**Part 1**

1. Read and done
2. Can’t run applet
3. Answer the following questions about RSA
   1. Who invented it and when?
      1. Ronald Rivest, Adi Ahamir and Leonard Adleman 1977
   2. How is it used in today’s world?
      1. Mostly RSA is used as digital signature and key exchange. It is also used in multiple Digital Rights Management applications as well.
   3. What makes RSA secure?
      1. There is lots of math involved with RSA, but I would say that the biggest thing that makes it secure is the two prime numbers that the algorithm uses as its base numbers. The larger the two prime numbers the harder it will be to crack, but the larger the prime numbers the more computational power is needed to run the algorithm.

**Part 2**

1. Read about hashes in your test, Chapter 11
   1. Done
2. Complete the project at the end of Chapter 11 in your text, Project 11-2 Command Line Hashes, pg. 440
   1. Do all the steps and answer the questions
      1. What is the length of the hash for Country1.docx: 32
      2. What is the length of the hash for MD5DEEP.txt: 32
      3. Even though they are the same length, they are completely different hashes
      4. By removing the period it makes it a different hash from Country1.docx
      5. Well the sha1deep.exe increases the length of the hash by a little which means it is a little more secure. Sh256deep.exe increased the length of the hash by an even greater amount that sha1deep.exe. Whirlpooldeep.exe really increased the length of the hash (I didn’t count it but almost tripled in length). For each file Country1.docx and Country2.docx each hash was unique for each hashing function. The different hashing functions provided different hash lengths that as the hash gets longer it becomes harder to figure out the original message of the hash.
   2. Plus, answer one more question, Are there problems published with regards to MD4 or MD5 or other hashes?
      1. With MD4 hashing a collision weakness was found back in 1991 and following that more efficient attacks were found. In 2011 MD4 became historic, meaning out of date.
      2. MD5 was a newer version of MD4 and like its predecessor MD5 has a weakness for collisions. Researchers were able to match a different pair of documents using the same hash and researchers were able to carry of an attack using MD5 hashing to create fake certificates that looked like they came from a legitimate source.