2019 국가암호공모전 Ⅱ 분야 답안 제출 양식

소속 : 서울시립대학교 **대표자 이름 : 방수민**

문제 01

답) Take the metal disc from Roswell

개요 :

1. DSA 문제 분석

입수한 메시지들을 순서대로 M_1, M_2, M_3, M_4, M_5라 하자.

각 $M_i (i = 1,2,3,4,5)$에 대한 난수를 r_i라하고 서명을 각각 $S_{i,1}, S_{i,2}$라 하자.

d는 개인키, h는 해시함수(SHA 256)라고 하자.

이때, $S_{i,1} = (g^{r_1} \pmod p) \pmod q, S_{i,2} = (h(M_i) + dS_{i,1}) r_i^{-1} \pmod q$이다.

2. Hint 발견하기

문제에서 $S_{1,1} = S_{4,1}$이므로 $r_1 = r_4$이다. 또한, $S_{1,2} = S_{2,2} = S_{3,2} = S_{5,2}$이다.

풀이 :

통신자들은 전자서명의 은닉채널을 이용하여 중요한 정보를 전달하고 있다. 서명의 식들에서 $g, p, q, h(M_i), S_{i,1}, S_{i,2}$들은 모두 알려져 있다. 알려지지 않은 것들은 d, r_i이다. 통신자들은 d를 알고 있을 것이므로 r_i를 통해 중요한 정보를 전달하고 있을 것이다.

$$S_{1,2} = (h(M_1) + dS_{1,1}) r_1^{-1} \pmod q \Rightarrow r_1 = (h(M_1) + dS_{1,1}) S_{1,2}^{-1} \pmod q$$
$$S_{4,2} = (h(M_4) + dS_{4,1}) r_4^{-1} \pmod q \Rightarrow r_4 = (h(M_4) + dS_{4,1}) S_{4,2}^{-1} \pmod q$$

이다. 또, $S_{1,1} = S_{4,1}$이고 $r_1 = r_4$이므로

$$\begin{aligned}
&(h(M_1) + dS_{1,1}) S_{1,2}^{-1} = (h(M_4) + dS_{1,1}) S_{4,2}^{-1} \pmod q \\
\Rightarrow\ &(h(M_1) + dS_{1,1}) S_{4,2} = (h(M_4) + dS_{1,1}) S_{1,2} \pmod q \\
\Rightarrow\ &h(M_1) S_{4,2} + dS_{1,1} S_{4,2} = h(M_4) S_{1,2} + dS_{1,1} S_{1,2} \pmod q \\
\Rightarrow\ &dS_{1,1}(S_{4,2} - S_{1,2}) = h(M_4) S_{1,2} - h(M_1) S_{4,2} \pmod q \\
\Rightarrow\ &d = (h(M_4) S_{1,2} - h(M_1) S_{4,2})(S_{1,1}(S_{4,2} - S_{1,2}))^{-1} \pmod q
\end{aligned}$$

이다. 따라서 d를 알 수 있다.

그리고 $r_i = (h(M_i) + dS_{i,1}) S_{i,2}^{-1} \pmod q$ 이므로 r_i들도 모두 알아낼 수 있다.

$S_{i,1} = (g^{r_1} \pmod p) \pmod q$를 통해 구한 r_i들이 맞는지 검산하였고, r_i들을 모두 분석하여 아스키코드로 변환한 결과 $r_1 = r_4$에 메시지가 담겨있었다. (r_2, r_3, r_5는 $S_{1,2} = S_{2,2} = S_{3,2} = S_{5,2}$를 만들어주기 위한 역할을 했다는 것을 이미 hint에서 예측할 수 있었다.)

r_1을 아스키코드로 변환하면 Take the metal disc from Roswell 이다.

이 숨겨진 정보는 1947년 7월 미국 뉴멕시코주 로즈웰에서 발생한 로즈웰 사건과 관련이 있다.