IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises X.

1. Consider the coin-flipping by telephone protocol (Protocol 2 from the lecture). Let $p = 11$, $q = 19$ and $y = 42$. Show all computation steps in detail.

2. You are given a black box that implements the following protocol between two parties:
   One party has no inputs and has two outputs, random bit strings s_0 and s_1 of length n. The other party has input bit c and its output is the string s_c. Use this black box to implement a 1-out-of-2 oblivious transfer for sending messages of n bits.

   Assuming the black box works exactly as described (the first party does not know c and the second party does not get to know $s_{c\oplus 1}$), show that your implementation is secure, *ie.* the sender of the oblivious transfer cannot learn which message was received and the receiver cannot learn both messages.

3. Alice and Bob are trying to use a binary symmetric channel with error probability $p = \frac{1}{2}$ to implement coin-tossing in the following way:
   Alice chooses a random bit b and sends it to Bob through the binary symmetric channel. Bob receives the bit b' and then sends it back to Alice using different channel without errors. Now Alice takes both bits and calculates the output of the coin-tossing protocol as $b \oplus b'$. After this she also sends b to Bob through the perfect channel so he can calculate the same output. Assuming neither party can influence the binary symmetric channel (other than inputing the input for Alice or accessing the output for Bob), discuss the security of this protocol.

4. Propose a generalization of the implementation of 1-out-of-2 oblivious transfer given in the lecture (the one which combines a public-key cryptosystem and a secret-key cryptosystem) that enables a k-out-of-n oblivious transfer.