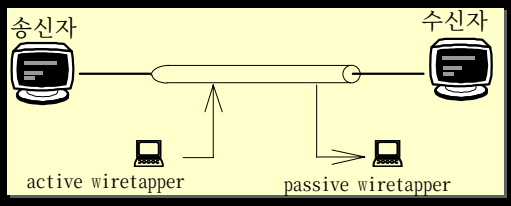
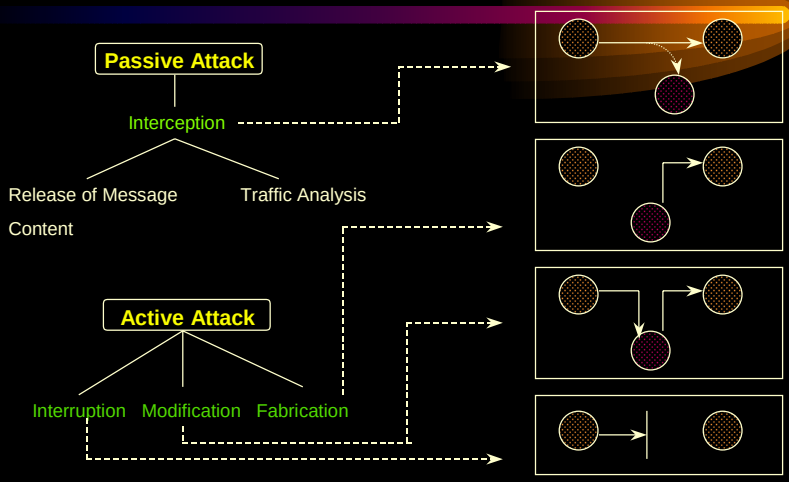
❑ Data, Information Security

- ❑ Computer Security, Network Security, Inter-network Security
- ❑ 컴퓨터 및 네트워크 시스템에서의 데이터 보호 (Protection)
  - e.g. File System, E-Mail
- ❑ 메시지의 기밀성과 무결성
- ❑ Security Attack, Security Service, Security Model



암호이론과 보안 INTRODUCTION

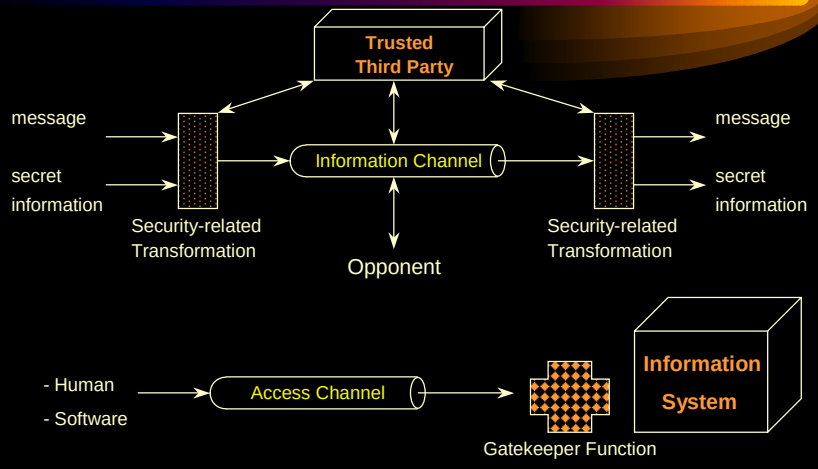
❑ Security Attack (보안공격)



❑ Security Service

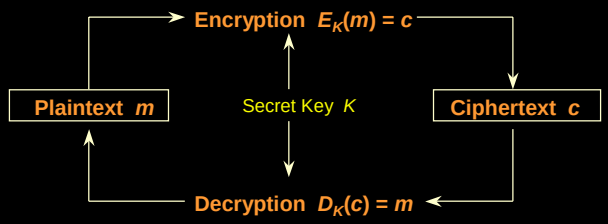
- ❑ Confidentiality (기밀성)
- ❑ Authentication (인증)
- ❑ Integrity (무결성)
- ❑ Non-repudiation (부인봉쇄)
- ❑ Access Control (접근제어)

❑ Security Model



❑ Cryptography

- ❑ **CRYPTOSYSTEM** (Cipher)의 설계
  - secrecy (비밀성)
  - authenticity (진위성)
- ❑ Plaintext(평문), Ciphertext (암호문)
- ❑ Encryption (암호화), Decryption (복호화)
- ❑ **SECRET KEY** (비밀키)



암호이론과 보안 INTRODUCTION

❑ Cryptosystem 구성요소

- ❑ M : Plaintext Message Space
- ❑ C : Ciphertext Message Space
- ❑ K : Key Space
- ❑ $E_k : M \rightarrow C$, a set of Encryption Transformations
- ❑ $D_k : C \rightarrow M$, a set of Decryption Transformations

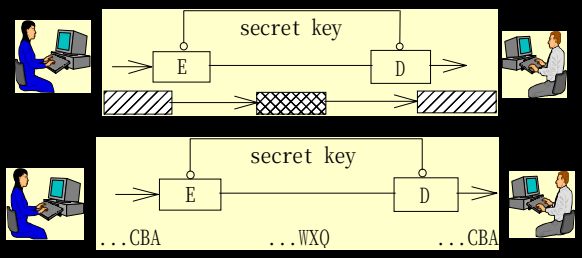
❑ Cryptosystem 제약조건

- ❑ $D_k = E_k^{-1}$ for a given k in K
- ❑ $D_k(E_k(m)) = m$ for all m in M
- ❑ 모든 Key k in K에 대해 E_k, D_k의 계산이 효율적
- ❑ Key의 비밀성(Secrecy)이 시스템의 안전성 결정

❑ 암호의 분류

- Symmetric Cryptosystem (Private-Key Cryptosystem)
- Asymmetric Cryptosystem (Public-Key Cryptosystem)

- Block Cipher
- Stream Cipher



암호이론과 보안 INTRODUCTION

❑ 암호분석 (Cryptanalysis)

- ❑ 암호문 공격 (Ciphertext-Only Attack)
- ❑ 선택된 평문 공격 (Chosen-Plaintext Attack)
- ❑ 선택된 암호문 공격 (Chosen-Ciphertext Attack)

- ❑ 무조건적으로 안전한 (Unconditionally Secure)
- ❑ 계산적으로 안전한 (Computationally Secure)