정보보호론 0320

비밀키 복구 가능하면 평문 복구(OW) 가능하다

평문 복구 가능하면 평문 구분(IND)이 가능하다

따라서 ind가 가장 쉽고 비밀키 복구가 가장 어렵다.

CCA >= CPA >= KPA >= COA (공개키 기준)

모듈라 연산 mod(%)

음수일 때, 주의

모듈라 사칙연산 => 나눗셈 제외

모듈라 사칙연산 연습!

모듈라 연산과 XOR 연산

Mod2 = XOR

대칭키 암호 시스템

치환(Substitution) : 평문의 문자를 다른 문자로 바꾸는 방식

전치(Transposition) : 평문의 문자 위치를 바꾸는 방식

시저 암호(Caesar Cipher) = 알파벳 오른쪽 3칸 뛰어서 사용하는 방식

단일 문자(Monoalphabetic) 치환 함호 : 1대1로 바뀐다.

덧셈암호는 여러 번 중복적으로 해도 한 번 한 것과 같다.

곱셈암호

-1승 : 역원(mod에서는 나눗셈을 사용하지 않기 때문이다.)

항상 곱셈의 역원은 존재하지 않는다.

곱셈암호에서 사용하는 키는 항상 역원이 존재해야 한다.

아핀 암호

덧셈 암호 + 곱셈 암호

단일 문자

치환 암호

키의 개수 : 2의 88승가지

전수 키 조사가 불가능 함

치환 암호 분석

통계적 특성을 그대로 유지