Ran Zhao

Weekly Report III

Date: October 6th, 2012

Summary

During this week, I finished the implementation of Identity-based encryption system (both BasicIdent and FullIdent version of Boneh-Franklin model).

System Overview

(1)Setup: Take security parameter K(QBITS,RBITS),return the system parameter ans master key of the PKG. The system parameters include a description of a finite message space M, and a description of a finite ciphertext space C. The system parameters will be publicly known, while the master-key will be known only to the PKG.
(2)Extract: The receiver extracts the corresponding private key from the PKG.
(3)Encrypt: The sender will generate a ciphertext based on the receiver ID.
(4)Decrypt: The receiver will use his private key to get the message digest.

BasicIdent version Detail:

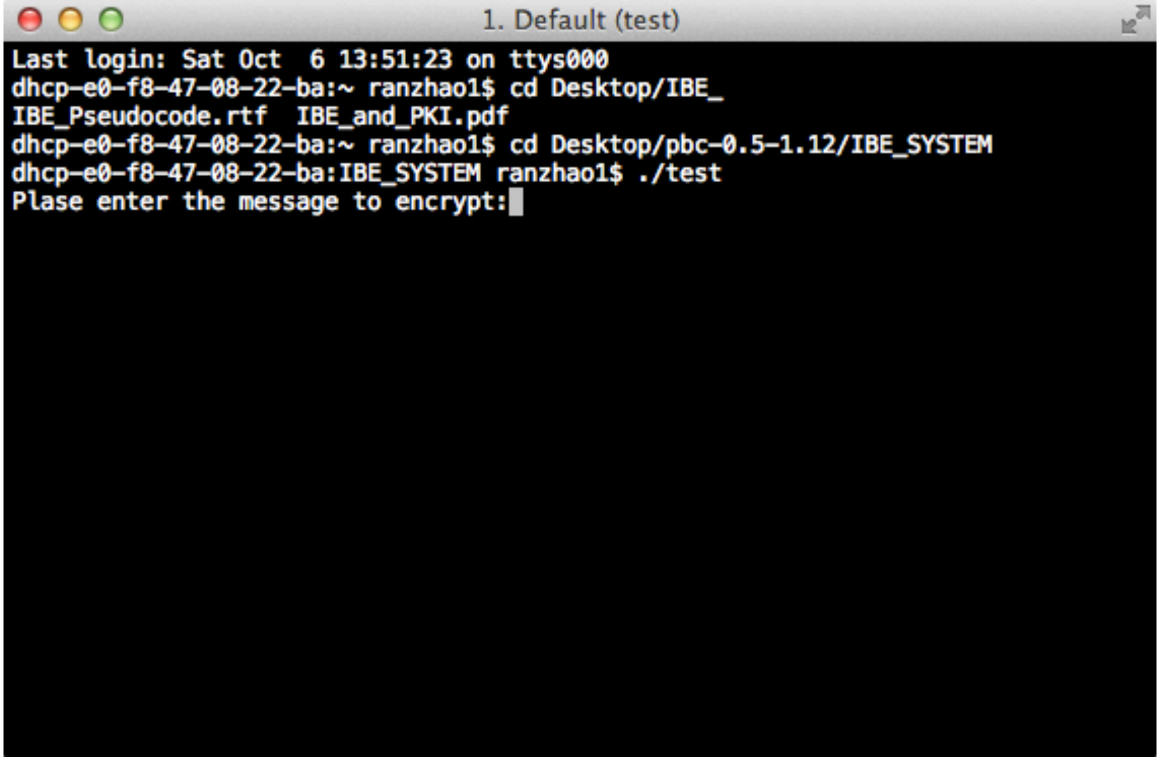
1.H1 function---Element build-in function (element_from_hash)
2.H2 function---SHA1 function generate 160 bit long number
3.As I use SHA1 function as H2 function, thus the n is automatically set as 160.
4.In my code, I use type A parameter(elliptic curve) to generate pairing.

FullIdent version Detail:

1.H1 function---Element build-in function (element_from_hash)
2.H2 function---SHA1 function generate 160 bit long number
3.H3 function---Concatenate the sigma and message digest, and then put it into build-in function element_random. The random number will between 0 and q
4.H4 function---Input a 160 bit long number and run SHA1 function to generate another 160 bit long number.
5.As I use SHA1 function as H2 function, thus the n is automatically set as 160.

