사용자 인증

사용자 인증은 서버 인증과 원리는 같지만, 서버와 클라이언트의 역할만 바뀌게 됩니다. 사용자 인증은 ① 클라이언트에서 비대칭키(공개키와 비밀키)를 ② 생성합니다. 여기서 생성된 공개키는 사용자가 서버에 있는 .ssh/authorized_keys 파일에 사전에 복사해둡니다. 서버는 공개키를 가지고 있고 클라이언트가 비밀키를 가지고 있게 됩니다.

만약 서버에 '.ssh' 디렉토리가 없으면, 해당 디렉토리를 생성해야 함.

③ 서버에서 난수값을 생성 뒤에 해시값 만들어 저장합니다. ④ 서버에서 난수값을 암호화해 클라이언트에 전송하게 되고, ⑤ 클라이언트에서 암호화된 난수값을 비밀키로 복호화를 합니다. ⑥ 복호화된 데이터로 해시값을 생성해 다시 서버에 보내게 됩니다.

⑦ 서버에 저장 하고 있던 해시값과 클라이언트로부터 다시 받은 해시값을 비교해 정상적인 사용자인지를 확인하게 됩니다. 이 과정을 사용자 인증이라고 합니다.