Information System Security HW#1 (fall 2020)

소감

1번

실제 암호화 알고리즘을 사용을 경험하여 다소 미지의 영역이었던 암호 분야를 조금이나마 경험해 본 것이 좋았다. 암호화가 막연하게 어려운 것이라고 생각했는데 막상 써보니 그렇게 어려운 것도 아닌것 같아 자신감을 얻었다.

IV값을 암호, 복호화에서 이용하게 되는데 암호화 할 때 IV값을 어떻게 처리할지 잘 몰랐다. 랜덤하게 생성하여 암호화 시키려고 하니 복호화에서도 동일한 값이 필요한데 랜덤값이다 보니 저장하고 있어야 하는 문제가 발생했다. 문서에 직접 기입하기엔 원본 문서를 해치는 영향이 있고 프로그램 내부에는 저장할 수 없으니 다소 고민되었다.

2번

어떠한 값이라도 256비트값으로 표현하고 같은 값을 가지기 매우 어렵다는 사실이 상당히 매력적인 부분이라고 생각한다. 또한 속도도 빨라서 많은곳에 이용될 것이라고 생각했다.

전체적 소감

암호/해시 알고리즘이 멀게만 느껴졌었는데 그렇게 어렵지 않은것이라 느끼게 되었다. 한편 암호화 값 등이 전부 바이트 단위로 이루어지기 때문에 base64인코딩이나 16진수화 하는 과정 등 사람이 알아보기에 여러 과정을 거쳐야 했는데 이점은 다소 아쉽다.

네트워크 상에서 해당 암호화 방법들이 사용되는 것을 만들어 보는것도 좋은 경험일것 같다는 생각이 들었다.