2019 암호경진대회

3번 문제 : 디지털 서명

주어진 ECDSA 파라미터 하에서 두 개의 메시지에 대응하는 ECDSA 서명 쌍이 아래와 같이 주어졌다. 해당 ECDSA 공개키에 대응하는 개인키(서명키) 값을 찾으시오.

p	0xFFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF
a	-3
b	0x5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
Gx	0x6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
Gy	0x4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5
n	0xFFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

[표 1] ECDSA secp256r1 커브와 파라미터

ECDSA 커브의 파라미터는 다음을 나타냄: Finite Fields F_p 상에서 정의된 타원곡선 ($y^2 = x^3 + ax + b$) 에서 생성원(generator) G 포인트(x,y좌표: Gx,Gy)로 생성된 그룹의 차수(order)는 n이다.

Public Key:

03DC9213E6CDA06195098C901C36C0F20D9B5DECD252F5F00BFC5A63CAE0C5AEAC

{0X03, 0XDC, 0X92, 0X13, 0XE6, 0XCD, 0XA0, 0X61, 0X95, 0X09, 0X8C, 0X90, 0X1C, 0X36, 0XC0, 0XF2, 0X0D, 0X9B, 0X5D, 0XEC, 0XD2, 0X52, 0XF5, 0XF0, 0X0B, 0XFC, 0X5A, 0X63, 0XCA, 0XE0, 0XC5, 0XAE, 0XAC}

Signature1 (ECDSA with sha256):

E45054EB5B1ABD976650F7F395BF51D0D8DD193E0174E7A14A1C8C127FBDF2DB

09371E411284D26B4FAE3BD85B9545BBBFACE1FFE0868BD7701660A50C6E3F17

{ 0XE4 ,0X50 ,0X54 ,0XEB ,0X5B ,0X1A ,0XBD ,0X97 ,0X66 ,0X50 ,0XF7 ,0XF3 ,0X95 ,0XBF ,0X51 ,0XD0 ,0XD8 ,0XDD ,0X19 ,0X3E ,0X01 ,0X74 ,0XE7 ,0XA1 ,0X4A ,0X1C ,0X8C ,0X12 ,0X7F ,0XBD ,0XF2 ,0XDB ,0X09 ,0X37 ,0X1E ,0X41 ,0X12 ,0X84 ,0XD2 ,0X6B ,0X4F ,0XAE ,0X3B ,0XD8 ,0X5B ,0X95 ,0X45 ,0XBB ,0XBF ,0XAC ,0XE1 ,0XFF ,0XE0 ,0X86 ,0X8B ,0XD7 ,0X70 ,0X16 ,0X60 ,0XA5 ,0X0C ,0X6E ,0X3F ,0X17 }

Signature2 (ECDSA with sha256):

E45054EB5B1ABD976650F7F395BF51D0D8DD193E0174E7A14A1C8C127FBDF2DB

B84ABC62455C570D5500186D83BFD1E1C23CB3135D4A32CE19B3DB61F1680EDC

{ 0XE4 ,0X50 ,0X54 ,0XEB ,0X5B ,0X1A ,0XBD ,0X97 ,0X66 ,0X50 ,0XF7 ,0XF3 ,0X95 ,0XBF ,0X51 ,0XD0 ,0XD8 ,0XDD ,0X19 ,0X3E ,0X01 ,0X74 ,0XE7 ,0XA1 ,0X4A ,0X1C ,0X8C ,0X12 ,0X7F ,0XBD ,0XF2 ,0XDB ,0XB8 ,0X4A ,0XBC ,0X62 ,0X45 ,0X5C ,0X57 ,0X0D ,0X55 ,0X00 ,0X18 ,0X6D ,0X83 ,0XBF ,0XD1 ,0XE1 ,0XC2 ,0X3C ,0XB3 ,0X13 ,0X5D ,0X4A ,0X32 ,0XCE ,0X19 ,0XB3 ,0XDB ,0X61 ,0XF1 ,0X68 ,0X0E ,0XDC }

※

Signature1에서 서명한 message hash 값(sha256("ECDSA")):

{0X38 ,0X9F ,0XA4 ,0X50 ,0X7C ,0XD5 ,0X36 ,0XC6 ,0X7D ,0XB3 ,0X5B ,0X80 ,0XB0 ,0X6A ,0XB0 ,0XB0 ,0XB0 ,0X34 ,0XB7 ,0XA5 ,0XC6 ,0X7C ,0XF9 ,0XA2 ,0XD0 ,0X6E ,0XD0 ,0X08 ,0X76 ,0XD5 ,0X68 ,0XF9};

Signature2에서 서명한 message hash 값(sha256("signature")):

{0X1A ,0X2F ,0XC2 ,0X6D ,0XC7 ,0XEA ,0X5A ,0X2A ,0X47 ,0X48 ,0XB7 ,0XCB ,0X2B ,0X1E ,0XF1 ,0X93 ,0XD9 ,0X6A ,0XB2 ,0XC9 ,0X9F ,0X93 ,0X09 ,0X2F ,0X69 ,0XE6 ,0X30 ,0X75 ,0XB2 ,0X8D ,0X12 ,0X78};

참고사항: 문제 생성시 사용한 ECDSA library - https://github.com/esxgx/easy-ecc