

## Week 4 Essay Questions

Answer all questions below in a single document. Then submit to the appropriate assignment folder. Responses should be no longer than half a page.

1. Cryptography has been used in one form or another for over 4,000 years, and the attacks on cryptography have probably been in place for 3,999 years and 364 days. As one group of people works to find new ways to hide and transmit secrets, another group of people is right on their heels finding holes in the newly developed ideas and products. This can be viewed as evil and destructive behavior, or as the thorn in the side of the computing world that pushes it to build better and more secure products and environments. Describe these two types of people where one can build to secure the cryptography, and another to break it.
2. Cryptographic algorithms provide the underlying tools to most security protocols used in today's infrastructures. The algorithms work off of mathematical functions and provide various types of functionality and levels of security. A big leap was made when encryption went from purely symmetric key use to public key cryptography. This evolution provided users and maintainers much more freedom and flexibility when it came to communicating with a variety of users all over the world. Explain these two types of cryptography with examples of real-world applications.
3. Encryption can be supplied at different layers of the OSI model by a range of applications, protocols, and mechanisms. Today, not much thought has to be given to cryptography and encryption because it is taken care of in the background by many operating systems, applications, and protocols. Explain each protocol stack where encryption can be used and how it is used in real-world applications. Support your argument with examples.