해시 함수

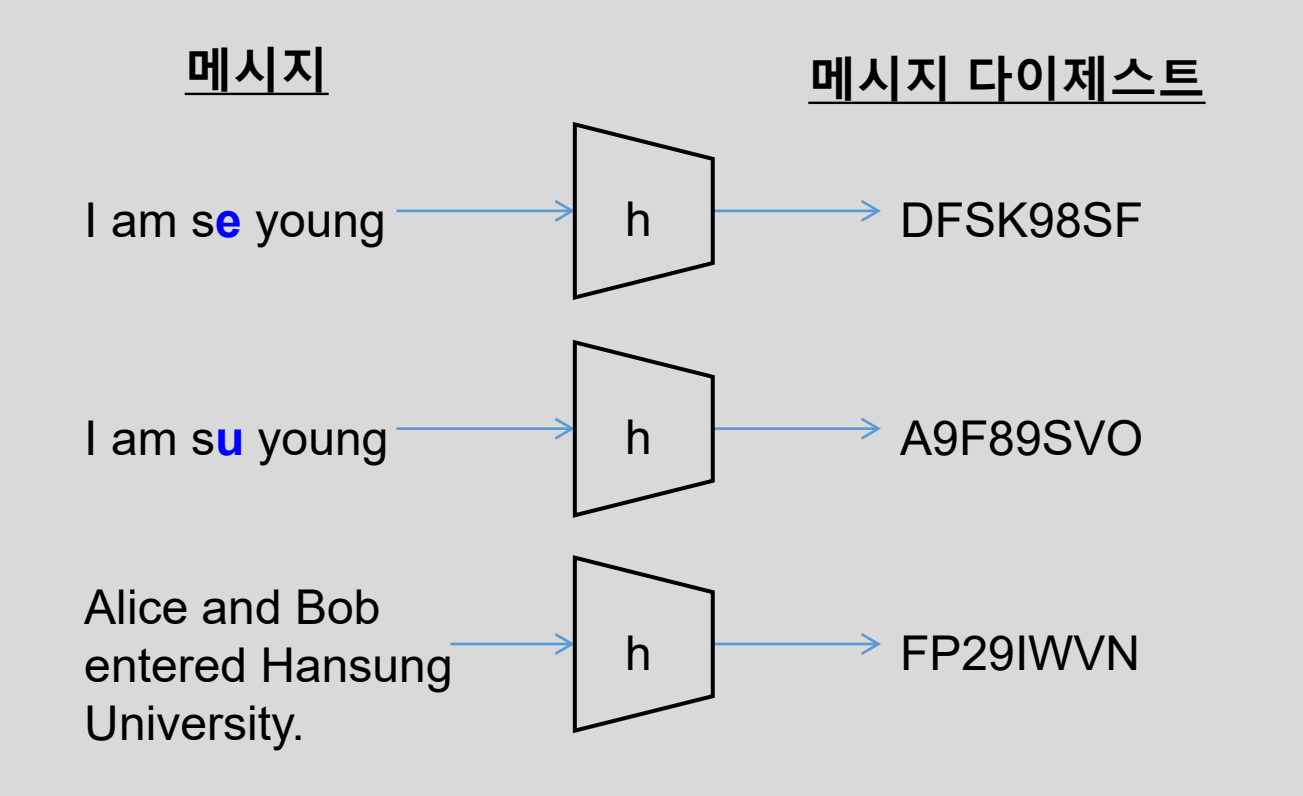
IT융합공학부 사이버보안트랙 윤세영

유투브 주소: https://youtu.be/A5FVNL6h-YU

- 해시 함수의 개념
- 해시 함수의 활용범위
- 해시 함수의 안전성 요구사항
- 해시 함수 알고리즘

해시 함수의 개념

- 해시함수에 의한 결과값은 해시값(Hash value)이라고 함
- **일방향 함수**(One-way Function)라고 불리기도 함
- 다른 암호 알고리즘과 달리 **키가 필요하지 않음**



