Lecture3: Data Security

Introduction to Data Security

- **Data security** is the practice of protecting data from unauthorized access, corruption, or theft. It involves implementing measures to safeguard sensitive data, ensuring its confidentiality, integrity, and availability. With the increasing reliance on digital technologies, data security has become a crucial aspect of protecting personal, corporate, and governmental data.
- **Why is Data Security Important?**

- **Protects Sensitive Information :** prevents unauthorized access to personal, financial, and business data.
- **Prevents Cyber Threats:** defends against cyber attacks, such as hacking, malware, and ransomware.
- **Maintains Trust:** protecting data enhances customer confidence and business reputation.
- **Avoids Financial Losses:** data breaches can lead to legal penalties, loss of revenue, and operational downtime.

Common Data Security Measures

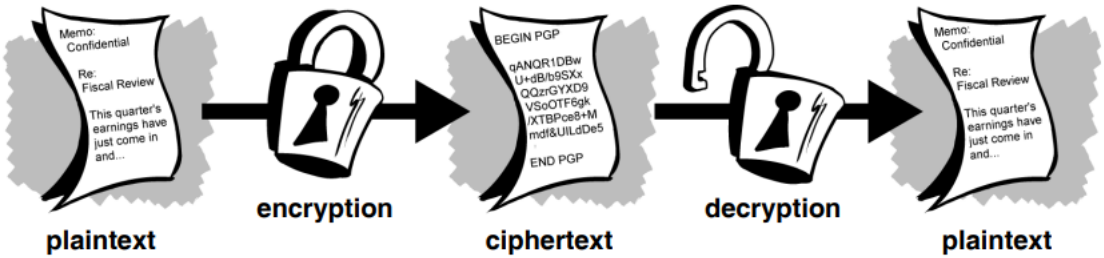
- **Encryption** – Converts data into unreadable formats for unauthorized users.
- **Access Control:** Uses authentication methods like passwords.
- **Firewalls & Antivirus Software:** Prevents unauthorized access and protects against malware.
- **Data Backup:** Ensures data recovery in case of loss or corruption.
- **Security Policies & Training:** Educates employees on best practices for data protection.

Encryption

- **encryption** is a process to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as **decryption**. The concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as **key**. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys

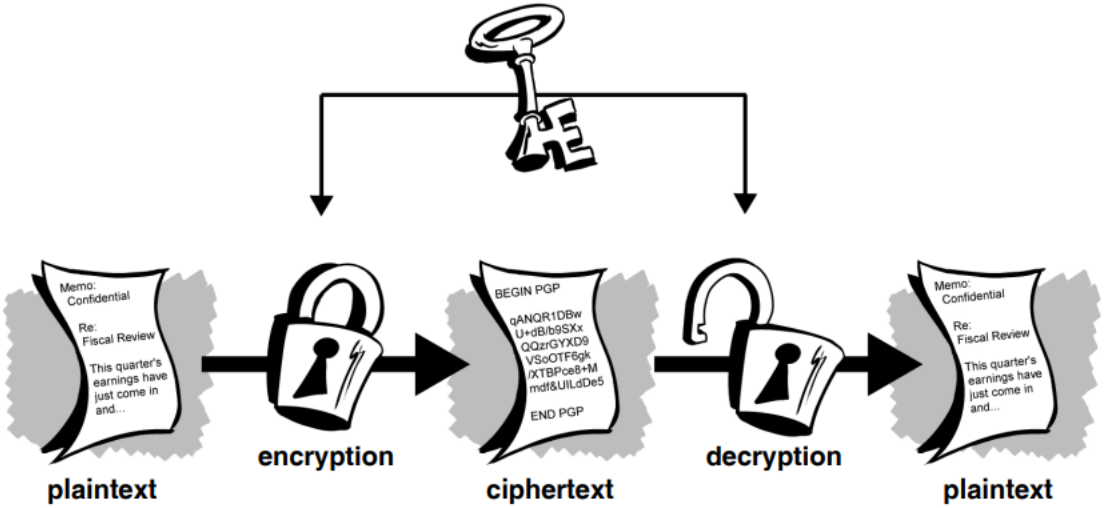
Encryption

- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret
  - Key is a string of numbers or characters
  - If same key is used for encryption & decryption the algorithm is called symmetric
  - If different keys are used for encryption & decryption the algorithm is called asymmetric



