2019 국가암호공모전 Ⅱ 분야 답안 제출 양식

소속 : 서울시립대학교 대표자 이름 : 방수민

문제 02

답) 0xbaba156dda

문제 분석 :

어떤 사용자 1, 2에 대하여 각각의 아이디를 ID_1, ID_2라 하자. 그리고 각자의 어떠한 평문을 U_1, U_2라 하자.

만약 $U_1 \oplus K_{ID_1} = U_2 \oplus K_{ID_2}$ 이면 $P(U_1 \oplus K_{ID_1}) = P(U_2 \oplus K_{ID_2})$일 것이다. 주어진 암호화 방식은 $E_{K_{ID}}(U) = P(U \oplus K_{ID}) \oplus K_{ID}$ 이므로 $E_{K_{ID}}(U) \oplus K_{ID} = P(U \oplus K_{ID})$ 이다. 따라서 두 사용자 1, 2에 대해

$$E_{K_{ID_1}}(U_1) \oplus K_{ID_1} = P(U_1 \oplus K_{ID_1}),\ E_{K_{ID_2}}(U_2) \oplus K_{ID_2} = P(U_2 \oplus K_{ID_2})$$

이다.

$P(U_1 \oplus K_{ID_1}) = P(U_2 \oplus K_{ID_2})$이므로 $E_{K_{ID_1}}(U_1) \oplus K_{ID_1} = E_{K_{ID_2}}(U_2) \oplus K_{ID_2}$ 이고, $E_{K_{ID_1}}(U_1) \oplus E_{K_{ID_2}}(U_2) = K_{ID_1} \oplus K_{ID_2}$ 이다. 또, $U_1 \oplus K_{ID_1} = U_2 \oplus K_{ID_2}$이므로 $U_1 \oplus U_2 = K_{ID_1} \oplus K_{ID_2}$이다.

따라서 $U_1 \oplus U_2 = E_{K_{ID_1}}(U_1) \oplus E_{K_{ID_2}}(U_2) = K_{ID_1} \oplus K_{ID_2}$($U_1 \oplus U_2 = K_{ID_1} \oplus K_{ID_2}$)이다.

두 식 $poly(K_{master}) \cdot poly(ASC(ID_1)) = poly(K_{ID_1}) \pmod{f(x)}$

$poly(K_{master}) \cdot poly(ASC(ID_2)) = poly(K_{ID_2}) \pmod{f(x)}$

을 더하면,

$$poly(K_{master}) \cdot (poly(ASC(ID_1)) + poly(ASC(ID_2))) = poly(K_{ID_1}) + poly(K_{ID_2}) \pmod{f(x)}$$

이고

$$poly(K_{ID_1}) + poly(K_{ID_2}) = poly(K_{ID_1} \oplus K_{ID_2})$$

$$poly(ASC(ID_1)) + poly(ASC(ID_2)) = poly(ASC(ID_1) \oplus ASC(ID_2))$$

이므로

$$poly(K_{master}) = poly(K_{ID_1} \oplus K_{ID_2}) \cdot poly(ASC(ID_1) \oplus ASC(ID_2))^{-1} \pmod{f(x)}.$$

따라서 $K_{ID_1} \oplus K_{ID_2}$을 알면 K_{master}을 구할 수 있다.

풀이 :

$ID_1 = charl, ID_2 = GO$ 에서 $U_1 \oplus U_2 = E_{K_{ID_1}}(U_1) \oplus E_{K_{ID_2}}(U_2)$을 만족하는

$$U_1 = 0\text{x}51462bdbbe,\ E_{K_{ID_1}}(U_1) = 0\text{x}c59aced47d$$
$$U_2 = 0\text{x}a7d618494e,\ E_{K_{ID_2}}(U_2) = 0\text{x}330afd468d$$

을 얻을 수 있었다.

$U_1 \oplus U_2 = E_{K_{ID_1}}(U_1) \oplus E_{K_{ID_2}}(U_2) = K_{ID_1} \oplus K_{ID_2}$를 이용하여

$poly(K_{master}) = poly(K_{ID_1} \oplus K_{ID_2}) \bullet poly(ASC(ID_1) \oplus ASC(ID_2))^{-1} (\text{mod } f(x))$을 계산하였고, 그 결과 $K_{master} = 0\text{x}baba156dda$ 를 얻었다.