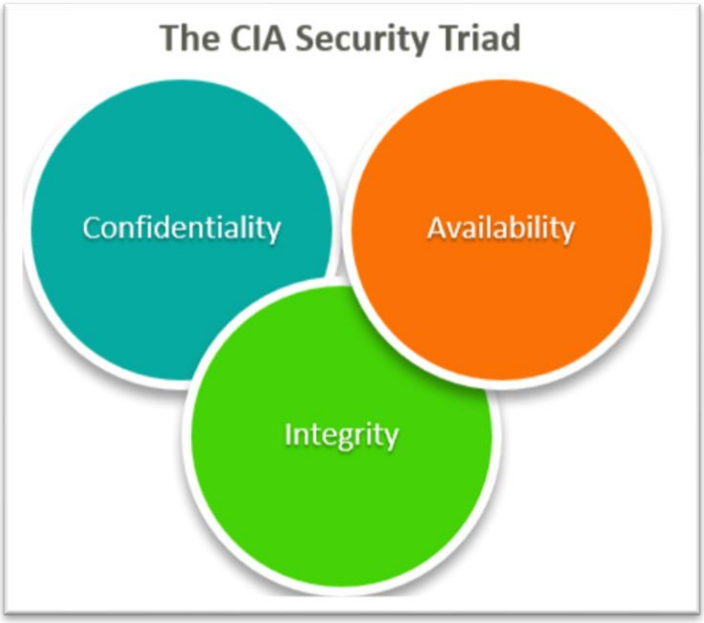
CIA TRAID: ASSIGNMENT 1

SHIVA SUPRITH CHENNA -G7 CS

CIA REFERS TO :

- Confidentiality
- Integrity
- Availability

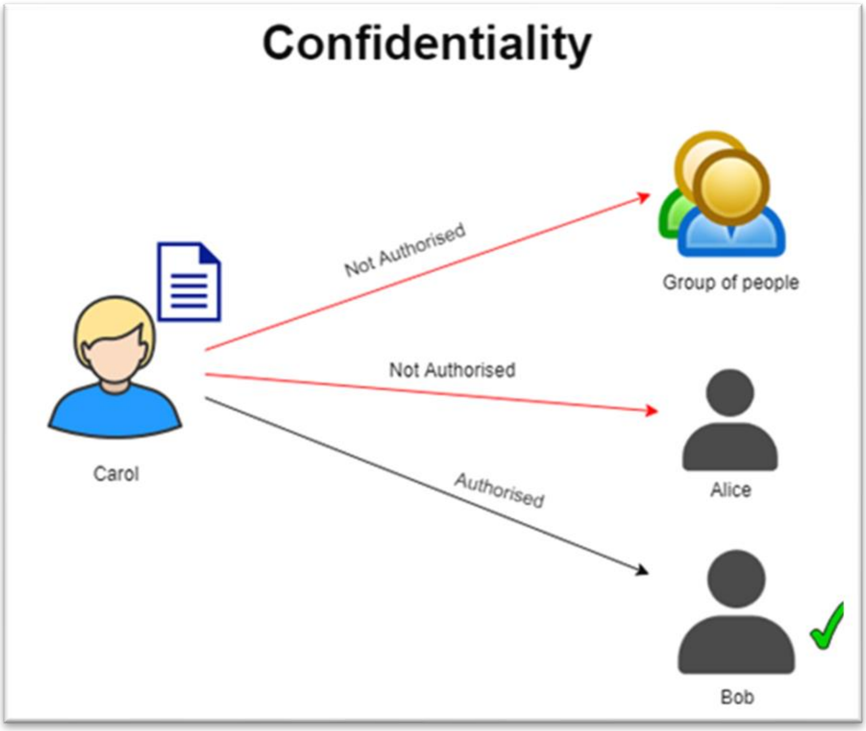
These three principles are really important in keeping information safe. They help us check if the security measures we use for our systems and networks are working well. These Principles are followed by every company to maintain safety across different things like data etc.



