Authentication and **Encryption** are distinct security mechanisms, each serving a unique purpose

- **Purpose**:
    - **Authentication**: Verifies the identity of a user, device, or system to ensure they are who they claim to be (e.g., logging into a system with a username and password).
    - **Encryption**: Protects data by transforming it into an unreadable format to prevent unauthorized access, ensuring confidentiality (e.g., scrambling a message so only the intended recipient can read it).
- **Function**:
    - **Authentication**: Confirms *who* is accessing a resource, often using credentials like passwords, biometrics, or tokens.
    - **Encryption**: Secures *data* itself, making it unreadable without the correct decryption key, regardless of who accesses it.
- **Mechanism**:
    - **Authentication**: Involves methods like passwords, multi-factor authentication (MFA), digital certificates, or OAuth tokens.
    - **Encryption**: Uses algorithms (e.g., AES, RSA) and keys to encode and decode data, such as encrypting files or network traffic.
- **Outcome**:
    - **Authentication**: Grants or denies access based on identity verification.
    - **Encryption**: Ensures data remains confidential, even if intercepted, but does not verify identity.
- **Example**:
    - **Authentication**: Entering a PIN to unlock a bank account.
    - **Encryption**: Encrypting a credit card number during an online transaction to protect it from eavesdroppers.