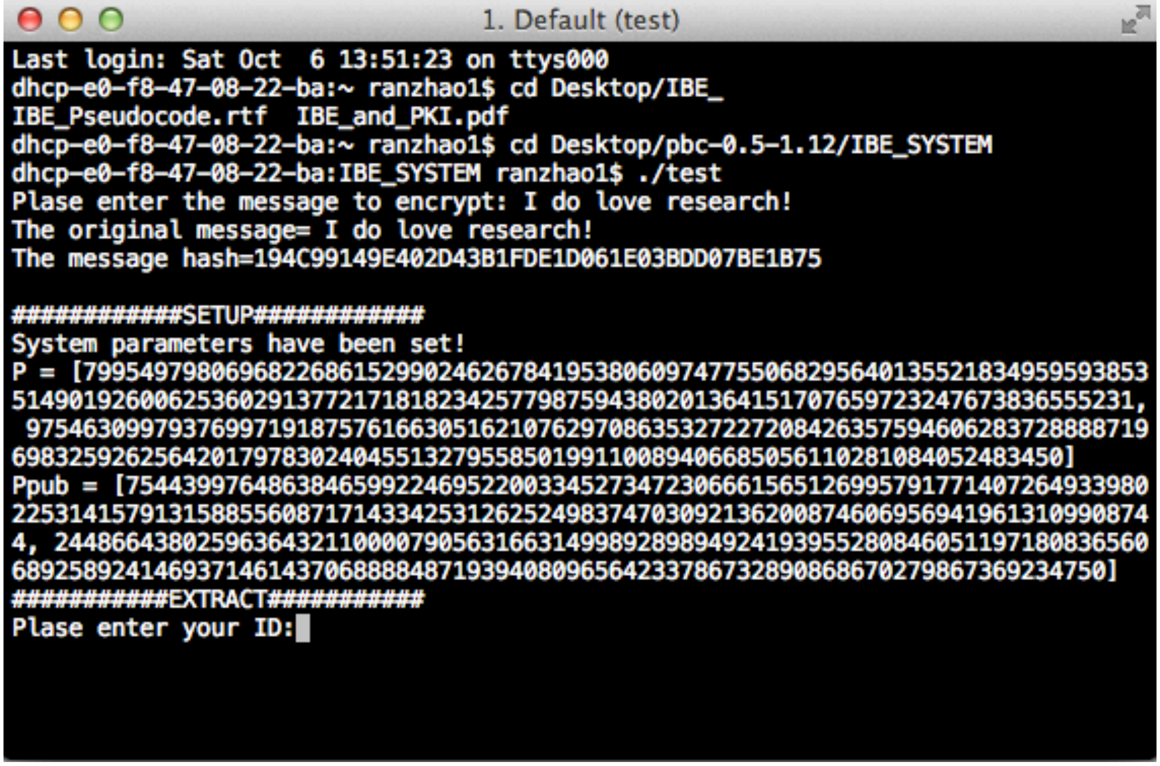
Experiment1 (BasicIdent version)

1.Firstly, type in the message to encrypt.



