1. Define “confidentiality”, “integrity” and “availability”.
   1. Integrity – Data and origin (authentication) integrity
   2. Availability – Allowing access to data and resources
   3. Confidentiality – Keeping data and resources hidden
2. Explain passive attack and active attack. Which one is more difficult to detect? Why?

## Active Attack

* Attempts to alter system resources or affect their operation
* Involve some modification of the data stream or the creation of a false stream
* Four categories
  + Replay
  + Masquerade
  + Modification of messages
  + Denial of Service

## Passive Attack

* Attempts to learn or make use of information from the system but does not affect system resources.
* Eavesdropping on, or monitoring of, transmissions
* Goal of attacker is to obtain information that is being transmitted

In general, the passive attacks are the more difficult attacks to detect. This is because passive attacks do not alter the state of its data or system, so it is not apparent that damage is being caused. An example of a passive attack could be simply listening to communications between its targets and gather information. Alternatively, active attacks change the data or resources on a system which can cause the damaged target to behave in a way that is different from its normal operations.