Cryptography – **Diffie-Hellman**

Public/Private Keys (Diffie-Hellman exchange)

1) With your partner, pick a prime number, *p.*

2) With your partner, pick a primitive root modulo *p*. This is an integer *r* between [1, *p* - 1] such that the values of (*r* ^ *x*) % *p* for all *x* in range [0, *p* - 2] are different.

3) Choose a secret number. Write it down. (this is your private key)

4) Compute your public key. Do this by computing *r* ^ (*private key*) % *p*. Tell your partner your public key. Write down the public keys here.

5) Compute your shared secret. Do this by computing (*your partner's public key*) ^ (*your private key*) % *p*.

6) Compare your shared secret with your partner. If they aren't the same, look for any errors you might have made.

7) What information would an eavesdropper have?

8) How could an eavesdropper check to see if they have guessed your secrets?

9) Get the information from another group that an eavesdropper would have. Try to reverse-engineer any of their secrets. Assume that you have a function that will tell you if you found a secret number.