201603867 조성환

채팅프로그램-RSA

이전 과제는 채팅 프로그램에서 AES 를 생성, AES 를 이용해 암,복호화를 했다.

이번 과제에는 저번 채팅 프로그램에서 key 를 그냥 보내는 대신, RSA 암,복호화를 이용해 보내는 내용을 추가했다.

pubKey 로 암호화해서 보내는 이유는 공개키는 말 그대로 배포를 함으로써 공개를 하는 공개키고, 개인키는 본인만 가지는 키이므로, 해당 개인키를 소유한 본인이 메시지 개인키로 복호화를 할 수 있도록 하기 위해서다. 그 반대로 하는 것은 전자서명의 개념이다.

구현 시 PKC11 모듈을 이용했다. ppt 에는 publick key 를 이용해 복,암호화를 하는 반면, 버전에 따라 달라서 PKC 를 이용해 encryptor 를 생성, 생성한 객체로 암,복호화를 진행하는 방식으로 했다.

암호화한 키는 클라이언트에서 prikey 를 이용해 encryptor 생성, 복호화를 진행함으로 써 key 를 전달했다. 이외에 나머지는 저번 과제와 같다.