정보보호론 중간고사 정리

**0. 정보보호의 3대 요소 (NIST CIA Triad)**

* **기밀성 (Confidentiality)**: 인가되지 않은 사용자로부터 정보를 보호
  + 예: 암호화, 접근 제어
* **무결성 (Integrity)**: 데이터가 인가되지 않은 방식으로 변경되지 않았음을 보장
  + 예: 해시함수, MAC, 전자서명
* **가용성 (Availability)**: 정당한 사용자가 필요할 때 정보와 시스템에 접근할 수 있어야 함
  + 예: 백업, 중복 시스템, DDoS 방어

**1. 암호학의 기본 개념 (2주차)**

* 암호학(Cryptology): 정보를 보호하기 위한 과학 및 기술의 총칭
  + 암호기술: 기밀성, 무결성, 인증성 제공하기 위한 방법과 기술
  + 암호해독: 암호문으로부터 평문 혹은 키를 추정하는 기술
  + 암호시스템: 키 생성, 암호화, 복호화 알고리즘으로 구성
  + 암호 프로토콜: 통신 중 보안을 위한 절차 및 알고리즘
* 암호 용어
  + 암호화(cipher): 평문 → 암호문 변환
  + 복호화: 암호문 → 평문 복원
  + 평문 / 암호문: 암호화 전/후의 데이터
* 대칭키 암호시스템
  + 동일한 키를 이용해 암호화와 복호화 수행
  + 속도 빠르고 효율적이나 키 분배 문제가 있음
* 공개키 암호시스템
  + 공개키와 비밀키를 쌍으로 사용
  + 암호화와 복호화 키가 다르며 키 분배 문제를 해결
* 케르크호프스(Kerckhoffs) 원리
  + 암호 알고리즘이 공개되어도 키가 비밀이면 안전성을 유지해야 함
* 의미적 안전성(Semantic Security)
  + 공격자의 목표: 비밀키 복구, 평문 복구(OW), 암호문 구분(IND)
  + 공격 유형
    - COA(암호문 단독 공격)
    - KPA(알려진 평문 공격)
    - CPA(선택 평문 공격)
    - CCA(선택 암호문 공격)
    - (CCA >= CPA >= KPA >=COA)
  + 계산 능력: 다항 시간, 무한 계산 등 기준에 따라 안전성 수준 분류
* 모듈라 연산
  + 합동 표현: a ≡ b mod n
  + 사칙 연산 가능, 나눗셈은 역원이 존재할 때만 가능

**2. 고전 암호 (3주차)**

* 고전 암호 설계 방식
  + 치환(Substitution): 문자를 다른 문자로 대체
  + 전치(Transposition): 문자의 위치를 바꿈
* 시저 암호:
  + 단일 문자 치환 암호
  + 알파벳을 고정된 거리만큼 이동하여 암호화
* 아핀 암호:
  + 덧셈(26)+곱셈(12) = 312가지
  + 암호, 수학적 함수 f(x) = ax + b mod m 이용
* 비제네르 암호:
  + 특정 길이의 키워드를 비밀키로 사용
  + 반복 키워드를 사용한 다중 시저 암호

