

## تمرین کامپیوتری اول

طنین زراعتی

۸۱۰۱۹۷۶۲۷

قسمت اول: تولید آدرس

### سوال ۱)

برای این بخش و تولید آدرس و کلید متناظر باید از Elliptic Curve را برای الگوریتم امضای دیجیتال استفاده کنیم. برای درست کردن private key که یک عدد ۲۵۶ بیتی است نیاز به عدد رندوم داریم که از کتابخانه secrets استفاده میکنیم. سپس کلید را به فرمت WIF تبدیل میکنیم.

```
def converPrivateKeyToWIF(private_key, compressed = False):
    extended = b"\xef" + private_key
    if(compressed):
        extended = extended + b"\x01"
    checksum = calculate_checksum(extended)
    WIF_private_key_not_encoded = extended + checksum
    return base58.b58encode(WIF_private_key_not_encoded)
```

همانطور که در کد قابل مشاهده است: ابتدا باید کلید را به "0xef" چپ گسترش دهیم (extend). در صورتی که بخواهیم compress کنیم باید بعد گسترش اولیه انرا به "0x01" راست نیز extend کنیم. چک سام را پیدا کرده (دوبار sha256 گرفته و ۴ بایت اول را گرفته و به چپ "0x01" گسترش میدهیم. در آخر جواب بدست آمده از این مراحل را با encode،base58 میکنیم تا جواب بدست آمده به فرمت WIF باشد).

```
def generateAddress(private_key):
    generating_point = Point.get_generator_point()
    integer_private_key = int.from_bytes(private_key, "big")
    public_key = (generating_point * integer_private_key).to_bytes()
    hashed_value = RipeMD160(Sha256(public_key))
    extended_address = b"\x6f" + hashed_value
    checksummed_address = extended_address + calculate_checksum(extended_address)
    return public_key, base58.b58encode(checksummed_address)
```

برای استفاده از elliptical curve از فایل ElypticalCurve.py استفاده میکنیم. میتوانستیم از ecdsa که کتابخانه آماده بود استفاده کنیم اما چون گفته شده بود مراحل به صورت دستی پیاده سازی شود آن تیکه نیز به طور جداگانه پیاده سازی شد.

در آخر sha256 گرفته و از RipeMD160 هش کلید عمومی را بدست می آوریم.

```
def Sha256(unhashed_data):
    digester = hash.new("sha256")
    digester.update(unhashed_data)
    return digester.digest()

def RipeMD160(unhashed_data):
    digester = hash.new("ripemd160")
    digester.update(unhashed_data)
    return digester.digest()

def calculate_checksum(key):
    hashed_data = Sha256(Sha256(key))
    return hashed_data[:4]
```

خروجی بدست آمده به شکل زیر است:

```
cryptoeval) tanin@DESKTOP-KVBQAK9:/mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 GenerateAddress.py
'929jTRQR2MHGz1hWuBX1oV1subFQ4JGb9GQwYSwsadXpvW4tdSm'
'mwiKubWRCAHVcuwBFvHKL9Hgu6M42eXLn2'
cryptoeval) tanin@DESKTOP-KVBQAK9:/mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$
```

برای تولید آدرس در شبکه از این کلید عمومی به ترتیب sha256, ripemd160 گرفته میشود و سپس به ابتدای عبارت حاصل 6f اضافه میشود که نشان دهنده آن است که این آدرس در شبکه ی testnet است و اگر میخواستیم آدرس در شبکه ی mainnet تولید کنیم باید به جای عبارت گفته شده 00 را اضافه میکردیم. در نهایت از حاصل checksum را محاسبه میکنیم و به انتهای آن اضافه میکنیم. آدرس نهایی عبارت حاصل به صورت base58 خواهد بود. در mainnet هش کلید عمومی به "0x80" به چپ گسترش پیدا میکند. (extend) اما در testnet هش کلید عمومی "0x6f" به چپ گسترش میابد .

## سوال ۲)

در این قسمت با استفاده از کد قسمت قبل و یک while تعدادی کلید تولید میکنیم تا شرایط مدنظر ما را داشته باشد.

```
produced_private_key, produced_address = generateAddress.produce_keys()
while produced_address[1:(len(first_bytes) + 1)] != first_bytes:
    produced_private_key, produced_address = generateAddress.produce_keys()
return produced_private_key, produced_address
```

با توجه به کد بالا، تلاش برای تولید آدرسی میکنیم که کاراکتر دوم تا چهارم آن شرایط مورد نظر ما را داشته باشد.

```
tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateVanityAddress.py
Enter the First Three Char:
h
93CmhZAVGtpL8yVcq3Z41RCBySguUvzfr9q8mHvU73ef4zGCjwD
mhobh9qJfKNGAFRjNtW1vpk7nhRkcxY2ha
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$
```

```
tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateVanityAddress.py
Enter the First Three Char:
mz
93KC938jc4ziDkatnwtHA6khybV6KimunwLFajtGAbxoiQ6x8V
mmzHhuwzUImoZTtLAeclPaqV7XSkTvcEKf
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$
```

```
tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateVanityAddress.py
Enter the First Three Char:
mnk
92KJ7b78Z5gUuc8uYEenBRrjwKsH28s82hUoqK3v3fPbTYudF2Z
mmnkHUYRGKpE2KbJ9ukJQZoyk3rCuJpAU3
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$
```

## قسمت دوم: انجام تراکنش

برای هر بخش کد مربوطه با عنوان Q2P مشخص شده است یک فایل هم برای خرج کردن تراکنش با همان عنوان و با 2\_ مشخص شده. همچنین به فایل `utils.py` هم چند تابع اضافه کرده ام. برای هر بخش هم از فایل `transaction.py` که قرار داده شده بود با کمی تغییر استفاده کرده ام.