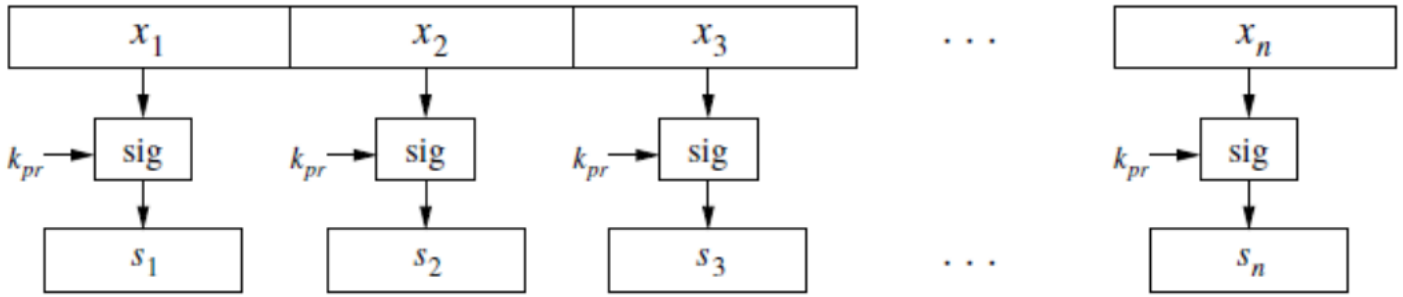
<해시 함수의 입력, 출력 동작 원리>

해시 함수의 활용범위

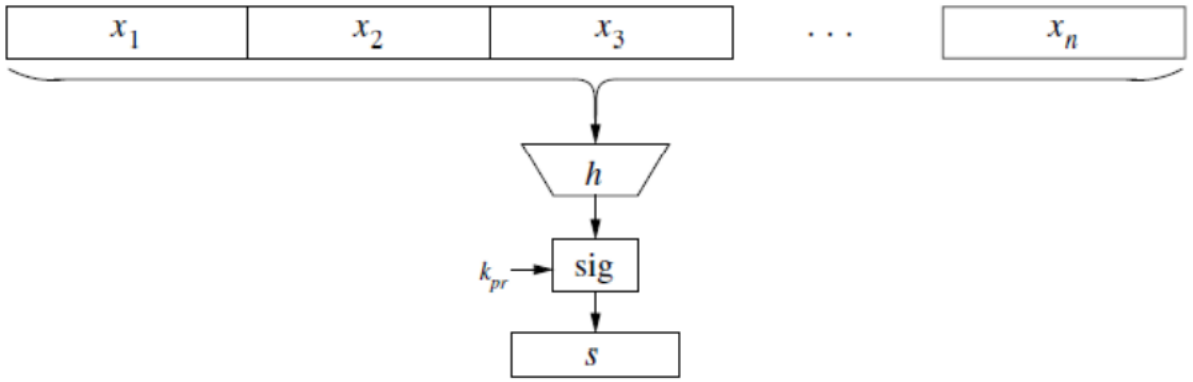
- **전자서명**
- **데이터 위·변조 검사**
- 패스워드의 안전한 보관
- 데이터의 빠른 검색
- 통신의 안전성 증명
- 불법 저작물 차단
- 홈페이지 해킹 여부 판단
- 암호화폐의 신뢰성 확보
- 전자투표 등

