Quantum Information Processing - Fall 2007

Problem set 10: Quantum cryptography
Due 7 Dec 2007

1) For the BB84 protocol, indicate what information is exchanged between Alice and Bob over a private channel, and what is sent over a public channel. In each case, indicate whether the channel must be a quantum channel or whether it can be a classical channel.

2) Suppose that Alice prepares a large number of pairs of entangled qubits, each in the state $(|01\rangle - |10\rangle)/\sqrt{2}$, and sends one half of each pair to Bob. Can you think of a procedure for Alice and Bob to use these Bell pairs in order to produce a secret, random, shared key? (the answer can be found in many books and other publications - try to come up with it by yourself) Describe what would happen if Eve uses the intercept-resend strategy for the qubits sent by Alice to Bob.