대칭키 & 공개키

개요

대칭키 암호화 방식

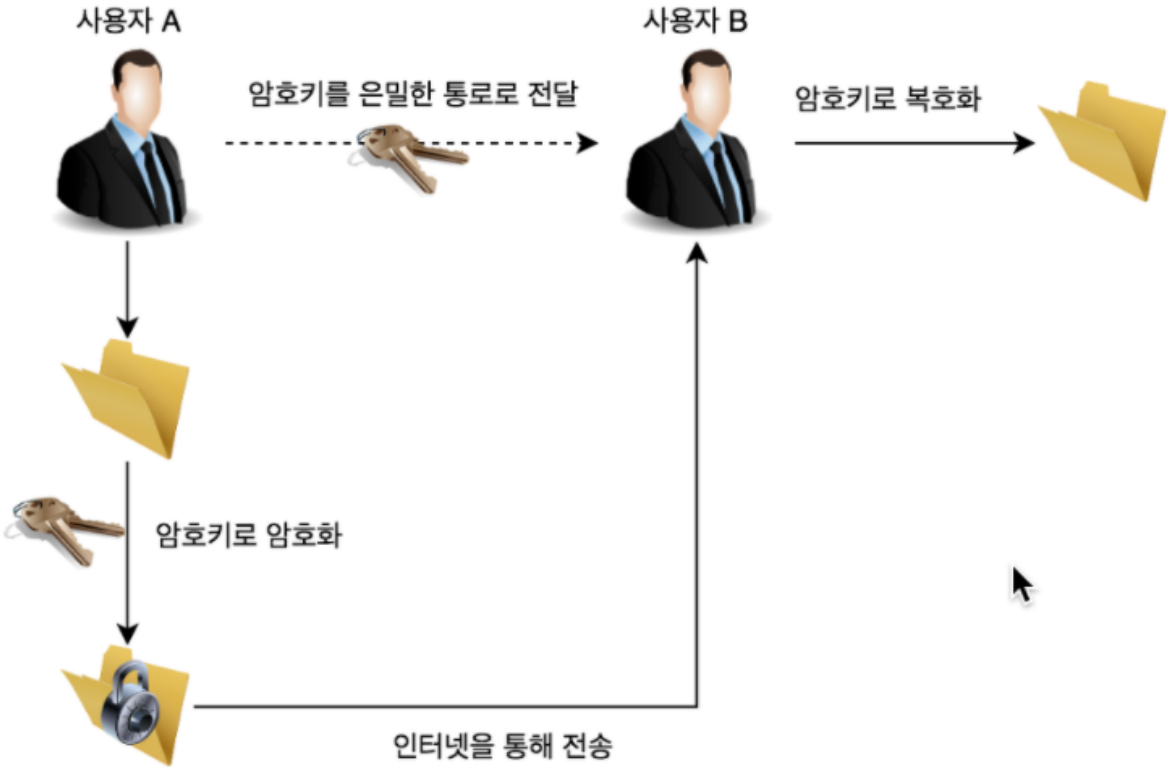
암복호화에 사용하는 키가 동일한 암호화 방식

공개키 암호화 방식

암복호화에 사용하는 키가 서로 다르며, 비대칭키 암호화라고도 함

송수신자 모두 한쌍의 키(개인키, 공개키)를 갖고 있게 됨

대칭키 (Symmetric-key)



암복호화 키가 동일하며, 해당 키를 아는 사람만이 문서를 복호화해 볼 수 있음

공개키 암호화 방식에 비해 빠르다는 장점이 있으나, 키를 교환해야한다는 문제인 키 배송 문제가 발생함

키를 교환하는 도중 탈취 가능성이 있고, 사용자가 증가할수록 전부 따로 키교환을 해야하므로, 관리해야할 키의 수가 매우 많아짐

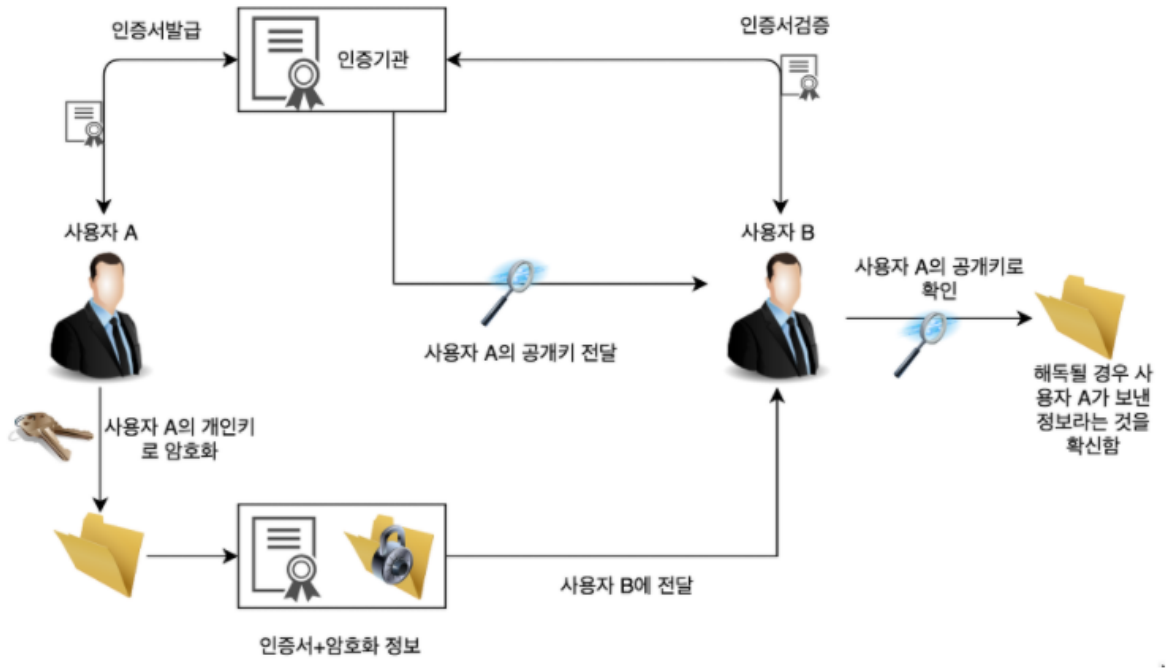
이러한 키 배송 문제를 해결하기 위한 방법으로, 키의 사전 공유에 의한 해결, 키 배포센터에 의한 해결, Diffie-Hellman 키 교환에 의한 해결, 공개키 암호에 의한 해결이 있음

