**3주차 요약정리**

**1. 대칭키 암호 시스템 분류**

* 고전 암호: 20세기 이전
* 현대 암호: 블록 암호 / 스트림 암호
* 블록 암호: 평문을 블록 단위로 암호화
* 스트림 암호: 평문을 비트 단위로 암호화

**2. 고전 암호 방식**

▶ 치환 (Substitution)

* 문자를 다른 문자로 대체
* 예: ABC → XYZ

▶ 전치 (Transposition)

* 문자의 위치를 변경
* 예: ABC → CAB

**3. 시저 암호 (Caesar Cipher)**

* 문자마다 +3 시프트 (고정된 거리)
* 예: c → f, a → d
* 수식:
* 암호화: Eₖ(m) = m + 3 (mod 26)
* 복호화: Dₖ(c) = c - 3 (mod 26)

**4. 덧셈 암호 (Additive Cipher)**

* 시저 암호의 일반화
* 수식
  + Eₖ(m) = m + k (mod 26)
  + Dₖ(c) = c - k (mod 26)

**5. 곱셈 암호 (Multiplicative Cipher)**

* k는 26과 서로소여야 함
* 가능한 k: {1, 3, 5, 7, ..., 25} (역원이 존재하는 숫자)
* 수식
  + Eₖ(m) = m × k (mod 26)
  + Dₖ(c) = c × k⁻¹ (mod 26)

**6. 아핀 암호 (Affine Cipher)**

* 덧셈 + 곱셈 결합
* 수식
  + 암호화: Eₖ₁,ₖ₂(m) = k₁ × m + k₂ (mod 26)
  + 복호화: Dₖ₁,ₖ₂(c) = k₁⁻¹ × (c - k₂) (mod 26)
* 키 개수: 26 × 12 = 312

**7. 일반 치환 암호**

* 26!개의 키 (약 2^88가지)
* 통계적 분석 가능 (E의 빈도수 높음

**8. 비제네르 암호 (Vigenère Cipher)**

* 다중 문자 치환
* 키워드 반복 사용: k = "math" 등
* 분석 방법:
* Kasiski Method로 키 길이 추정
* 반복된 거리의 공통 약수 = 키 길이 후보

**9. 전치 암호 (Transposition Cipher)**

* 문자의 위치만 변경
* 문자 빈도 유지 → 빈도분석에 덜 효과적

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.