1:1 암호화 통신 201603867 조성환

Socket을 통해 1:1 통신을 구현 후 암호화로 문자를 보낸 후, 데이터를 복호화 하는 통신을 구현.

이전 과제에서 Iv, key를 이용해 aes 암호화를 진행했다. 이를 살짝 잘못된 방식으로 했는데, 인코딩과 디코딩을 이해 못한점에서 발생한 문제였다.

애초에 인코딩 디코딩을 하는 이유는 한가지 타입으로 맞추기 위함이었고, 예를들어 디비에 문자열을 넣기 위해서는 해당 db에서 사용하는 문자로, 이런식으로 맞춰야한다.

AES 암호문에서 인코딩을 하는 이유는, C++을 이용하는데, c코드에서는 문자열이 없고 char 배열 밖에없기 때문에 인코딩을 통해 바이트로 바꾸고, python에서 문자열로 바꾸기 위해 인코딩한 방식으로 디코딩을 하는 것이다.

가장 많이 발생한 오류는 byte don't have encode 라는 내용인데, string을 인코딩하면 byte로, byte를 디코딩 함으로써 string이 되는 방식인데, 이미 인코딩된 바이트를 인코딩했기 때문에 생긴 오류였다.

이를 해결하기 위해 만든 체계는 서버에 전송 및 암호화, 복호화에는 인코딩, 문자열 출력 시에는 디코딩을 하는 체계이다.

이런 기준을 잡고 과제를 시작했다.

먼저 소켓을 이용한 통신을 구현하기 위해, 로컬로 돌린 후, 포트를 잡아 서버와 클라이언트를 만든다. 서버는 리슨을 통해 클라이언트를 기다리고, 클라이언트가 접속하면 대화가 시작하는 형식이다.

데이터를 보내고 받을때는 문자열을 인코딩해서 보냄, 디코딩해서 받는데, 방식은 상관없지만 여러 가지 이유 때문에 binary파일을 보내는 걸로 이해했다.

통신 프로그램을 만들면 Mcipher를 통해 암호화 복호화를 한다. AES set을 하는 방법은, set AES 함수를 통해 하는데, c코드이기 때문에 key, iv를 인코딩해야한다.

인코딩한 값을 넣으면 aes를 리턴하고 이 aes를 통해 암호화 혹은 복호화를 진행한다.

다만, 채팅 프로그램에서 입력값을 암호화후 전달, 받은 바이너리 파일을 복호화해서 출력하는 방식으로 진행하는데, 한번 set한 aes를 연속으로 암호화 복호화 순으로 진행할 순 없다. 그러기 때문에 암호화에서 복호화 혹은 반대의 방식을 이용하려면 다시 set해야한다. 이런식으로 반복하다가 클라이언트에서 bye를 입력하면 프로그램이 종료되도록 설계했다.

중배엽 내배엽 외배엽

트레이닝의 원리 ㅈㄴ 중요

모든 트레이닝 프로그램은 자신의 운동 종목이나 기술에 필요한 생리학적 능력을 발달시킬 수 있도록 계획되어져야한다.

평가