**3. 현대 대칭키 암호 (4주차)**

* 블록 암호(64bit)
  + 고정 크기 블록 단위로 암호화 수행 (예: DES, AES)
  + 혼돈(S-box) : 난해하게 만드는 것
  + 확산(P-box) : 분산시키는 것
  + SPN 구조(전치+확산)
  + 페이스텔 구조 기반 설계
    - 라운드 마지막에 왼쪽과 오른쪽 교차
    - 마지막 라운드 제외
    - 암호화 복호화 과정 동일, 라운드 키가 역순 사용
* 스트림 암호(유연)
  + 평문과 같은 길이의 키 스트림 생성, XOR로 암호화
* 메시지 부호화:
  + 부호화는 암호화가 아니다(기밀성 제공 x)
  + 평문을 이진 비트로 표현 (ASCII 등)
* XOR 연산: 동일하면 0, 다르면 1 → 기본 암호 연산
* DES (Data Encryption Standard)
  + 64비트(평문) 블록, 56비트(키), 16라운드 Feistel 구조
  + 키 스케줄링
    - {패리티비트 제거(8bit), 쉬프트, 압축 순열} 구성
    - 64비트 비밀키 입력 -> 실제56비트만 사용
    - 16개의 48bit 라운드키 출력
    - 16라운드 중 14번 정도 사용
  + 초기, 최종 순열
    - 초기와 최종은 서로 역관계
    - 64비트 입력 받아 비트 단위 자리 바꿈이 일어남
  + 페이스텔 구조의 F 함수
    - {확장 순열, 라운드 키 결합, 치환 테이블 8개, 고정 순열} 구성
    - 오른쪽 32bit R\_i-1, 48비트 라운트키 K\_i 입력 받음
    - 32bit 값 출력
  + 전사적 공격(brute force attack)
    - 무차별 공격, DES에 특화된 공격
  + 차분 분석(CPA), 선형 분석(KPA)에 취약
* 2DES
  + 서로 다른 2개 키를 이용하여 DES 2번 사용
  + 2\*2^56 -> 57비트 안전성 제공
* 3DES (Triple DES)
  + DES를 3번 적용 (암/복/암)
  + 2TDES(k\_1 = k\_3) 또는 3TDES(모든 키 다름) 방식 존재
  + 2^112 계산량 필요
* AES (Advanced Encryption Standard)
  + 128비트 블록, 키: 128/192/256비트, 라운드 수: 10/12/14
  + 비페이스텔 구조
  + 원소가 한 바이트인 4x4 행렬로 표현하며 상태라고함 (128 bits = 16bytes)
  + 주요 라운드
    - SubBytes(치환)
    - ShiftRows(행 이동)
    - MixColumns(열 섞기)
    - AddRoundKey(XOR연산)
  + 키 확장 함수로 128bit 라운드 키 생성
  + 안전성
    - AES를 대체 암호가 필요한 것은 아니며 라운드 수 (비밀키 길이)를 증가시키는 것으로 높은 안전성을 확보할 수 있음
    - 알고리즘 키를 변경할 필요가 없음
* 국산 블록 암호
  + SEED: 128비트, 국내 인증서에 사용됨(공인인증서)
  + ARIA: 국가보안연구소 주도 개발, 국방용 암호화에 활용
* 블록 암호 운영모드
  + ECB: 패턴 노출, 병렬 처리 가능
    - 오류 확산 : 1bit만 변경되면, 절반 이상 변경
  + CBC: IV 필요, 자기 복구 기능, 연결성(재사용 불가능)
    - 오류 확산 : 다음 블록에만 영향을 준다.
  + CFB/OFB: 스트림 암호처럼 사용 가능
  + CTR:
    - 평문과 키 스트림을 XOR연산하여 암호문 블록 생성
    - 전처리와 병렬처리
    - 오류 확산 : 암호문과 평문의 한 비트에만 영향
* 스트림 암호
  + 비트 단위 암호화
  + 패딩과 운영모드 필요 없음
  + 실시간 암호화 처리 가능
  + 속도가 빠름, 초 경향 블록 암호 존재
* 패딩 : 빈 공간을 채워 완전한 블록을 만드는 작업
  + Zero Padding : 부족한 길이 0으로 채움(=패딩의 크기를 알 수 없음)
  + PKCS#7 : 패딩 바이트 크기로 패딩 값을 사용
* 난수 생성기
  + TRNG: 물리 기반 난수, 예측 불가능
  + PRNG: 알고리즘 기반, 반복 가능성 존재
* One-Time Pad
  + 무조건적 보안 제공, 현실적 사용 어려움

**4. 공개키 암호시스템 (5주차)**

* 대칭키 vs 공개키
  + 대칭키: 빠르지만 키 분배 어려움
  + 공개키: 분배 용이, 연산 복잡도 높음
* 하이브리드 암호 시스템
  + 대칭키로 데이터 암호화 + 공개키로 대칭키 전달
* 트랩도어 일방향 함수
  + 정방향 계산 쉬움, 역방향 어려움 (단, 트랩도어 있으면 가능)
* RSA 암호시스템
  + 수학적 배경: 소인수분해 기반, 오일러 정리 활용
    - 소수의 곱을 소인수분해를 할 수 있으면 서로 역원 관계인 e, d를 계산 가능
    - 지수에서 e, d가 곱해지면 상쇄된다.
  + 공개키 (e, n), 개인키 d: ed ≡ 1 mod φ(n)
  + 암호화: c = m^e mod n / 복호화: m = c^d mod n
  + 공격 가능성: IND-CPA, OW-CCA
  + N은 적어도 2048bit
  + 서로 다른 두 소수P, q는 1024bit 이상
* ElGamal 암호시스템
  + DH 키 교환 기반 공개키 암호
  + 암호화: (c1 = g^r, c2 = m·A^r), 복호화: c2 · c1^-a
* 증명 가능한 안전성
  + 리덕션 : 문제 B를 풀 수 있다면 문제 A도 풀 수 있다.
    - RSA → 소인수분해
    - ElGamal → DLP/CDH
    - DLP(이산 대수 문제)
    - DDH(결정적 Diffie-Hellman 문제)
    - CDH(계산적 결정적 Diffie-Hellman 문제)
    - DDH <= CDH <= DLP
* 양자 내성 암호
  + 양자 컴퓨터 등장 대비 암호기술 (PQC) - 격자 기반 문제

**5. 해시함수와 전자서명 (6주차)**

* 해시함수 정의
  + 임의 입력 → 고정된 길이의 해시 값 생성
  + 변경에 민감함 → 디지털 지문 역할
* 암호학적 해시함수의 특성
  + 역상 저항성: h(x) = y일 때 x 추정 불가(2^l비트)
  + 제2 역상 저항성: 동일 해시값을 만드는 다른 입력 찾기 어려움
  + 충돌 저항성: 서로 다른 입력값으로 동일 해시값 생성 어려움(2^l/2 비트)
* 생일 문제
  + 해시 길이 n일 때 약 2^(n/2) 시도로 충돌 가능
* 해시 구조 및 발전
  + MD 구조 → SHA-1(160bit), SHA-2, SHA-3(스펀지 구조)
* 메시지 인증 코드 (MAC)
  + 무결성 + 인증 제공, 키 기반 해시 (예: HMAC, CMAC)
* MAC 종류
  + 해시 기반: NMAC, HMAC
  + 블록 암호 기반: CBC-MAC, CMAC