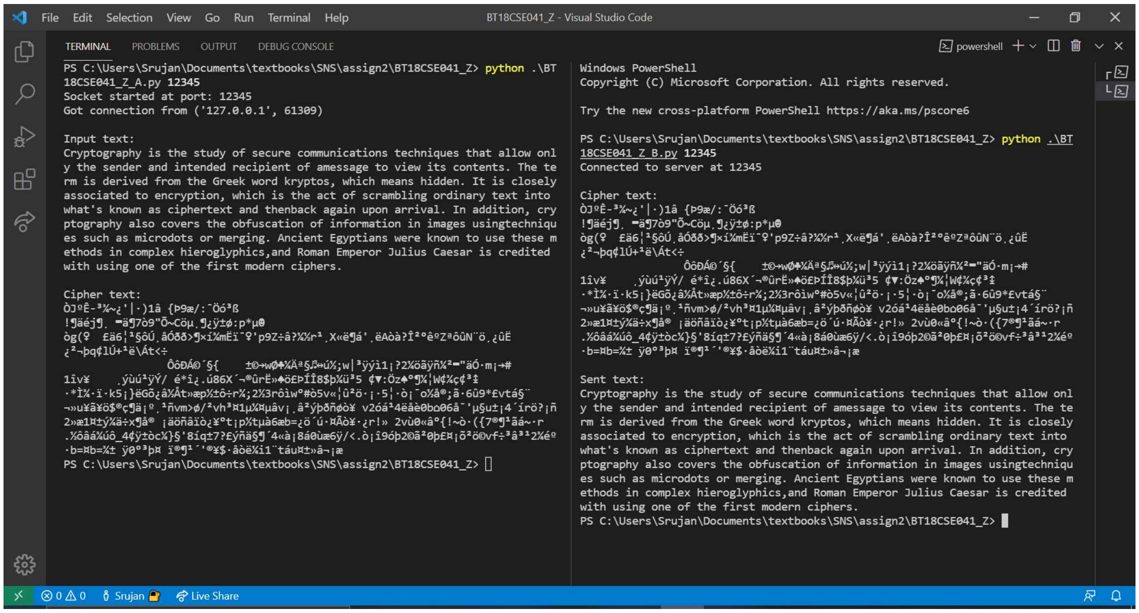
SNS ASSIGNMENT-2 PROGRAM INSTRUCTIONS

Srujan R, BT18CSE041

Z – 2-round Feistel Cipher:

1. First run Alice program with port number as command line input.
   Ex: python BT18CSE041_Z_A.py 12345
2. Next run Bob program with the same port number as Alice as command line input.
   Ex: python BT18CSE041_Z_B.py 12345

