CSI4108 Assignment 3

Hongyi Lin, 300053082

Question 1

source code: `q1.py`

The running results of my code:

```
TERMINAL  PROBLEMS  DEBUG CONSOLE  OUTPUT  JUPYTER

C:\Users\honyl\Desktop\CSI4108 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q1.py
private key: xa = 30
public key: q = 89, alpha = 13, ya = 49

plaintext: m = 87

ciphertext: c1 = 82, c2 = 84

decrypted plaintext: m_decrypted = 87

Data integrity is verified
C:\Users\honyl\Desktop\CSI4108 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q1.py
private key: xa = 30
public key: q = 89, alpha = 13, ya = 49

plaintext: m = 76

ciphertext: c1 = 41, c2 = 7

decrypted plaintext: m_decrypted = 76

Data integrity is verified
C:\Users\honyl\Desktop\CSI4108 (a3)
> |
```

During the encryption process, we get get the ciphertext from m_1 and m_2 as:

- For m_1, $C_{1,1} = \alpha^k \mod q$, $C_{2,1} = Km_1 \mod q$
- For m_2, $C_{1,2} = \alpha^k \mod q$, $C_{2,2} = Km_2 \mod q$

As for $K = (Y_A)^k \mod q$ when k is the same, K must be the same. Hence, we have

$$\frac{C_{2,2}}{C_{2,1}} = \frac{Km_2 \mod q}{Km_1 \mod q} = \frac{m_2 \mod q}{m_1 \mod q}$$

From this, we can calculate $m2$ as $m_2 = (C_{2,1})^{-1} C_{2,2} m_1 \mod q$.

From the question, we know that $q = 89$, $\alpha = 13$ and for $m_1 = 56$ and m_2, the $k = 37$ is the same. Suppose that $X_A = 15$, then $Y_A = 7$ and $C_{2,1} = 31$ can be calculated. With $C_{2,1} = 31$, $(C_{2,1})^{-1} \mod q = (C_{2,1})^{-1} \mod 89 = 23$. Now, if we can know that $C_{2,2} = 11$, then the plaintext $m_2 = (C_{2,1})^{-1} C_{2,2} m_1 \mod q = 23 \times 11 \times 56 \mod 89 = 17$ can be calculated.

Question 2

source code: `q2.py`

After checking the table in the given link, 11027, 9127 and 10477 are all prime numbers.

```
TERMINAL  PROBLEMS  DEBUG CONSOLE  OUTPUT  JUPYTER

C:\Users\honyl\Desktop\CSI4108 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q2.py
Try the number 9219...
Oops, 9219 is not 14-bit prime.

Try the number 9898...
Oops, 9898 is not 14-bit prime.

Try the number 10815...
Oops, 10815 is not 14-bit prime.

Try the number 9472...
Oops, 9472 is not 14-bit prime.

Try the number 9996...
Oops, 9996 is not 14-bit prime.

Try the number 11027...
Ah ha, 11027 is a probably 14-bit prime!
C:\Users\honyl\Desktop\CSI4108 (a3)
> |
```

```
TERMINAL  PROBLEMS  DEBUG CONSOLE  OUTPUT  JUPYTER

C:\Users\honyl\Desktop\CSI4108 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q2.py
Try the number 9127...
Ah ha, 9127 is a probably 14-bit prime!
C:\Users\honyl\Desktop\CSI4108 (a3)
> |
```

```
TERMINAL  PROBLEMS  DEBUG CONSOLE  OUTPUT  JUPYTER

C:\Users\honyl\Desktop\CSI4108 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q2.py
Try the number 10477...
Ah ha, 10477 is a probably 14-bit prime!
C:\Users\honyl\Desktop\CSI4108 (a3)
> |
```

Question 3

Part a

source code: `q3a.py`

```
TERMINAL  PROBLEMS  DEBUG CONSOLE  OUTPUT  JUPYTER                Python

C:\Users\honyl\Desktop\CSI4108\a3 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q3a.py
Decrypt c without CRT:
25000600 ns
Decrypt c with CRT:
16001900 ns
C:\Users\honyl\Desktop\CSI4108\a3 (a3)
> |
```

Part b

source code: `q3b.py`

It seems that the speed of the normal D-H is faster than ECDH with the help of the fast exponentiation algorithm. Besides, this timing result may also be related to the implementation. For the ECDH, the whole process involves much more function calls than normal D-H, which may cause the longer execution time.

```
TERMINAL  PROBLEMS  DEBUG CONSOLE  OUTPUT  JUPYTER                Python

C:\Users\honyl\Desktop\CSI4108 (a3)
> & C:/Users/honyl/AppData/Local/Programs/Python/Python38/python.exe c:/Users/honyl/Desktop/CSI4108/a3/q3b.py
EllipticCurve(p=115792089210356248762697446949407573530086143415290314195533631308867097853951, a=-3, b=41058363725152142129326129780047268409114441015993725554835256314039467401291, g=(48439561293906451759052585252797914202762949526041747995844080717082404635286, 36134250956749795798585127919587881956611106672985015071877198253568414405109), n=115792089210356248762697446949407573529996955224135760342422259061068512044369, h=1)
ECDH Time: 73999700 ns
ECDH data:
Alice:
        private_key = 45624042915785829979616214320596637469784592005145838050023499518501432316830
        public_key = (13624288971455067361351292371927217284835843957819072405118104080833553748643, 115230336908617905457599414115367582328550751078971856956994501974490480635372)
        shared_secret = (45416945665490754205657288555863705189589724856771040205549373208481738669733, 70867388111776559843800583044322557100096462779113058117604475711217250972867)
Bob:
        private_key = 108491377381597327122173722180673749535570580130826498213943396379544742689819
        public_key = (102660709396236950944603586109324102570136347789717497284881685186123171831846, 4787930958503442953399400135500742267755808075381085006427450079281920991857)
        shared_secret = (45416945665490754205657288555863705189589724856771040205549373208481738669733, 70867388111776559843800583044322557100096462779113058117604475711217250972867)

ordinary D-H Time: 999300 ns
ordinary D-H data:
p = 115792089210356248762697446949407573530086143415290314195533631308867097853951
g = 3
Alice:
        private_key = 21671362394092914919999136563688308255950216736074990468415199085351685083642
        public_key = 71127505041840234368220808233940577388871545657742458239569915420033634916454
        shared_secret = 76313176683768102811429250224788745707910218452374173313100174329141721082045
Bob:
        private_key = 22738744015094884331729240985680217460159626785951295285708339393656022790789
        public_key = 47994079784933988970799740657571821634623920128792872397476724834578525658844
        shared_secret = 76313176683768102811429250224788745707910218452374173313100174329141721082045
C:\Users\honyl\Desktop\CSI4108 (a3)
> |
```