**컴퓨터 보안 실습과제 보고서**

변형된 AES-128 구현

컴퓨터보안 002분반 [이문규 교수님]

12150981 박중규

[wndrb3@naver.com](mailto:wndrb3@naver.com)

010-3348-4311

**- 프로그램 동작원리 및 설명**

**• Encryption**

* 2차원 배열을 이용하여 “key.bin”과 “plain.bin” 파일의 데이터를 각각 “kState”, “pState”에 저장했습니다.
* “plain.bin”의 16바이트 데이터 당 한 번 while문 loop를 돌면서 Encryption을 수행하게 됩니다. 매 루프마다 더 이상 읽을 데이터가 있는지 확인하고, 없다면 Encryption을 종료하게 됩니다.
* “cipher.bin” 파일을 생성하여 while문 loop를 돌면서 암호화가 완료된 데이터들을 작성하였습니다.
* Encryption 수행을 위해 SB(SubBytes), SR(ShiftRows), MC(MixColumns), KE(KeyExpansion), AR(AddRounndkey) 함수를 작성하였습니다.
* key 데이터를 담은 2차원 배열인 “kState”는 round가 진행됨에 따라 KeyExpansion이 진행되고,  
  round를 진행할 데이터를 담은 2차원 배열인 “cState”는 round가 진행됨에 따라 위의 Encryption 과정을 수행하게되고, 10번 째 round가 끝나면 fwrite 함수를 이용하여 암호화된 16바이트 데이터를 작성합니다. 이 과정을 반복합니다.

**• Decryption**

* Encryption과 유사한 방식으로 진행하였습니다.
* 2차원 배열을 이용하여 “key.bin”과 “cipher.bin” 파일의 데이터를 저장했습니다.
* “plain2.bin” 파일을 생성하여 while문 loop를 돌면서 복호화가 완료된 데이터들을 작성했습니다.
* Decryption 수행을 위해 SB, SR, MC 함수의 역연산 함수를 작성하였습니다.
* Decryption 과정에서는 Roundkey가 역순으로 필요하므로, 매 Round마다 필요한 key를 expansion해주고, 다음 round를 위해 초기화하는 과정을 진행하였습니다.
* 10번 째 round가 끝나면 fwrite 함수를 이용하여 복호화된 16바이트 데이터를 작성합니다. 이 과정을 반복합니다.

