For the Encrypted Key Exchange (EKE) authentication protocol described in class (Authentication slide set), answer the following:

A. (10 points) Describe what the security goals are. (A few sentences).
B. (10 points) Describe what the assumptions are. (One-third page)
C. (25 points) Why is the protocol secure given the assumptions? (One page)
D. (15 points) What would an adversary’s goals be? How might an adversary achieve these goals (note that an assumption would need to be violated)? (Half a page)
E. (15 points) Suppose you were to prototype the protocol in software, using Java, C or C++. The input to your program would be interactive. You would use standard libraries for the cryptographic primitives – encryption, secure hash functions and random number generator algorithms. What would your choices for the various cryptographic primitives be? Why? (Half a page)