22.12.18

📌 SHA-1

- 문서변조여부를 확인하기 위한 해싱에서 해시함수 중 하나
- 입력을 받고 메시지 다이제스트라는 160비트(20바이트) 해시값을 만드는 암호화 해시 함수
- **인터넷 보안 프로토콜과 공개키 인증서에 적용(TLS/SSL 인증서)**
- **SHA-1은 160비트의 메세지 다이제스트를 생성하는데 무차별 대입 공격으로 동일한 해시를 만들 수 있는 취약점**
- 해시 충돌의 위험이 있음 (해싱되는 결과값이 같아지는 경우가 존재한다.)
- 해시함수를 통해 압축 적용단계가 많아질수록 복잡해져서 문서의 변조를 막는다.

📌 해싱과 암호화

- 해싱 : 단방향, 변조 여부 확인, 해시함수를 이용해 더 짧은 길이의 값이나 키로 변경한다.
- 암호화 : 양방향, 전송중 데이터를 보호하기 위함

📌 세션 서버가 날아갔을 경우

1. 레플리카
    - Master , Slave
    - 트래픽 분산과 백업을 위해 사용
2. Redis를 사용하고 백업으로 RDB 사용

📌 Rest API uniform interface

- url로 자원을 식별한다.

- GET, PUT, POST, DELECT 4가지 인터페이스(HTTP 메소드)로 한정지어서 해당하는 Resource를 접근한다