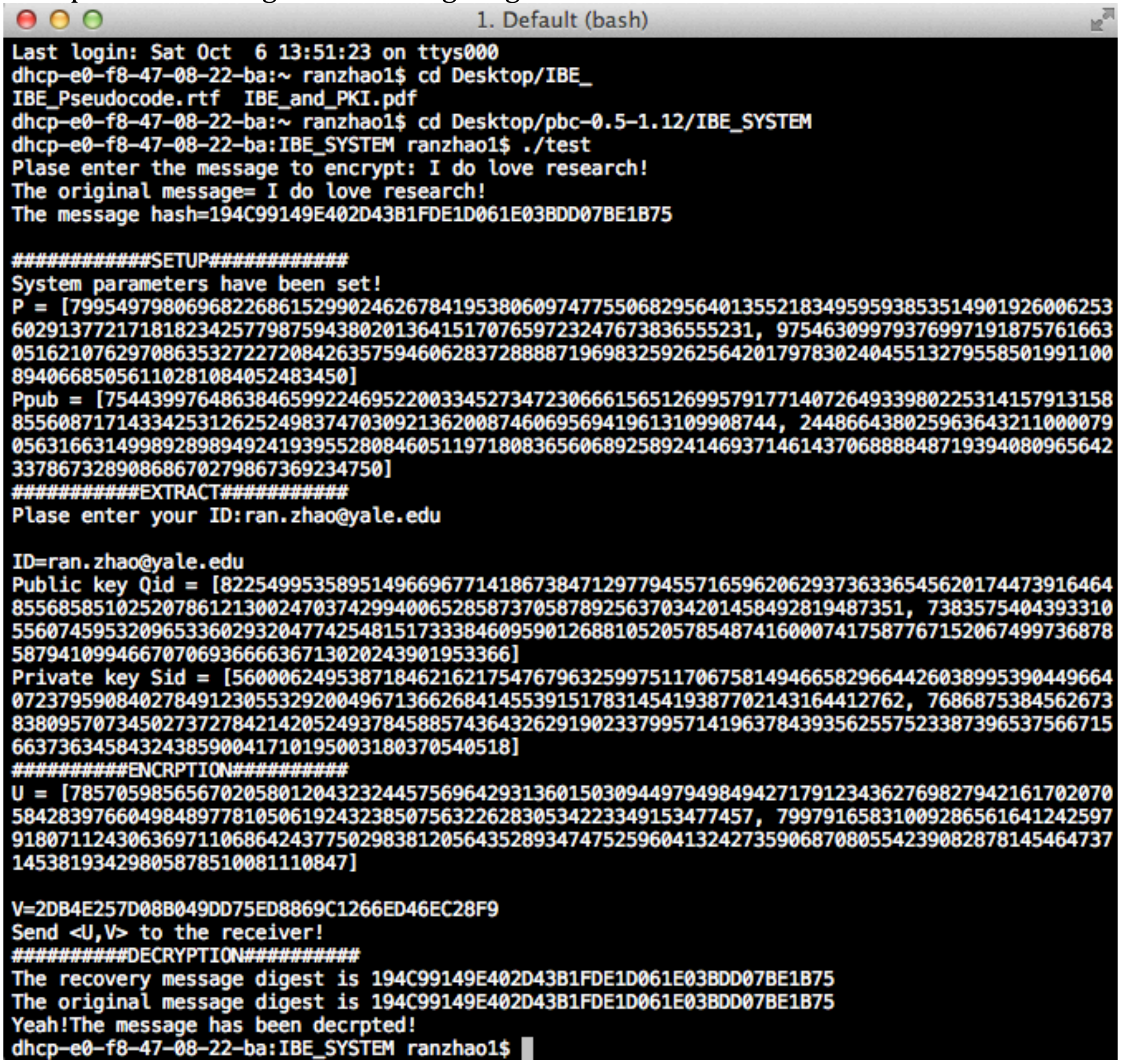
```
Last login: Sat Oct  6 13:51:23 on ttys000
dhcp-e0-f8-47-08-22-ba:~ ranzhao1$ cd Desktop/IBE_
IBE_Pseudocode.rtf  IBE_and_PKI.pdf
dhcp-e0-f8-47-08-22-ba:~ ranzhao1$ cd Desktop/pbc-0.5-1.12/IBE_SYSTEM
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ ./test
Plase enter the message to encrypt:
```

2.Secondly,after system has been setup, you should type your ID to get private key.



```
Last login: Sat Oct  6 13:51:23 on ttys000
dhcp-e0-f8-47-08-22-ba:~ ranzhao1$ cd Desktop/IBE_
IBE_Pseudocode.rtf  IBE_and_PKI.pdf
dhcp-e0-f8-47-08-22-ba:~ ranzhao1$ cd Desktop/pbc-0.5-1.12/IBE_SYSTEM
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ ./test
Plase enter the message to encrypt: I do love research!
The original message= I do love research!
The message hash=194C99149E402D43B1FDE1D061E03BDD07BE1B75

############SETUP############
System parameters have been set!
P = [799549798069682268615299024626784195380609747755068295640135521834959593853
5149019260062536029137721718182342577987594380201364151707659723247673836555231,
 9754630997937699719187576166305162107629708635327227208426357594606283728888719
69832592625642017978302404551327955850199110089406685056110281084052483450]
Ppub = [754439976486384659922469522003345273472306661565126995791771407264933980
22531415791315885560871714334253126252498374703092136200874606956941961310990874
4, 24486643802596364321100007905631663149989289894924193955280846051197180836560
68925892414693714614370688884871939408096564233786732890868670279867369234750]
###########EXTRACT###########
Plase enter your ID:
```

