암호학 및 블록체인 핵심 요약

목차

---

1. 암호학 기초

1.1 대칭키 암호화

기본 개념

- **정의**: 동일한 키로 암호화와 복호화를 모두 수행
- **공식**:

```
암호화: C = E_K(P)
복호화: P = D_K(C)
```

- **특징**: 빠른 처리 속도, 키 분배 문제 존재

대치 암호(Substitution Cipher)

- **단일문자 암호(Monoalphabetic Ciphers)**:
  - **덧셈 암호**: `C = (P + k) mod n`, `P = (C − k) mod n`
  - **곱셈 암호**: `C = (P * k) mod n`, `P = (C * k^(−1)) mod n`

- **아핀 암호**: `C = (a*P + b) mod n`, `P = a^(-1)*(C - b) mod n`

- **예제**: 곱셈 암호(키=3, n=26)로 "hello" 암호화

```
h(7) → C = (7*3) mod 26 = 21 → v
e(4) → C = (4*3) mod 26 = 12 → m
결과: "vmhhq"
```

현대적 대칭키 알고리즘: AES

- **특징**:
  - 128비트 블록 크기
  - 128/192/256비트 키 길이
  - 10/12/14 라운드 수행
- **암호화 과정**:
  1. SubBytes: S-box를 통한 대체
  2. ShiftRows: 행 단위 바이트 순환
  3. MixColumns: 열 단위 혼합
  4. AddRoundKey: 라운드 키와 XOR

1.2 비대칭키 암호화

기본 개념

- **정의**: 공개키와 개인키라는 서로 다른 두 키 사용
- **특징**:
  - **공개키**: 누구에게나 공개
  - **개인키**: 소유자만 보관
  - n명 통신 시 필요 키 수: 2n개 (대칭키: n(n-1)/2개)

RSA 암호 시스템

- **키 생성**:
  1. 두 소수 p, q 선택
  2. n = p × q 계산
  3. φ(n) = (p-1) × (q-1) 계산
  4. e 선택 (1 < e < φ(n), gcd(e, φ(n)) = 1)
  5. d 계산 (e × d ≡ 1 (mod φ(n)))
  6. 공개키 = (e, n), 개인키 = d
- **암호화/복호화**:

    - 암호화: C = P^e mod n
    - 복호화: P = C^d mod n
- **예제**: p=5, q=11, e=7

```
n = 55, φ(n) = 40
d = 23 (7×23 mod 40 = 1)
암호화 19: C = 19^7 mod 55 = 24
```

타원 곡선 암호 시스템(ECC)

- **정의**: 타원 곡선 상의 점 연산을 이용한 암호화
- **특징**: RSA보다 짧은 키로 동일한 보안 수준
- **곡선 방정식**: $y^2 = x^3 + ax + b$
- **키 생성**:
    - 개인키: 정수 k
    - 공개키: K = k × G (G는 생성점)
- **Double-and-Add 알고리즘**: k의 이진 표현에 따라 점을 효율적으로 곱함

1.3 암호 해싱과 메시지 인증

암호 해시 함수 특성

- **정의**: 임의 길이 데이터 → 고정 길이 값 변환
- **특성**:
    1. **단방향성(Preimage Resistance)**: 해시→원본 변환 불가
    2. **약한 충돌 저항성(Second Preimage)**: 같은 해시 값 가진 다른 메시지 찾기 어려움
    3. **강한 충돌 저항성(Collision)**: 충돌쌍 찾기 어려움

주요 해시 알고리즘

- **SHA-256**: 비트코인 사용, 256비트 출력
- **SHA-512**: 512비트 출력
- **RIPEMD-160**: 비트코인 주소 생성에 사용

메시지 인증 코드(MAC)

- **MDC vs MAC**:
    - **MDC**: 해시만 사용, 송신자 인증 불가, 별도 채널 필요
    - **MAC**: 비밀 키 + 해시, 송신자 인증 가능, 동일 채널 가능
- **HMAC 구조**:

```
HMAC = H((K ⊕ opad) || H((K ⊕ ipad) || M))
```

---

2. 블록체인 메커니즘

2.1 비트코인 구조

키와 주소 시스템

- **개인키**: 256비트 무작위 수
- **공개키**: K = k × G
- **주소 생성**:
  1. 공개키 해시: RIPEMD160(SHA256(공개키))
  2. 버전 + 해시 + 체크섬
  3. Base58Check 인코딩