### سوال (۱)

با استفاده از کد بخش قبل کلید و آدرس ایجاد میکنیم:

آدرس:

```
mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp
```

کلید به فرمت WIF:

```
92hM9Lk9Q1S8xVjvNiso94FmBijW2phRA8EB25ewzEiMhGjUm1x
```

هش tx:

```
7f8ab79cffd80b71bc11f65831ab55ec83f61d36b2dc15075e7d489a345cdc31
```

و با استفاده از فاست های داده شده پولی را دریافت کرده و به ادرس ساخته شده منتقل میکنیم و حال میخواهیم باتوجه به شرایط گفته شده در صورت سوال آن را خرج کنیم.


Current wallet balance is ₪ 364.068. You can get up to ₪ 0.00041.

Linode - \$100 Free Credit For New Account For 60 Days

0.0001 coins sent to mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp

₪ mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp 0.0001 [Send testnet bitcoins](#)

**BTC Address**  
Send coins back, when you don't need them anymore: tb1q7w62ek9ucw4qj5lgw4i028hmux80undrntxt



**Last Transactions**

7f8ab79cfdd8b71bc11f65831ab55ec83fe1d36b2dc15075e7d489a345cdc31	Sat, 18 Jun 2022 11:57:05
mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp	-0.0001
pending	0.00000145 fee
9a0c3010bd709c2ef94bb5bfb28bdae7c8d88005f27fa937e2a7d5780c3be0	Sat, 18 Jun 2022 11:51:10

برای خروجی اول ترنزاکشن که باید توسط همه قابل خرج باشد از OP\_CHECKSIG استفاده میکنیم که هرکسی بتواند یک signature اعمال کند و از آن استفاده کند. برای خروجی دیگر که نباید توسط کسی قابل خرج باشد از OP\_RETURN استفاده میکنیم که همواره سر استک را برمیگرداند و هیچکس نمیتواند signature را روی آن اعمال کند.

برای بازگرداندن پول به حساب خود در مرحله ای که همه میتوانند پول را خرج کنند کافی است signature خود را روی آن اعمال کنیم.

```
(cryptoevo) tanin@DESKTOP-KVBIQAK9:/mnt/d/term 8/CryptoCurrency/LA/1/CryptoCurrency$ python3 generateAddress.py
b'92pWOLkQ15Bv4jyWiso94Fe8ijNzphRABEB25ewzE3PhGjUe1x'
b'mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp'
(cryptoevo) tanin@DESKTOP-KVBIQAK9:/mnt/d/term 8/CryptoCurrency/LA/1/CryptoCurrency$ python3 transactionQ1P1.py
mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp
047faacb492fe12699c209c0a9eb71fddb53b23a76431bd821135131250c7f71fd451be8f968baee3694e2322ff7a292b184ba6e5b6aebf5295cf2f4ba7411f859
924c3d0027958eac2953448b65a8ee768b63912137929a7476c04bf848d41e
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "0a3d7911a92c615c728d6cb804621cae001f190fc254a22e15f6c2a033bb9d4",
    "addresses": [
      "mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp"
    ],
    "total": 9000,
    "fees": 1000,
    "size": 209,
    "vsize": 209,
    "preference": "low",
    "relayed_by": "80.82.77.206",
    "received": "2022-06-18T11:57:27.240Z82457Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 2,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "7f8ab79cfdd8b71bc11f65831ab55ec83fe1d36b2dc15075e7d489a345cdc31",
        "output_index": 0,
        "script": "4730848e22100c7f78540d4f013c8c092f41f677aacaf624f636e2467aa99290c373b8184fdb3021f53c2777b8b6aeb384bb41c909e9de20c20aef93088e6dae44f8cdbc32490070141047faacb492fe12699c209c0a9eb71fddb53b23a76431bd821135131250c7f71fd451be8f968baee3694e2322ff7a292b184ba6e5b6aebf5295cf2f4ba7411f859",
        "output_value": 10000,
        "sequence": 4294967295,
        "addresses": [
          "mwxACSvznZKiCPymBuUCMyzhsMZ3ZMMetp"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 1000,
        "script": "6a",
        "addresses": null,
        "script_type": "null-data"
      }
    ]
  }
}
```

```

tamin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency
{"tx": {
  "block_height": -1,
  "block_index": -1,
  "hash": "6a3d7911a92c615c728d6cb804621ca0e001f190fc254a22e15f6c2a033bb9d4",
  "addresses": [
    "mo0K5vznZK1CPyBuUjChzshM23Z9Wetp"
  ],
  "total": 9000,
  "fees": 1000,
  "size": 209,
  "vsize": 209,
  "preference": "low",
  "relayed_by": "80.82.77.206",
  "received": "2022-06-18T11:57:27.240Z82457Z",
  "ver": 1,
  "double_spend": false,
  "vin_sz": 1,
  "vout_sz": 2,
  "confirmations": 0,
  "inputs": [
    {
      "prev_hash": "7f8ab79cffd88b71bc11f65831ab55ec83f61d36b2dc15075e7d489a345cdc31",
      "output_index": 0,
      "script": "473844022100e7f78549d4f013c8c092f41f677aaca6c24f636e2467aa99290c373b8384fdb3021f53c2777b8b6aeb384bb41c809e90e20e20aef93888e6dae44f8cdbc32490070141047faacb492fe12699e209c0a9eb71fddb53b23a76431bd821135131250c7f71fd451be8f968baee3694e2322ff7a292b184ba6e5b6aebf5295cf2f4ba7411f859",
      "output_value": 18000,
      "sequence": 4284967295,
      "addresses": [
        "mo0K5vznZK1CPyBuUjChzshM23Z9Wetp"
      ],
      "script_type": "pay-to-pubkey-hash",
      "age": 0
    }
  ],
  "outputs": [
    {
      "value": 1000,
      "script": "6a",
      "addresses": null,
      "script_type": "null-data"
    },
    {
      "value": 8000,
      "script": "ac",
      "addresses": null,
      "script_type": "unknown"
    }
  ]
}
}
(cryptoevo) tamin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$