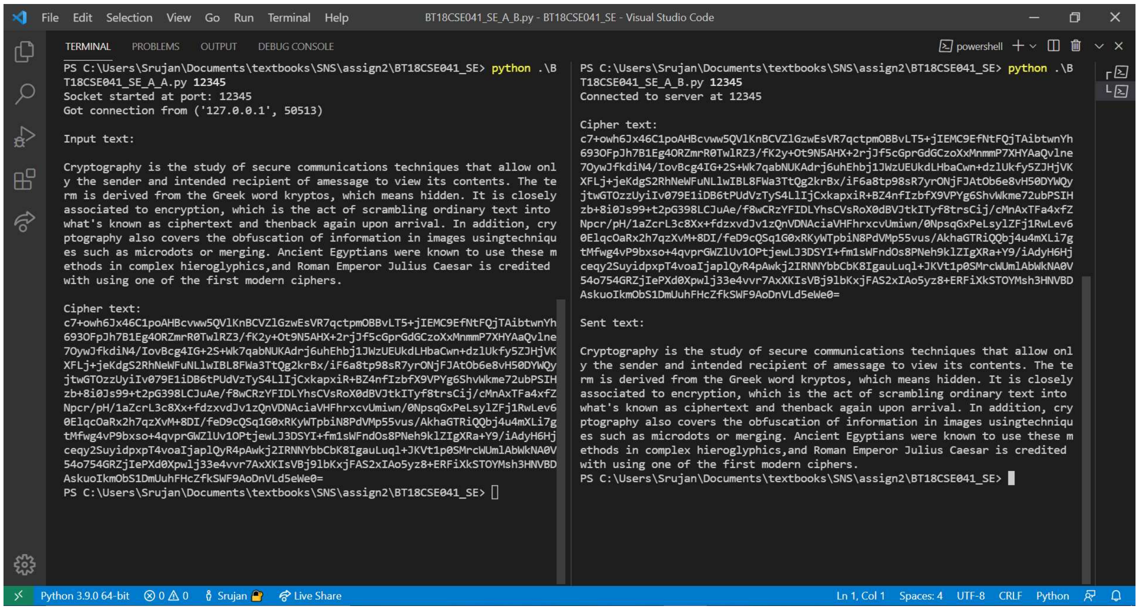


```
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_Z> python .\BT
18CSE041_Z_A.py 12345
Socket started at port: 12345
Got connection from ('127.0.0.1', 61309)

Input text:
Cryptography is the study of secure communications techniques that allow onl
y the sender and intended recipient of amessage to view its contents. The te
rm is derived from the Greek word kryptos, which means hidden. It is closely
associated to encryption, which is the act of scrambling ordinary text into
what's known as ciphertext and thenback again upon arrival. In addition, cry
ptography also covers the obfuscation of information in images usingtechniqu
es such as microdots or merging. Ancient Egyptians were known to use these m
ethods in complex hieroglyphics,and Roman Emperor Julius Caesar is credited
with using one of the first modern ciphers.

Cipher text:
ÒJºÊ-³¾~¿'|·)1â {Þ9æ/:¯Öó³ß
!¶äéj¶‚ ▬ä¶7ò9"Õ~Cöµ‚¶¿ÿ±ø:p*µ⊕
òg(♀  £ä6¦¹§ôÚ‚åÓðð>¶×í¾mËï¯♀'p9Z÷â?¼½r¹‚X«ë¶á'‚ëAòà?Î²°êºZªôûN¨ö‚¿ûË
¿²¬þq¢lÚ+¹ë\Át<÷
                ÔôÐÁ©´§{    ±©→wØ♣¼Äª§♫↔ú½;w|³ÿýì1¡?2¼öãÿñ¼²▬"äÓ·m¡→#
1îv¥    ‚ýùú¹ÿÝ/ é*î¿.ú86X´¬®ûrË»♠ö£ÞÍÎ8$þ¼ü³5 ¢▼:Öz♠°¶¼¦W¢¾ç¢³↨
·*Ì¼·ï·k5¡}ëGõ¿â½Åt»æp½±ô÷r¾;2⅓rôìw°#ò5v«¦û²ö·¡·5¦·ò¡¯o½å®;ã·6û9*£vtá§¨
¬»u¥ã¥ö$®ç¶ä¡º‚¹ñvm>ø/²vh³¤1µ¼¤µâv¡‚â²ýþðñøò¥ v2óá¹4ëåè0b⌂06å¯'µ§u±¡4´írö?¡ñ
2»æ1¤±ý¾ä÷x¶å® ¡äöñâïò¿¥°t¡p½tµà6æb=¿ö´ú·¤Ãò¥·¿r!» 2vù0«â°{!~ò·({7®¶¹ãá~·r
.½ôâá¾úô_4¢ÿ±òc¼}§'8íq±7?£ýñä§¶´4«à¡8á0ùæ6ÿ/<.ò¡î9óþ2©ã²0þ£¤¡õ²ö©vf÷³â³¹2¾éº
·b=¤b=¼± ÿ0°³þ¤ ï®¶¹´'®¥$·åòë¼i1¨táu¤±»â¬¡æ
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_Z> ▯
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_Z> python .\BT
18CSE041_Z_B.py 12345
Connected to server at 12345

Cipher text:
ÒJºÊ-³¾~¿'|·)1â {Þ9æ/:¯Öó³ß
!¶äéj¶‚ ▬ä¶7ò9"Õ~Cöµ‚¶¿ÿ±ø:p*µ⊕
òg(♀  £ä6¦¹§ôÚ‚åÓðð>¶×í¾mËï¯♀'p9Z÷â?¼½r¹‚X«ë¶á'‚ëAòà?Î²°êºZªôûN¨ö‚¿ûË
¿²¬þq¢lÚ+¹ë\Át<÷
                ÔôÐÁ©´§{    ±©→wØ♣¼Äª§♫↔ú½;w|³ÿýì1¡?2¼öãÿñ¼²▬"äÓ·m¡→#
1îv¥    ‚ýùú¹ÿÝ/ é*î¿.ú86X´¬®ûrË»♠ö£ÞÍÎ8$þ¼ü³5 ¢▼:Öz♠°¶¼¦W¢¾ç¢³↨
·*Ì¼·ï·k5¡}ëGõ¿â½Åt»æp½±ô÷r¾;2⅓rôìw°#ò5v«¦û²ö·¡·5¦·ò¡¯o½å®;ã·6û9*£vtá§¨
¬»u¥ã¥ö$®ç¶ä¡º‚¹ñvm>ø/²vh³¤1µ¼¤µâv¡‚â²ýþðñøò¥ v2óá¹4ëåè0b⌂06å¯'µ§u±¡4´írö?¡ñ
2»æ1¤±ý¾ä÷x¶å® ¡äöñâïò¿¥°t¡p½tµà6æb=¿ö´ú·¤Ãò¥·¿r!» 2vù0«â°{!~ò·({7®¶¹ãá~·r
.½ôâá¾úô_4¢ÿ±òc¼}§'8íq±7?£ýñä§¶´4«à¡8á0ùæ6ÿ/<.ò¡î9óþ2©ã²0þ£¤¡õ²ö©vf÷³â³¹2¾éº
·b=¤b=¼± ÿ0°³þ¤ ï®¶¹´'®¥$·åòë¼i1¨táu¤±»â¬¡æ

Sent text:
Cryptography is the study of secure communications techniques that allow onl
y the sender and intended recipient of amessage to view its contents. The te
rm is derived from the Greek word kryptos, which means hidden. It is closely
associated to encryption, which is the act of scrambling ordinary text into
what's known as ciphertext and thenback again upon arrival. In addition, cry
ptography also covers the obfuscation of information in images usingtechniqu
es such as microdots or merging. Ancient Egyptians were known to use these m
ethods in complex hieroglyphics,and Roman Emperor Julius Caesar is credited
with using one of the first modern ciphers.
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_Z> █
```

