2024 암호분석경진대회

4번 문제

ECDSA (Elliptic Curve Digital Signature Algorithm) 유한체에 정의된 타원곡선에서의 이산대수 문제를 푸는 어려움을 기반으로 둔 전자서명 알고리즘이다. 안전성에 기반이 되는 문제를 푸는데 하지수시간이 걸리는 FFC (Finite Field Cryptography)나 IFC (Integer Factorization Cryptography)에 비해 ECC (Elliptic Curve Cryptography) 기반 암호는 지수시간이 걸리기 때문에 같은 보안강도에서 더 작은 키와 서명 사이즈를 가져 IoT 장비의 인증이나 블록체인에도 많이 활용되고 있다. ECDSA의 키 생성, 서명생성, 서명 검증은 다음 과정을 통해 진행된다.

[Domain Parameters]

- 유한체 F_p를 정의하는 소수 p
- F_p에서 정의된 타원곡선 $E: y^2 = x^3 + ax + b$
- Generator $G \in E(F_p)$, $G = (Gx, Gy)$
- Group G의 order (위수) n
- Cofactor $h = \#E(F_p)/n$

[Key Generation]

- $[1, n-1]$ 범위에서 랜덤한 정수 d를 선택한다.
- 개인키 : d
- 공개키 : $Q = [d]G$

[Signature Generation]

* Input : 메시지 m, 개인키 d
* Output : 서명 (r, s)

- 암호학적 해시함수 h를 사용해서 메시지에 대한 해시값 $e = h(m)$을 연산한다.
- $[1, n-1]$범위에서 랜덤한 정수 k를 선택한다.
- $(x, y) = kG$를 연산한 뒤, $r = x \bmod n$ 을 연산한다. 만약 $r = 0$일 경우 k를 다시 선택한다.
- $s = k^{-1}(e + rd) \bmod n$을 연산한다. 만약 $s = 0$일 경우 k를 다시 선택한다

[Signature Verification]

* Input : 메시지 m, 서명 (r, s), 공개키 Q
* Output : Accept/Reject

- 서명값 r, s가 $1 \le r, s \le n-1$인지 확인한다.
- 암호학적 해시함수 h를 사용해서 메시지에 대한 해시값 $e = h(m)$을 연산한다.
- $u_1 = es^{-1} \bmod n$ $u_2 = rs^{-1} \bmod n$을 연산한다.
- $(x', y') = u_1 G + u_2 Q$를 연산한다.
- $r \equiv x' \bmod n$일 경우 accept, 아니면 reject한다.

철수는 영수로부터 다음 메시지에 대해서 ECDSA 전자서명으로 서명한 결과를 받았다. ECDSA에서 사용한 해시 함수는 SHA-256이다.

	값	
메시지	helloecdsa	
해시	0x568b4901cc2dac4a13af161bbf6b2087c94d8b8223755fd121ec6aa0519ecee2	
서명	r	0xda7866632109e77f0d3c5bdd49031e6d9a940fcb7d29ea2f858b991d1f17cef8
	s	0xa4a700ac4f18634ac845739e0342cd8335bf6e0606ca9dc9d668abf9ed812e6d
공개키	Qx	0xa51208adff894cdd79d4d7d967aa4d492256ba4d527661b10ae7cfd6e15f28a6
	Qy	0x6fbfd9a270cd717afb0949e1c40fd2754b46f4f8472ac5711de0351fe81bbd80

철수는 마침 자기도 서명할 메시지가 있어서 영수한테 프로그램을 달라고 요청하였고, 해당 프로그램을 활용하여 자신의 개인키와 메시지로 서명한 결과를 다음과 같이 얻게 되었다.

	값	
메시지	cryptoanalysiscontest	
해시	0x9a2e62818ad55aeb8ac319820b2d595660b9af57c0c7123bd6c6dfde2d9a1753	
서명	r	0xeb71f24ce44aa99d891bba7623414355e63bf92a74d753f7cbaab7831a357908
	s	0x8060d40bc3bf41f5d845e3ef6ae2270047a1e2a3e6c057bfc577d7d884089d47
개인키	0xbde07e98f0437a531c014a1fe6fd69c2cfb6c3657072696e7432303233383431	

철수는 영수의 전자서명 생성 프로그램이 문제가 있음을 확인하였고, 영수의 개인키를 복원할 수 있었다.

[문제]
영수의 개인키를 복원하시오.

[참고] : 영수 프로그램의 ECDSA 파라미터 (secp256k1)
- p =0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f
- $E: y^2 = x^3 + 7 \in F_p$
- Gx =0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
- Gy =0x483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
- n =0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141