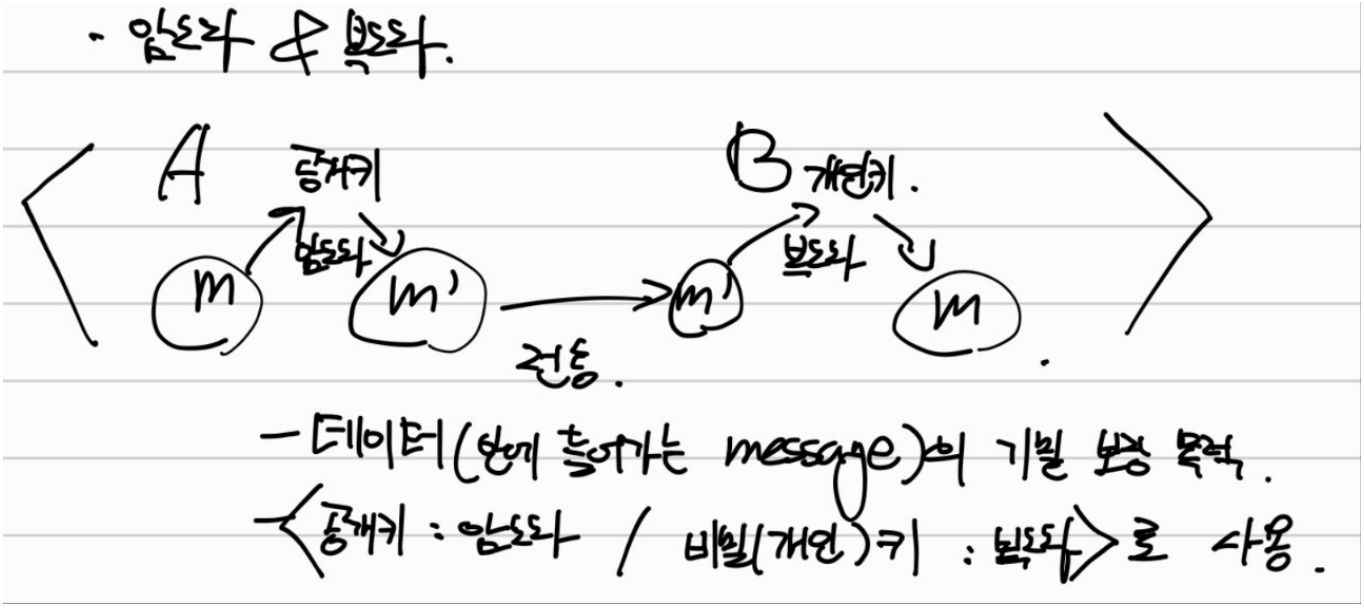
공개 키, 개인 키, 암호화와 복호화, 서명 생성 및 검증

공개 키, 개인 키

- 공개 키 / 비밀 키 란? : 암호화 과정에서 사용되는 키 쌍. 이 친구들을 활용하여 보통 암호화 / 복호화 / 서명 검증 / 서명 생성을 함. (암호화 과정에서 사용되는 인수라고 생각하면 될 듯.)
  - 공개 키 : 데이터를 암호화하거나 디지털 서명을 검증하는 데 사용.
    - 공개적으로 배포 가능. 공유되어도 보안 상 문제 없음.
    - ex - A가 B 에게 보낼 Message c 를 작성했다 할 때, c 를 암호화 할 때 사용. c를 암호화 c' 은 비밀 키가 있어야 c 로 복호 가능.
  - 비밀 키 : 암호화된 데이터를 해독하거나 디지털 서명을 생성하는 데 사용.
    - 이 키는 매우 중요, 오직 키의 소유자만이 알고 있어야 함.
    - B는 자신이 받은 암호화 c' 을 비밀 키를 이용하여 복호화 하여 c 로 만들 수 있음.

암호화 (Encoding) / 복호화 (Decoding)



디지털 서명 생성 (Signing) / 디지털 서명 검증 (Verification)