**2주차 요약 정리**

**암호의 기초**

**암호 용어 정리**

* **암호화(Encryption)**: 평문 → 암호문
  + **Cipher** : 암호화의 핵심 기술
* **복호화(Decryption)**: 암호문 → 평문
* **평문(Plaintext)**: 원래 데이터
* **암호문(Ciphertext)**: 암호화된 데이터
* **암호시스템(Cryptosystem)**: 키 생성, 암호화, 복호화 알고리즘의 집합

**대칭키 vs 공개키 암호**

텍스트, 폰트, 번호, 스크린샷이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

**암호의 안전성**

**케르크호프스 원리**

"알고리즘은 공개되어도 키가 노출되지 않으면 안전해야 한다."

**키만 비밀로 유지**하면 됨

* 다양한 사용자가 동일 시스템, 키만 다르게 사용

**암호의 의미적 안전성(Semantic Security)**

안전하다는 의미를 어떻게 정의할 것인가??

공격자를 정의하는 것이 선행되어야 함

**공격 유형 (Semantic Security 기준)**

**텍스트, 폰트, 스크린샷, 번호이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.**

**목표 난이도 순:** 평문 구분 (IND) > 평문 복구 (OW) > 키 복구

**공격자 능력 순:** CCA >= CPA >= KPA >= COA

**공격자의 목표**

* 비밀키 복구
  + 복호화 할 수 있는 키 찾고, 시스템 파괴
* 평문 복구 (breaking **o**ne-**w**ayness) = **ow**
  + 평문 찾기
* 암호화된 평문 구분 (breaking **ind**istinguishability) = **ind**
  + 공격자가 두 평문을 선택하고 암호문이 제공될 때, 둘 중 어떤 평문이 암호화 되었는지 구분함

**수학적 배경 – 모듈라(Mod) 연산**

**기본 정의**

* a mod b = r
* 정수 a를 b로 나눈 나머지

**모듈라 합동**

* a ≡ b (mod n) : a와 b를 n으로 나눈 나머지가 같음

**모듈라 사칙연산**

* 덧셈: (a+b)mod n=[ (a mod n)+(b mod n)] mod n
* 뺄셈도 동일하게 적용
* 곱셈: (a x b)mod n=[ (amod n) x (bmod n) ] mod n
* 나눗셈은 제외 (역원을 사용한다)

**XOR 연산 = mod 2**

* 0 ⊕ 0 = 0, 0 ⊕ 1 = 1, 1 ⊕ 0 = 1, 1 ⊕ 1 = 0
* mod 2의 덧셈과 동일