현대암호학기초

조별과제

9조 송희원, 권혜민, 이현정, 윤명지

앨리스가 생각한 모드가 가지고 있는 성질

1. CBC 모드와 다르게 암호화를 먼저 한 후 초기화 벡터와 XOR시키고, 그 이후의 블록부터는 암호문블록과 XOR시키는 것이 아니라 평문블록과 XOR시킨다. 그렇기 때문에 평문블록 2를 암호문 블록2로 암호화하는 과정에서 문제가 발생해도 평문블록2가 온전하다면 그 평문블록3부터는 연속적으로 문제가 발생하지 않는다.
2. 하지만 복호화 할 때 CBC모드와 다르게 깨진 암호문이 있으면 그 이후 평문 블록 전체에 영향을 미친다. (평문이 된 상태에 결과를 다음 단계의 XOR로 사용하기 때문),비트 누락 또한
3. 복호화를 하다 보면 전 단계의 평문을 알아내기가 쉽다고 생각한다.
4. 도중의 평문 블록만 뽑아서 암호화 할 수 없다.
5. XOR을 이용하기 때문에 평문반복이 암호문에 반영되지 않는다.
6. CBC 모드와 비슷한 이유로 초기화 벡터가 필요하다. (1단계에서 평문을 암호화 하고 XOR할 무언 가가 필요하기 때문)
7. 평문1과 평문2가 같더라도 암호문1과 암호문2의 결과는 다르다. ( IV와 XOR 취한 것이 암호문1이 되고, 평문1과 XOR 취한 것이 암호문2이 되기때문 )