정보보호론 0318

케르크호프스 원리 : 알고리즘 공개, 키는 비공개

암호의 의미적 안전성 : 공격자를 정의(유형, 능력, 목표)하는 것이 선행

* 공격자의 목표
  + 비밀키 복구(key recovery) : 비밀키 알아내는 것
  + 평문 복구(breaking one-wayness, ow) : 평문을 알아내는 것
  + 평문 구분(breaking indistinguishability, ind)
    - 평문을 완전히 복구하는 것
    - 여러 평문을 알아냈고, 어떤 종류인지 알아내는 것
  + 비밀키 복구하면, 평문 복구 가능하므로 평문 복구가 더 쉽다.
  + 평문 구분이 평문 복구보다 쉽다.
  + 비밀키 복구 > 평문 복구 > 평문 구분(난이도)
* 공격 유형(공격자 정의)
  + 암호문 단독 공격(COA, Ciphertext Only Attack)
    - 공격자가 암호문(Ciphertext)으로만 공격한 것
    - 수동적 공격(ex 도청 공격)
  + 알려진 평문 공격(Known Plaintext Attack, KPA)
    - 평문/암호문 쌍을 가지고 공격하는 것(선택 X)
    - 수동적 공격
    - 에니그마를 해킹하는데 사용한 방법
  + 선택 평문 공격(Chosen Plaintext Attack, CPA)
    - 공격자가 선택한 평문/암호문 쌍을 가지고 공격
    - 2차세계대전 사용
    - 능동적 공격
  + 선택 암호문 공격(Chosen Ciphertext Attack, CCA)
    - 공격자가 선택한 암호문에 대하여 평문을 알아낼 수 있는 경우
    - 공격자가 Tacket Ciphertext만 복호화를 못하는 경우
    - 공격자가 Tacket Ciphertext 제외한 나머지 복호화 가능
    - 능동적
    - CCA가 검증되어야 실생활 사용 가능
* 계산 능력
  + 무한
  + 제한(주로 가정) : 알고리즘 현실 반영 판단

안전성 수준 분류

* 높은 수준의 안전성 = 강한 공격자로부터 안전
* 강한 공격자 = 공격환경이 유리함 = 달성하려는 목표는 쉽고 능력이 많음
* 공격자의 목표 난이도 비교(목표는 쉬울수록 공격이 강해진다)
  + (attack easy)IND > OW > key recovery(attack hard)
* 공격자의 능력 비교
  + 무한적 계산 능력 > 제한적 계산 능력
  + (public키 환경만) CCA >= CPA >= KPA >= COA
  + 대칭키는 능력 비교 불가능
  + 공개키 환경은 CPA가 기본으로 주어진다.
* 현대 암호 기법은 IND-CCA공격자로부터 안전함을 증명

모듈라 연산(mod, %)

A mod B = R (A를 B로 나눈 나머지 값=R)

나머지는 음수가 되면 안된다.

모듈라 합동

합동 : 비슷한 성질

모듈라 사칙연산 계산하는 연습!