Scott Christensen
09/26/16
C.S. 465

H.W. #5 Diffie-Hellman

1. How the Diffie-Hellman protocol works is that two people can share a message across an insecure network by both using two values g and p. P is an incredibly large prime integer while g is an integer less than p and for every number n such that 0<n<p, there is a power k of g such that n=g^k %p. Alice and Bob each generate a secret value only they know, a and b, respectively. Alice then relays the value g^a % p to Bob and Bob relays the value g^b % p to Alice. Each of them then use the number they were given, raise it to their own secret value, then mod it by p. By the distributive property of mods and powers, both Alice and Bob will have the same value of g^ab %p as their final number, which is the shared secret key k. No passive attacker overhearing their exchange can guess what k is.

2. Mallory could intercept and change some values that are exchanged between Alice and Bob. Mallory could replace the public values of g and p as they move from one person to the next so she can know what k will be for both people. Mallory could also simply stop both messages from moving from one person to the next and give 1 to both Alice and Bob so that no matter what the values of a and b are both will end up with 1 as k.

3. P should be 1024 – 2048 bits in order to be considered safe.
   Source: http://security.stackexchange.com/questions/47204/dh-parameters-recommended-size

4. The recommended size of p in DH is much larger that the recommended key size for AES because DH is an asymmetric algorithm while AES is a symmetric algorithm. In an asymmetric algorithm, the strength of the key is based off of the modulus' resistance to factorization into its prime components, which is roughly O((log n)^(2/3)). In symmetric algorithms the strength of the key is based upon its resistance to brute-force attacks because the key is literally just a random number and that complexity is O(2^n).
   Source: http://crypto.stackexchange.com/questions/6236/why-does-the-recommended-key-size-between-symmetric-and-asymmetric-encryption-di