대칭키/ 공개키

대칭키(Symmetric Key)

> 암호화와 복호화에 같은 암호키(대칭키)를 사용하는 알고리즘

연산 속도가 빠르고 구현이 용이하다.

수신자는 각 송신자의 대칭키를 관리해야함.

키가 탈취되면 데이터 노출

공개키(Public Key)/비대칭키(Asymmetric Key)

> 암호화와 복호화에 사용하는 암호키를 분리한 알고리즘

연산속도가 느리지만 안전하다.

수신자는 개인키만 보관하고, 송신자들이 공개키로 암호화해서 데이터를 보내도록 한 뒤 개인키로 복호화한다. 공개키가 탈취되어도 상관없다.

데이터가 공개키로 복호화된다면, 어떤 개인키로 서명된것이다. 이를 이용해 SSL 인증서를 발급한다.

대칭키 + 비대칭키 혼합 방식

- 대칭키를 관리할 때 비대칭키를 이용한다.

대칭키를 공개키로 암호화하여 전달하고, 개인 키로 복호화하는 방식이다. 대칭키가 암호화되어 있어서 탈취되어도 안전하다. 이후 대칭키를 이용해 암호화 통신한다.

1. A → B 연결 요청
2. B → A : 공개 키 전송
3. A → B : 공개키로 대칭키를 암호화해 전송
4. B: 암호화된 대칭키를 개인키로 복호화
5. 이후 통신