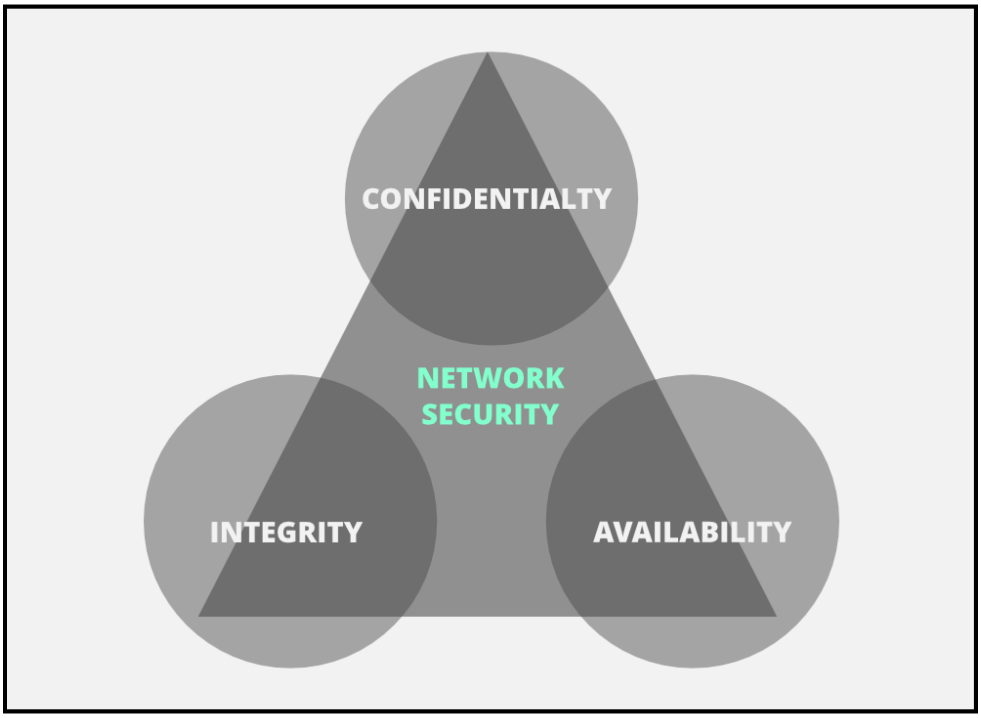
Assignment 1: CIA Triad

G7 CS – Name: Vinayak Vilaspure

CIA stands for:

1. Confidentiality
2. Integrity
3. Availability

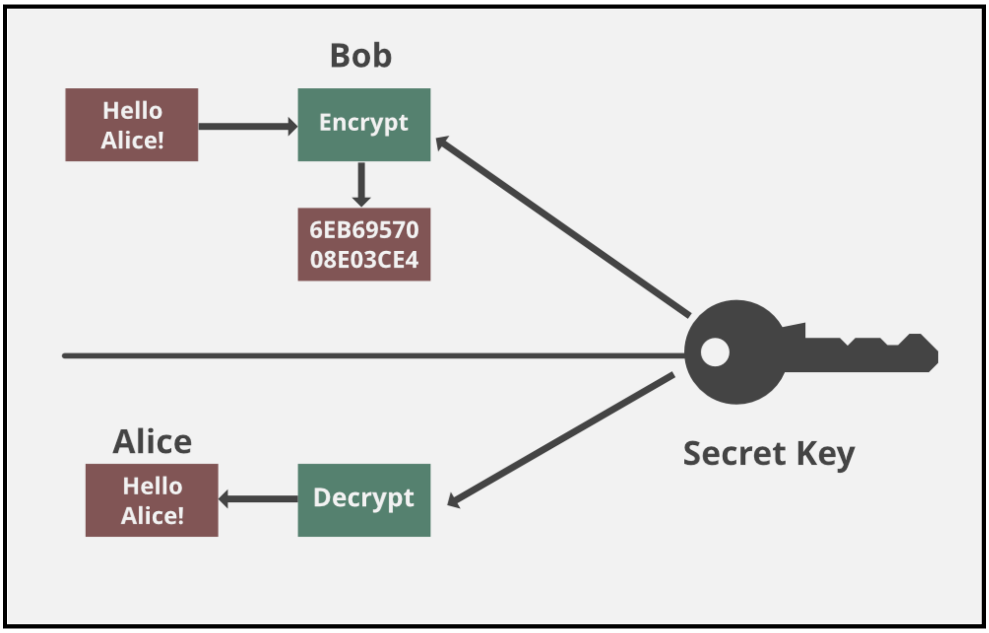
These three principles are fundamental to information security and are used to assess and ensure the effectiveness of security measures within systems and networks.



These are the objectives that should be kept in mind while securing a network:

- ## Confidentiality

Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. 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.

