CONFIDENTIALITY

- The goal of *confidentiality* is to keep the contents of a transient communication or data on temporary or persistent storage secret.

MESSAGE/DATA INTEGRITY

- When Alice and Bob exchange messages, they do not want a third party such as to be able to modify the contents of their messages.

ACCOUNTABILITY

- The goal of accountability is to ensure that you are able to determine who the attacker or principal is in the case that something goes wrong or an erroneous transaction is identified.

AVAILABILITY

- An *available* system is one that can respond to its users' requests in a reasonable timeframe

Non-Repudiation

- The goal of *non-repudiation* is to ensure Undeniability of a transaction by any of the parties involved.

AUTHENTICATION

AUTHENTICATION

- When exploring authentication with Alice and Bob, the question we want to ask is:

- if Bob wants to communicate with Alice, how can he be sure that he is communicating with Alice and not someone trying to impersonate her?

AUTHENTICATION

- Bob may be able to authenticate and verify Alice's identity based on one or more of 3 types of methods:
  - something you know,
  - something you have, and
  - something you are.