SE – A Cipher Block Chaining (CBC):

1. First run Alice program with port number as command line input.
   Ex: python BT18CSE041_SE_A_A.py 12345
2. Next run Bob program with the same port number as Alice as command line input.
   Ex: python BT18CSE041_SE_A_B.py 12345

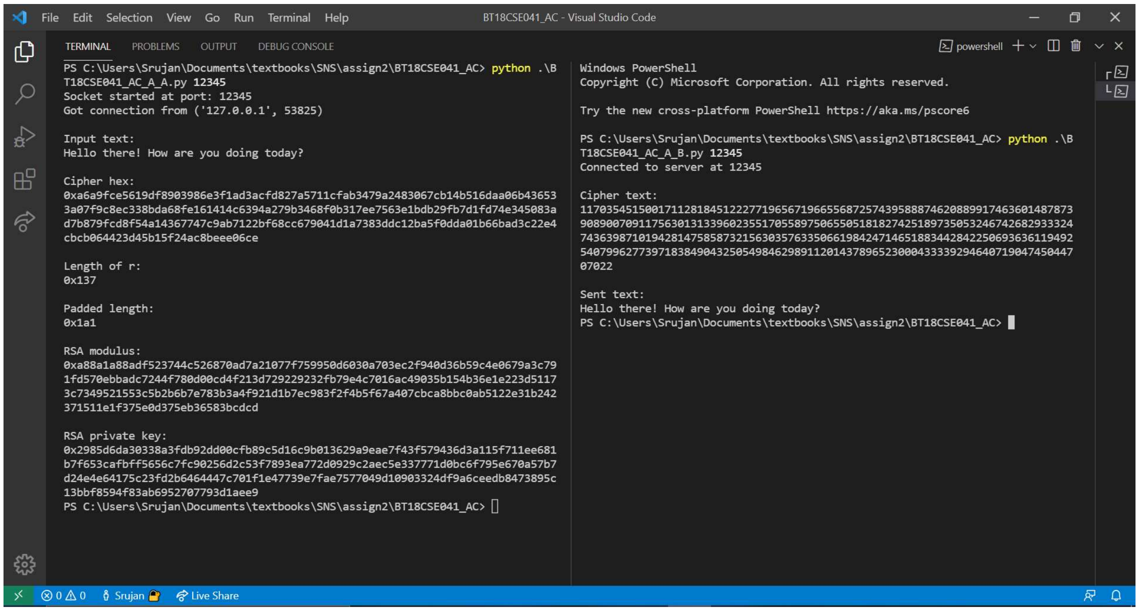


```
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_SE> python .\B
T18CSE041_SE_A_A.py 12345
Socket started at port: 12345
Got connection from ('127.0.0.1', 50513)

Input text:

Cryptography is the study of secure communications techniques that allow onl
y the sender and intended recipient of amessage to view its contents. The te
rm is derived from the Greek word kryptos, which means hidden. It is closely
associated to encryption, which is the act of scrambling ordinary text into
what's known as ciphertext and thenback again upon arrival. In addition, cry
ptography also covers the obfuscation of information in images usingtechniqu
es such as microdots or merging. Ancient Egyptians were known to use these m
ethods in complex hieroglyphics,and Roman Emperor Julius Caesar is credited
with using one of the first modern ciphers.

Cipher text:
c7+owh6Jx46C1poAHBcvww5QVlKnBCVZlGzwEsVR7qctpmOBBvLT5+jIEMC9EfNtFQjTAibtwnYh
693OFpJh7B1Eg4ORZmrR0TwlRZ3/fK2y+Ot9N5AHX+2rjJf5cGprGdGCzoXxMnmmP7XHYAaQvlne
7OywJfkdiN4/IovBcg4IG+2S+Wk7qabNUKAdrj6uhEhbj1JWzUEUkdLHbaCwn+dzlUkfy5ZJHjVK
XFLj+jeKdgS2RhNeWFuNLlwIBL8FWa3TtQg2krBx/iF6a8tp98sR7yrONjFJAtOb6e8vH50DYWQy
jtwGTOzzUyiIv079E1iDB6tPUdVzTyS4LlIjCxkapxiR+BZ4nfIzbfX9VPYg6ShvWkme72ubPSIH
zb+8i0Js99+t2pG398LCJuAe/f8wCRzYFIDLYhsCVsRoX0dBVJtkITyf8trsCij/cMnAxTFa4xfZ
Npcr/pH/1aZcrL3c8Xx+fdzxvdJv1zQnVDNAciaVHFhrxcvUmiwn/0NpsqGxPeLsylZFj1RwLev6
0ElqcOaRx2h7qzXvM+8DI/feD9cQSq1G0xRKyWTpbiN8PdVMp55vus/AkhaGTRiQQbj4u4mXLi7g
tMfwg4vP9bxso+4qvprGWZlUv1OPtjewLJ3DSYI+fm1sWFndOs8PNeh9klZIgXRa+Y9/iAdyH6Hj
ceqy2SuyidpxpT4voaIjaplQyR4pAwkj2IRNNYbbCbK8IgauLuql+JKVt1p0SMrcWUmlAbWkNA0V
