CSC 300: Assignment 7

Total: (10 pts + 5 pts E.C.)

1. **(10 pts)** Determine if 667 is a prime, and if not find its prime factors, using the procedure shown in class.

2. **(5 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, B makes the call ('H' or 'T') over the telephone, A verifies it, 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.