{AB}. Note that K_{AB} was securely shared in the first place, and r_a and r_b are randomly generated on each challenge.

(b) Present **TWO** ways to modify this authentication protocol in order to avoid the reflection attack. Write down the modified protocols in details and state your assumptions clearly.

Solution: