Lab Diffie-Hellman Algorithm

Q1. GenerateParams (notes)

Write a Java program to generate DH parameters and print them out.

Q2. SaveDHKeys (notes)

Write a Java program to read in the DH parameters from file, and generate public and private DH keys. The keys should be stored in the file “data/argv[0]Public” and “data/argv[0]Private”.

Create two run configurations for the above program, one with argv[0] equal to Alice and the other with argv[0] equal to Bob.

Q3. GenerateAESKeyAndCheck (notes)

Read in both pairs of keys. Generate an AES key from AlicePrivate and BobPublic. Generate an AES key from BobPrivate and AlicePublic. Show they are the same.

Q4. DHClient (given)

TCP/IP Socket client

- Connect to the server
- Send Diffie Hellman parameters
- Generate a Diffie Hellman public key private key pair
- Base64 encode the public key and send it
- Read back the the Servers public key and Base64 decode it
- Convert it into a PublicKey object
- Generate a symmetric key using own private key and servers public key.
- Print out symmetric key (Base64encoded)

Q5. DHServer (skeleton given)

Write a TCP/IP Socket server to

- Accept a connection
- Read DH parameters
- Read the clients public key and Base64 decode it
- Convert it into a PublicKey object
- Generate own public key private key pair
- Send own public key as Base64 encoded string
- Generate a symmetric key using own private key and servers public key.
- Print out symmetric key (Base64 encoded)
- Close the connection