Let's look at each in more detail and also understand what the objectives of each principle

CONFIDENTIALITY:

Simply, Confidentiality ensures that sensitive information is accessible only to authorized individuals or entities. This principle aims to prevent unauthorized access and exposure of confidential data. Measures to maintain confidentiality include encryption, access controls, user authentication, and secure transmission protocols. By preserving confidentiality, organizations can protect sensitive information from falling into the wrong hands and mitigate the risks associated with data breaches and unauthorized disclosures. Some of the Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.



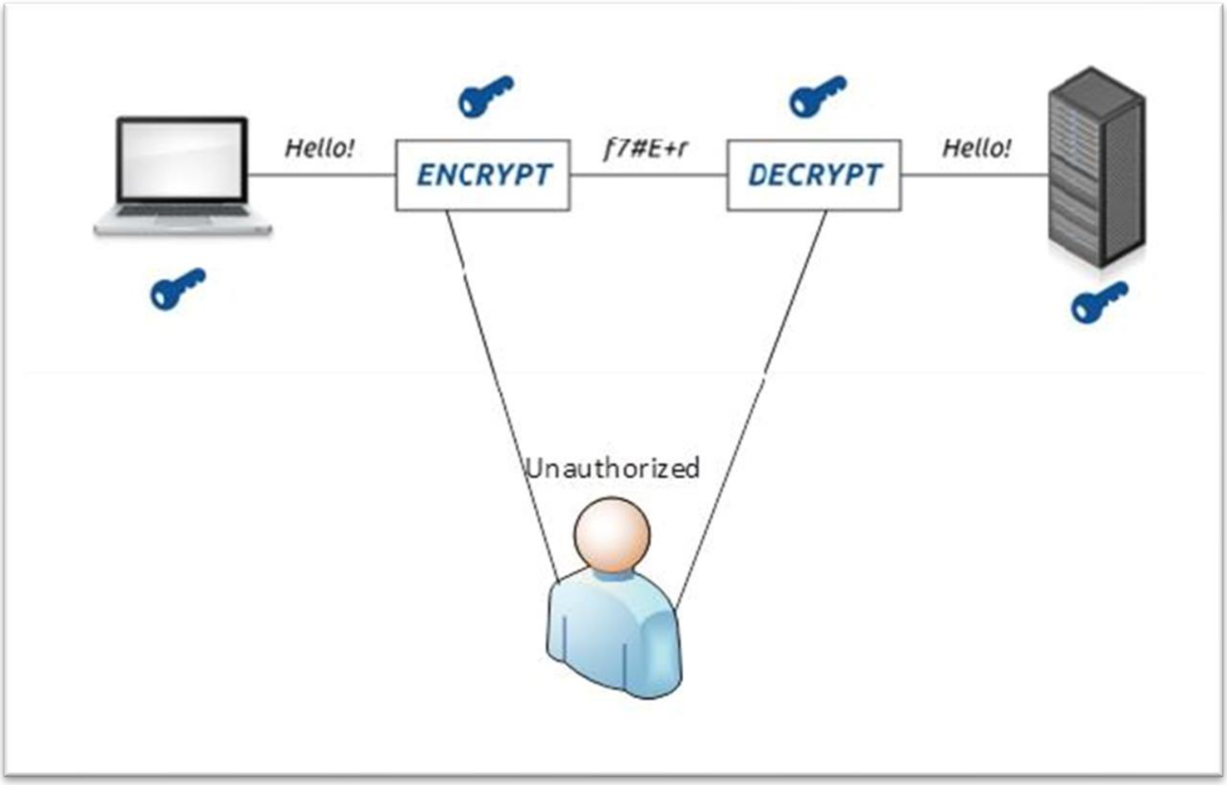
IMPORTANCE OF CONFIDENTIALITY:

Maintaining confidentiality helps organizations comply with regulations (e.g., GDPR, HIPAA) and industry standards, safeguarding against data breaches, identity theft, espionage, and insider threats. It fosters trust among customers, partners, and stakeholders by demonstrating a commitment to protecting their privacy and confidentiality.

