

**SSN College of Engineering,
Department of Computer Science and Engineering
CS 6711 Security Laboratory**

Exercise 6:

To implement the Diffie Hellman Key Exchange algorithm

Programming Language: Java

Hints:

1. Choose a prime number p and g is a primitive root modulo p .
2. Check for the primality of the number p (using Miller Rabin Method)
3. Read X_A , the secret key of A, such that $X_A < p$.
4. Compute the public key of A, $Y_A = g^{X_A} \bmod p$
5. Read X_B , the secret key of B, , such that $X_B < p$..
6. Compute the public key of B, $Y_B = g^{X_B} \bmod p$
7. Compute A's shared secret key, $K = Y_B^{X_A} \bmod p$
8. Compute B's shared secret key, $K = Y_A^{X_B} \bmod p$
9. Display A and B's shared secret keys.