```

و برای خرج کردن آن از فایل transactionQ1P2.py استفاده کرده و هشی که در اینجا بدست آمده را خرج میکنیم.

هش tx خرج شده :

**6a3d7911a92c615c728d6cb804621ca0e001f190fc254a22e15f6c2a033bb9d4**

پس از انجام transaction هم در این قسمت هم قسمت های بعدی باید مدتی صبر کنیم تا confirm شود. در این سوال چون پول کمی برای miner ها در نظر گرفته شده مدت زمان زیادی طول کشید.

و در نهایت خروجی تایید شده :

blockchain.com

WalletExchangeExplorer

Buy BitcoinTrade

b446591638e10b5a80f53079fdb467d419f329fa

OP\_EQUALVERIFY

OP\_CHECKSIG

Sigscript

3044022100e7f78549d4f013c8c092f41f677aaca6c24f636e2467aa99290c373b8384fdb3021f53c2777b8b6aeb384bb41c809e9de20e20aef93088e6dae44f8cd

bc324900701

047faacb492fe12699e209c0a9eb71fddb53b23a78431bd821135131250c7f71fd451be8f968baee3694e2322ff7a292b184ba8e5b6aebf5295cf2f4ba7411f859

Witness

Outputs

Index

0

Details

Unspent

Address

Value

0.00001000 BTC

Pkscript

OP\_RETURN

Index

1

Details

Spent

Address

Value

0.00008000 BTC

Pkscript

OP\_CHECKSIG

own cookies and third-party cookies on our websites to enhance your experience, analyze our traffic, and increase site security.

Manage preferences

Accept all

Explorer

Bitcoin Testnet

Transaction

USD

Search your transaction, an address or a block

Summary

USD

BTC

Fee

0.00001000 BTC  
(4.785 sat/B - 1.196 sat/WU - 209 bytes)

0.00009000 BTC

3 Confirmations

Hash

6a3d7911a92c615c728d6cb804621ca0e001f190fc254a22e15f6c2a...

2022-06-18 16:27

mwXACSvznZKiCPymBuUCMyzhsMZ3ZMMetp

0.00010000 BTC

OP\_RETURN

Unable to decode output address

0.00001000 BTC

This transaction was first broadcast to the Bitcoin network on June 18, 2022 at 4:27 PM GMT+4:30. The transaction currently has 3 confirmations on the network. At the time of this transaction, 0.00009000 BTC was sent with a value of \$1.73. The current value of this transaction is now \$1.73. Learn more about how transactions work.

Details

and third-party cookies on our websites to enhance your experience, analyze our traffic, and increase site security.

Manage preferences

Accept all

blockchain.com/btc-testnet/tx/6a3d7911a92c615c728d6cd04621ca0w00111908c254a2e15f6c2a033bb9d4

