보안s/w 구현-HW1 3번(20192233 박진철)

(a)

(b) 역행렬 구하기 위한 연산 함수들은 대부분 동일

텍스트이(가) 표시된 사진

자동 생성된 설명

-행렬 A의 크기는 8x8이므로, 연산을 위해서는 최대 크기를 16x16으로 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

-GF(2)에서의 곱셈은 AND 연산과 같으므로, AND 연산 함수 생성

텍스트, 모니터, 화면, 검은색이(가) 표시된 사진

자동 생성된 설명

-GF(2)의 원소 값인 0과 1만 나올 수 있도록 함수 수정

텍스트이(가) 표시된 사진

자동 생성된 설명

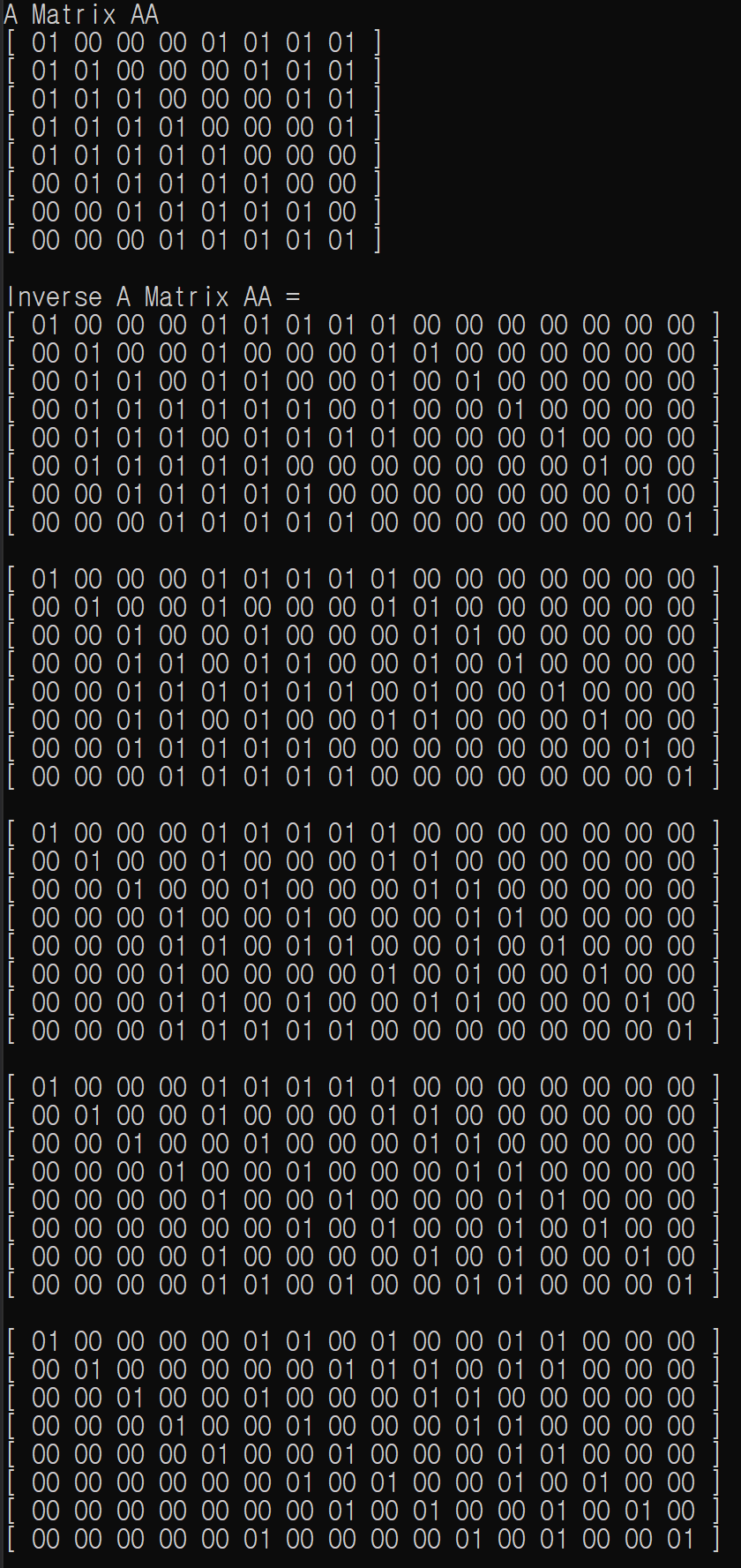
GF(2)={0, 1}. 0의 곱셈의 역원은 0, 1의 곱셈의 역원은 1이됨.