대표적인 알고리즘 : DES, 3DES, AES, SEED, ARIA 등

장점 : 수행시간이 짧음

단점 : 키 배송 문제로 인해 안전한 키 교환 방식이 추가로 요구되며, 사용자가 증가할수록 키 관리가 어려워짐

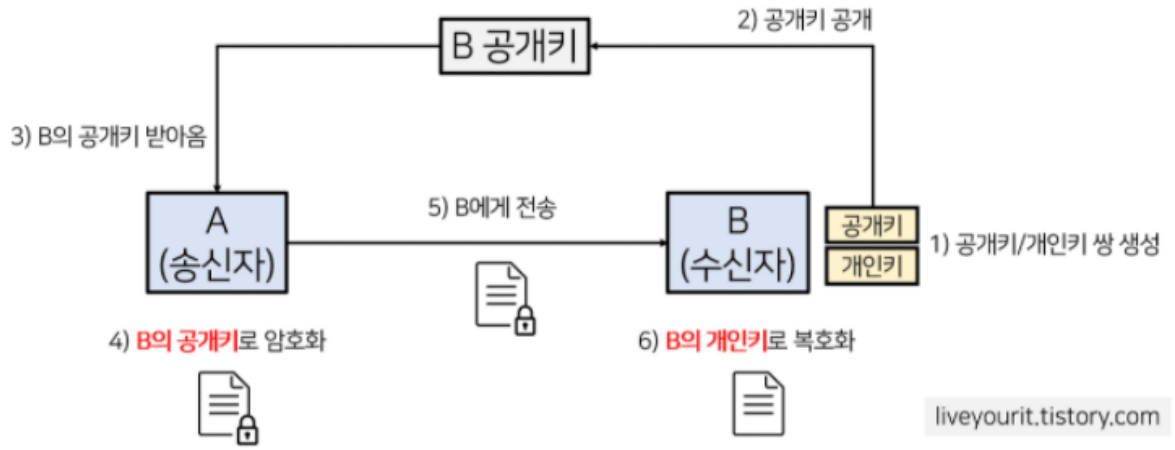
공개키 (비대칭키, Public-Key)



대칭키의 키 교환 문제를 해결하기 위해 등장한 암호화 방식

공개키와 개인키로 이루어져있음

이름 그대로 키가 공개되어 있으므로, 키를 교환할 필요가 없어지며, 공개키는 모든 사람이 접근이 가능하고, 개인키는 각 사용자만이 가지고 있는 키



A 가 B에게 데이터를 보낼 경우, A는 B의 공개키로 암호화한 데이터를 보냄

B는 본인의 개인키로 해당 암호화된 데이터를 복호화해서 확인함

따라서 암호화된 데이터는 B의 공개키에 대응되는 개인키를 가진 B만이 볼 수 있음

⇒ **안전한 데이터 전송이 가능함**

대표적인 알고리즘 : RSA, 전자서명

장점 : 키분배가 필요 없으며, 기밀성/인증/부인방지 기능을 제공함

단점 : 대칭키 암호화 방식에 비해 속도가 느림

대칭키, 공개키 비교표

비교 항목	비밀키 암호화	공개키 암호화
키 개수	한 개의 키를 사용	두 개의 키를 사용
키 보관 형태	비밀리에 보관	개인키는 비밀리에 보관, 공개키는 어디든지 배포
키 교환	키를 교환하는 것이 어려우며 위험하다.	공개키를 교환하는 것은 매우 쉽다.
키 길이	주로 64비트, 128비트 등 작은 길이	주로 512, 1024, 2048비트 등 큰 길이
암호화 속도	빠르다	느리다
암호화할 수 있는 평문의 길이	제한 없음	제한 있음
기밀성	가능함	가능함
인증	부분적 가능함	가능함
무결성	부분적 가능함	가능함
부인 방지	불가능	가능함

https://gaeko-security-hack.tistory.com/123

https://liveyourit.tistory.com/183

https://brownbears.tistory.com/332