Wallet Exchange Explorer Buy Bitcoin Trade

Value when transacted \$1.73

### Inputs

HEX ASM

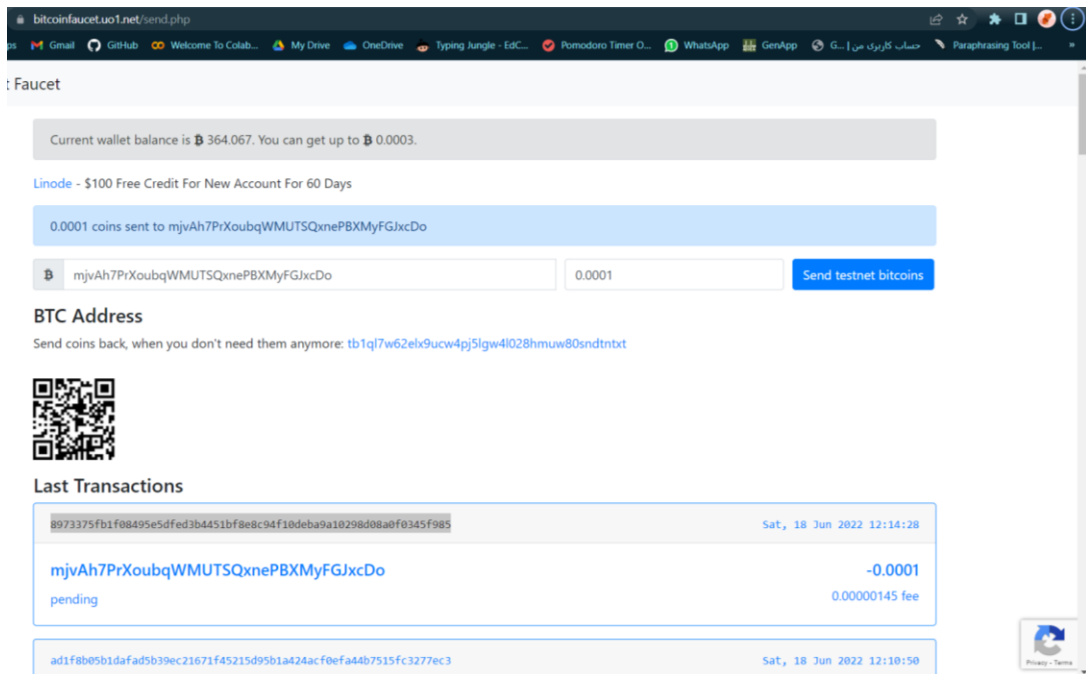
Index	Details	Output
0		
Address	mwXAC5vznKICPymBUJCMyzhSMZ3ZMMetp	Value 0.00010000 BTC
Pkscript	OP_DUP OP_HASH160 b446591638e10b5a80f53079fdb467d419f329fa OP_EQUALVERIFY OP_CHECKSIG	
Sigscript	3044022100e7f78549d4f013c8c0924f1f677aaca6c24f636e2467aa99290c373b8384fdb3021f53c2777b8b6aeb384bb41c809e9de20e20aef93088e5dae44f8cd bc324900701 047faacb492fe12699e209c0a9eb71fddb53b23a76431bd821135131250c7f71fd451be8f968baee3694e2322ff7a292b184ba6e5b6aebf5295cf2f4ba7411f859	
Witness		

### Outputs

Manage preferences Accept all

## سوال ۲)

در این سوال مجدد از سوال ۱ بخش ۱ استفاده کرده ام تا کلید و آدرس هارا ایجاد کنم و یک کوین با میزان مشخص برای آدرس زیر ارسال شد.



```
tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateAddress.py
b'91reHt5Tr814sehT3NKxcFZzgaU7prUNWPGq7UTfihw9wniek3'
b'mjbvAh7PrXoubqWMUTSQxnePBXMyFGJxcDo'
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateAddress.py
b'91yZ28eTGeLbqUJgRwSuF6pJf9eRFQJNdoZD2Lk3EPfeUZGJblbx'
b'mhmKwDnWYSF9BqUPz4Qk8o3KsLvUPWLLct'
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateAddress.py
b'9283Nd6PsC8sHTMi8awuEzZ4T9G7SxkYqRZXsTZLRDGP3wgGAV'
b'mocgUxwrpUsYURV5RwFBCGR7polWha69kG'
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 generateAddress.py
b'92BShYbCv4mSLEDmZrLLyY7xutPUzM5xme6Sjhy16Mmthw5wQFF'
b'n4QzeqTbYA7yuLJaocLKjLJp3wRjbeedwh'
(cryptoenv) tanin@DESKTOP-KVBQAK9: /mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$
```

کلید این درس:

91c2c2h9a2FyVSHCJh5MNF6dVH1ZzscePUzX556hSKhjLrQUUz4

کلید نفر اول:

91xjMw6VyHaD93QC751Kb8XZeor9Xi7rKLBdVaCtuhb9Wz56eg7

کلید نفر دوم:

92Pk448RcQDfhZEzP8xagBwcfMLtH5HZkmnVXgXWBFeyYmhiHR

کلید نفر سوم:

92FVhnu9hWDANY4LG4eL9nnNytcfuhDb7fAPKBwYttwwZFK3nTYX



هش tx :

77d13fccd61a5eb9c8cc089f25cd139c7217bd6bd93fe4c8894b9817f98832dd

bitcoinfaucet.uo1.net/send.php

Maps Gmail GitHub Welcome To Colab... My Drive OneDrive Typing Jungle - EdC... Pomodoro Timer O... WhatsApp GenApp حساب کاربری من | G... Paraphrasing Tool |...

et Faucet

Current wallet balance is ₪ 364.066. You can get up to ₪ 0.0002.

