## Math 316, 7.4, 7.5 Diffie-Hellman Key Exchange, ElGamal Cipher

Name:	
Read and take notes on 7.4 Diffie-Hellman Key Exchange, 7.5 ElGamal Cipher.	
Reading Questions	
1. What is the Diffie-Hellman Key Exchange? (It is not a cipher; it is a protocol. What does that mean? And what is it a protocol for?)	
2. What is the "man-in-the-middle attack"?	
3. What is the trapdoor for the ElGamal cipher?	
4. Describe the public key (the numbers known to everyone) and the private decryption key (the number known only to the person who will decrypt messages) for the ElGamal cipher.	
5. What is the private encryption key (the number known only to the person encrypting a message) for the ElGamal cipher?	

## Math 316, 7.4, 7.5 Diffie-Hellman Key Exchange, ElGamal Cipher

6.	What additional information needs to be sent, as a header, along with the ciphertext, in order for the decryptor to decrypt the ciphertext?
7.	What struck you in this reading? What is still unclear? What remaining questions do you have?