- Cryptography: The science of securing information by transforming it into a form that only intended recipients can understand. It's like writing a secret message in a special code that only your friend knows how to read.

- Encryption: The process of converting plain text (readable data) into cipher text (encoded data) using a key. It's like locking a message in a box, and only someone with the key can open it and read it.

- Decryption: The reverse process of encryption, where cipher text is turned back into plain text. It's like unlocking the box to read the message inside.

- Hashing/One-way encryption: A method of encryption where data is converted into a fixed-size string of characters, which is not meant to be decrypted. It's like shredding a document; you can't piece it back together.

- Confidentiality: Ensuring that information is not disclosed to unauthorized individuals or systems. It's like whispering a secret to someone in a language that only the two of you understand.

- Authentication: The process of verifying the identity of a user or device. It's like showing your ID card to prove who you are.

- Authorization: The process of giving someone permission to do or have something. It's like a bouncer at a club checking if you're on the guest list before letting you in.

- Integrity: Ensuring that information is not altered by unauthorized parties. It's like sealing a letter with wax so that you can tell if someone has tampered with it. - Non-Repudiation: The assurance that someone cannot deny the validity of something they have done. It's like signing a contract so you can't say later that you didn't agree to it.

- Plain text: Unencrypted information that is readable without any special measures. It's like a book that anyone can read.

- Cipher text: Information that has been encrypted and is not readable without decrypting it. It's like a message written in a secret code.

- Symmetric encryption: A type of encryption where the same key is used for both encryption and decryption. It's like a lock and key system where the same key locks and unlocks the door. • Asymmetric encryption: A type of encryption that uses a pair of keys, a public key for encryption and a private key for decryption. It's like having a mailbox with a slot that anyone can drop a letter through (public key), but only you have the key to open it and read the letters (private key). • Key: A piece of information that determines the output of a cryptographic algorithm. It's like the actual key for a lock. • Salt: Random data that is used as an additional input to a hash function to ensure that the output (hash) is unique. It's like adding a unique spice blend to a recipe so that even if someone knows the recipe, they can't replicate the exact flavor without your special spices. These terms are fundamental to understanding the field of cybersecurity and are used to protect information in the digital world.