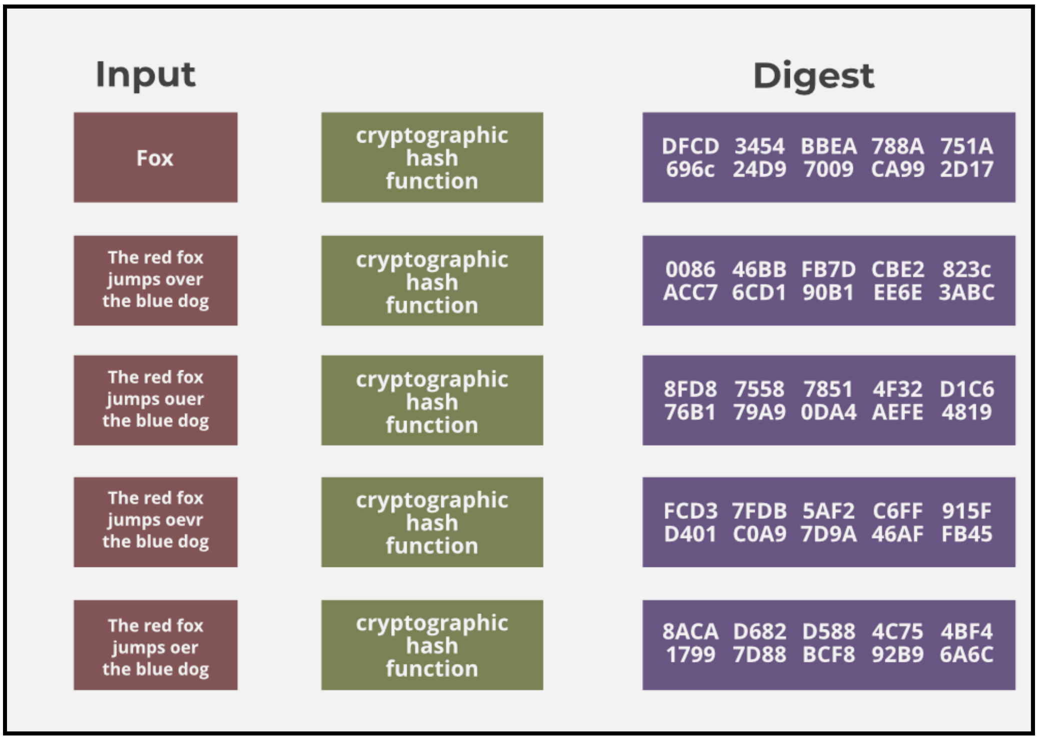


- **Integrity**

The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.
We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, and SHA-3.

Let's assume Host 'A' wants to send data to Host 'B' to maintain integrity. A hash function will run over the data and produce an arbitrary hash value H1 which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value of H2. Now, if

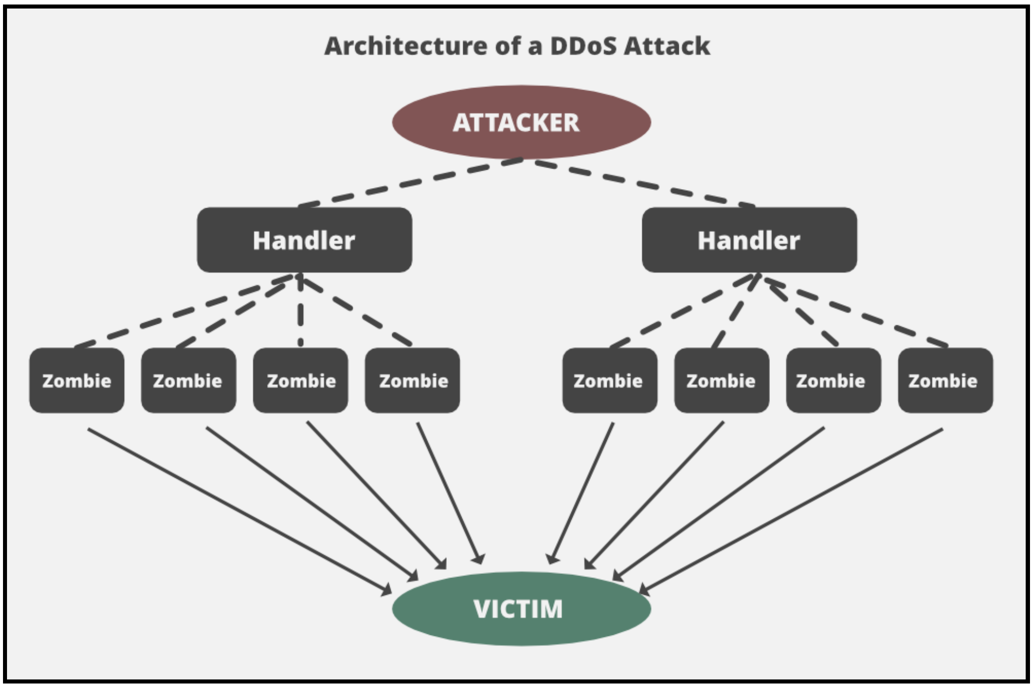
H1 = H2, this means that the data's integrity has been maintained and the contents were not modified.



Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696c 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823c ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

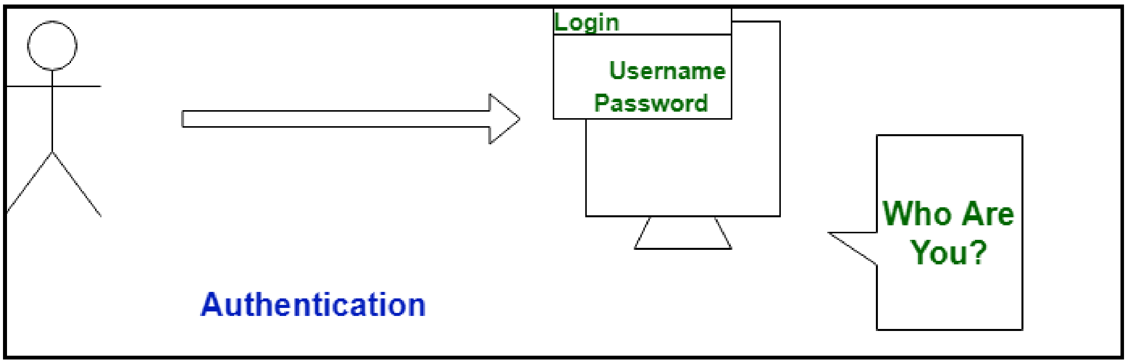
- **Availability**

This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.



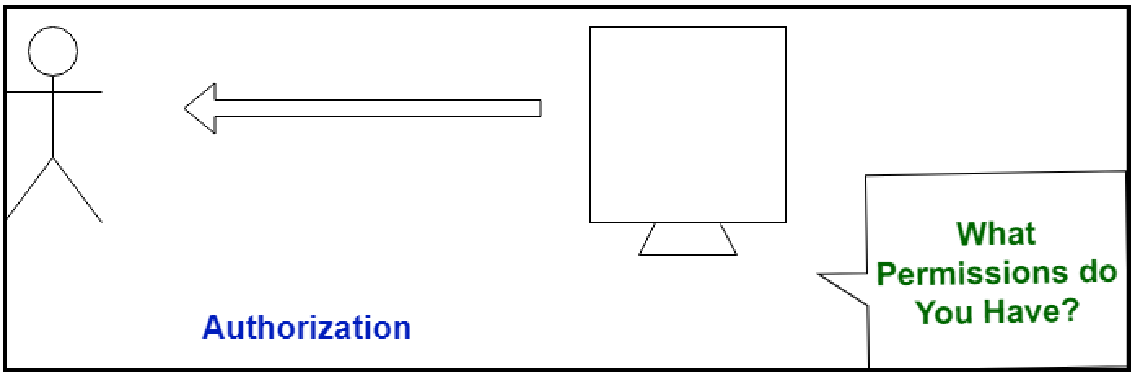
- **Authentication**:

Authentication is the process of verifying the identity of a user or entity attempting to access a system, network, or resource. It ensures that the user is who they claim to be before granting them access to sensitive information or functionalities. Authentication methods can include something a user knows (like a password), something they have (like a smart card or token), something they are (like biometric characteristics such as fingerprints or facial recognition), or a combination of these factors. By authenticating users, organizations can control access to their systems and prevent unauthorized individuals from gaining entry.



- **Authorization:**

Authorization is the process of determining what actions or resources a user or entity is allowed to access or perform within a system, network, or application, after they have been authenticated. Once a user's identity is verified, authorization mechanisms determine the permissions and privileges associated with that identity. These permissions dictate what actions the user can take, what data they can view or modify, and what functionalities they can access. Authorization ensures that users have appropriate access rights based on their roles, responsibilities, and level of trust within the organization. It helps enforce the principle of least privilege, which means granting users only the minimum level of access required to perform their tasks.



- **Non-Repudiation:**

Non-repudiation is the assurance that a user cannot deny the validity of their actions or transactions conducted within a system or network. It provides evidence that a particular user performed a specific action, such as sending a message, making a payment, or signing a document, and prevents them from later denying their involvement. Non-repudiation mechanisms typically involve the use of digital signatures, timestamps, and audit trails to create a tamper-evident record of user activities. By ensuring non-repudiation, organizations can hold users accountable for their actions, deter fraudulent behavior, and establish trust in electronic transactions and communications.