

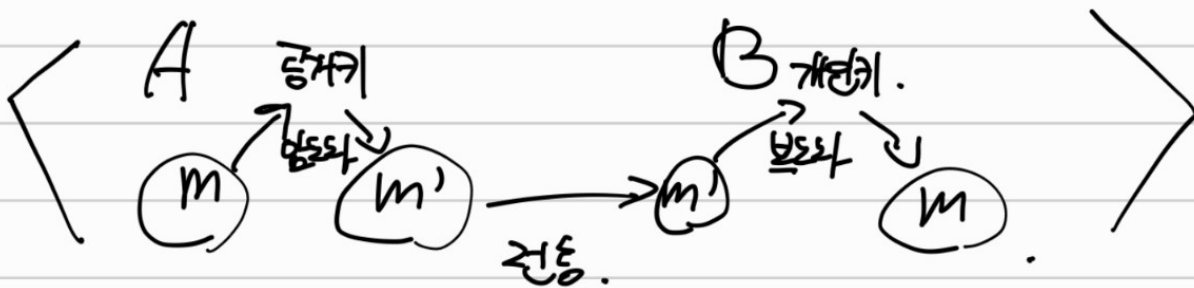
공개 키, 개인 키, 암호화와 복호화, 서명 생성 및 검증

공개 키, 개인 키

- 공개 키 / 비밀 키란? : 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 B에게 보낼 Message c 를 작성했다 할 때, c 를 암호화 할 때 사용. c 를 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)

- 암호화 & 복호화.

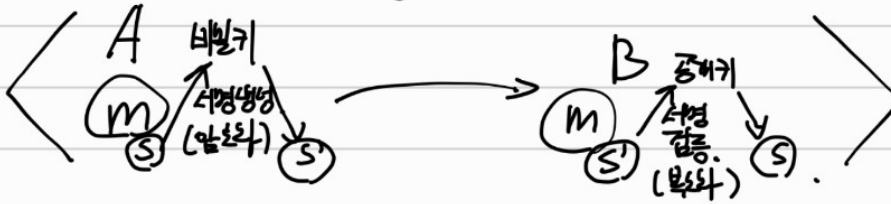


- 데이터 (보내려는 message)의 기밀 보강 목적.

<공개키 : 암호화 / 비밀(개인)키 : 복호화>로 사용.

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

· 디지털 서명 생성 (Signing) & 검증 (Verification)



- 데이터의 무결성 / 발신자의 신원성 보장.
- <증거: 복호화 / 비밀키: 암호화>로 사용.

이런 과정의 이점 :

이 증거를 이용해서 복호화
해줄 때 "~~"라 따져줍니다
라 하. ① 볼때, ②가 포함된
비밀키 가지고 있는 사람에게 못보들.
즉, 누가 보았는지 검증/인증가능.
또한, 데이터를 전송할 때
데이터를 기반으로 어떻게 만드는지
개인이 하고 있는 것들 밖에 못보들,
무결성 보장.