트랜잭션 구조

- **UTXO 모델**: 이전 트랜잭션 출력을 참조
- **구성 요소**:
  - **입력**: txid, vout, scriptSig, sequence
  - **출력**: value, scriptPubKey
- **스크립트 시스템**:
  - **scriptPubKey**: 출력 잠금 조건
  - **scriptSig**: 잠금해제 데이터

블록과 블록체인

- **블록 구조**:
  - **헤더(80바이트)**: version, prevHash, merkleRoot, timestamp, bits, nonce
  - **트랜잭션 리스트**
- **머클 트리**: 트랜잭션 요약하는 이진 트리

2.2 채굴과 합의 메커니즘

작업 증명(Proof of Work)

- **과정**:
  1. 트랜잭션 수집 → 머클 트리 구성
  2. 블록 헤더 생성
  3. nonce 변경하며 해시 계산

4. 목표값보다 작은 해시 찾으면 블록 배포

- **난이도 조정**:

```
목표값 = coefficient × 2^(8 × (exponent − 3))
```

  - 2016블록(약 2주)마다 조정

2.3 이더리움 특성

계정 기반 모델

- **계정 유형**:
  - **EOA**: 개인키 제어
  - **CA**: 코드 제어
- **계정 상태**:
  - nonce: 트랜잭션 수
  - balance: ETH 잔액
  - storageRoot: 저장소 해시
  - codeHash: 코드 해시

가스와 수수료 시스템

- **가스**: 연산 복잡성 측정 단위
- **트랜잭션 수수료**: 가스 x 가스 가격
- **London 업그레이드 이후**:
  - **기본 수수료**: 자동 조정, 소각
  - **우선 수수료**: 검증자에게 지급
  - **최대 수수료**: 지불 상한

이더리움 PoS

- **특징**:
  - **검증자**: 32 ETH 예치
  - **블록 제안자**: 12초마다 선택
  - **최종성**: 2/3 이상 투표 받은 체크포인트

---

3. 스마트 컨트랙트와 솔리디티

3.1 스마트 컨트랙트 개념

- **정의**: 조건 충족 시 자동 실행되는 블록체인 프로그램

- **특징**: 중개자 없음, 투명성, 수정 불가
- **응용**: 토큰 거래, DeFi, 투표, 공급망 관리

3.2 솔리디티 프로그래밍

변수 유형과 저장 위치

- **상태 변수**: 블록체인에 영구 저장
- **지역 변수**: 함수 내 임시 사용
- **저장 위치**:
  - **storage**: 영구 저장
  - **memory**: 함수 실행 중 존재
  - **calldata**: 읽기 전용 매개변수

함수 수정자

- **가시성**:
  - **public**: 외부/내부 모두 호출 가능
  - **private**: 현재 컨트랙트만
  - **internal**: 현재/파생 컨트랙트
  - **external**: 외부에서만
- **상태 수정자**:
  - **pure**: 상태 읽기/수정 없음
  - **view**: 읽기만, 수정 없음
  - **payable**: 이더 수신 가능

중요 패턴

- **Fallback 함수**: 매치되는 함수 없을 때 실행
- **이벤트**: 블록체인에 로그 저장, 프론트엔드 감지 용이

시험 대비 핵심 정리

계산 문제 대비

1. **대칭키 암호 계산**:
   - 곱셈 암호: `C = (P * k) mod n`, `P = (C * k^(-1)) mod n`
   - 역원 계산법 숙달
2. **RSA 계산**:
   - 키 생성: p, q → n, ϕ(n) → e, d

- 암호화/복호화: `C = P^e mod n`, `P = C^d mod n`

3. **비트코인 난이도 계산**:
   - Target = coefficient × 2^(8 × (exponent - 3))

개념 이해 문제 대비

1. **해시 함수 특성** 구별:
   - Preimage, Second Preimage, Collision
2. **MDC vs MAC**:
   - MDC: 송신자 인증 불가
   - MAC: 송신자 인증 가능
3. **대칭키 vs 비대칭키**:
   - 키 개수, 장단점 비교
4. **타원 곡선 원리**:
   - 공개키 계산: K = k × G

용어/정의 문제 대비

1. **이더리움 용어**:
   - Gas, Wei, Gwei, PoS
2. **솔리디티 용어**:
   - Storage vs Memory
   - Payable, Fallback 함수