54o754GRZjIePXd0Xpwlj33e4vvr7AxXKIsVBj9lbKxjFAS2xIAo5yz8+ERFiXkSTOYMsh3HNVBD
AskuoIkmObS1DmUuhFHcZfkSWF9AoDnVLd5eWe0=
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_SE> 
```

```
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_SE> python .\B
T18CSE041_SE_A_B.py 12345
Connected to server at 12345

Cipher text:
c7+owh6Jx46C1poAHBcvww5QVlKnBCVZlGzwEsVR7qctpmOBBvLT5+jIEMC9EfNtFQjTAibtwnYh
693OFpJh7B1Eg4ORZmrR0TwlRZ3/fK2y+Ot9N5AHX+2rjJf5cGprGdGCzoXxMnmmP7XHYAaQvlne
7OywJfkdiN4/IovBcg4IG+2S+Wk7qabNUKAdrj6uhEhbj1JWzUEUkdLHbaCwn+dzlUkfy5ZJHjVK
XFLj+jeKdgS2RhNeWFuNLlwIBL8FWa3TtQg2krBx/iF6a8tp98sR7yrONjFJAtOb6e8vH50DYWQy
jtwGTOzzUyiIv079E1iDB6tPUdVzTyS4LlIjCxkapxiR+BZ4nfIzbfX9VPYg6ShvWkme72ubPSIH
zb+8i0Js99+t2pG398LCJuAe/f8wCRzYFIDLYhsCVsRoX0dBVJtkITyf8trsCij/cMnAxTFa4xfZ
Npcr/pH/1aZcrL3c8Xx+fdzxvdJv1zQnVDNAciaVHFhrxcvUmiwn/0NpsqGxPeLsylZFj1RwLev6
0ElqcOaRx2h7qzXvM+8DI/feD9cQSq1G0xRKyWTpbiN8PdVMp55vus/AkhaGTRiQQbj4u4mXLi7g
tMfwg4vP9bxso+4qvprGWZlUv1OPtjewLJ3DSYI+fm1sWFndOs8PNeh9klZIgXRa+Y9/iAdyH6Hj
ceqy2SuyidpxpT4voaIjaplQyR4pAwkj2IRNNYbbCbK8IgauLuql+JKVt1p0SMrcWUmlAbWkNA0V
54o754GRZjIePXd0Xpwlj33e4vvr7AxXKIsVBj9lbKxjFAS2xIAo5yz8+ERFiXkSTOYMsh3HNVBD
AskuoIkmObS1DmUuhFHcZfkSWF9AoDnVLd5eWe0=

Sent text:

Cryptography is the study of secure communications techniques that allow onl
y the sender and intended recipient of amessage to view its contents. The te
rm is derived from the Greek word kryptos, which means hidden. It is closely
associated to encryption, which is the act of scrambling ordinary text into
what's known as ciphertext and thenback again upon arrival. In addition, cry
ptography also covers the obfuscation of information in images usingtechniqu
es such as microdots or merging. Ancient Egyptians were known to use these m
ethods in complex hieroglyphics,and Roman Emperor Julius Caesar is credited
with using one of the first modern ciphers.
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_SE> 
```