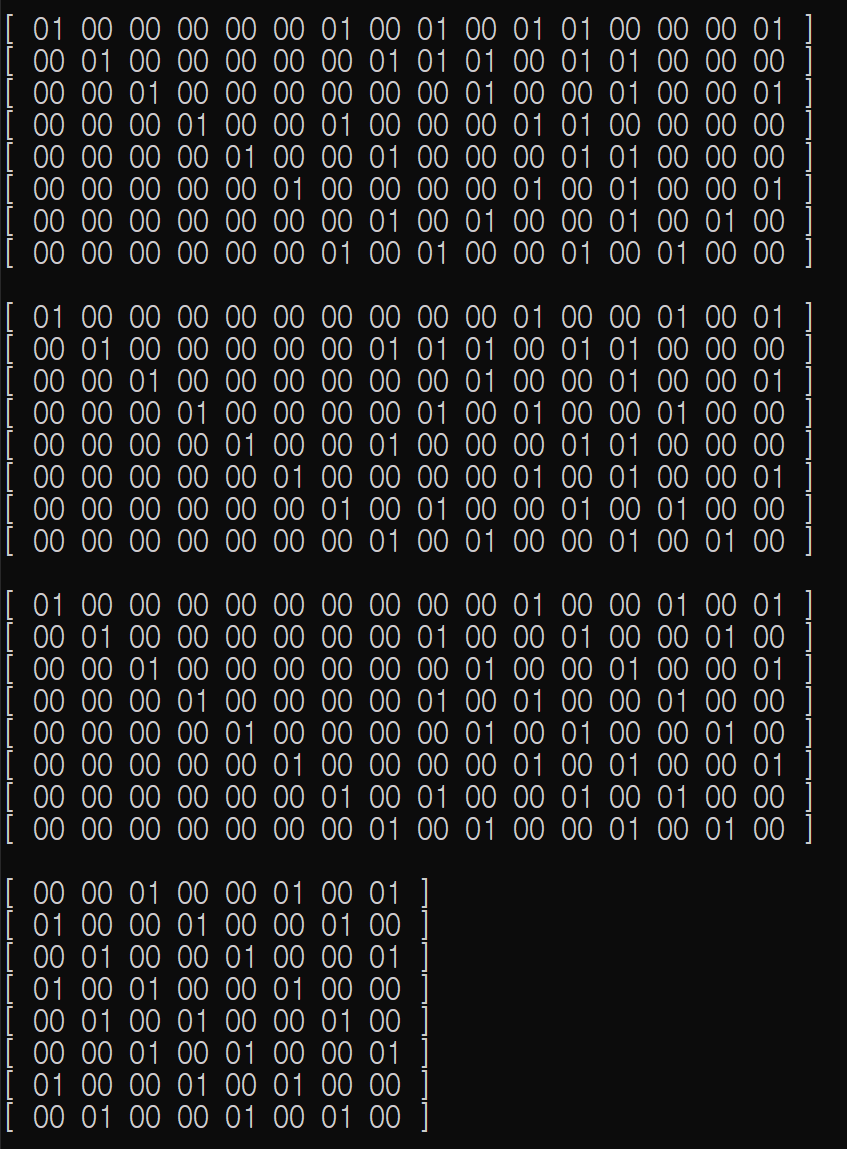
텍스트이(가) 표시된 사진

자동 생성된 설명

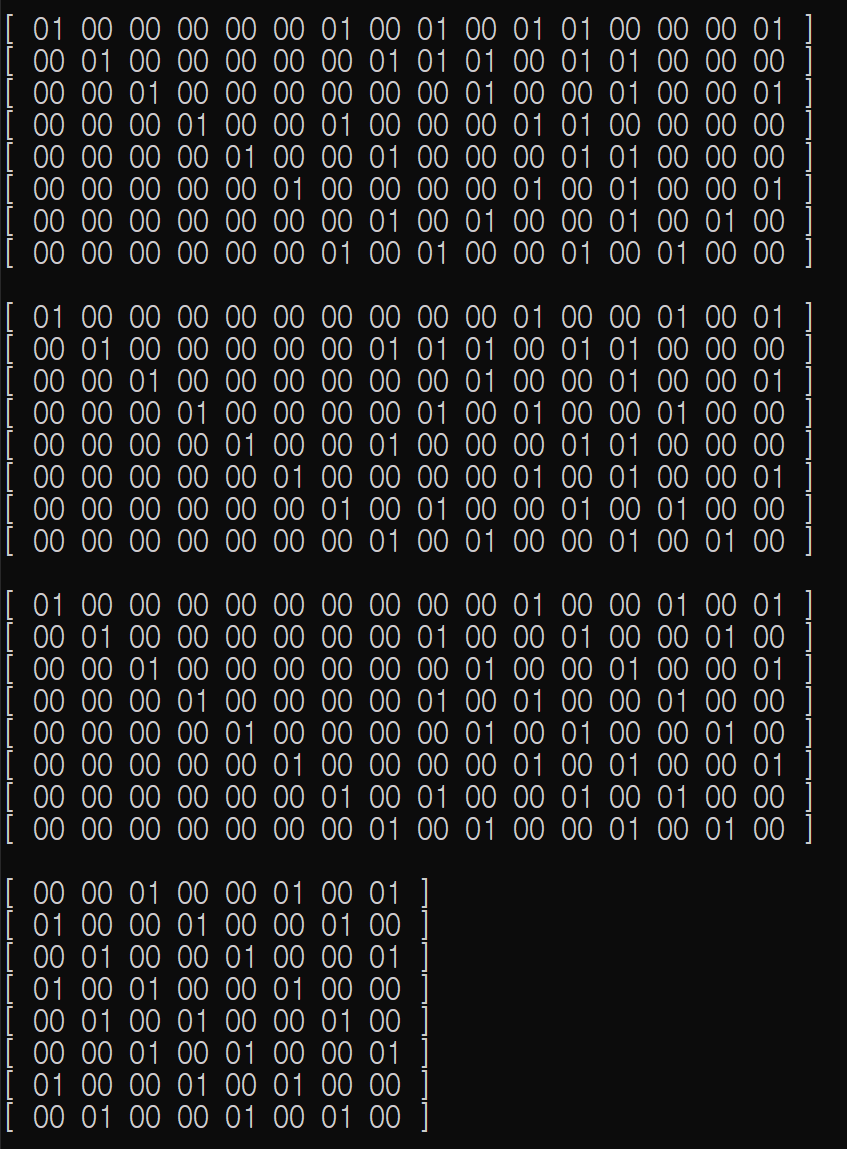
-행렬A를 GF2\_Mat\_inverse(AA)함수에 넣어 나온 역행렬 InvA 출력

=>실행 결과





-Gauss-Jordan 소거법을 이용해 역행렬 계산



-역행렬 출력

(c)

텍스트, 전자기기이(가) 표시된 사진

자동 생성된 설명

-(b)를 통해 A의 역행렬 계산

-이므로 를 구한 후 inv 함수를 통해 곱셈의 역원 계산

텍스트이(가) 표시된 사진

자동 생성된 설명

-0x00~0xFF에 대응하는 x를 계산하여 InvSbox 테이블의 원소 생성

텍스트이(가) 표시된 사진

자동 생성된 설명

-Get\_ISbox함수를 통해 InvSbox테이블 출력

=>출력결과

