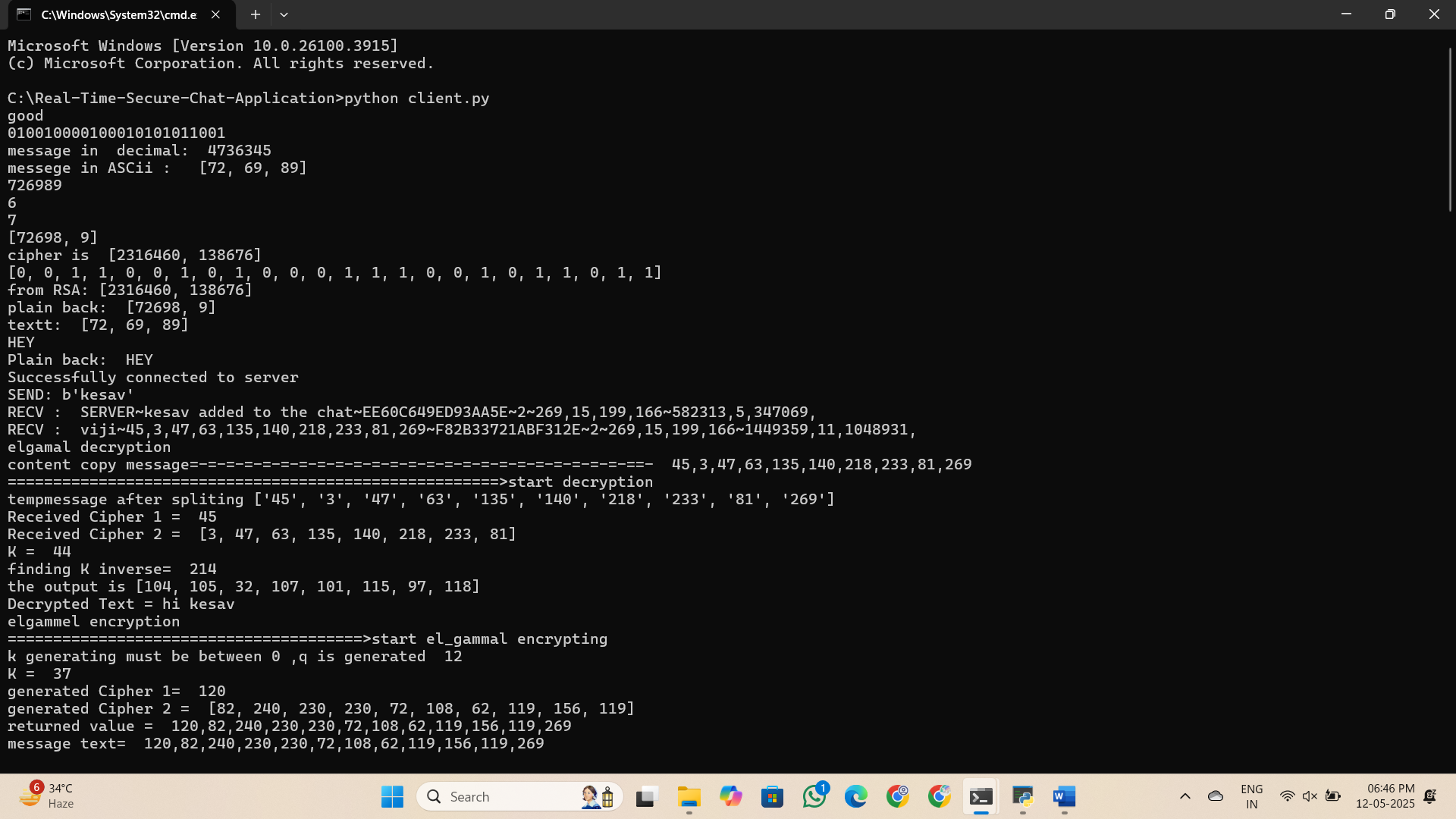
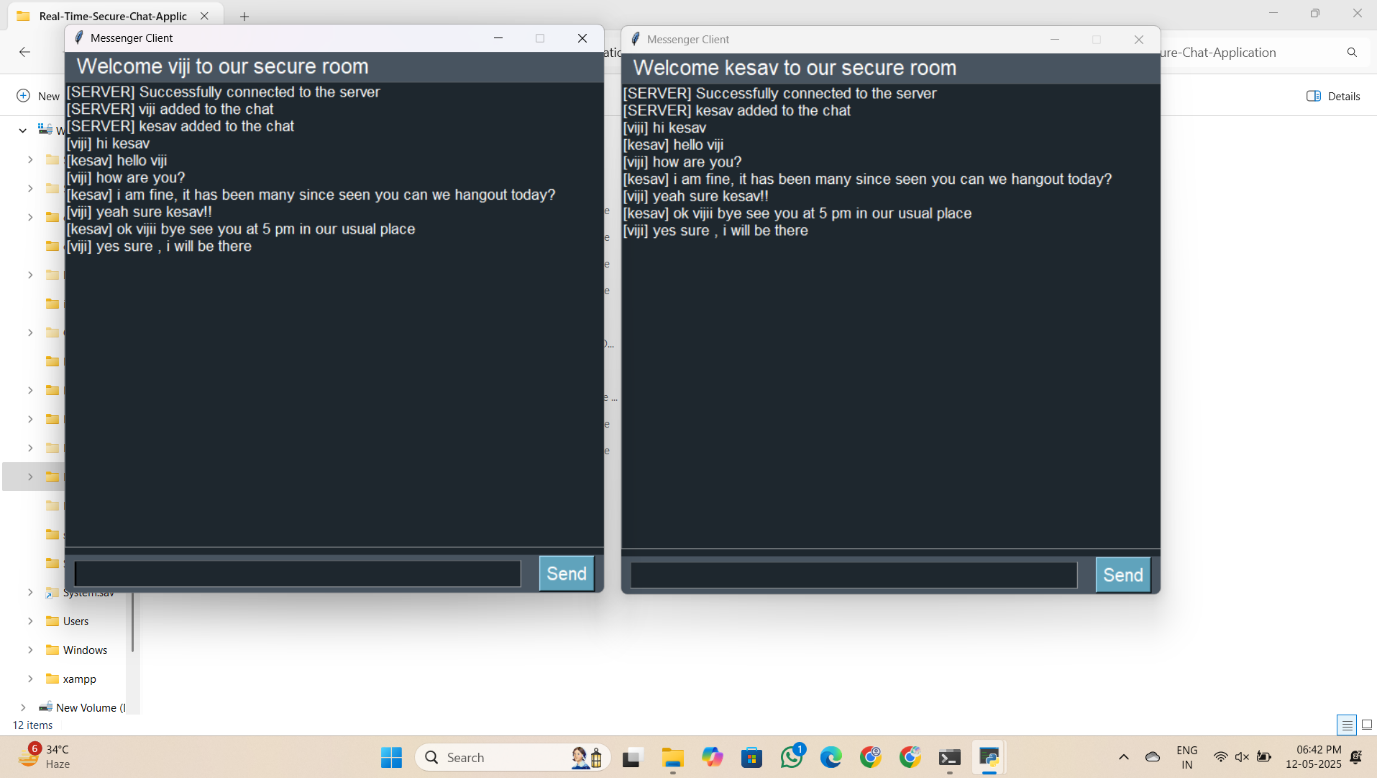
REAL TIME SECURE CHAT E2EE CONNECTION



