Homework 03

ECE 443/518, Fall 2025

Due Date: 11/16, by the end of the day (Chicago time)

Let's work on the garbled circuit between Alice and Bob who want to compute $f = NAND(a, b)$.

1. *(1 point)* Suppose 0 and 1 on each wire is encrypted into a 5-bit number (0 to 31). Alice chooses $A_0 = 7$, $A_1 = 17$, $B_0 = 19$, $B_1 = 3$, and $O_0 = 18$, $O_1 = 6$. What are S_A and S_B?

2. *(1 point)* For the encryption function $e_{k_1||k_2}(x) = (k_1 + k_2 + x) \bmod 32$, show how Alice garbles the circuit. Suppose Alice chooses $a = 1$. What Alice should send to Bob as her input?

3. *(1 point)* Suppose Bob chooses $b = 0$. Show how Bob encrypts his input with Alice's help using OT. Assume Alice's RSA public key to be $(n = 35, e = 5)$.

4. *(1 point)* Show how Bob computes with the garbled circuit and the encrypted inputs, and then communicates with Alice to determine f.

5. *(1 point)* Show that Bob cannot decide Alice's choice of a (assuming OT only reveals B_0 but no additional information). As a hint, is it possible for Alice to choose $A_0 = 17$, $A_1 = 7$ while sending Bob exactly the same garbled circuit and inputs?