컴퓨터 보안

1. 컴퓨터 시스템은 어떻게 사용자들을 구부낳고, 각 사용자들이 정당한 사용자들인지 알 수 있는가

- 사용자 식별(identification)과 인증(authorization)의 문제

2. 사용자 인증에 사용될 수 있는 것들

- 아이디 ,패스워드

- 열쇠(카드키), 토큰, 스마트 카드

- 지문, 홍채, 싸인

- 기타, 키보드를 두드리는 습관

암호이론

1강

개요

정보를 안전하게 보관, 교환할 수 있는 기본적인 방법중 하나가 암호화

송신자S가 수신자 R에게 전달매체(유,무선) T를 통해 어떤 메시지를 보낼 때 발생할 수 있는 위협(제3자 O)

Blocking : O가 전달되는 메시지 막음

Intercept : 중간에 가로채서 읽음

Modify : 변조

Fabricate : o가 보내는 메시지를 s가 보내는 것처럼 위장

용어

암호화(encryption) : 메시지 내용을 확인하기 어렵도록 다른 형태로 바꾸는 것

복호화(decryption) : 암호화된 내용을 원래 내용으로 복원하는 것

평문(plaintext) : 암호화가 되기 이전 메시지

암호문(ciphertext) : 암호화 과정을 거친 메시지

C = e(k,p) // 키를 사용한 암호화

C = e(ke,p), p = d(kd,C)

Y=2x

Abcdefg…………………………..(1,2,3,~~~~~~~)

Y=2x+3(키) a= 1 -> 5(e)

대칭키 암호화

암호문과 키를 상대방에게 알려주어야 복호화 가능

비대칭키 암호화

암호화 할 때 키와 복호화 할 때 키가 다르다.

암호를 보내주는 사람은 키를 상대방에 알려줄 필요가 없다.