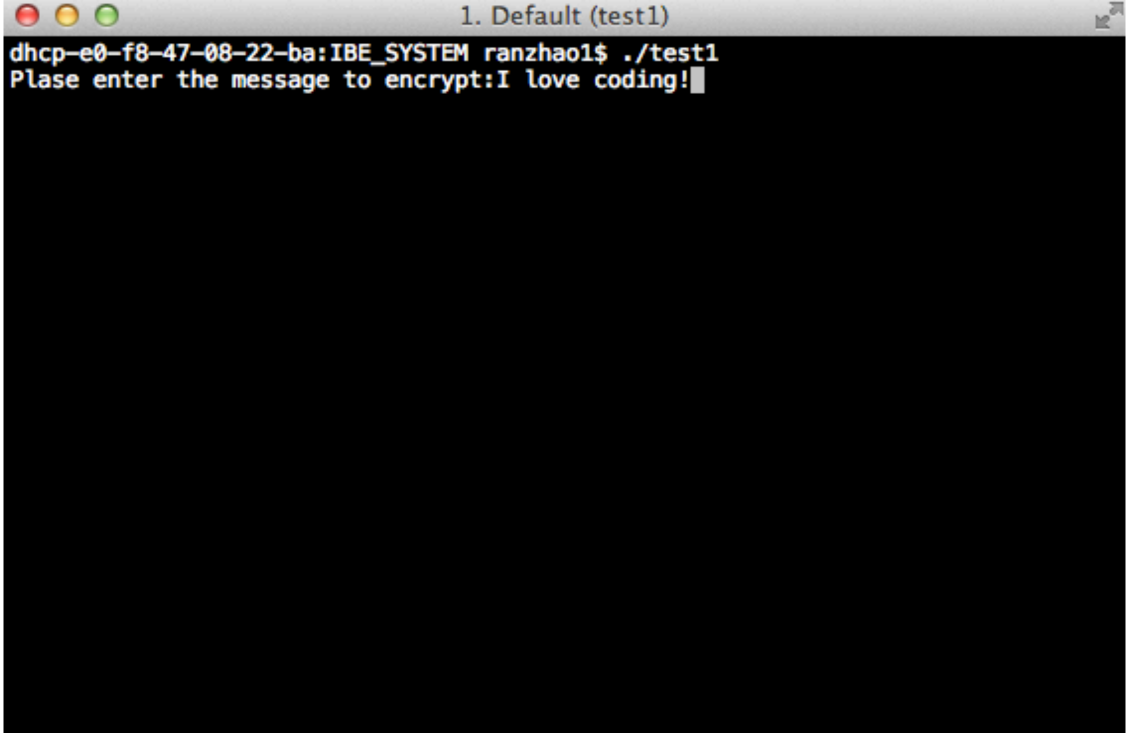
3.Thirdly, the cipheretext has been sent to the receiver. The receiver will decrypt the cipheretext and get the message digest.



```
Last login: Sat Oct  6 13:51:23 on ttys000
dhcp-e0-f8-47-08-22-ba:~ ranzhao1$ cd Desktop/IBE_
IBE_Pseudocode.rtf  IBE_and_PKI.pdf
dhcp-e0-f8-47-08-22-ba:~ ranzhao1$ cd Desktop/pbc-0.5-1.12/IBE_SYSTEM
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ ./test
Plase enter the message to encrypt: I do love research!
The original message= I do love research!
The message hash=194C99149E402D43B1FDE1D061E03BDD07BE1B75

###########SETUP###########
System parameters have been set!
P = [79954979806968226861529902462678419538060974775506829564013552183495959385351490192600625360291377217181823425779875943802013641517076597232476738365552231, 975463099793769971918757616630516210762970863532722720842635759460628372888871969832592625642017978302404551327955850199110089406685056110281084052483450]
Ppub = [754439976486384659922469522003345273472306661565126995791771407264933980225314157913158855608717143342531262524983747030921362008746069569419613109908744, 244866438025963643211000079056316631499892898949241939552808460511971808365606892589241469371461437068884871939408096564233786732890868670279867369234750]
##########EXTRACT##########
Plase enter your ID:ran.zhao@yale.edu

ID=ran.zhao@yale.edu
Public key Qid = [822549953589514966967714186738471297794557165962062937363365456201744739164648556858510252078612130024703742994006528587370587892563703420145849281948735l, 738357540439331055607459532096533602932047742548151733384609590126881052057854874160007417587767152067499736878587941099466707069366663671302024390195336 6]
Private key Sid = [560006249538718462162175476796325997511706758149466582966442603899539044966407237959084027849123055329200496713662684145539151783145419387702143164412762, 768687538456267383809570734502737278421420524937845885743643262919023379957141963784393562557523387396537566715663736345843243859004171019500318037054051 8]
##########ENCRPTION##########
U = [785705985656702058012043232445756964293136015030944979498494271791234362769827942161702070584283976604984897781050619243238507563226283053422334915347745 7, 799791658310092865616412425979180711243063697110686424377502983812056435289347475259604132427359068708055423908287814546473714538193429805878510081110847]

V=2DB4E257D08B049DD75ED8869C1266ED46EC28F9
Send <U,V> to the receiver!
##########DECRYPTION##########
The recovery message digest is 194C99149E402D43B1FDE1D061E03BDD07BE1B75
The original message digest is 194C99149E402D43B1FDE1D061E03BDD07BE1B75
Yeah!The message has been decrpted!
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ 
```