Hetzner Cloud - Get €20 Free Credit For New Account


0.0001 coins sent to mhc7s1ATHDLBZnFH73y6geT7Td4X69wygx

₪ mhc7s1ATHDLBZnFH73y6geT7Td4X69wygx

0.0001


Send testnet bitcoins

**BTC Address**  
Send coins back, when you don't need them anymore: tb1ql7w62elx9ucw4pj5lgw4l028hmuw80sndtntxt



**Last Transactions**

2a09612304fdb73f43df045c7fd008aec693dd32879f4a62a20c19090b25475	Sat, 18 Jun 2022 12:30:31
<div>mhc7s1ATHDLBZnFH73y6geT7Td4X69wygx</div> <div>pending</div>	<div>-0.0001</div> <div>0.00000145 fee</div>
6e35ff9fe1f73a29ac6087a940358206f5fc8624b696818f3b07ad7da979ad7c	Sat, 18 Jun 2022 12:22:46



```
(cryptoevo) tani@DESKTOP-KVBQAK9:/mnt/d/term_8/CryptoCurrency/CA/1/CryptoCurrency$ python3 transactionQ2P1.py
01 Created

{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "77d13fccd61a5eb9c8cc089f25cd139c7217bd6bd93fedc8894b9817f98832dd",
    "addresses": [
      "mhc7s1A1HDLBznFH73y6geT7TdAX69wygx",
      "zARndvyruspMAMa2ZhThvM19pgK0RizH"
    ],
    "total": 5000,
    "fees": 5000,
    "size": 399,
    "vsize": 399,
    "preference": "low",
    "relayed_by": "80.82.77.206",
    "received": "2022-06-18T12:47:38.124412456Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "2a09612304fdba73f43df045c7fd008aec693dd32879f4a62a20c19090b25475",
        "output_index": 1,
        "script": "473044022055cc8c6ef7e2fe902e9b50d5cf1ac17caed96ed6d5ae180012891e5cbe2f913b022039a5f35e37ffdd08a69e1b0b2f7dd345c4b6831157fe8a126228fb9b44f4f98401410415676cd5423ee67de2a6319da2173da2d1a4590005a95a52d8cdf54037a5952808f1b929041bd84cfc8f23685a803bbf5e3900dfc388f8baf8e677e54103fa",
        "output_value": 10000,
        "sequence": 4294967295,
        "addresses": [
          "mhc7s1A1HDLBznFH73y6geT7TdAX69wygx"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2280184
      }
    ],
    "outputs": [
      {
        "value": 5000,
        "script": "52a10415676cd5423ee67de2a6319da2173da2d1a4590005a95a52d8cdf54037a5952808f1b929041bd84cfc8f23685a803bbf5e3900dfc388f8baf8e677e54103fa410497b5853d777f2fb291698e277d8325f57608c82b791fa19f908c04b96e0b9328125705756da241ac1df39f79c2505d92bc84a681f5bb8b71397c47309af2c68e410452cc2dbc3b3626c2c50527409d67826006caf62c3ecddadfa5f9745943d52c2c57516f611d93f6038db8467063c177bd561e683d7231f77b0c187bd4d847843653ae",
        "addresses": [
          "zARndvyruspMAMa2ZhThvM19pgK0RizH"
        ],
        "script_type": "pay-to-multi-pubkey-hash"
      }
    ]
  }
}
```

```
(cryptoevo) tani@DESKTOP-KVBQAK9:/mnt/d/term_8/CryptoCurrency/CA/1/CryptoCurrency$ python3 transactionQ2P1.py
01 Created

{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "77d13fccd61a5eb9c8cc089f25cd139c7217bd6bd93fedc8894b9817f98832dd",
    "addresses": [
      "mhc7s1A1HDLBznFH73y6geT7TdAX69wygx",
      "zARndvyruspMAMa2ZhThvM19pgK0RizH"
    ],
    "total": 5000,
    "fees": 5000,
    "size": 399,
    "vsize": 399,
    "preference": "low",
    "relayed_by": "80.82.77.206",
    "received": "2022-06-18T12:47:38.124412456Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "2a09612304fdba73f43df045c7fd008aec693dd32879f4a62a20c19090b25475",
        "output_index": 1,
        "script": "473044022055cc8c6ef7e2fe902e9b50d5cf1ac17caed96ed6d5ae180012891e5cbe2f913b022039a5f35e37ffdd08a69e1b0b2f7dd345c4b6831157fe8a126228fb9b44f4f98401410415676cd5423ee67de2a6319da2173da2d1a4590005a95a52d8cdf54037a5952808f1b929041bd84cfc8f23685a803bbf5e3900dfc388f8baf8e677e54103fa",
        "output_value": 10000,
        "sequence": 4294967295,
        "addresses": [
          "mhc7s1A1HDLBznFH73y6geT7TdAX69wygx"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2280184
      }
    ],
    "outputs": [
      {
        "value": 5000,
        "script": "52a10415676cd5423ee67de2a6319da2173da2d1a4590005a95a52d8cdf54037a5952808f1b929041bd84cfc8f23685a803bbf5e3900dfc388f8baf8e677e54103fa410497b5853d777f2fb291698e277d8325f57608c82b791fa19f908c04b96e0b9328125705756da241ac1df39f79c2505d92bc84a681f5bb8b71397c47309af2c68e410452cc2dbc3b3626c2c50527409d67826006caf62c3ecddadfa5f9745943d52c2c57516f611d93f6038db8467063c177bd561e683d7231f77b0c187bd4d847843653ae",
        "addresses": [
          "zARndvyruspMAMa2ZhThvM19pgK0RizH"
        ],
        "script_type": "pay-to-multi-pubkey-hash"
      }
    ]
  }
}
```

