CSC 300: Assignment 7

Solution to Extra Credit problem

1. **(10 pts; Extra Credits)** Can you apply the idea of using the computational hardness of finding the prime factors of a large composite, to enable two people, A and B, to perform a coin-toss over the telephone, such that none of them has any reason to suspect that the other person cheated? This means, say A tosses, then B calls (i.e., H/T) over the telephone, and then A verifies whether B's call is correct over the telephone, but somehow B is satisfied that A has not cheated even though he did not personally witness the toss. They will clearly need to exchange more information (relating to security) than I just outlined. Can you specify the exact procedure? Credits only for clear answers.

**Solution:** A chooses two large primes, \( p \) and \( q \), and encodes the result of the toss with the key \( n=p*q \). Then he passes the encoded message along with \( n \), to B. At this point B does not know the result of the toss since he cannot decrypt the message without \( p, q \). He then calls the toss ('H' or 'T') over the phone. A then verifies if this is correct and sends B the private keys, \( p \) and \( q \). At this point B can verify if his call was correct by decrypting the original message from A, using \( p \) and \( q \). He can also verify that indeed \( n=p*q \), i.e., A did not select \( p, q \) post-facto to claim that B was wrong. Since the message encoding the result of the toss was passed to him before his call, B is sure that A has not cheated. Since B made the call before receiving the decryption key, A is also sure that B could not have cheated.