해시 함수의 활용범위 - 전자서명

- 전자서명의 **높은 계산적 부담**, **메시지 오버헤드**, **안전성의 한계**를 해시 함수를 이용해서 해결할 수 있음



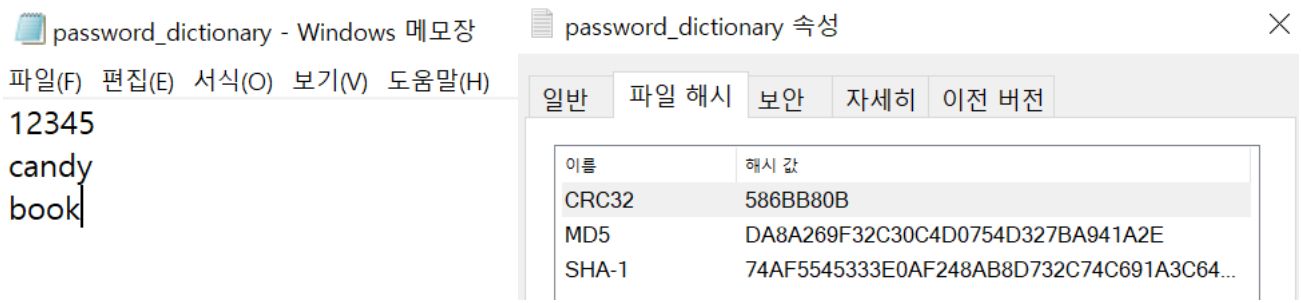
<긴 메시지를 서명하기 위한 안전하지 않은 방법>



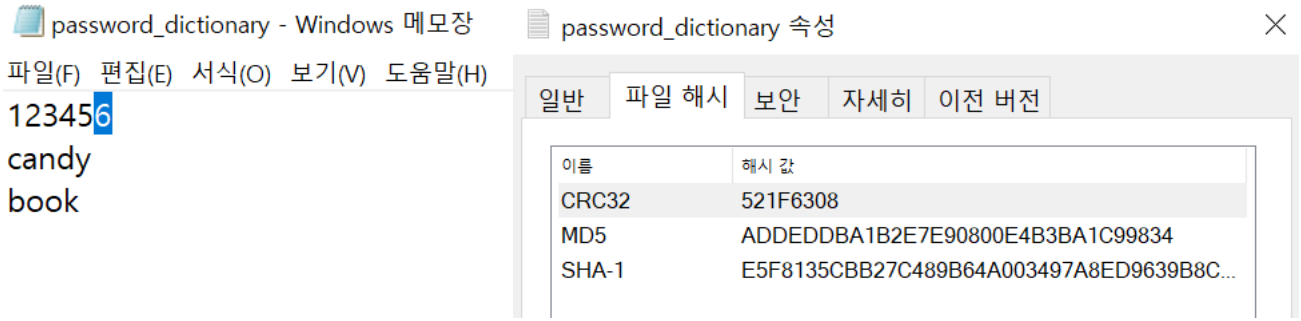
<해시 함수를 이용한 긴 메시지의 서명>

해시 함수의 활용범위 - 데이터 위·변조 검사

- 디지털 증거의 증거능력을 확보하기 위해서는 '**무결성**'을 검증해야 함
- 해시 함수의 '제 2의 역상 저항성' 성질 이용



<텍스트 파일의 원본 해시 값>



<수정한 텍스트 파일의 해시 값>

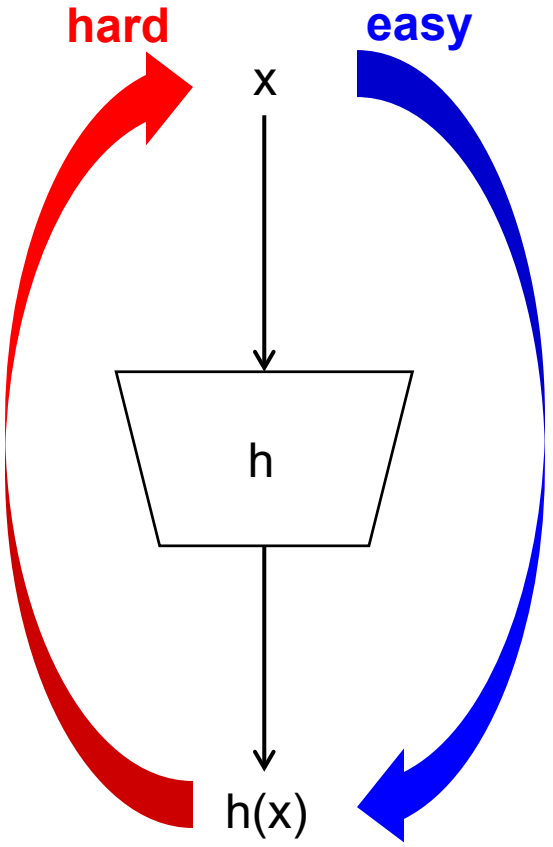
해시 함수의 안전성 요구사항

- 해시 함수가 안전하기 위한 3가지 핵심 특성:

