2019 암호경진대회 : 3번 문제 답안

답) 개인키 : 0xe7c75894035786766d704d1dd9e9136297f7d26c97d4be078bd1c4fd1feabc15

개요 :

1. ECDSA 문제 분석

   $G=(G_x,G_y)$, 개인키를 d라 하고, $Q=dG$에 대해 Q의 x좌표를 Public Key라 하자.

   주어진 ECDSA 파라미터 하에서 두 개의 메시지에 대응하는 ECDSA 서명 쌍이 문제에 주어졌으므로, 우선 두 개의 메시지를 m_1, m_2라고 하자.

   그리고 문제에서 주어진 m_1, m_2에 대한 각각의 hash 값을 h_1, h_2라 하자. (문제에서 주어져있음)

   난수 k_1을 뽑아 점 k_1G의 x좌표 $x(k_1G)$에 대해 $r_1=x(k_1G)\pmod n$라 하면,

   $s_1=k_1^{-1}(h_1+dr_1)\pmod n$를 계산한다. 문제에서 주어진 Signature1은 (r_1,s_1)이다.

   난수 k_2을 뽑아 점 k_2G의 x좌표 $x(k_2G)$에 대해 $r_2=x(k_2G)\pmod n$라 하면,

   $s_2=k_2^{-1}(h_2+dr_2)\pmod n$를 계산한다. 문제에서 주어진 Signature2는 (r_2,s_2)이다.

2. Hint 발견하기

   문제에서 Signature1과 Signature2를 보면 r_1, r_2가 같다. $r=r_1=r_2$라 하자.

   $r_1=x(k_1G)\pmod n$, $r_2=x(k_2G)\pmod n$이고 $r_1=r_2$이므로 $k_1=k_2\pmod n$ 또는 $k_1=-k_2\pmod n$이다.

풀이 :

1. **$k_1=k_2\pmod n$인 경우**

   $k=k_1=k_2\pmod n$라 하자.

   $$s_1=k^{-1}(h_1+dr)\pmod n \;\Rightarrow\; k=s_1^{-1}(h_1+dr)\pmod n$$
   $$s_2=k^{-1}(h_2+dr)\pmod n \;\Rightarrow\; k=s_2^{-1}(h_2+dr)\pmod n$$

   이므로

   $$s_1^{-1}(h_1+dr)=s_2^{-1}(h_2+dr)\pmod n$$

   이고

   $$s_2h_1+s_2dr=s_1h_2+s_1dr\pmod n$$
   $$\Rightarrow\; (s_2-s_1)dr=s_1h_2-s_2h_1\pmod n$$
   $$\Rightarrow\; d=(s_1h_2-s_2h_1)((s_2-s_1)r)^{-1}\pmod n$$

   이다. 따라서 마지막 식을 계산하면

   $$d=0xe7c75894035786766d704d1dd9e9136297f7d26c97d4be078bd1c4fd1feabc15$$

   이다. 이 때, dG를 계산하여 문제에서 주어진 public key와 비교함으로써 같다는 것을 검산하였다.

2. $k_1 = -k_2 \pmod n$인 경우

$$s_1 = k_1^{-1}(h_1 + dr) \pmod n \;\Rightarrow\; k_1 = s_1^{-1}(h_1 + dr) \pmod n$$
$$s_2 = k_2^{-1}(h_2 + dr) \pmod n \;\Rightarrow\; k_2 = s_2^{-1}(h_2 + dr) \pmod n$$

이고,

$$k_1 = -k_2 \pmod n$$

이므로 다음 식을 도출할 수 있다.

$$s_1^{-1}(h_1 + dr) = -s_2^{-1}(h_2 + dr) \pmod n$$

이 식을 풀면,

$$s_2 h_1 + s_2 dr = -s_1 h_2 - s_1 dr \pmod n$$
$$\Rightarrow (s_1 + s_2)dr = -s_1 h_2 - s_2 h_1 \pmod n$$
$$\Rightarrow d = -(s_1 h_2 + s_2 h_1)((s_1 + s_2)r)^{-1} \pmod n$$

이 되고 이것을 계산하면,

$$d = 0x943e2873e9ede3bb639a7a79b88b1172330ec73be6cd3e5f0710926aa8aba2b0$$

이다. 이 때, dG를 계산해봄으로써 $Q \neq dG$임을 검산하였다.

3. 결과

$$d_1 = 0xe7c75894035786766d704d1dd9e9136297f7d26c97d4be078bd1c4fd1feabc15,$$
$$d_2 = -d_1 \pmod n = 0x1838a76afca8798a928fb2e22616ec9d24ef28410f42e07d67e805c5dc78693c$$

에 대해서도 d_2G를 계산하여 문제에서 주어진 public key와 비교함으로써 같다는 것을 검산하였다. 그리고

$$k_1 = s_1^{-1}(h_1 + d_1 r) \pmod n \;\Rightarrow\; s_1 = k_1^{-1}(h_1 + d_1 r) \pmod n$$
$$k_2 = s_2^{-1}(h_2 + d_1 r) \pmod n \;\Rightarrow\; s_2 = k_2^{-1}(h_2 + d_1 r) \pmod n$$

를 이용하여 문제에서 주어진 s_1, s_2와 비교해서 같다는 것을 검산하였고, 마찬가지로

$$k_1 = s_1^{-1}(h_1 + d_2 r) \pmod n \;\Rightarrow\; s_1 = k_1^{-1}(h_1 + d_2 r) \pmod n$$
$$k_2 = s_1^{-1}(h_1 + d_2 r) \pmod n \;\Rightarrow\; s_2 = k_2^{-1}(h_2 + d_2 r) \pmod n$$

에 대해서도 계산하여 s_1, s_2와 비교해서 같다는 것을 검산하였다.

d_1G의 y좌표는 홀수이고, d_2G의 y좌표는 짝수이다. Public Key는 03으로 시작하므로 dG의 y좌표는 홀수일 것이다.

따라서 비밀키는 $d = 0xe7c75894035786766d704d1dd9e9136297f7d26c97d4be078bd1c4fd1feabc15$ 이다.