Lab 4 Theory

This assignment is due **at 10:00pm ET** on **Thursday, November 18, 2021**.

Please make note of the following instructions:

- Remember that your solutions must be submitted on Gradescope. Please sign-up for 6.S060 Fall 2021 on Gradescope, with the entry code `KYRBPK`, using your MIT email.
- We require that the solution to the problems is submitted as a PDF file, **typeset on LaTeX**, using the template available on the course website (`https://6s060.csail.mit.edu/2021/`). Each submitted solution should start with your name, the course number, the problem number, the date, and the names of any students with whom you collaborated.
- We will have bug bounties for Lab 3 and beyond. If you are the first to report a bug in either the Coding or the Theory parts of the lab you will receive a $10 Toscanini's Gift Certificate! Serialization is via Piazza – report the bug as a private question on Piazza and we will respond as soon as possible as to whether it is a real bug or not.

Problem 4-1. Metadata-hiding messaging [50 points]

A student group at MIT has n students in it. Each pair of students shares a secret random bit. That is, for every $i, j \in \{1, \ldots, n\}$, Student i and Student j, $i \neq j$, have shared secret random bit $s_{ij} \leftarrow_R \{0, 1\}$.

The students must decide whether their next outing will be to a bubble tea store or a coffee shop. To protect the privacy of group members' beverage preferences, the students decide to run an *anonymous* poll on this question.

Each student $i \in \{1, \ldots, n\}$ encodes their preference as a bit β_i: "0" for bubble tea and "1" for coffee. Each student i then publishes the value:

$$v_i = \beta_i \oplus \left(\bigoplus_{j=1}^{i-1} s_{ji} \right) \oplus \left(\bigoplus_{j=i+1}^{n} s_{ij} \right)$$

based on the s_{ij} values known to student i. The output of the poll is the value $v = v_1 \oplus \cdots \oplus v_n$.

(a) [10 points] Explain why $v = \beta_1 \oplus \cdots \oplus \beta_n$.

(b) [10 points] Assume that one of Student 1 or Student 2 is a coffee drinker but not both. Say that, after the students run this poll honestly, students $\{3, \ldots, n\}$ get together to try to figure out whether Student 1 or 2 drinks coffee. Explain why the values that Students 1 and 2 publish reveal no information about their beverage preferences.

(c) [10 points] The protocol sketched above has a correctness problem. That is, the output value v does not exactly reveal the number of students who drink coffee. Explain how to modify the protocol so that it still provides beverage privacy but also provides correctness. (*Hint:* Work modulo $n + 1$ instead of modulo 2. Also, be careful of signs, since $x - y = x + y \bmod 2$, but when n is large $x - y \neq x + y \bmod (n + 1)$.)

(d) [20 points] After the students run the poll, they find that there are more coffee drinkers than boba drinkers. The students now want to anonymously poll the group to figure out which coffee place they should visit. That is, each student $i \in \{1, \ldots, n\}$ now holds an ℓ-bit string β_i. You may assume that each pair of students shares a long sequence of secret random bits.

Show that by running the original protocol (modulo 2) many many times in sequence, each student can anonymously broadcast the name of their desired coffee shop.

The students should recover the exact names of all n coffee shops with all but negligible probability in the security parameter λ.

Hint: Remember Ethernet from 6.033? The Wikipedia page at https://en.wikipedia.org/wiki/ALOHAnet#Pure_ALOHA may be helpful.

Problem 4-2. Implementing delegation [50 points]

Alice and Bob wish to generate a shared secret key. In class we saw how this can be done using the Diffie-Hellman key exchange protocol. Suppose this protocol is too slow for Alice and Bob, and they wish to only use (fast) symmetric cryptography, such as a symmetric encryption scheme and a MAC. Recall, as we mentioned in class, we do not know how to do key exchange using only symmetric cryptography!

Suppose, Alice and Bob each share a secret key with Carol, denoted by K_A and K_B, respectively, and suppose Alice and Bob trust Carol (and do not wish to hide any information from her). In this case, Carol can simply generate a fresh secret key K for Alice and Bob, and send it using an authenticated encryption scheme to Alice using K_A and to Bob using K_B, and then Alice and Bob can use K as their joint secret key. Note that Carol is the only party who knows their secret key K.

(a) [15 points]

Suppose Carol can only communicate with Alice (though she does share also a key K_B with Bob). What message can she send to Alice that will help Alice and Bob agree on a shared secret key (that only Alice, Bob, and Carol know)? The protocol should only use symmetric cryptography (encryption and MAC).

(b) [20 points]

Suppose that there is no *single* party that Alice and Bob trust. Suppose that there are two parties, Carol and David, each which shares a secret key with both Alice and Bob. Namely, Carol shares a secret key K_A with Alice and a secret key K_B with Bob, and David shares a secret key K'_A with Alice and a secret key K'_B with Bob.

Suppose Carol and David do not communicate with each other, and do not even know of each other. Design a protocol between these four parties such that at the end (assuming all parties follow the protocol) Alice and Bob share a secret key that is not known to either Carol or David (assuming that Carol and David do not collude). The protocol should only use symmetric cryptography.

(c) [15 points]

Suppose Carol and David can only communicate with Alice (though they do share a key K_B and K'_B respectively with Bob). What messages can they send to Alice that will help Alice and Bob agree on a shared secret key (that neither Carol nor David knows)?