Q1: Consider auctions done using textbook RSA Encryption. Alice is selling a Phone and has public key PK. Bob would like to Bid 100 dollars. He encrypts his bid under public key PK and sends it to Alice. Trudy is watching over the channel and sees the ciphertext. He doesn't know Bob's bid. But he would like to bid exactly double of Bob and win the auction in style. Show that this is possible in RSA encryption.
Note: textbook RSA means without using hash

Q2: We saw that textbook RSA signatures are not secure because you can multiply two different signatures to obtain new signatures on new messages. However is textbook RSA at least a one-time signature scheme? That is, suppose that the adversary only gets a signature on a SINGLE message m. Can the adversary produce a signature on a different message m' not equal to m?

Q3: Consider the following variant of the ElGamal commitment scheme we saw in the class. The committer chooses a,b and sends g, m.g^ab to the receiver (where m is the message to be committed). In the opening phase, the committer sends a, b to the receiver. The receiver computes g^ab and then recovers the message. Is this commitment scheme binding? Is this hiding? Please give brief 2-3 line arguments.

Q4: Consider the following protocol for 2-party coin flipping. First, Alice commit to her bit b0. Then Bob commits to his bit b1. Then Alice opens b0 following which Bob opens b1. The output is the XOR of these two bits. Is this secure?

Next class: proposal presentation

EVERY student has to present

please prepare slides