AC – A OAEP construction of RSA:

1. First run Alice program with port number as command line input.
   Ex: python BT18CSE041_AC_A_A.py 12345
2. Next run Bob program with the same port number as Alice as command line input.
   Ex: python BT18CSE041_AC_A_B.py 12345

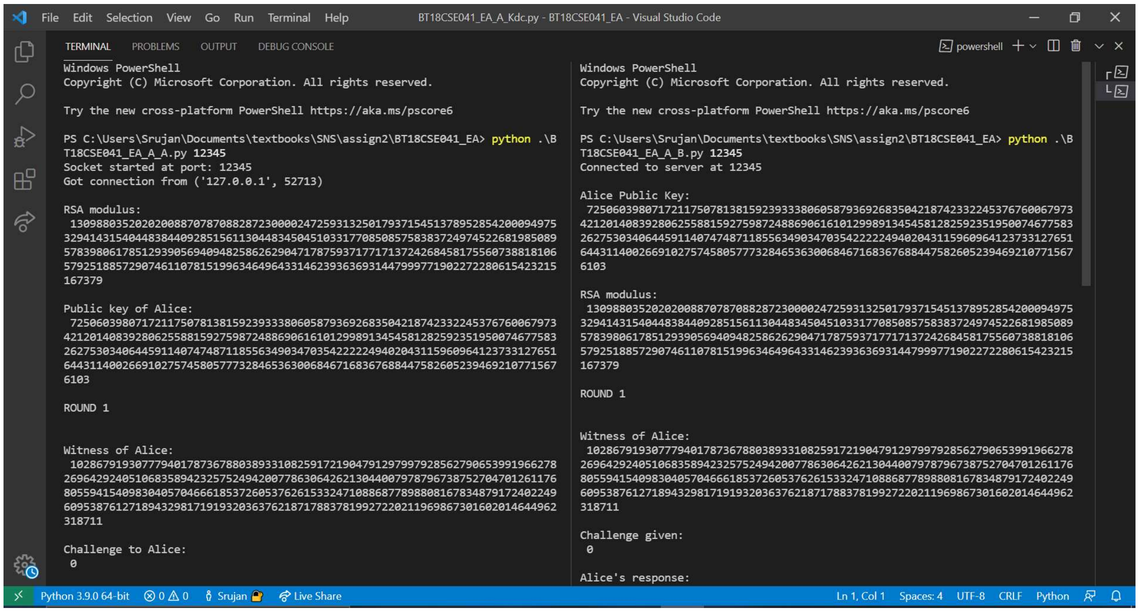


```
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_AC> python .\B
T18CSE041_AC_A_A.py 12345
Socket started at port: 12345
Got connection from ('127.0.0.1', 53825)

Input text:
Hello there! How are you doing today?

Cipher hex:
0xa6a9fce5619df8903986e3f1ad3acfd827a5711cfab3479a2483067cb14b516daa06b43653
3a07f9c8ec338bda68fe161414c6394a279b3468f0b317ee7563e1bdb29fb7d1fd74e345083a
d7b879fcd8f54a14367747c9ab7122bf68cc679041d1a7383ddc12ba5f0dda01b66bad3c22e4
cbcb064423d45b15f24ac8beee06ce

Length of r:
0x137

Padded length:
0x1a1

RSA modulus:
0xa88a1a88adf523744c526870ad7a21077f759950d6030a703ec2f940d36b59c4e0679a3c79
1fd570ebbadc7244f780d00cd4f213d729229232fb79e4c7016ac49035b154b36e1e223d5117
3c7349521553c5b2b6b7e783b3a4f921d1b7ec983f2f4b5f67a407cbca8bbc0ab5122e31b242
371511e1f375e0d375eb36583bcdcd

RSA private key:
0x2985d6da30338a3fdb92dd00cfb89c5d16c9b013629a9eae7f43f579436d3a115f711ee681
b7f653cafbff5656c7fc90256d2c53f7893ea772d0929c2aec5e337771d0bc6f795e670a57b7
d24e4e64175c23fd2b6464447c701f1e47739e7fae7577049d10903324df9a6ceedb8473895c
13bbf8594f83ab6952707793d1aee9
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_AC> 
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_AC> python .\B
T18CSE041_AC_A_B.py 12345
Connected to server at 12345

Cipher text:
1170354515001711281845122277196567196655687257439588874620889917463601487873
9089007091175630131339602355170558975065505181827425189735053246742682933324
7436398710194281475858732156303576335066198424714651883442842250693636119492
5407996277397183849043250549846298911201437896523000433339294640719047450447
07022

Sent text:
Hello there! How are you doing today?
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_AC> 
```

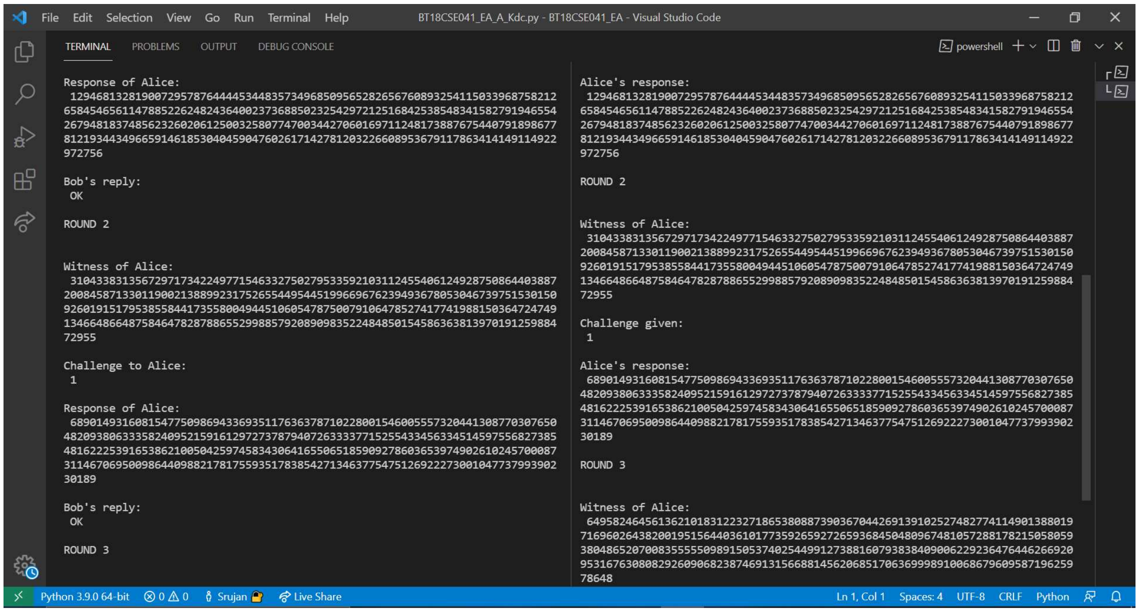
EA – A Fiat-Shamir Protocol:

1. First run Alice program with port number as command line input.
   Ex: python BT18CSE041_EA_A_A.py 12345
2. Next run Bob program with the same port number as Alice as command line input.
   Ex: python BT18CSE041_EA_A_B.py 12345


