One of the main challenge to use a security key algorithm such as RC4 is the key exchange. Very often the key exchange must be done offline, otherwise you run the risk of the key being eavesdropped by a hacker.

Now implement Diffie-Hellman Key Exchange Algorithm in C++ or JAVA. A user will be asked to enter two prime numbers *g*and *p*, in the range 1 to 10000 (<https://primes.utm.edu/lists/small/10000.txt>). Then user A enters a number *a*, and user B enters a number *b*, both in the range of 1 to 100. Now compute the security keys generated by user A and user B respectively, and verify they are the same.

Submit the following:

1.       Source code

2.       A screen shot showing the keys generated by A and B.