INTEGRITY:

Now let’s talk about integrity. Integrity is like making sure things are correct and haven't been messed with. In information security, it means ensuring that data stays accurate and reliable.

For example: imagine you write a message to a friend. Integrity ensures that the message doesn't get changed or tampered with before it reaches your friend. It's about keeping information trustworthy and making sure it hasn't been altered by mistake or on purpose.

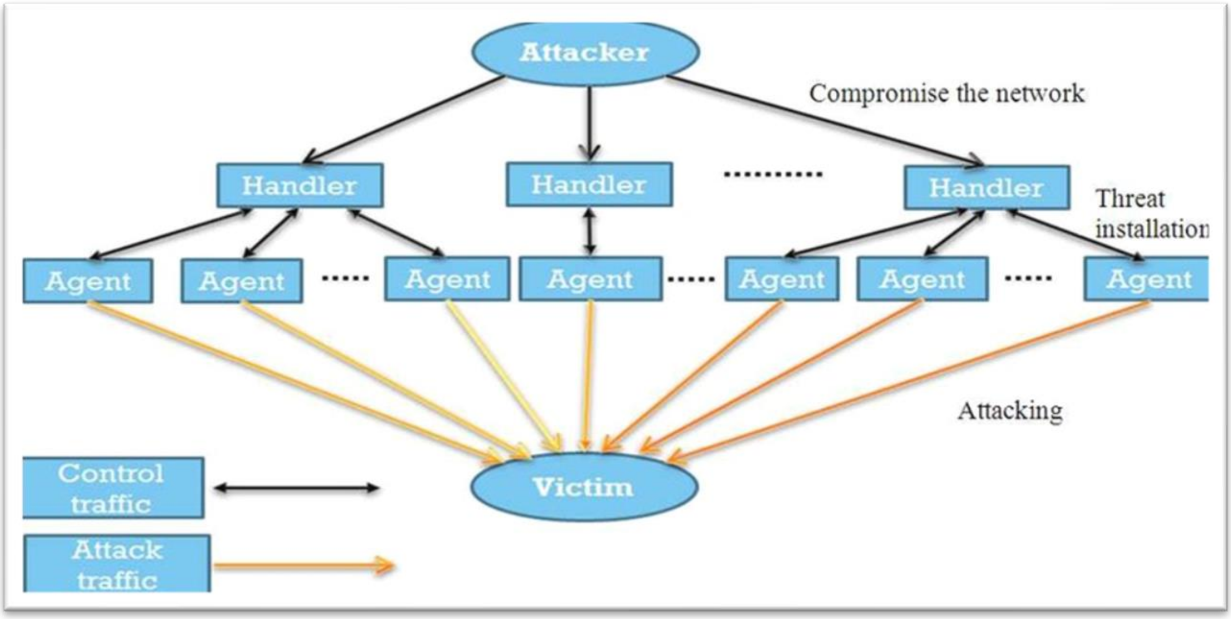


IMPORTANCE OF INTEGRITY:

Data integrity helps organizations prevent unauthorized modification, deletion, or corruption of critical data, thereby mitigating the risks of fraud, manipulation, and errors. It ensures the consistency and reliability of information, enhancing trust among users and stakeholders and reducing the likelihood of financial losses or reputational damage.

AVAILABILITY:

Availability in the CIA Triad is all about making sure that things are always there when you need them. It's like having your favorite website up and running whenever you want to visit it. Availability means preventing anything from stopping you from accessing important information or services. It's about keeping systems and data accessible and usable, even when faced with challenges like cyber attacks, technical failures, or other disruptions. In simple terms, availability ensures that the things you need are reliably available whenever you need them.