File Edit Selection View Go Run Terminal Help
BT18CSE041_EA_A_Kdc.py - BT18CSE041_EA - Visual Studio Code
TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE
powershell
Python 3.9.0 64-bit ⊗ 0 ⚠ 0 Srujan Live Share
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF Python

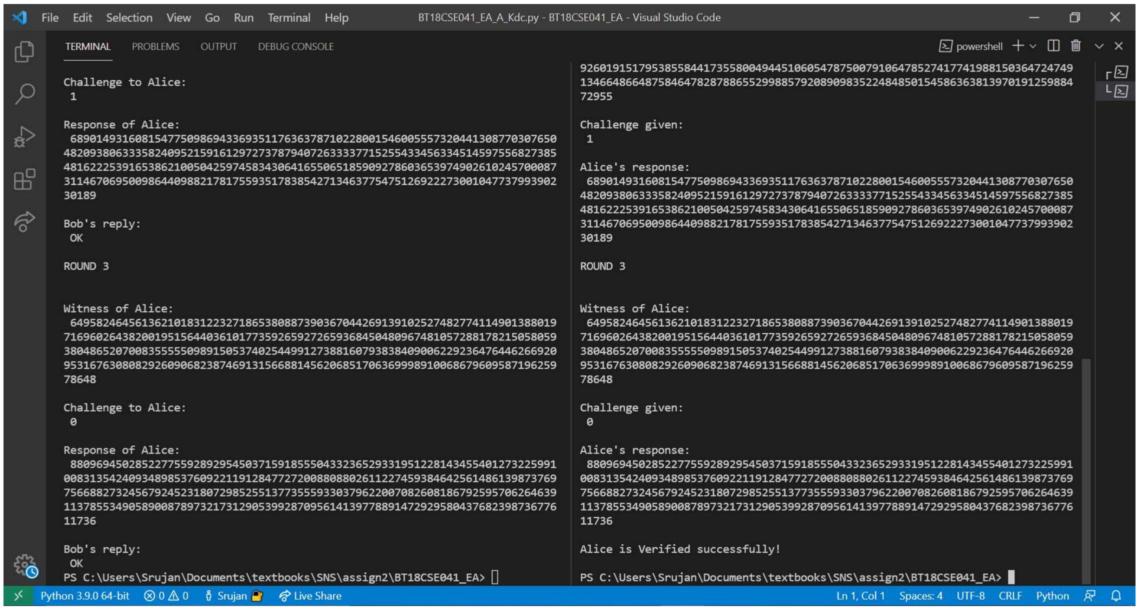
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_EA> python .\B
T18CSE041_EA_A_A.py 12345
Socket started at port: 12345
Got connection from ('127.0.0.1', 52713)

RSA modulus:
 130988035202020088707870882872300002472593132501793715451378952854200094975
3294143154044838440928515611304483450451033177085085758383724974522681985089
5783980617851293905694094825862629047178759371771713724268458175560738818106
5792518857290746110781519963464964331462393636931447999771902272280615423215
167379

Public key of Alice:
 725060398071721175078138159239333806058793692683504218742332245376760067973
4212014083928062558815927598724886906161012998913454581282592351950074677583
2627530340644591140747487118556349034703542222249402043115960964123733127651
6443114002669102757458057773284653630068467168367688447582605239469210771567
6103

ROUND 1


Witness of Alice:
 102867919307779401787367880389331082591721904791297997928562790653991966278
2696429240510683589423257524942007786306426213044007978796738752704701261176
8055941540983040570466618537260537626153324710886877898808167834879172402249
6095387612718943298171919320363762187178837819927220211969867301602014644962
318711

Challenge to Alice:
 0
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_EA> python .\B
T18CSE041_EA_A_B.py 12345
Connected to server at 12345

Alice Public Key:
 725060398071721175078138159239333806058793692683504218742332245376760067973
4212014083928062558815927598724886906161012998913454581282592351950074677583
2627530340644591140747487118556349034703542222249402043115960964123733127651
6443114002669102757458057773284653630068467168367688447582605239469210771567
6103

RSA modulus:
 130988035202020088707870882872300002472593132501793715451378952854200094975
3294143154044838440928515611304483450451033177085085758383724974522681985089
5783980617851293905694094825862629047178759371771713724268458175560738818106
5792518857290746110781519963464964331462393636931447999771902272280615423215
167379

ROUND 1


Witness of Alice:
 102867919307779401787367880389331082591721904791297997928562790653991966278
2696429240510683589423257524942007786306426213044007978796738752704701261176
8055941540983040570466618537260537626153324710886877898808167834879172402249
6095387612718943298171919320363762187178837819927220211969867301602014644962
318711

Challenge given:
 0

Alice's response:
```


File Edit Selection View Go Run Terminal Help
BT18CSE041_EA_A_Kdc.py - BT18CSE041_EA - Visual Studio Code
TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE
powershell
Python 3.9.0 64-bit ⊗ 0 ⚠ 0 Srujan Live Share
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF Python

```
Response of Alice:
 129468132819007295787644445344835734968509565282656760893254115033968758212
6584546561147885226248243640023736885023254297212516842538548341582791946554
2679481837485623260206125003258077470034427060169711248173887675440791898677
8121934434966591461853040459047602617142781203226608953679117863414149114922
972756