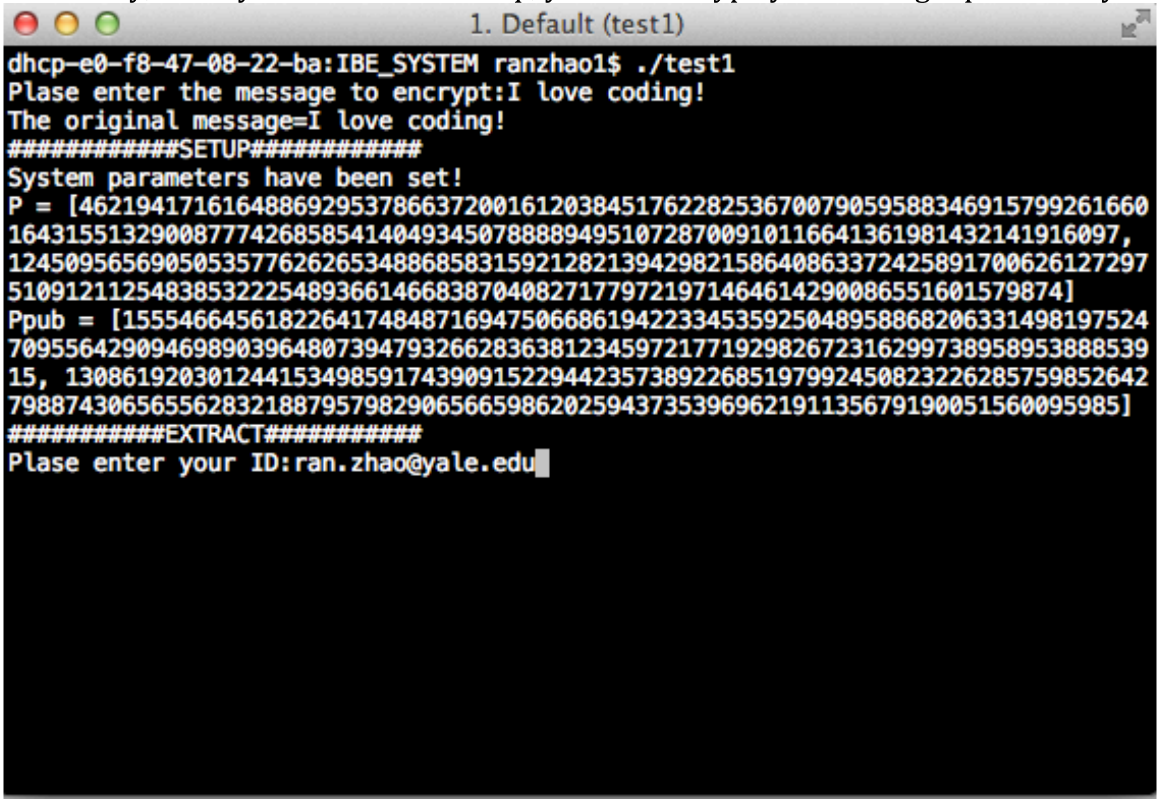
Experiment2 (FullIdent version)

1.Firstly, type in the message to encrypt.