1. **역상 저항성**(역상 찾기의 어려움) 또는 일방향성
2. **제 2의 역상 저항성** 또는 약한 충돌 저항성
3. **충돌 방지**(저항성) 또는 강력한 충돌 방지

해시 함수의 안전성 요구사항 - 1. 역상 저항성

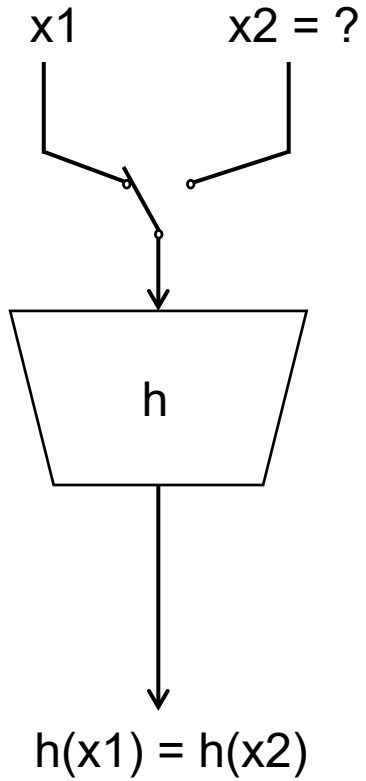
- 역상 저항성(Preimage Resistance) 또는 일방향성(One-Way ness)
- 주어진 임의의 출력값 z에 대해, z = h(x)를 만족하는 입력값 x를 찾는 것이 불가능함(Infeasible).
- 즉, $h(\cdot)$는 일방향 함수임.



해시 함수의 안전성 요구사항 - 2. 제 2의 역상 저항성

- 제 2의 역상 저항성(Second Preimage Resistance) 또는 약한 충돌 저항성(Weak Collision Resistance)

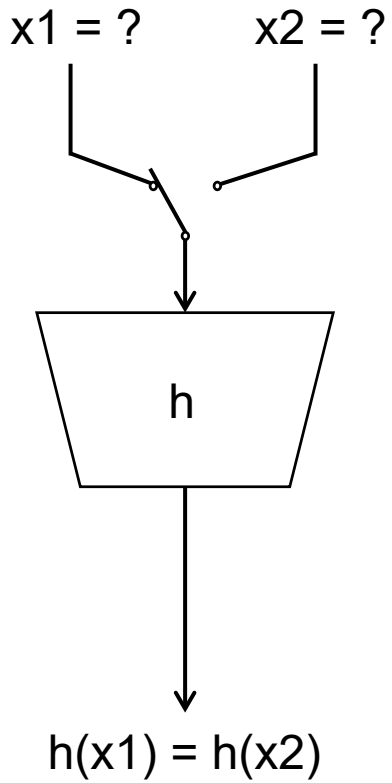
- 주어진 입력값 x1에대해 h(x1) = h(x2), x1 ≠ x2 를 만족하는 다른 임의의 입력값 x2를 찾는 것이 불가능함