Bob's reply:
 OK

ROUND 2


Witness of Alice:
 310433831356729717342249771546332750279533592103112455406124928750864403887
2008458713301190021388992317526554495445199669676239493678053046739751530150
9260191517953855844173558004944510605478750079106478527417741988150364724749
1346648664875846478287886552998857920890983522484850154586363813970191259884
72955

Challenge to Alice:
 1

Response of Alice:
 689014931608154775098694336935117636378710228001546005557320441308770307650
4820938063335824095215916129727378794072633337715255433456334514597556827385
4816222539165386210050425974583430641655065185909278603653974902610245700087
3114670695009864409882178175593517838542713463775475126922273001047737993902
30189

Bob's reply:
 OK

ROUND 3
```

```
Alice's response:
 129468132819007295787644445344835734968509565282656760893254115033968758212
6584546561147885226248243640023736885023254297212516842538548341582791946554
2679481837485623260206125003258077470034427060169711248173887675440791898677
8121934434966591461853040459047602617142781203226608953679117863414149114922
972756

ROUND 2


Witness of Alice:
 310433831356729717342249771546332750279533592103112455406124928750864403887
2008458713301190021388992317526554495445199669676239493678053046739751530150
9260191517953855844173558004944510605478750079106478527417741988150364724749
1346648664875846478287886552998857920890983522484850154586363813970191259884
72955

Challenge given:
 1

Alice's response:
 689014931608154775098694336935117636378710228001546005557320441308770307650
4820938063335824095215916129727378794072633337715255433456334514597556827385
4816222539165386210050425974583430641655065185909278603653974902610245700087
3114670695009864409882178175593517838542713463775475126922273001047737993902
30189

ROUND 3


Witness of Alice:
 649582464561362101831223271865380887390367044269139102527482774114901388019
7169602643820019515644036101773592659272659368450480967481057288178215058059
3804865207008355555098915053740254499127388160793838409006229236476446266920
9531676308082926090682387469131566881456206851706369998910068679609587196259
78648
```

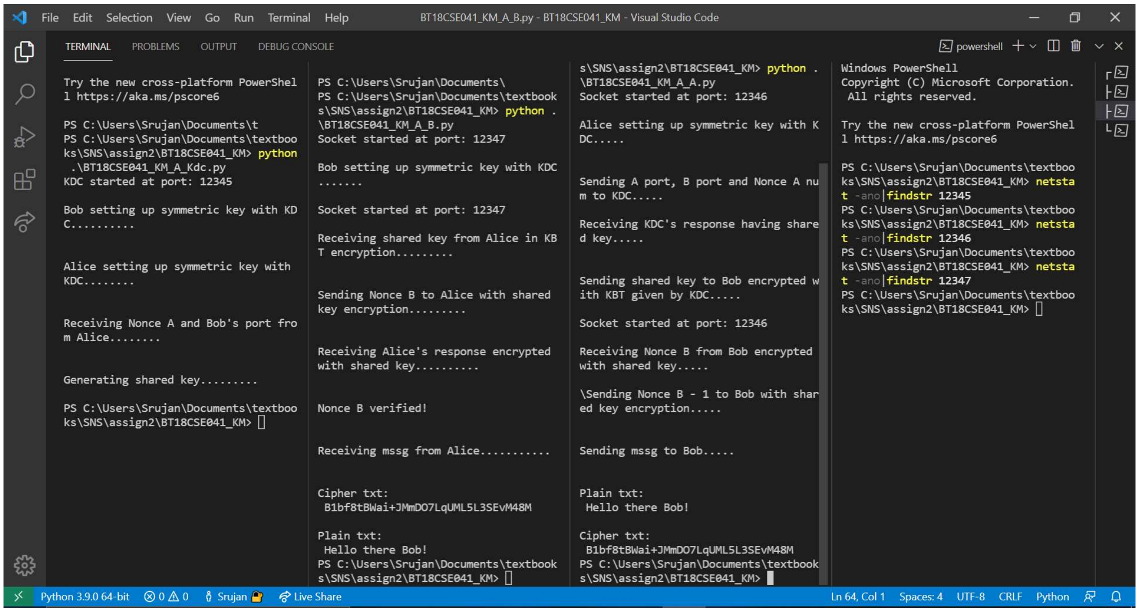

File Edit Selection View Go Run Terminal Help
BT18CSE041_EA_A_Kdc.py - BT18CSE041_EA - Visual Studio Code
TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE
powershell
Python 3.9.0 64-bit ⊗ 0 ⚠ 0 Srujan Live Share
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF Python

```
Challenge to Alice:
 1

Response of Alice:
 689014931608154775098694336935117636378710228001546005557320441308770307650
4820938063335824095215916129727378794072633337715255433456334514597556827385
4816222539165386210050425974583430641655065185909278603653974902610245700087
3114670695009864409882178175593517838542713463775475126922273001047737993902
30189

Bob's reply:
 OK

ROUND 3


Witness of Alice:
 649582464561362101831223271865380887390367044269139102527482774114901388019
7169602643820019515644036101773592659272659368450480967481057288178215058059
3804865207008355555098915053740254499127388160793838409006229236476446266920
9531676308082926090682387469131566881456206851706369998910068679609587196259
78648