پس از خرج شدن:

```
(cryptomv) tamin@ESKTOP-KVBQAK9:/mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$ python3 transactionQP2.py
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "e6466efb306dd04ec28c1b986b97110496f6b14b9c75236cf2cA78fbcd02a50",
    "addresses": [
      "zAbnAvyrusPMAFa2ZhTPhvP19pgK08Nzi",
      "mhc7s1ATHDLBZnFH73y6geT7Td4X69wygx"
    ],
    "total": 2000,
    "fees": 3000,
    "size": 231,
    "vsize": 231,
    "preference": "low",
    "relayed_by": "178.63.253.154",
    "received": "2022-06-18T13:41:04.064167782Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "77d13fcd61a5eb9c8cc089f25cd139c7217bd6bd93fe4c8894b9817f98832dd",
        "output_index": 0,
        "script": "00473044022070eb32b94aa40e4fc283b5be0758bd90e36982e98493edc:b01b5c4a9ca400402205690a421241e3ca788aaab8d751a320f1803584435a9247b8a3b8bafbf7bcf6001483045022100e1e0cc6c512c8ef9fb6ca57c4478b5107dfa39e7ecb57c9047bd215a7b9b0f2502203383e655574951f5cfad1de3894bd7da2b8aa008a71257cf95f39d1e15ead501",
        "output_value": 5000,
        "sequence": 4294967295,
        "addresses": [
          "zAbnAvyrusPMAFa2ZhTPhvP19pgK08Nzi"
        ],
        "script_type": "pay-to-multi-pubkey-hash",
        "age": 2280186
      }
    ],
    "outputs": [
      {
        "value": 2000,
        "script": "78e91a416ea51840ff10ed2ffce6e66bef880cf90187c88ac",
        "addresses": [
          "mhc7s1ATHDLBZnFH73y6geT7Td4X69wygx"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
(cryptomv) tamin@ESKTOP-KVBQAK9:/mnt/d/term 8/CryptoCurrency/CA/1/CryptoCurrency$
```

و confirm شدن آن :

The screenshot shows the Blockchain.com Explorer interface. The transaction details are as follows:

Index	Address	Pkscript	Witness	Value
0	mhc7s1ATHDLBZnFH73y6geT7Td4X69wygx	OP_DUP OP_HASH160 16ea51840ff10ed2ffce6e66bef880cf90187c OP_EQUALVERIFY OP_CHECKSIG	3044022055cc8c6e7e2fe902e9b50d5cf1ac17caed96ed6d5a180012891e5cbe2f913b022039a5f35a37ffdd08a6e9e1b0b27dd345c4b6831157fe8a126228fb9b44f4f984010415676cd5423ee67de2a6319da2173da2d1a14590005a95a52d8cdf54037a5952808fb929041bd84cf8f23685a803bbfe5e3900dfc388f8baf8e677e54103fa	0.00010000 BTC
0		OP_2 0415676cd5423ee67de2a6319da2173da2d1a14590005a95a52d8cdf54037a5952808fb929041bd84cf8f23685a803bbfe5e3900dfc388f8baf8e677e54103fa 0497b5853d7772fb291698e277d8325f5608c82b791fa19fd8c04b96e0b9328125705756da241ac1df39f79c2505d92bc84a681f5bb8b71397c47309af2c68e 0452cc2dbcc3b3626c2c50527409d678260066caf62c3ecd6adfa5f9745943d52c2c57516f61d93f6038db8467063c177bd561e683d7231f77b0c187b4d0478436 OP_3 OP_CHECKMULTISIG	0.00050000 BTC	

At the bottom, there is a cookie consent banner: "We use both our own cookies and third-party cookies on our websites to enhance your experience, analyze our traffic, and increase site security." with buttons for "Manage preferences" and "Accept all".

