**Encrypting a File**:

A screen shot of a computer program

Description automatically generated

**Decrypting the File:**

**A screen shot of a computer program

Description automatically generated**

**Significance of Encryption in Data Security**

Encryption transforms readable data into an unreadable format, protecting it from unauthorized access. It secures data:

* **Data in Transit**: This refers to data actively moving through a network, like when it’s transmitted over the internet or between devices. During transit, data is vulnerable to interception, such as through “man-in-the-middle” attacks. Encrypting data in transit ensures that intercepted information remains unreadable without the decryption key. Protocols like SSL/TLS (used in HTTPS) secure sensitive information, like passwords and payment details, when sent from one location to another.
* **Data at Rest**: Data at rest includes any information stored on devices or systems, such as databases or cloud storage. This data is at risk if unauthorized users gain access to the storage. Encrypting data at rest ensures that, even if attackers access storage devices, they cannot read or misuse the data without the decryption key. Organizations commonly encrypt entire databases to protect sensitive information, like customer data and financial records, even if storage is compromised.