해시 함수의 안전성 요구사항 - 3. 충돌 방지

- 충돌 저항성((Strong) Collision Resistance) 또는 (강력한)충돌 방지

- h(x1) = h(x2) 를 만족하는 임의의 서로 다른 두 입력값 x1, x2 (x1 ≠ x2)를 찾는 것이 불가능함

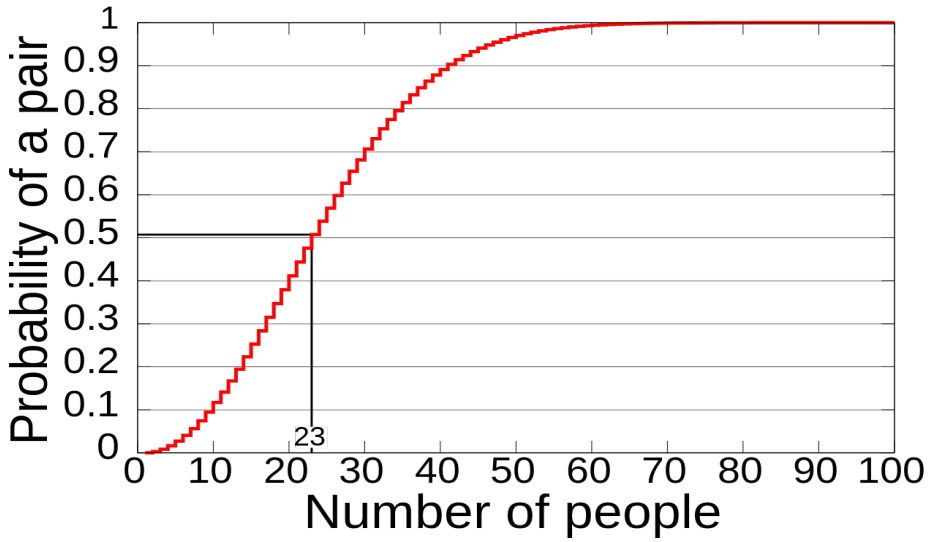


해시 함수의 안전성 요구사항 - 3. 충돌 방지

- 생일 공격 (Birthday Attack)

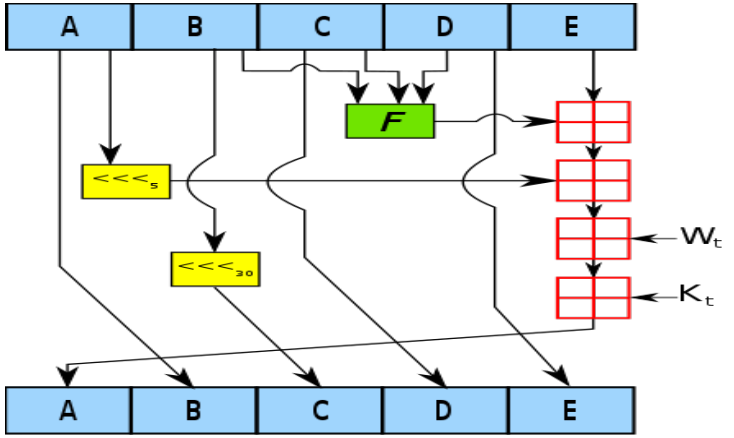
- **생일 역설** (Birthday Paradox)에 기반한 공격

- 생일 역설이란? 23명 이상의 사람들이 임의로 모였을 때, 그중에 생일이 같은 두 명이 존재할 확률이 50퍼센트가 넘는 현상을 말함



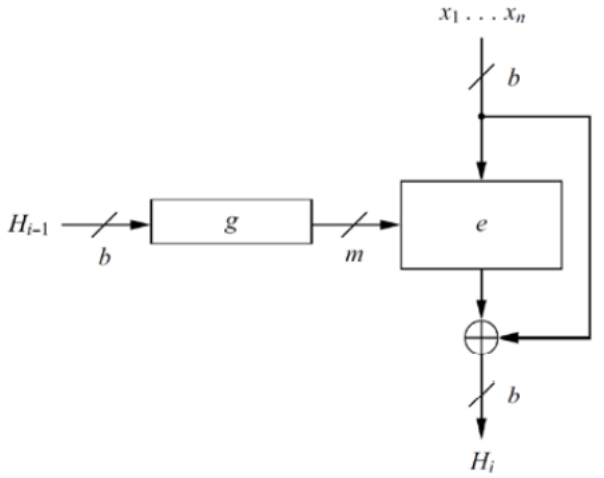
해시 함수 알고리즘

- 전용 해시 함수
  - 해시 함수로 동작하도록 특별히 설계된 알고리즘
  - MD4, MD5: 일방향 해시 함수, 128비트의 해시 값을 가짐
  - SHA: 일방향 해시 함수, 160비트의 해시 값을 가짐



<SHA-1 알고리즘>

- 블록 암호 기반 해시 함수
  - 해시 함수를 구성하기 위해
    AES와 같은 블록 암호를 이용함
  - 블록 암호 체이닝 기술을 이용해서 구현 가능



<ex: Matyas-Meyer-Oseas 해시 함수>

Q & A