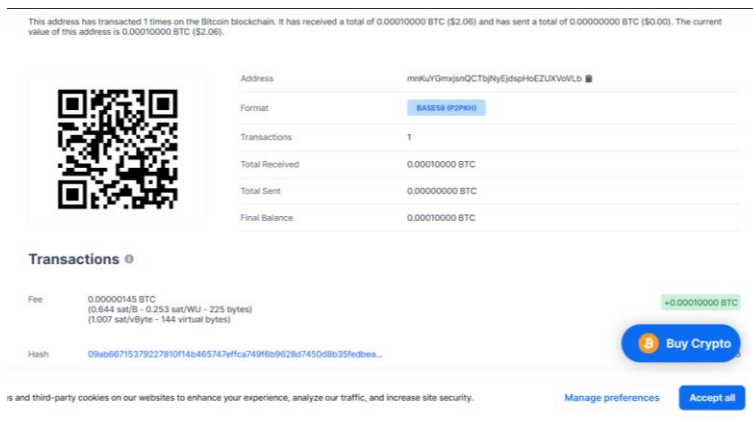
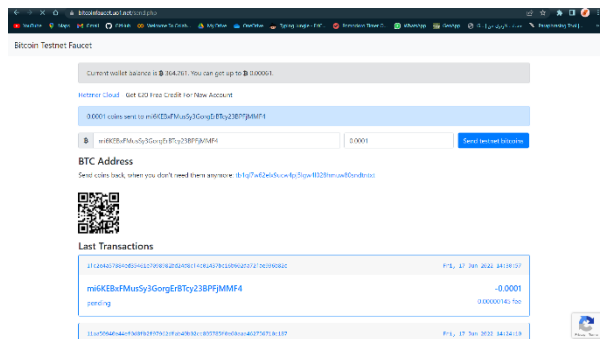
### سوال (۳)

دو عدد اول انتخاب کرده:

```
prime_one = 5
prime_two = 3
```

و با استفاده از `OP_ADD` , `OP_SUB` تفاضل و جمع این دو عدد را محاسبه کرده و در صورتی که درست وارد شود جواب میگیرد. برای ترنزاکشن اول هرکس این دو عدد را داشته باشد جمع و تفاضل را حساب میکند و در صورت دست بودن ترنزاکشن انجام میشود و برای ادرس خود را قرار میدهیم که با وارد کردن درست این اعداد به ادرس خودمان بازگردد.

همانند بخش های قبل از فاست برای گرفتن پول استفاده میکنیم



```
(cryptomv) taniq@DESKTOP-KV9QK09:/mnt/d/term_8/CryptoCurrency/CA/1/CryptoCurrency$ python3 transactionQ2P1.py
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "99208c1dd4d013c5b07b6d71c0c297f2280cae6d821a3d115907c08261e75",
    "addresses": [
      "mkuGmcjcnQCbJHyEjdsphoE2UxVoVb"
    ],
    "total": 500,
    "fees": 9900,
    "size": 205,
    "vsize": 205,
    "preference": "low",
    "relayed_by": "77.104.81.12",
    "received": "2022-06-18T09:06:04.448385627Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "09abb671537227810f14b465747cfcfa79f6b0628d745d0b35fcbca00a03",
        "output_index": 0,
        "script": "403040022100b040b45d5059e0401c16252e0ff4056950b321a25c348abdb5f4bc403221e02207b5cbcc16da418773da2c2705ec1f47b6fa59269122fc7015b28806b2bc8450141041a324c0c10c7f32a59038a0a22d597e50bd57405204a3dbb7796c73404a321c82c1560af12207cc083a717461a2ace7ae7c5d6095ff8e087956722ccc00c9",
        "output_value": 10000,
        "sequence": 4204067295,
        "addresses": [
          "mkuGmcjcnQCbJHyEjdsphoE2UxVoVb"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2270000
      }
    ],
    "outputs": [
      {
        "value": 500,
        "script": "933088945287",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
(cryptomv) taniq@DESKTOP-KV9QK09:/mnt/d/term_8/CryptoCurrency/CA/1/CryptoCurrency$
```

Figure ۱ ترزاكشن را میسازیم

```
(cryptomv) taniq@DESKTOP-KV9QK09:/mnt/d/term_8/CryptoCurrency/CA/1/CryptoCurrency$ python3 transactionQ2P3_2.py
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "9f50a90b30775aefb35fc7d75b7e99fd24c2c82b0d8eaf602f1ccc72d82e598",
    "addresses": [
      "mkuGmcjcnQCbJHyEjdsphoE2UxVoVb"
    ],
    "total": 100,
    "fees": 400,
    "size": 89,
    "vsize": 89,
    "preference": "low",
    "relayed_by": "77.104.81.12",
    "received": "2022-06-18T09:33:00.783174356Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "99208c1dd4d013c5b07b6d71c0c297f2280cae6d821a3d115907c08261e75",
        "output_index": 0,
        "script": "55535553",
        "output_value": 500,
        "sequence": 4204067295,
        "script_type": "unknown",
        "age": 2280127
      }
    ],
    "outputs": [
      {
        "value": 100,
        "script": "76a9144ab20159633c13ae7b08b7bee0f19a43b854277d88ac",
        "addresses": [
          "mkuGmcjcnQCbJHyEjdsphoE2UxVoVb"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
(cryptomv) taniq@DESKTOP-KV9QK09:/mnt/d/term_8/CryptoCurrency/CA/1/CryptoCurrency$
```

Figure ۲ خرج میکنیم

Explorer > Bitcoin Testnet > Transaction

USD

Search your transaction, an address or a block

Summary

USD BTC

Fee

0.00000400 BTC  
(4.494 sat/B - 1.124 sat/WU - 89 bytes)

0.00000100 BTC

4 Confirmations

Hash

9f50030b30775aef635fe7475b7e99fd24e2e82b0d8eaf602f71ccc7...

