Week10

Zhen Shen
Student number:10725458
Group number:23

December 2020

Question 1

(a)

Matlab code:

```
p=sym('636449999');
a=sym('557229101');
v=sym('340924010');
g=0;% The start of circulation
while isPrimitiveRoot(g,p)~=1
      %To judge if g is a primitive root modulo p
      g=g+1;
      % Find the 'smallest' positive primitive root modulo p
end
g % Output the value
```

From the output, we have g=11.

(b)

Matlab code:

```
u=powermod(g,a,p)% Calculate the value of u and output it
k=powermod(v,a,p)% Calculate the value of k and output it
```

$$u \equiv g^a \bmod p$$

$$k \equiv v^a \bmod p$$

The answer is u=18122020, k=20201218.

Question 2

(a)

Matlab code:

```
n=sym('943159985217865332709236813899783185092653155840586898288 01');
s=n-1;
r=0;
while mod(s,2)==0
      % Determine if s is even
      s=s/2;
      % Make s continues dividing by 2 until the result is odd
      r=r+1;
end
r% Output the value of r (the exponent)

i=s;% Use to control the value of exponent
j=1;
while i~=2*(n-1)
      %
      a=powermod(7,i,n)
      % Output the sequence of remainders
      data(j)=a;
      % Storage the remainders in a vector (data)
      j=j+1;
      i=2*i;
end
```

Calculation steps:

$$s = (n-1)/2/2/2/2/2/2$$

$$Remainders \equiv 7^{is} \bmod n$$

Results: r=6,
The sequence of remainders

$a^{2^r s}$	Remainders
7^s	518363887056320047255205584827992538087613135320505177915 26
$7^2 s$	165882891544690792473094541274727073697371870062006208299 50
$7^4 s$	509151786553878232884114852285371679739643477919843917838 55
$7^8 s$	905288814333729973513577599770552590734471442708745733033 14
$7^{16} s$	666591655056887481644508505748728671651346973107887317954 33
$7^{32} s$	150603125894171644277464880778 9035033609
$7^{64} s$	1

Conclusion: though the last term in the sequence is 1, but neither the first term of the sequence is 1 nor the first 1 in the sequence is preceded by n-1, so the number n fails the test, it is composite.

(b)

Matlab code:

```
k=1;
while k<=7
      m=gcd(data(k)+1,n);
      % Add 1 to remainders and calculate the greatest common
        divisor of each of the resulting numbers with n
      p=gcd(data(k)-1,n);
      % Subtract 1 from the remainders and calculate the
        greatest common divisor of each of the resulting
        numbers with n
      data2(k)=m;
      % Storage the value of gcds in a vector(+1)
      data3(k)=p;
      % Storage the value of gcds in a vector(-1)
      k=k+1;
end

data4=[data2,data3];
% Combine the vector "data2" and "data3"(the gcds)
for o=1:14% 14 is the number of elements
    if isprime(data4(o))==0
       % Judge if the elements in data4 is prime or not
       data4(o)=1;
       % Make the non-prime number elements equal to 1
    end
end
data4=unique(data4)
% Delete repeat elements.
data4(data4==1)=[]
% Delete 1 which is not a prime number.This is the vector which
  containing the prime factorisation of n
```

So the prime factorisation of n is output as
data4= [25050210070158064801, 50100420140316129601, 75150630210474194401]

Question 3

Matlab code:

```
H=sym('3424781706');
r=sym('8859445681');
s=sym('15992960169');
p=3016767493687098042636 7');
q=sym('17456345243');
g=sym('18008617784390347685963');
y=sym('6172647251731232412543');
% Input the value of numbers
w=powermod(s,-1,q);
% Intermediate step to help find u1 and u2
u1=mod(H*w,q)
% Find and output u1
u2=mod(r*w,q)
% Find and output u2
a=powermod(g,u1,p);
b=powermod(y,u2,p);
c=mod(mod(a*b,p),q);
% Because g^u1*y^u2 is too large, so use a.b to assist.
if isequal(c,r)==0
% Judge is the remainder equal to r.
   disp('Invalid')
else disp('Valid')% Show the results valid or invalid
end
```

Main steps:
$w \equiv s^{-1} \bmod q$
$u1 \equiv H * w \bmod q$
$u2 \equiv r * w \bmod q$
$a \equiv g^{u1} \bmod p$
$b \equiv y^{u2} \bmod p$
$z \equiv a * b \bmod p$
$c \equiv z \bmod q$
We have outputs u1=12268294885, u2=11756299598, and the final remainder is 8859445681, which is equal to the value of r, so the signature (r,s) is valid.

Question 4

(a)

Matlab code:

```
S=sym('10725458');
% Though the number is small, but for the further calculate,
  use 'sym'
p=nextprime(10*(S^4));
```

```
while isprime((p-1)/2)==0
      p=nextprime(p+1);
% Because nextprime function find the smallest prime greater
  than or 'equal to', so we have to add 1 otherwise the number
  will keep unchange
end
p% Output the value of p

q=prevprime(4*(S^5));
while isprime((q-1)/2)==0
      q=prevprime(q-1);
% Similar to nextprime function, subtract 1
end
q% Output the value of p

e=65537;
d=(powermod(e,-1,(p-1)*(q-1)))
% Use powermod to deal with e, move it to the right as e^-1
```

Having the outputs:
p=132331545978992827440257359463,
q=56772657538910258120469111650619292 7,
d=7346593243992579383612520520988966114179371152 0-404475717141679085

(b)

Matlab code:

```
c1=sym('24443637667912083611097084771805234845805567745941696161106355 95');
c2=sym('54165492371574924964670228300407737522306612118787636666325107 864');
n=p*q;
m1=powermod(c1,d,n)
m2=powermod(c2,d,n)
% Decrypt messages with d
```

Mean steps:
$n = p * q$
$m1 \equiv c_1^d \bmod n$ $m2 \equiv c_2^d \bmod n$
With the output:
$m1 = 13012008051301200903190009190020080500041515180001140400110525 00$
$m2 = 20150020080500190309051403051900181507051800020103151400000000 00$
After converting the pair of 2 digit blocks to letters by using the table, I have the message
'MATHEMATICS IS THE DOOR AND KEY TO THE SCIENCES ROGER BACON'