Exercises

1. Suppose that m users want to be able to communicate with one another using a classical cryptosystem. Each user insists on being able to communicate with each other user without the remaining $m-2$ users eavesdropping. How many keys $K = (K_E, K_D)$ must be developed? How many keys are needed if they are using a public key cryptosystem? How many keys are needed for each type of cryptosystem if $m = 1000$?
2. Suppose that a network of investors and stockbrokers is using public key cryptography. The investors fear that their stockbrokers will buy stock without authorization (in order to receive the commission) and then, when the investor's money is lost, claim that they had received instructions (producing as evidence an enciphered message to buy the stock, claiming that it came from the investor). The stockbrokers, on the other hand, fear that in cases when they buy according to the investor's instructions and the stock loses money, the investor will claim that he never sent the instruction, and that it was sent by an imposter or by the stockbroker himself. Explain how this problem can be solved by public key cryptography, so that when all of these sleazy people end up in court suing one another, there is proof of who is to blame for the reckless investing and consequent loss of money. (Suppose that, in the case of a lawsuit between investor A and stockbroker B, the judge is given all of the relevant enciphering/deciphering information — the keys $K_A = (K_{E,A}, K_{D,A})$ and $K_B = (K_{E,B}, K_{D,B})$ and the software necessary to encipher and decipher.)
3. Suppose that two countries A and B want to reach an agreement to ban underground nuclear tests. Neither country trusts the other, in both cases for good reason. Nevertheless, they must agree on a system of verification devices to be implanted at various locations on the territory of the two countries. Each verification device consists of a sophisticated seismograph, a small computer for interpreting the seismograph reading and generating a message, and a radio transmitter. Explain how public key cryptography can be used to enable all of the following (at first glance seemingly contradictory) conditions to be met:
   a. Country A insists on knowing the plaintext content of all messages emanating from its territory, in order to be sure that the devices are not used in coordination with espionage activities by Country B.
   b. Country B insists that Country A cannot fabricate a message from the devices which broadcast from its territory (i.e., a message saying that everything's OK, when in fact the seismograph has detected a treaty violation).
   c. Country A insists that, if Country B falsely claims to have received notification from the device of a treaty violation, then any interested third country will be able to determine that, in fact, no such message was sent.