2022-06-18 14:03

0.00000500 BTC

mnKuYGmxjsnQCTbjNyEjdsphoEZUXVoVLb

0.00000100 BTC

This transaction was first broadcast to the Bitcoin network on June 18, 2022 at 2:03 PM GMT+4:30. The transaction currently has 4 confirmations on the network. At the time of this transaction, 0.00000100 BTC was sent with a value of \$0.02. The current value of this transaction is now \$0.02. Learn more about [how transactions work](#).

Details

Hash

9f50030b30775aef635fe7475b7e99fd24e2e82b0d8eaf602f71ccc72d82e450

ookies and third-party cookies on our websites to enhance your experience, analyze our traffic, and increase site security.

Manage preferences

Accept all

سوال ۴)

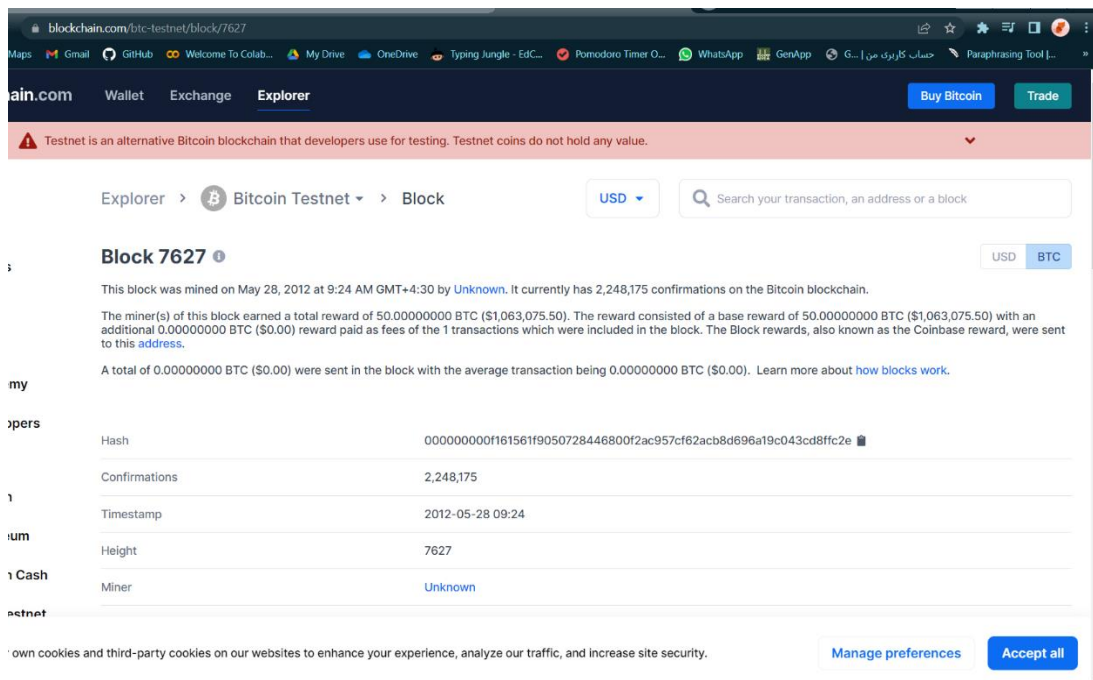
همان سوال ۱ است.

قسمت سوم: استخراج بلوک  
mineBlock.py

شماره دانشجویی : ۸۱۰۱۹۷۶۲۷

ارتفاع درخت مورد نظر : ۷۶۲۷

که اطلاعات آن :



حال باید یک coinbase transaction با اطلاعات زیر بسازیم:

Txid برای خرج: 00

ایندهکس: 0xFFFFFFFF

ورودی scriptSig: 810197627TaninZeraati (هش شده آن)

```
tanin@DESKTOP-KVBQAK9:/mnt/d/term 8/CryptoCurrency/CA/1/test$ python3 ascii.py
88313031393736323754616e696e5a657261617469
tanin@DESKTOP-KVBQAK9:/mnt/d/term 8/CryptoCurrency/CA/1/test$
```

خروجی script: A P2PKH output script to our address sending 6.25 BTC

پس از آن باید merkle root را حساب کنیم. برای اینکار از `serialize()` استفاده می‌کنیم تا بتوانیم stream format بگیریم چراکه merkle root برابر با coinbase است (ما در اینجا یک‌گونه transaction داریم). در مرحله بعد برای mine کردن نیاز داریم target را محاسبه کنیم. همان `calculated nBits` است که با توجه به میزان سختی باید تعداد صفر آن مشخص شود. در اینجا ۴ صفر در نظر گرفته شده است. "0x1f010000".

در آخر mine کردن را شروع میکنیم. از nounce صفر تا ماکس ادامه میدهیم. nounce را به partial\_header که با sha256 بدست آمده وصل میکنیم و چک میکنیم که کمتر از target باشد. در صورتی که شرط گفته شده برقرار باشد بلوک ماین شده و در خروجی چاپ میشود در غیر اینصورت این فرایند را مجدد انجام میدهیم.

کد ها با استفاده از منابع زیر پیاده سازی شده اند:

<https://www.investopedia.com/terms/b/block-height.asp#:~:text=Block%20height%20refers%20to%20a,size%20or%20time%20in%20existence.>