IMPORTANCE OF AVAILABILITY:

Availability safeguards against disruptions caused by system failures, cyber-attacks, and human errors, ensuring continuity of operations and minimizing downtime. It enables organizations to meet service-level agreements (SLAs), sustain customer satisfaction, and mitigate the impact of incidents on revenue, reputation, and operational resilience.

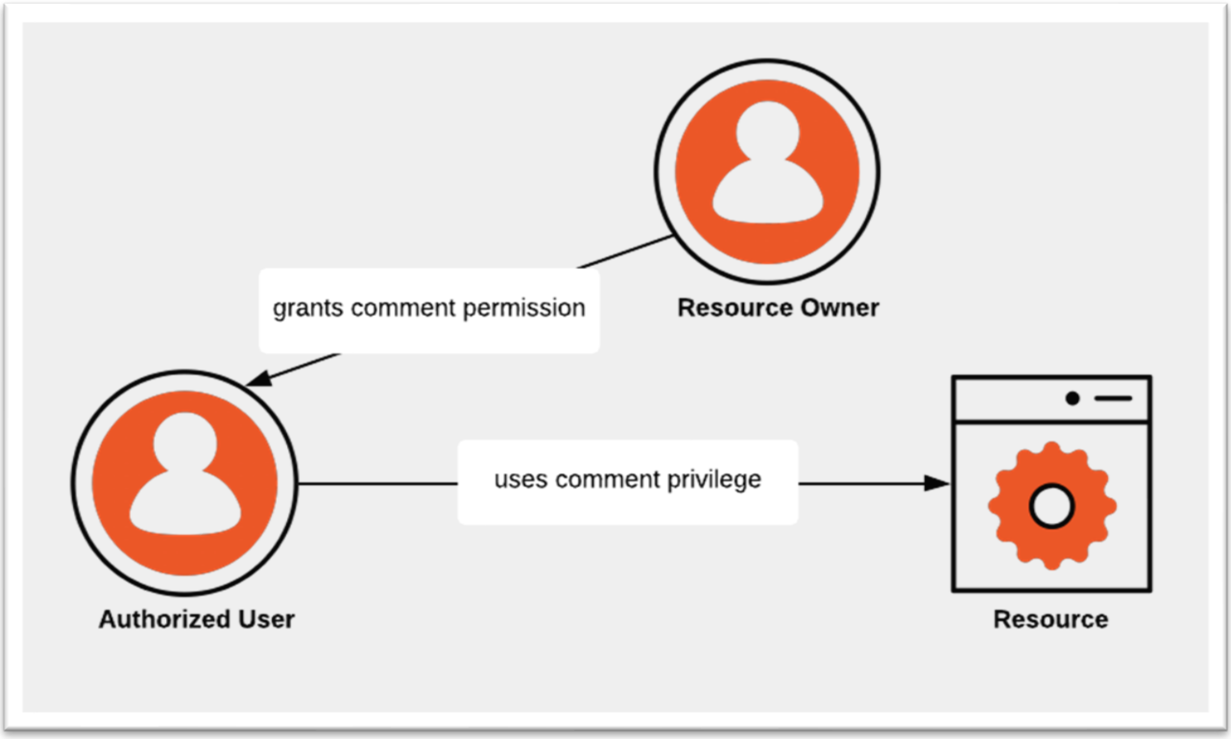
Authentication:

Authentication confirms a user's identity before granting access to a system or network. It's like checking identification before entering a secure facility. This process employs various methods such as passwords, smart cards, or biometric traits like fingerprints. By authenticating users, organizations prevent unauthorized entry, protecting sensitive information and from misuse. Effective authentication ensures that only legitimate users can access resources, bolstering security and minimizing the risk of data breaches or unauthorized access attempts.

In general, authentication acts as a gatekeeper, ensuring that only those with proper credentials or verified characteristics can gain entry. It's comparable to having a bouncer at a club entrance, verifying each guest's identity before granting admission. By employing robust authentication measures, organizations establish trust in their systems, mitigating the threat of unauthorized access and reinforcing the confidentiality and integrity of their data and resources.