OUTPUT :



C:\Real-Time-Secure-Chat-Application>python server.py

good

010010000100010101011001

message in decimal: 4736345

messege in ASCii : [72, 69, 89]

726989

6

7

[72698, 9]

cipher is [2316460, 138676]

[0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1]

from RSA: [2316460, 138676]

plain back: [72698, 9]

textt: [72, 69, 89]

HEY

Plain back: HEY

prime random number q generated 269

finding primitive number for the prime number q

15

private key XA is generated= 166

public key YA is generated= 199

---------Welcome to our secure chat

1- DES (Data encryption standard)

2- ElGamal encryption system

3- RSA (Rivest–Shamir–Adleman)

Choose the encryption system: 2

ELGAMAL mode has been started

Running the server on 0.0.0.0 8080

Successfully connected to client 127.0.0.1 64996

RECV : viji

good

public and private key paramters:

n: 1449359

E: 11

D: 1048931

elgamal public key 269,15,199,166

SEND : b'SERVER~viji added to the chat~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

Sessison key successfully generated for viji ==> F82B33721ABF312E

Successfully connected to client 127.0.0.1 64997

RECV : kesav

good

public and private key paramters:

n: 582313

E: 5

D: 347069

elgamal public key 269,15,199,166

SEND : b'SERVER~kesav added to the chat~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

SEND : b'SERVER~kesav added to the chat~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

Sessison key successfully generated for kesav ==> EE60C649ED93AA5E

RECV : 45,3,47,63,135,140,218,233,81,269

SEND : b'viji~45,3,47,63,135,140,218,233,81,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

