Homework 6

Mathematics in Computer Science

1. Given an encoding algorithm E and a decoding algorithm D such that $E(D(m)) = m$ and $D(E(m)) = m$ how would you set up a public key cryptosystem?

   (a) What is made public?

   (b) How is a message sent? You do not need to explain padding or any sophisticated aspect, just a one sentence explaining the basic method.

   (c) How does one sign an encriptic message?

2. Give a brief description of how to attach a signature to a message in a public key crypto system. Two or three lines are sufficient for your answer.