Practical 3

Draw and explain diagram of CIA

- **CIA - Confidentiality, Integrity and Availability.**

  Together, these three principles form the cornerstone of any organization's security infrastructure; in fact, they (should) function as goals and objectives for every security program. **The CIA triad is so foundational to information security** that anytime data is leaked, a system is attacked, a user takes a phishing bait, an account is hijacked, a website is maliciously taken down, or any number of other security incidents occur, you can be certain that one or more of these principles has been violated.

Security professionals evaluate threats and vulnerabilities based on the potential impact they have on the confidentiality, integrity, and availability of an organization's assets—namely, its data, applications, and critical systems.

Based on that evaluation, the security team implements a set of security controls to reduce risk within their environment.

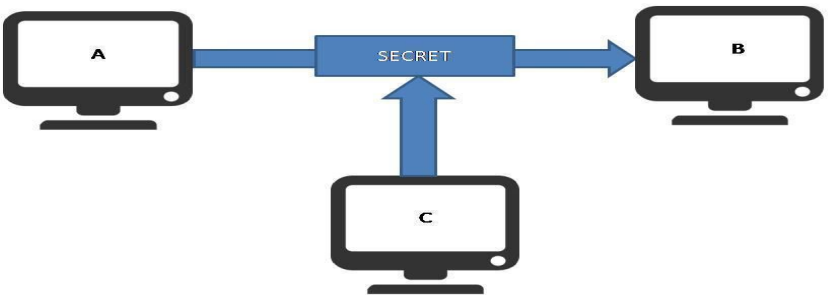
- **Confidentiality:**

Confidentiality refers to an organization's efforts to keep their data private or secret. In practice, it's about controlling access to data to prevent unauthorized disclosure.

Typically, this involves ensuring that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access.

As an example, only authorized Payroll employees should have access to the employee payroll database. Furthermore, within a group of authorized users,

there may be additional, more stringent limitations on precisely which information those authorized users are allowed to access.



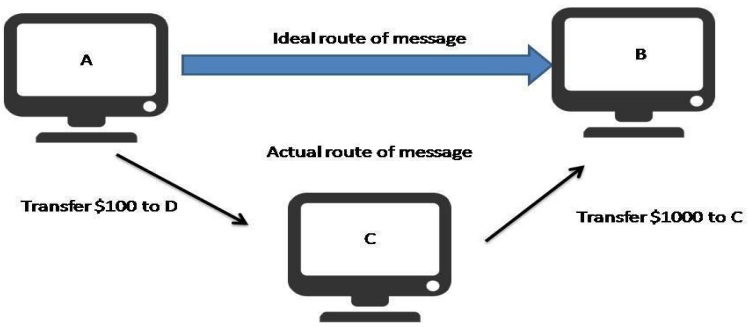
Countermeasures to protect confidentiality include data classification and labelling; strong access controls and authentication mechanisms; encryption of data in process, in transit, and in storage; steganography; remote wipe capabilities; and adequate education and training for all individuals with access to data.

- **Integrity :**

In everyday usage, integrity refers to the quality of something being whole or complete. In InfoSec, integrity is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable.

Ecommerce customers, for example, expect product and pricing information to be accurate, and that quantity, pricing, availability, and other information will not be altered after they place an order.

Banking customers need to be able to trust that their banking information and account balances have not been tampered with. Ensuring integrity involves protecting data in use, in transit (such as when sending an email or uploading or downloading a file), and when it is stored, whether on a laptop, a portable storage device, in the data center, or in the cloud.



Note that integrity goes hand in hand with the concept of non-repudiation: the inability to deny something. By using digital signatures in email, for example, a sender cannot deny having sent a message, and the recipient cannot claim the message received was different from the one sent. Non-repudiation assists in ensuring integrity.

- **Availability:**

Systems, applications, and data are of little value to an organization and its customers if they are not accessible when authorized users need them. Quite simply, availability means that networks, systems, and applications are up and running. It ensures that authorized users have timely, reliable access to resources when they are needed.

Many things can jeopardize availability, including hardware or software failure, power failure, natural disasters, and human error. Perhaps the most well-known attack that threatens availability is the denial-of-service attack, in which the performance of a system, website, web-based application, or web-based service is intentionally and maliciously degraded, or the system becomes completely unreachable.

Attack on Availability

Countermeasures to help ensure availability include redundancy (in servers, networks, applications, and services), hardware fault tolerance (for servers and storage), regular software patching and system upgrades, backups, comprehensive disaster recovery plans, and denial-of-service protection solutions.