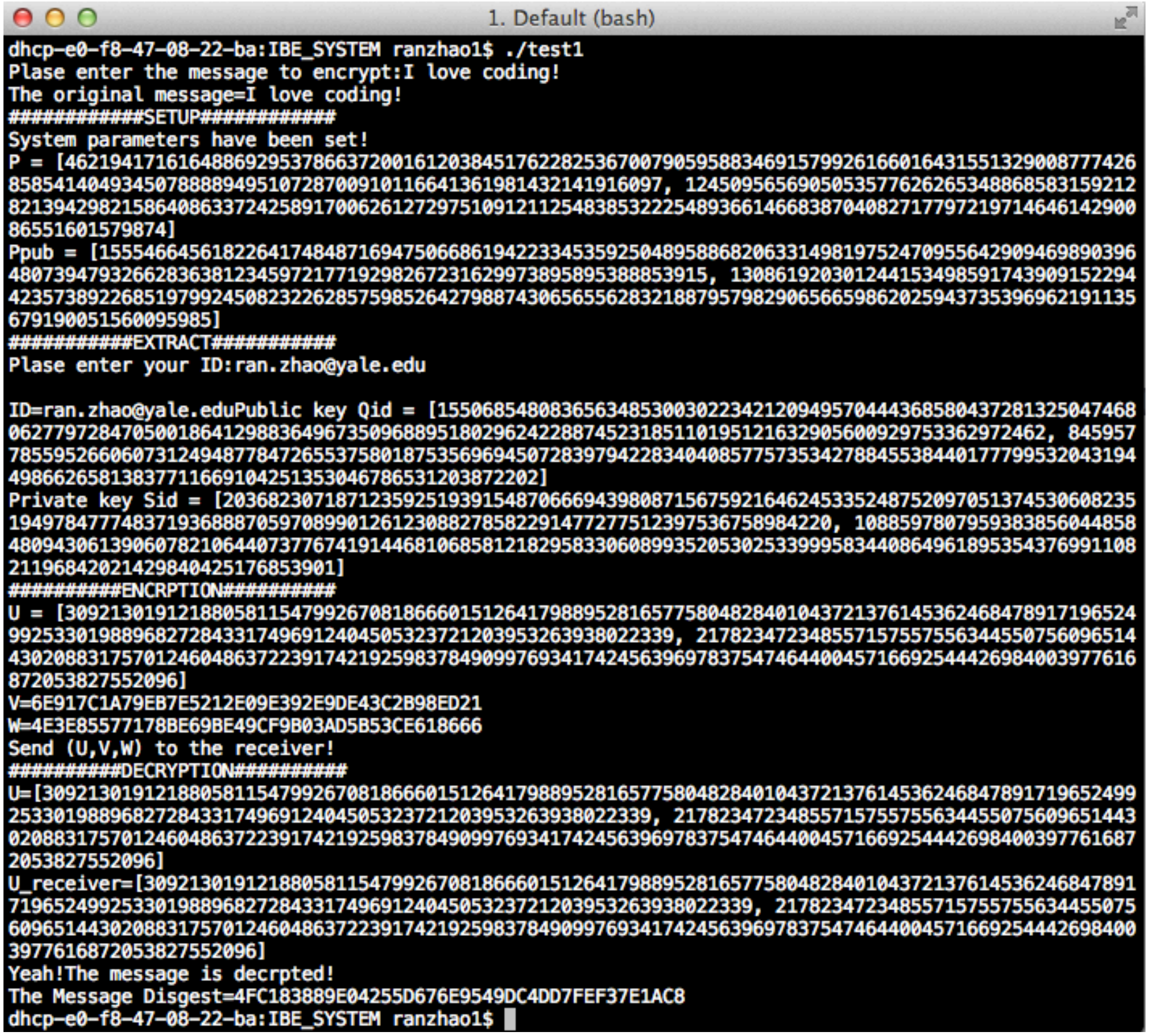
```
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ ./test1
Plase enter the message to encrypt:I love coding!
```

