CS4355 Assignment 1

October 31, 2019

Avery Briggs

3471065

**Question 1:**

1. Please answer the following questions:

1. List and briefly define categories of passive and active security attacks.

Passive – An attack that does not act but silently waits or listens for a trigger to activate.

Active – Attacks that run malicious software immediately and continuously.

1. List and briefly define the basic security requirements in computer and network security.

The main components

1. Describe the Kerckhoffs Principles.
2. Describe the functions of confusion and diffusion in symmetric ciphers.
3. Describe the Strict Avalanche Conditions in symmetric ciphers.
4. Describe the key management problem in conventional cryptosystems.