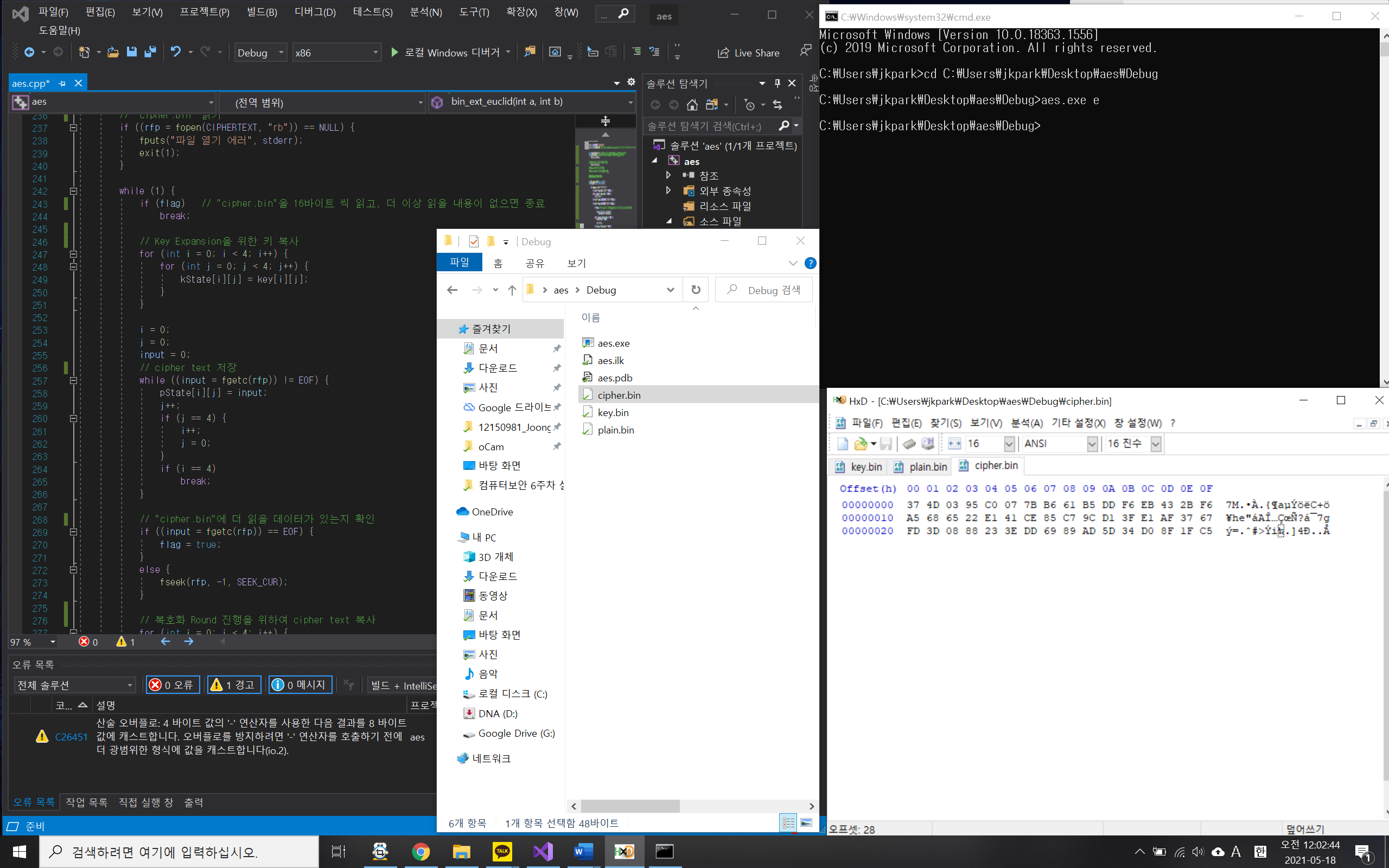
**• 함수 설명**

* **SB 함수**  
  각 바이트마다 연산을 진행합니다.  
  SubBytes에 순서에 따라,  
  모듈러 곱셈의 역원으로 바꾸기 → 정수를 비트로 바꾸기 → A행렬(SubBytes행렬)과 연산 후 열벡터와 XOR → 비트를 정수로 바꾸기 → 결과값 저장  
  의 과정을 16개의 바이트가 거치게 됩니다.  
  binary polynomial상의 모듈러 곱셈의 역원을 구하기 위하여 “bin\_inv” 함수를 사용하게 됩니다.  
  “SB\_inv” 함수는 이 함수의 역연산 함수입니다.
* **SR 함수**  
  ShiftRows에 따라 각 바이트의 값을 바꾸어 줍니다.  
  “SR\_inv” 함수는 이 함수의 역연산 함수입니다.
* **MC 함수**  
  각 바이트마다 연산을 진행합니다.  
  mixcolumns table과 행렬연산 후 값을 저장합니다.  
  행렬연산 시 binary polynomial상의 모듈러 곱셈을 위하여 “bin\_mul” 함수를 사용하게 됩니다.  
  “MC\_inv” 함수는 이 함수의 역연산 함수입니다.
* **KE 함수**  
  key의 4개의 word 중 마지막 word를 가지고 연산을 먼저 진행합니다.  
  바이트의 순서를 바꾸고, 각각의 바이트를 SB함수처럼 S-box에 통과시키는 연산을 진행합니다.  
  또 phase에 따라 RC의 첫 번째 원소값을 구합니다. 첫 번째 원소값은 모듈러 연산을 얻을 수 있는 값입니다.  
  위에서 계산한 word와 RC를 XOR시키고, 그 결과를 이용해 첫 번째 word를 XOR시켜서 다음 첫 번째 word를 구하고, 그 이후로 첫 번째 word를 시작으로 이전 word와 XOR하여 다음 word들을 구합니다.
* **AR 함수**  
  key와 XOR를 수행합니다.

다음은 유한체 관련 계산 함수들 입니다.

* **deg 함수**  
  binary polynomial의 degree를 구하는 함수입니다.
* **bin\_ext\_euclid 함수**  
  binary polynomial상에서의 확장 유클리드 함수입니다.  
  모듈러 곱셈의 역원을 구하기 위해 사용됩니다.
* **bin\_inv 함수**  
  binary polynomial상에서의 모듈러 곱셈 역원을 구하는 함수입니다.
* **bin\_mul 함수**  
  binary polynomial상에서의 모듈러 곱셈을 구하는 함수입니다.
* **carry 함수**  
  carry 발생 시 처리 함수입니다.

**- 실행 샘플 이미지**

Encryption 시  


Decryption 시

