* CIA:
  + 1. Confidentiality: The avoidance of the unauthorized disclosure of information (involves the protection of data).   
       Tools: encryption, Access control, Authentication, Authorization, Physical security.
    2. Integrity: The property that information has not been altered in an unauthorized way.  
       Tools: Backups, Checksums, Data correcting codes.
    3. Availability: The property that information is accessible and modifiable in a timely fashion by those authorized to do so.  
       Tools: Physical protection, computational redundancies.
  + AAA:
    1. Assurance: refers to how trust is provided and managed in computer systems. It depends on: Policies, Permissions, Protections.
    2. Authenticity: the ability to determine that statements, policies and permissions issued by persons or systems are genuine. Tools include: Digital signatures
    3. Anonymity: The property that certain records or transactions not to be attributable to any individual. Tools: Aggregation, Mixing, Proxies, Pseudonyms

1. Security Attacks:
   * Active: is when an attacker tries to modify the content of the message.
   * Passive: is when the attacker observes the messages, copy them and makes use of them.
     1. Examples of Active: Denial Of service, Man in the middle, Session hijacking.
     2. Examples of Passive: Eavesdropping, Traffic Analysis.
2. Digital Signatures:
   * Public Key Encryption: this type of encryption uses two separate keys instead of 1 shared key. It uses a public and a private key.
   * Private Key Encryption: This type of encryption where only a single private key can encrypt and decrypt information.
3. Passwords:
   * Strong Password: Upper/lower cases, special chaacters, numbers.

Text, letter

Description automatically generated

1. Access control matrix is a table that defines permissions.  
   Text

   Description automatically generated  
   Table

   Description automatically generated

<https://www.calculatorsoup.com/calculators/math/gcf-euclids-algorithm.php>

Ceasar Cipher example:

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

<https://www.dcode.fr/caesar-cipher>

Row Transposition

Text

Description automatically generated

Fiestal Algorithm

Diagram

Description automatically generated

GF(n)

Text, calendar

Description automatically generated