The Importance of Encryption in Data Security

Maintains Confidentiality

> Encryption ensures that sensitive information—such as financial records, personal data, and proprietary business information—remains private.

Ensures Data Integrity

> By adding layers of security, encryption makes it harder for hackers to tamper with data, which can prevent unauthorized changes.

Enhances Compliance

> Many industries have strict regulations (such as GDPR, HIPAA, and PCI DSS) that mandate encryption for the protection of personal and sensitive data.

▼ Protecting Data in Transit

> **Data in transit** refers to information actively moving between locations, like emails being sent, data transferred over networks, or information traveling across the internet.

> To secure data in transit, encryption protocols like **Transport Layer Security (TLS)** and **Secure Sockets Layer (SSL)** are commonly used. These protocols establish an encrypted channel, making data unreadable to anyone attempting to intercept it during transmission.

▼ Protecting Data at Rest

> **Data at rest** refers to information stored in databases, file systems, or any other storage medium, not actively being transferred or processed.

> Encryption of data at rest can be achieved through algorithms that convert the stored data into ciphertext. Often, **AES (Advanced Encryption Standard)** is used for this purpose due to its strong security.