IIC3272 — Criptomonedas y contratos inteligentes

Tarea 2: Serialización y direcciones de Bitcoin

Entrega: Mayo 16, 2020

1. Cosas administrativas

Cada tarea en este curso equivale a 5 % de la nota final. En total tendremos 5 tareas, pero la peor tarea que solucionan no cuenta para la nota final. Quiere decir que pueden botar una tarea.

En esta tarea se les pide implementar ciertos métodos en las clases implementadas durante la actividad sobre las curvas elípticas, y después ejecutar una secuencia de comandos que imprime ciertos resultados. La salida de los comandos será su entrega.

Deben enviar la solución a los siguiente correos (**a los dos al mismo tiempo por favor**):

- dvrgoc@ing.puc.cl
- rrrodriguez@uc.cl

El uso de materiales (o soluciones) encontrados en Internet está permitido. Solo se les pide citar la fuente que utilizaron. No se aplica ninguna penalidad para su uso. Si entienden como usar una billetera electrónica comercial para resolver la tarea tampoco se aplica una penalidad.

2. La tarea

En esta tarea vamos a extender nuestra implementación de elementos de criptografía de curva elíptica, para poder transmitir llaves públicas en el formato SEC, transmitir las firmas en el formato DER, y generar direcciones de Bitcoin.

El código desarrollado durante las clases nos permite definir los elementos del campo finito utilizado en Bitcoin, definir puntos de la curva elíptica secp256k1, y firmar/verificar mensajes utilizando esta curva elíptica. En esta tarea recibirán el código extendido con algunas funciones como el hash160 que nos ayuda en calcular direcciones de Bitcoin, o transformación de una secuencia de bytes a base 58.

Objetivo de la tarea es extender tres de las clases definidas en el código de siguiente manera:

- En la clase `S256Point` (acuérdense que una llave pública es simplemente un punto de esta curva) tienen que implementar el método:

  `def sec(self, compressed=True)`

  que produce serialización SEC del punto con cual estamos trabajando. El parámetro `compressed` nos dice si vamos aplicar el formato comprimido o descomprimido de SEC. El objeto que devuelve el método debe ser en formato bytes.

- En la clase `Signature` deberán implementar el método:

  `def der(self)`

  que devuelve el formato DER de la firma, en formato bytes.

- Volviendo a la clase `S256Point`, se les pide generar llaves de Bitcoin correspondiente a la llave pública con cual estamos trabajando. Para esto, deberían implementar el método:

  `def address(self, compressed=True, testnet=False)`

  que genera la dirección de Bitcoin basada en la llave pública con cual estamos trabajando (i.e. el objeto `S256Point`).

  El parámetro `compressed` nos dice si vamos a generar la dirección desde el formato SEC comprimido, o desde el formato SEC no comprimido. Para convertir el punto de la curva al formato deseado, deben utilizar el método `sec(...)` implementado en el ejercicio 1 arriba.

  El parámetro `testnet` nos dice si vamos a generar una dirección de mainnet o del testnet de Bitcoin. Como un sanity check, cuando generan una dirección de mainnet, dicha debería empezar con un 1, y una dirección de testntet con n o m. Más sobre los prefijos pueden leer en `https://en.bitcoin.it/wiki/List_of_address_prefixes`.

Para evaluar su trabajo, esta vez no les pedimos entregar el código, sino la salida de su programa cuando se ejecutan los siguientes comandos (en la secuencia especificada abajo):

1. **SEC [3 puntos]**.

```
# Generating my private key:
secret = hash256(b'IIC3272Sucks')
intSecret = int(secret.hex(),16)

privKey = PrivateKey(intSecret)

# Displaying the public key in the two SEC formats:
print('Uncompressed SEC format: ',privKey.point.sec(False).hex())

print('Compressed SEC format: ',privKey.point.sec(True).hex())
```

2. **DER** [**1 punto**].

```
# Signing a message:
message = hash256(b'This course is boring!')
z = int(message.hex(),16)

signature = privKey.sign(z)


# What is the signature: raw vs DER
print('Raw signature: ',signature)

print('DER signature: ',signature.der().hex())
```

3. **Direcciones** [**3 puntos**].

```
# Bitcoin address assuming compressed SEC format for the public key
testnet = privKey.point.address(compressed = True, testnet = True)
mainnet = privKey.point.address(compressed = True, testnet = False)

print('Testnet address: ',testnet)
print('Mainnet address: ',mainnet)
```

Para no complicar las cosas demasiado, el código que se les entregará con esta tarea tendrá estos comandos listos para ejecutar.

Bonus 1. [**2% de la nota final**] Utilizando la dirección de testnet generada con el código arriba, consigan alguna denominación de testcoins en un faucet de testnet de Bitcoin. Una buena alternativa para esto es: `https://bitcoinfaucet.uo1.net/send.php`. Para confirmar esto pueden ingresar a un block explorer como por ejemplo `https://live.blockcypher.com/`, seleccionar la opción de BTC Testnet, y buscar la dirección generada en la pregunta 3. Allá debería aparecer la transacción que manda los testcoins a la dirección especificada. Si no entienden de que se trata esta pregunta tomen en cuenta que es una pregunta bonus, y solo sirve para conseguir extra puntos.

Bonus 2. [**Sentimiento de satisfacción**] Usando los métodos arriba y los links de la pregunta bonus ahora pueden generar sus propias direcciones de Bitcoin y conseguir testcoins. Felicitaciones!