정보보호론 0402

공격자를 정의

계산 능력( 무한한 능력, 제한된 능력 )

2^128 이상 무한한, 이하 제한된

무한한 공격자에게는 키의 크기가 상관이 없다.

일회용 암호 : 무한한 공격자에게도 안전한 암호

COA 공격만 가능

TRNG 사용(PRNG는 계산적이기 때문에)

Secrecy = 기밀성과 가깝다.

대칭키 : 송,수신자가 같은 대칭키를 가지는 암호방식