

보안SW구현 - 과제 1

제출 마감: 2022년 10월 16일

- 유한체 $GF(2^8)$ 의 원소의 다음 곱을 구하면?

$$0xa1 \times 0x63 =$$

바이트를 Rijndael Field의 7차 이하 다항식으로 변환하고, $m(x) = x^8 + x^4 + x^3 + x + 1$ 로 나눈 나머지를 계산하여 곱을 구하는 과정을 손글씨로 작성하라.

- 확장 유클리드 알고리즘(Extended Euclidean algorithm)을 이용하여 유한체 $GF(2^8)$ 의 원소 0xf6의 곱셈의 역원을 구하라. 풀이 과정은 손글씨로 작성하라.

- AES 알고리즘에 사용하는 Sbox는 다음 식으로 표현할 수 있다.

$$\begin{array}{l} y = S[x] \\ \downarrow \\ x = S^{-1}[y] \\ y = A\bar{x} + b \\ \downarrow \\ x = \boxed{\quad} \end{array} \quad \forall y = Sbox[x] = \boxed{S(x) = Ax^{-1} + b} \quad \begin{array}{l} x^{-1}: GF(2^8) \text{의 역원} \\ A\bar{x} + b \\ \text{Affine}(\text{선형}) \\ GF(2)^8 \text{의 벡터공간} \end{array}$$
$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

- Sbox의 역함수 InvSbox를 $x = \text{InvSbox}[y]$ 식으로 쓰면?

- [구현문제] 프로그램을 작성하여 A^{-1} 를 계산하라.

힌트: $GF(2)$ 의 역행렬을 구할 수 있도록 수업에서 사용한 역행렬 프로그램을 수정하라.

- [구현문제] InvSbox를 구하는 C 프로그램을 작성하라.

$GF(2^8)$ Field (체) — The Design of Rijndael (AES proposal v.2) $(x \neq 0) x \in GF(2^8), x = \alpha^{k_x}$

4. 유한체 $GF(2^8)$ 의 0이 아닌 원소는 곱셈에 대하여 순환군(cyclic group)을 이룬다. 즉, 어떤 $\alpha \in GF(2^8) \setminus \{0\}$ 가 존재하여, 모든 $x \in GF(2^8) \setminus \{0\}$ 는 $x = \alpha^{k_x}$ 으로 표현된다. 이 때, α 를 $GF(2^8)$ 의 생성자(generator)라 한다.

$$\forall x \in GF(2^8) \setminus \{0\}, \exists k_x \in \{0, 1, \dots, 254\} \text{ s.t. } x = \alpha^{k_x}.$$

- (a) [구현문제] $x \in GF(2^8) \setminus \{0\}$ 에 대하여 $x^n = 1 \pmod{255}$ 인 가장 작은 자연수 n 을 x 의 위수(order)라고 하며, 위수가 255인 원소는 생성자이다. 프로그램을 작성하여 $x = 1, 2, \dots, 255$ 의 위수를 구하라. 생성자가 될 수 있는 x 는 몇 개인가?
 (b) [구현문제] α 를 0x03과 함께 (a)에서 찾은 다른 생성자로 선택하고, 프로그램을 작성하여 아래 표를 완성하라.

α	α^0	α^1	α^2	\dots	α^{254}
0x03	0x01	0x03			
다른 α 값					

L3
X = CA
161 99
0xa1 x0x63
 $\alpha^6 \alpha^{225}$

- (c) 0이 아닌 두 원소 x, y 의 곱을 다음과 같이 계산할 수 있다.

$$x \cdot y = \alpha^{k_x} \cdot \alpha^{k_y} = \alpha^{k_x + k_y} \pmod{255}$$

- (b)의 표에서 사용한 두 가지 생성자를 이용하여 $0xa1 \times 0x63$ 를 계산하라. 이 결과는 문제 1의 결과와 일치하는가?

- (d) [구현문제] 생성자 α 를 선택한다. $k = 1, 2, \dots, 255$ 에 대하여 α^k 를 테이블 $\text{ExpTable}(k)$ 로 만들어라.

$$k \mapsto \alpha^k = \underline{\text{ExpTable}(k)}$$

역으로 주어진 α^k 에 대하여 k 를 테이블 $\text{LogTable}(\alpha^k)$ 로 만들어라.

$$\alpha^k \mapsto k = \underline{\text{LogTable}(\alpha^k)}$$

- (e) [구현문제] 테이블 $\text{ExpTable}()$ 과 $\text{LogTable}()$ 을 이용하여 $GF(2^8)$ 의 곱을 계산하는 함수를 작성하라.

- (f) 이 결과로부터 AES의 Sbox를 만들기 위해 필요한 역원 $x \mapsto x^{-1}$ 의 계산을 쉽게 할 수 있음을 보여라.

$$k \mapsto \alpha^k \quad \text{if } k$$

□ 주의:

모든 문제 (구현문제 포함)는 답과 설명을 작성해야 하며 소스 코드는 문제별로 하나 혹은 다수의 파일로 만들 수 있으며 실행에 필요한 모든 코드가 실행방법과 함께 제출되어야 한다.