This homework covers the material on cryptography. Remember that you are welcome to use references as long as they are properly cited, but you are expected to work the problems yourself and be able to justify your answers. You are also welcome to use programs or software tools to help, but please note what you use (mostly because I'm curious which tools you will choose).

1. Let $p = 67$ and $q = 53$. Demonstrate the RSA algorithm with the following steps. (Note: you can use a computer if you want to, but you can probably also do this one by hand with a calculator if you prefer - totally up to you.)

   (a) Compute a private and a public key. (This is the part where you may want a computer - you need to find a number relatively prime to $\phi(n)$, as well as it's inverse mod $\phi(n)$. Again, these are small, you can probably do this by hand, but you are also welcome to use a software package such as sage or matlab, or walk through the Euclidean algorithm in order to get it.)

   (b) Encipher the message 48 65 108 108 111 (Hello in ASCII) with your public key; you can do this by treating each letter as a 8-bit character.

   (c) Decipher your answer to part b, demonstrating that the algorithm works.

2. Now two individuals have decided to use Diffie-Hellman key exchange to agree on a keyword. They agree that $p = 67$ and $s = 13$. Choose two private keys that will work for this algorithm, and verify that they do indeed wind up with the same keyword.

3. It is well understood that Diffie-Hellman key exchange is vulnerable to man-in-the-middle attacks. Look up the meaning of man-in-the-middle attacks, and explain (in your own words) how would you target the Diffie-Hellman protocol.

4. Extra credit: In the RSA algorithm, it is *extremely* important to use large numbers when generating keys. Demonstrate this fact by finding the private keys of the following individuals from their (relatively small public) keys:

Person	n	e
A	98662273	1313
B	99633329	2791