201603867 CTR

AES 의 encrypt, decrypt 를 통해 암호화, 복호화를 함.

CBC 와는 달리 iv 값 대신 counter 를 통해 암호화를 진행한다. Counter 객체를 128bit 로 생성, 16 자리 key 값과 xor 연산을 통해 key 를 만든 후 이 값과 평문을 암호화한다.

ctr 모드는 iv 값이 없고 다음 암호문, 평문에 영향을 주지 않기 때문에 계산이 순차적으로 이뤄지지않고 병렬적으로 이뤄져서 속도가 더 빠르다는 장점이 있다.