Encryption：Symmetric Algorithms

- In symmetric-key, also called conventional or secret-key encryption, one key is used both for encryption and decryption.
- Example: Caesar Cipher , (DES)
- Types:
  1. Block Ciphers
     - Encrypt data one block at a time (typically 64 bits, or 128 bits)
  2. Stream Ciphers
     - Encrypt data one bit or one byte at a time



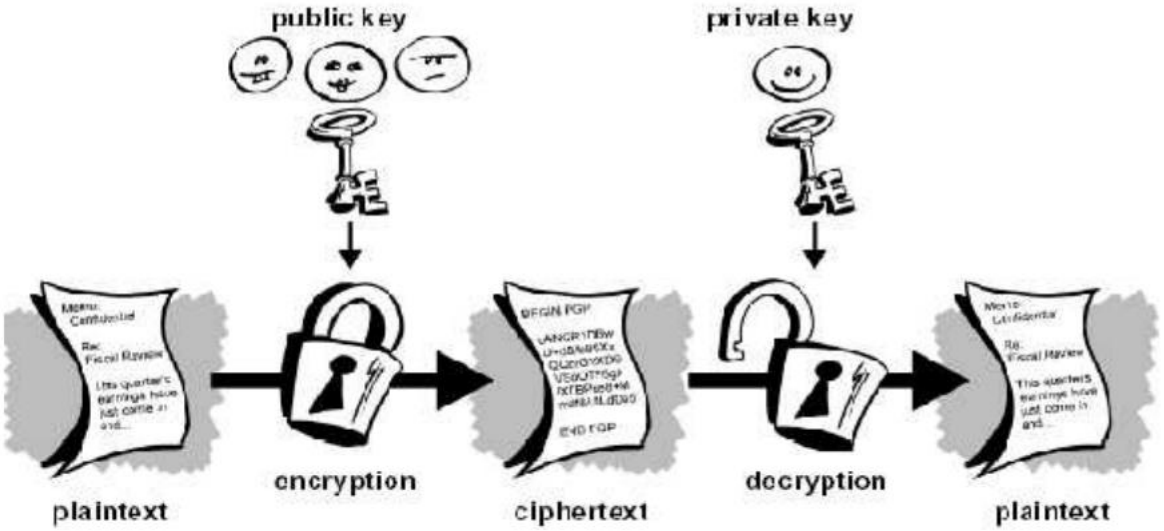
Encryption：Symmetric Algorithms

Limitations

- Any exposure to the secret key compromises secrecy of ciphertext
- A key needs to be delivered to the recipient of the coded message for it to be deciphered
- Potential for eavesdropping attack during transmission of key

Encryption：Asymmetric Algorithms

- Public key encryption is an asymmetric scheme that uses a pair of keys for encryption, a public key, which encrypts data, and a corresponding private, or secret key for decryption.
- Messages encoded using public key can only be decoded by the private key
  - Secret transmission of key for decryption is not required
  - Every entity can generate a key pair and release its public key



Asymmetric Encryption

Types

- Two most popular algorithms are RSA & El Gamal
  - **RSA**
    - Developed by Ron Rivest, Adi Shamir, Len Adelman
    - Both public and private key are interchangable
    - Variable Key Size (512, 1024, or 2048 bits)
    - Most popular public key algorithm
  - **El Gamal**
    - Developed by Taher ElGamal
    - Variable key size (512 or 1024 bits)
    - Less common than RSA, used in protocols like PGP

Asymmetric Encryption

Weaknesses

- Efficiency is lower than Symmetric Algorithms
- Potential for man-in-the middle attack
- It is problematic to get the key pair generated for the encryption