Anthony Constantino
HW 5

Diffie-Hellman

1) Diffie-Hellman is a way for to share a secret key in a public setting using prime numbers without giving away what is that secret key. Both parties start with a large prime number p and a prime number g which is a prime root modulo p. Each of the parties sends the other a number calculated A = g^s % p (s being the secret integer and A being the result) then those results are used A^s % p on each side to generate the key by which the two parties can communicate with each other.

2) If Mallory can intercept each message between Alice and Bob, she can establish the keys from her end for each user and transfer the messages to Alice and Bob while acting as the middle man the entire time, and maintain the keys she had established between them from the beginning.

3) The recommended size is more than 512 bits but more realistically it would be 1028, 1536, or 2048 bits because with current machines and with a lot of effort 512 bits can be compromised.

   http://crypto.stackexchange.com/questions/1963/how-large-should-a-diffie-hellman-p-be
   http://security.stackexchange.com/questions/47204/dh-parameters-recommended-size

4) From what I could fine AES is using a symmetric key while DH uses an asymmetric key. Symmetric keys can be smaller because to calculate them is exponential 2^n where n is the number of bits. Asymmetric keys are calculated by pq which means p must be much larger to make it unfeasible to calculate. This is why p in DH must be so much larger than in AES.