2019 국가암호공모전 Ⅱ 분야

문제 02

본 문제는 첨부된 평문-암호문 파일로부터 블록암호의 비밀키를 찾는 문제이다.

각 사용자의 키 K_{ID}는 (전체 사용자 공통의) 40비트 마스터 키와 각 사용자 고유의 40비트 ID에 의하여 정의된다. 블록암호 E는 치환함수 P를 사용하는 (Single-Key) Even-Mansour 구조로서, 40비트 사용자 키 K_{ID}에 대하여 40비트 평문 U는

$$E_{K_{ID}}(U) = P(U \oplus K_{ID}) \oplus K_{ID}$$

로 암호화된다 (그림 1 참조).

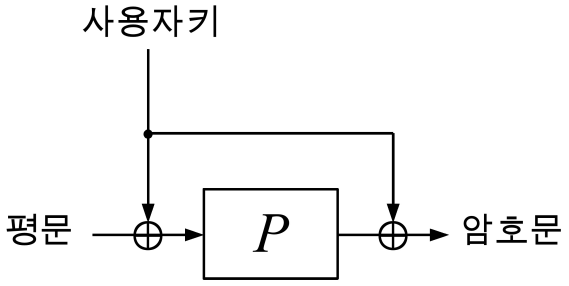

그림 1. 블록암호 E

ASCII 코드표를 통해 1바이트의 문자 또는 숫자를 8비트로 변환하는 함수를 $asc(\ )$라 하자. 또한 5바이트(40비트)의 사용자 $ID = ID[0] \| ID[1] \| ID[2] \| ID[3] \| ID[4]$에 대하여,

$$ASC(ID) = asc(ID[0]) \| asc(ID[1]) \| asc(ID[2]) \| asc(ID[3]) \| asc(ID[4])$$

라 하자. 단, ID가 5개의 문자 또는 숫자를 모두 사용하지 않는 경우, ID 앞에 모자란 개수만큼 null 문자를 붙이자. 또한 모든 16진수는 빅엔디언으로 저장한다. 예를 들어, $ASC(a2) = 0x0000006132$ 이다.

한편, 40비트 이진수열 $B = B[0] \| \cdots \| B[39]$ ($i = 0, \cdots, 39$ 에 대하여 $B[i] \in \{0,1\}$)를 입력으로 받아 이를 39차 이진 다항식으로 변환하는 함수 $poly$는 다음과 같이 정의된다.

$$poly(B) = \sum_{i=0}^{39} B[i] x^{39-i}.$$

예를 들어, $poly(0x0000000043) = x^6 + x + 1$ 이다.

이제 40 비트 마스터 키 K_{master}와 5바이트 사용자 ID에 대하여, 40비트 사용자 키 K_{ID}는 다음과 같은 관계가 성립되도록 정의된다; 이진 다항식

$$f(x) = x^{40} + x^{23} + x^{21} + x^{18} + x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^5 + x^3 + x^1 + 1$$

에 대하여,

$$poly(K_{master}) \bullet poly(ASC(ID)) = poly(K_{ID}) \pmod{f(x)}.$$

예를 들어, $K_{master} = 0x0000001234$, 사용자 $ID = Crypt$ 에 대해 $K_{ID} = 0x9519f123b4$이다.

블록암호 E 내부에 사용되는 40비트 치환함수 P는 5-라운드 Feistel 구조로서 다음과 같이 정의된다.

표기:

i) 양의 정수 m과 1비트 $\delta \in \{0,1\}$에 대하여, δ^m 은 m개의 δ로 이루어진 비트열이다.

ii) A가 n비트 비트열이고, $m < n$일 때, $A|_m$은 A의 처음 m비트로 구성된 비트열이다.

예를 들어, $A = 0^m \| 1^{n-m}$에 대하여, $A|_m = 0^m$.

iii) 십진법으로 나타낸 수 X에 대해 $X_{(2)}$는 이를 2진법으로 치환한 비트열이다.

이제 40비트 입력값 X에 대하여 $P(X)$는 다음과 같이 계산된다.

1) 입력값 X를 20비트 블록 $L[0]$, $R[0]$의 연접으로 분해한다. 즉, $X = L[0] \| R[0]$으로 표현한다.

2) 라운드 $i = 1, \cdots, 5$에 대하여,

$$1 \le i \le 2 \text{ 일 때, } k_i = 0^{127} \| (i-1)_{(2)}$$

$$3 \le i \le 4 \text{ 일 때, } k_i = 0^{126} \| (i-1)_{(2)}$$

$$i = 5 \text{ 일 때, } k_i = 0^{125} \| 100$$

$$L[i] = R[i-1],$$
$$R[i] = L[i-1] \oplus \mathrm{AES}_{k_i}(R[i-1] \| 0^{108})|_{20}$$

을 계산한다.

3) $P(X) = L[5] \| R[5]$로 정의된다.

공격자는 이 블록암호를 사용하는 32명의 사용자에 대하여 각 2^{16}개의 평문-암호문 쌍을 첨부파일과 같이 수집하였다. 이 정보를 이용하여 16진법으로 표현한 마스터 키를 구하여라.

첨부파일:

XXX_plaintext.txt : *ID*가 XXX인 사용자의 평문쌍. 각 평문은 모두 40비트 비트열.
XXX_ciphertext.txt : *ID*가 XXX인 사용자의 암호문쌍. 각 암호문은 모두 40비트 비트열이며, XXX_plaintext.txt의 같은 위치에 있는 평문을 암호화한 결과이다.