보안 s/w 구현-HW1 4번(20192233 박진철)

(a)

텍스트이(가) 표시된 사진

자동 생성된 설명

-x[]: 생성자인 x를 저장하는 변수

-Sum: 생성자의 개수를 저장하는 변수

-0~255인 숫자 x를 각각 255번 곱함. 그 값이 1이면서 연산 중간에 1이 없으면 숫자 x는 생성자

=>실행 결과





(b)

텍스트이(가) 표시된 사진

자동 생성된 설명

-a1: 생성자의 원시근

-a2=a가 제곱되며 나오는 수들의 집합(a[n]=a^n)

-위 함수에서는 a를 0x05로 설정

-a2[0] = a^0=0x01=a^255

-a2[1] = a^1=a

-a[i+2]=a^i+2=a^(2+i)

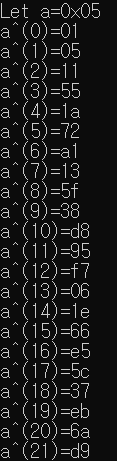
-연산 후 a의 제곱값들을 출력

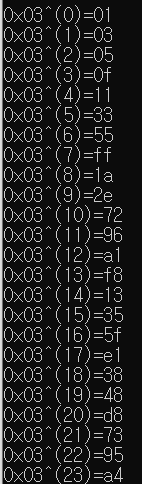
텍스트이(가) 표시된 사진

자동 생성된 설명

-0x03도 위의 연산과 마찬가지로 계산

=>실행 결과





(c)

Let a=0x05

(d)

1. ExpTable 구현

텍스트이(가) 표시된 사진

자동 생성된 설명

-생성자 a, ExpTable이 들어갈 etable을 받음

-etable[1]=a로 취함

- etable [1] = a^1=a

- etable [i+2]=a^i+2=a^(2+i)

2. LogTable 구현

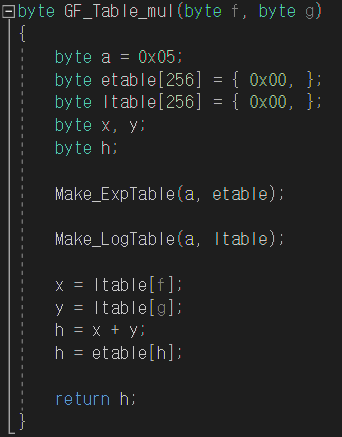
텍스트이(가) 표시된 사진

자동 생성된 설명

- 생성자 a, LogTable이 들어갈 ltable을 받음

-ltable=(etable)^(-1)

(e)



-곱해야하는 두 수 f, g를 받음

-여기서 생성자 a는 0x05로 가정

-f와 g에 대응하는 수를 LogTable에서 찾아 각각 x, y에 대입

-x+y은 f\*g=a^(x=y)를 만족함

-h를 ExpTable에서 찾아 곱한 값을 구함

=>실행 결과(f=0xa1, g=0x63)

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명



(f) 두 수의 곱을 쉽게 찾을 수 있으므로 x와 곱해져서 1이 되는 x의 역원 x^(-1)을 쉽게 구할 수 있다.