2.Secondly,after system has been setup, you should type your ID to get private key.



```
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ ./test1
Plase enter the message to encrypt:I love coding!
The original message=I love coding!
###########SETUP###########
System parameters have been set!
P = [462194171616488692953786637200161203845176228253670079059588346915799261660
164315513290087774268585414049345078888949510728700910116641361981432141916097,
124509565690505357762626534886858315921282139429821586408633724258917006261272 97
51091211254838532225489366146683870408271779721971464614290086551601579874]
Ppub = [155546645618226417484871694750668619422334535925048958868206331498197524
709556429094698903964807394793266283638123459721771929826723162997389589538885 39
15, 1308619203012441534985917439091522944235738922685197992450823226285759852642
798874306565562832188795798290656659862025943735396962191135679190051560095985]
##########EXTRACT##########
Plase enter your ID:ran.zhao@yale.edu
```

3.Thirdly, the cipheretext has been sent to the receiver. The receiver will decrypt the cipheretext and get the message digest.



```
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ ./test1
Plase enter the message to encrypt:I love coding!
The original message=I love coding!
###########SETUP###########
System parameters have been set!
P = [46219417161648869295378663720016120384517622825367007905958834691579926166016431551329008777426
858541404934507888894951072870091011664136198143214191609 7, 1245095656905053577626265348868583159212
82139429821586408633724258917006261272975109121125483853222548936614668387040827177972197146461429 00
86551601579874]
Ppub = [1555466456182264174848716947506686194223345359250489588682063314981975247095564290946989039 6
480739479326628363812345972177192982672316299738958953888539 15, 130861920301244153498591743909152294
4235738922685197992450823226285759852642798874306565562832188795798290656659862025943735396962191135
67919005156009598 5]
###########EXTRACT###########
Plase enter your ID:ran.zhao@yale.edu

ID=ran.zhao@yale.eduPublic key Qid = [15506854808365634853003022342120949570444368580437281325047468
06277972847050018641298836496735096889518029624228874523185110195121632905600929753362972462, 845957
78559526606073124948778472655375801875356969450728397942283404085775735342788455384401777995320431 94
49866265813837711669104251353046786531203872202]
Private key Sid = [20368230718712359251939154870666943980871567592164624533524875209705137453060823 5
1949784777483719368887059708990126123088278582291477277512397536758984220, 108859780795938385604485 8
48094306139060782106440737767419144681068581218295833060899352053025339995834408649618953543769911 08
211968420214298404251768539 01]
##########ENCRPTION##########
U = [30921301912188058115479926708186660151264179889528165775804828401043721376145362468478917196524
99253301988968272843317496912404505323721203953263938022339, 21782347234855715755755634455075609651 4
43020883175701246048637223917421925983784909976934174245639697837547464400457166925444269840039776 16
872053827552096]
V=6E917C1A79EB7E5212E09E392E9DE43C2B98ED21
W=4E3E85577178BE69BE49CF9B03AD5B53CE618666
Send (U,V,W) to the receiver!
##########DECRYPTION##########
U=[3092130191218805811547992670818666015126417988952816577580482840104372137614536246847891719652499
2533019889682728433174969124045053237212039532639380223 39, 21782347234855715755755634455075609651443
020883175701246048637223917421925983784909976934174245639697837547464400457166925444269840039776168 7
2053827552096]
U_receiver=[30921301912188058115479926708186660151264179889528165775804828401043721376145362468478 91
7196524992533019889682728433174969124045053237212039532639380223 39, 21782347234855715755755634455075
60965144302088317570124604863722391742192598378490997693417424563969783754746440045716692544426984 00
397761687205382755209 6]
Yeah!The message is decrpted!
The Message Disgest=4FC183889E04255D676E9549DC4DD7FEF37E1AC8
dhcp-e0-f8-47-08-22-ba:IBE_SYSTEM ranzhao1$ █
```

Next-week task

Next week, I will learn Facebook authorization protocol (OAuth2.0). Also, based on OAuth2.0 protocol, I will write a “private key pick up” protocol for IBE-PKG.