Challenge to Alice:
 0

Response of Alice:
 880969450285227755928929545037159185550433236529331951228143455401273225991
0083135424093489853760922119128477272008808802611227459384642561486139873769
7566882732456792452318072985255137735559330379622007082608186792595706264639
1137855349058900878973217312905399287095614139778891472929580437682398736776
11736

Bob's reply:
 OK
PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_EA> 
```

```
9260191517953855844173558004944510605478750079106478527417741988150364724749
1346648664875846478287886552998857920890983522484850154586363813970191259884
72955

Challenge given:
 1

Alice's response:
 689014931608154775098694336935117636378710228001546005557320441308770307650
4820938063335824095215916129727378794072633337715255433456334514597556827385
4816222539165386210050425974583430641655065185909278603653974902610245700087
3114670695009864409882178175593517838542713463775475126922273001047737993902
30189

ROUND 3


Witness of Alice:
 649582464561362101831223271865380887390367044269139102527482774114901388019
7169602643820019515644036101773592659272659368450480967481057288178215058059
3804865207008355555098915053740254499127388160793838409006229236476446266920
9531676308082926090682387469131566881456206851706369998910068679609587196259
78648

Challenge given:
 0

Alice's response:
 880969450285227755928929545037159185550433236529331951228143455401273225991
0083135424093489853760922119128477272008808802611227459384642561486139873769
7566882732456792452318072985255137735559330379622007082608186792595706264639
1137855349058900878973217312905399287095614139778891472929580437682398736776
11736

Alice is Verified successfully!

PS C:\Users\Srujan\Documents\textbooks\SNS\assign2\BT18CSE041_EA> 
```

KM – A Needham - Schroeder Protocol:

1. First check whether the port numbers 12345 (KDC program), 12346 (Alice program) and 12347 (Bob program) are free or not.
   Ex: netstat -ano|findstr 12345 , if any process with pid present can stop it using – kill pid
2. Run the KDC program.
   Ex: python BT18CSE041_KM_A_Kdc.py
3. Run the Bob program.
   Ex: python BT18CSE041_KM_A_B.py
4. Run the Alice program.
   Ex: python BT18CSE041_KM_A_A.py



```
Try the new cross-platform PowerShel
l https://aka.ms/pscore6

PS C:\Users\Srujan\Documents\t
PS C:\Users\Srujan\Documents\textboo
ks\SNS\assign2\BT18CSE041_KM> python
 .\BT18CSE041_KM_A_Kdc.py
KDC started at port: 12345

Bob setting up symmetric key with KD
C..........


Alice setting up symmetric key with
KDC........


Receiving Nonce A and Bob's port fro
m Alice........


Generating shared key.........

PS C:\Users\Srujan\Documents\textboo
ks\SNS\assign2\BT18CSE041_KM> ▯
```

```
PS C:\Users\Srujan\Documents\
PS C:\Users\Srujan\Documents\textbook
s\SNS\assign2\BT18CSE041_KM> python .
\BT18CSE041_KM_A_B.py
Socket started at port: 12347

Bob setting up symmetric key with KDC
.......

Socket started at port: 12347

Receiving shared key from Alice in KB
T encryption.........


Sending Nonce B to Alice with shared
key encryption.........


Receiving Alice's response encrypted
with shared key..........


Nonce B verified!


Receiving mssg from Alice...........


Cipher txt:
 B1bf8tBWai+JMmDO7LqUML5L3SEvM48M

Plain txt:
 Hello there Bob!
PS C:\Users\Srujan\Documents\textbook
s\SNS\assign2\BT18CSE041_KM> ▯
```

```
s\SNS\assign2\BT18CSE041_KM> python .
\BT18CSE041_KM_A_A.py
Socket started at port: 12346

Alice setting up symmetric key with K
DC.....


Sending A port, B port and Nonce A nu
m to KDC.....

Receiving KDC's response having share
d key.....


Sending shared key to Bob encrypted w
ith KBT given by KDC.....

Socket started at port: 12346

Receiving Nonce B from Bob encrypted
with shared key.....

\Sending Nonce B - 1 to Bob with shar
ed key encryption.....


Sending mssg to Bob.....


Plain txt:
 Hello there Bob!

Cipher txt:
 B1bf8tBWai+JMmDO7LqUML5L3SEvM48M
PS C:\Users\Srujan\Documents\textbook
s\SNS\assign2\BT18CSE041_KM> █
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation.
 All rights reserved.

Try the new cross-platform PowerShel
l https://aka.ms/pscore6

PS C:\Users\Srujan\Documents\textboo
ks\SNS\assign2\BT18CSE041_KM> netsta
t -ano|findstr 12345
PS C:\Users\Srujan\Documents\textboo
ks\SNS\assign2\BT18CSE041_KM> netsta
t -ano|findstr 12346
PS C:\Users\Srujan\Documents\textboo
ks\SNS\assign2\BT18CSE041_KM> netsta
t -ano|findstr 12347
PS C:\Users\Srujan\Documents\textboo
ks\SNS\assign2\BT18CSE041_KM> ▯
```