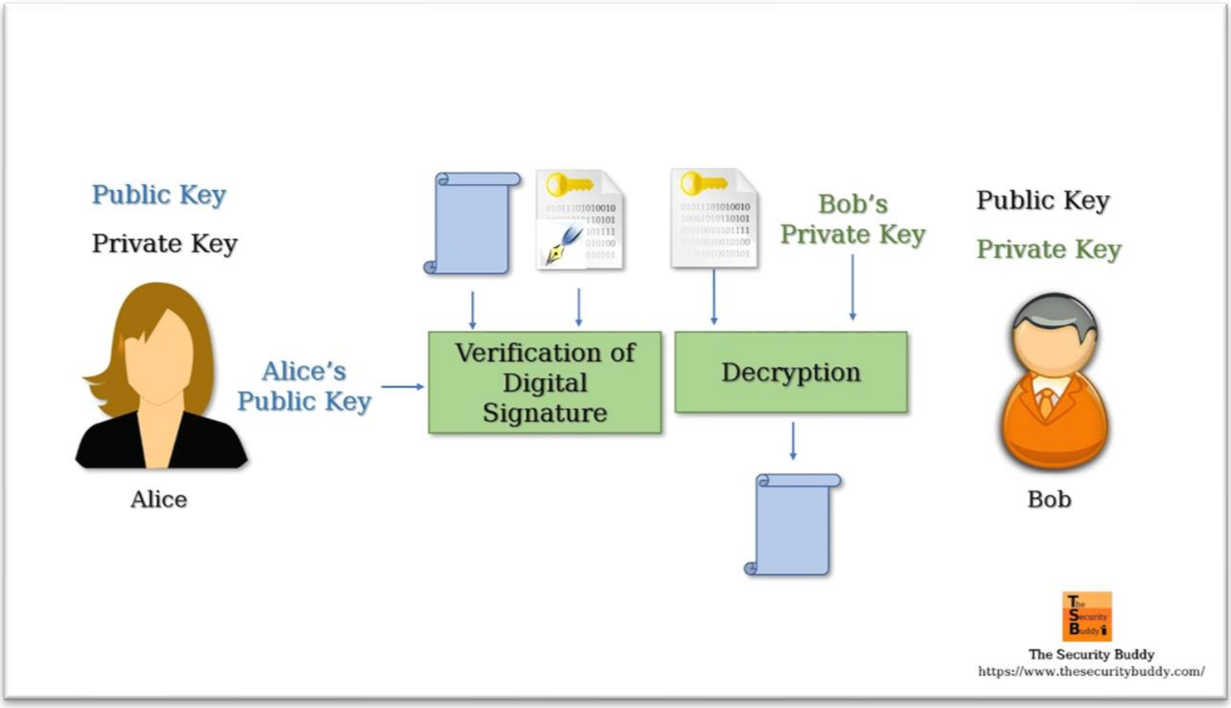
Authorization:

Authorization is the process of deciding what a user can do once they've proven who they are. After confirming a user's identity, authorization determines what actions or resources they're allowed to access in a system or network. It sets permissions based on the user's role or level of trust, specifying what tasks they can perform and what data they can see or change. This ensures that users only have access to what they need to do their job, following the principle of least privilege, which means giving them the minimum necessary access to get their work done securely.



NON-REPUDATION:

Non-repudiation guarantees that a user cannot deny their actions or transactions in a system or network. It offers proof that a specific user carried out certain actions, like sending a message or making a payment, preventing them from later denying it. Methods for non-repudiation include digital signatures, timestamps, and audit trails, creating tamper-proof records of user activities. By ensuring non-repudiation, organizations can hold users responsible for their actions, deter fraud, and build trust in electronic transactions and communications.


Public Key
Private Key
Alice
Alice's Public Key
Verification of Digital Signature
Decryption
Bob's Private Key
Public Key
Private Key
Bob
The Security Buddy
https://www.thesecuritybuddy.com/