2025 암호분석경진대회

5번 문제

Alice와 Bob은 서로 암호화된 메시지를 주고받기 위해 먼저 공유키를 생성하고자 하였다. 서로 안전한 채널을 통해 통신이 이루어지기 때문에 school-book ECDH (Elliptic curve Diffie-Hellman) 알고리즘을 사용하였다. 사용한 파라미터는 FIPS 186-2 에 명시된 P-521 파라미터이다. Alice와 Bob이 공유키를 생성하는 과정은 다음과 같다.

1) 먼저 Alice는 자신의 개인키로 연산한 결과를 Bob에게 전달한다. 아래는 Alice가 Bob에게 전달한 타원곡선 위의 점 (x,y)를 16진수로 나타낸 결과이다

x	0000000000000147 873c82bd6c0e4ec6 926f7bf0bd31e819	362b1ed07c17feff c15ebeee2062c10d	add963c398e7d337 3394260b8c964659	6eebd2bdfca7b92c b6a4c9e3d27c8fda
y	0000000000000121 2c4bfb3767f2db0e ace1eee5e7f0e2a4	e806baa3a46652ae c9f5a1b517a7b2cd	6caca563359403ad 2e8007939ac1284d	474715481970356c 01e8121b31b0af2e

2) Bob도 마찬가지로 자신의 개인키로 연산한 결과를 Alice에 전달한다. 아래는 Bob이 Alice에게 전달한 타원곡선 위의 점 (x,y)를 16진수로 나타낸 결과이다

x	000000000000014a 2460833eb1bdb8f9 b8f45d634b053022	3ad15b04eeef7042 1cb509a50da7f773	f1bc7c1c30b24388 5b81a9ef5aa95c8d	430db032ec6c009d 7a10b228a644d8bb
y	00000000000000ef f7c2531aef6c7d8c a9cd89ba403bf4c0	a32abda489cc48b1 cdb09f562c40096c	ff9b97fd3ede2b3a 6a36cea86e5477cf	382d12270cfe36de 24fa5a4b7a04f6ac

Bob은 통신 과정에서 암복호화가 안 되는 일을 방지하기 위해 서로 공유한 비밀키를 확인하자고 Alice에게 제안했다. Alice는 공유한 비밀키 $P_{shared}=(x,y)$의 x,y 좌표를 각각 66바이트가 되도록 0을 패딩하였다. Alice는 Bob에게 서명 확인을 통해 Alice 자신이 전달한 값이 맞도록 증명하도록 하기 위해 메시지를 16진수로 변환한 $x \mid\mid y$를 string으로 여겨 ECDSA로 전자서명하였다. 전자서명에 사용된 타원곡선 파라미터는 ECDH에 사용한 파라미터와 동일하다.

아래는 Alice가 Bob에게 전달한 메시지 m과 서명값이다. ECDSA에 사용한 해시 함수는 SHA-256이다.

m	0077e4b10dd38932457fd96eb1852129f09c1c0ed2973b09e1b8d8b8caf95da0bdcd99d744a0 e4f84734e3a1aed4562ed376b3689beedff67d0b42b415e743608a190156ece822bc48e444e8 e8435c8f7ba66da953c82e6629b3f7456566c5f61fb88b65a9d4cea62299bd1b3d7e652382b8 c1afcbe938a04abb57108116ffe83d172d0a			
$h(m)$	4dcbafbe63fdcdbe59ff00f8540fae3d01967713a9cb3248495398d21a96f807			
r	000000000000014e ee14349f8aaae764 73b9699c327dbbf4	a73daf911317794b da51066050faf6f4	0686862e1f35c7ee 7571df1797b6f076	cc79e2e3f152fe32 b06df0f31a670ade
s	0000000000000087 1f0acb7b8348332a 60a16e506a28570a	f6eab4762228518b d9a1d0b881d6e070	d8e7eefc0008638d c49998fc42ac29c5	14377fcc710ca02c 1e10e6372f6d08b7

[문제]

Alice의 개인키를 복원하시오.

[참고] : ECDH와 ECDSA에 사용한 타원곡선 파라미터 (p-521)

- p =0x1ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
- $E: y^2 = x^3 - 3x + b \in F_p$
- b =
  0x051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
- Gx =
  0xc6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
- Gy =
  0x11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
- n =0x1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffa51868783bf2f966b7fcc0148f709a5d03bb5c9b8899c47ae bb6fb71e91386409