SEND : b'viji~45,3,47,63,135,140,218,233,81,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

rsaaaaaaa: viji~45,3,47,63,135,140,218,233,81,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

RECV : 120,82,240,230,230,72,108,62,119,156,119,269

SEND : b'kesav~120,82,240,230,230,72,108,62,119,156,119,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

SEND : b'kesav~120,82,240,230,230,72,108,62,119,156,119,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

rsaaaaaaa: kesav~120,82,240,230,230,72,108,62,119,156,119,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

RECV : 202,167,186,54,10,148,2,82,10,21,186,87,171,269

SEND : b'viji~202,167,186,54,10,148,2,82,10,21,186,87,171,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

SEND : b'viji~202,167,186,54,10,148,2,82,10,21,186,87,171,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

rsaaaaaaa: viji~202,167,186,54,10,148,2,82,10,21,186,87,171,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

RECV : 252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269

SEND : b'kesav~252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

SEND : b'kesav~252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

rsaaaaaaa: kesav~252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

RECV : 147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269

SEND : b'viji~147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

SEND : b'viji~147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

rsaaaaaaa: viji~147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

RECV : 253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269

SEND : b'kesav~253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

SEND : b'kesav~253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,'

rsaaaaaaa: kesav~253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

RECV : 144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269

SEND : b'viji~144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

SEND : b'viji~144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,'

rsaaaaaaa: viji~144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

1.ON CLIENT SIDE [VIJI]

Real-Time-Secure-Chat-Application>python client.py

good

010010000100010101011001

message in decimal: 4736345

messege in ASCii : [72, 69, 89]

726989

6

6

[7269, 89]

cipher is [330677, 260092]

[0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1]

from RSA: [330677, 260092]

plain back: [7269, 89]

textt: [72, 69, 89]

HEY

Plain back: HEY

Successfully connected to server

SEND: b'viji'

RECV : SERVER~viji added to the chat~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

RECV : SERVER~kesav added to the chat~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 222

K = 44

generated Cipher 1= 45

generated Cipher 2 = [3, 47, 63, 135, 140, 218, 233, 81]

returned value = 45,3,47,63,135,140,218,233,81,269

message text= 45,3,47,63,135,140,218,233,81,269

SEND : b'45,3,47,63,135,140,218,233,81,269'

This message has been delivered

RECV : viji~45,3,47,63,135,140,218,233,81,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 45,3,47,63,135,140,218,233,81,269

======================================================>start decryption

tempmessage after spliting ['45', '3', '47', '63', '135', '140', '218', '233', '81', '269']

Received Cipher 1 = 45

Received Cipher 2 = [3, 47, 63, 135, 140, 218, 233, 81]

K = 44

finding K inverse= 214

the output is [104, 105, 32, 107, 101, 115, 97, 118]

Decrypted Text = hi kesav

RECV : kesav~120,82,240,230,230,72,108,62,119,156,119,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 120,82,240,230,230,72,108,62,119,156,119,269

======================================================>start decryption

tempmessage after spliting ['120', '82', '240', '230', '230', '72', '108', '62', '119', '156', '119', '269']

Received Cipher 1 = 120

Received Cipher 2 = [82, 240, 230, 230, 72, 108, 62, 119, 156, 119]

K = 37

finding K inverse= 80

the output is [104, 101, 108, 108, 111, 32, 118, 105, 106, 105]

Decrypted Text = hello viji

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 82

K = 118

generated Cipher 1= 202

generated Cipher 2 = [167, 186, 54, 10, 148, 2, 82, 10, 21, 186, 87, 171]

returned value = 202,167,186,54,10,148,2,82,10,21,186,87,171,269

message text= 202,167,186,54,10,148,2,82,10,21,186,87,171,269

SEND : b'202,167,186,54,10,148,2,82,10,21,186,87,171,269'

This message has been delivered

RECV : viji~202,167,186,54,10,148,2,82,10,21,186,87,171,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 202,167,186,54,10,148,2,82,10,21,186,87,171,269

======================================================>start decryption

tempmessage after spliting ['202', '167', '186', '54', '10', '148', '2', '82', '10', '21', '186', '87', '171', '269']

Received Cipher 1 = 202

Received Cipher 2 = [167, 186, 54, 10, 148, 2, 82, 10, 21, 186, 87, 171]

K = 118

finding K inverse= 57

the output is [104, 111, 119, 32, 97, 114, 101, 32, 121, 111, 117, 63]

Decrypted Text = how are you?

RECV : kesav~252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269

======================================================>start decryption

tempmessage after spliting ['252', '189', '219', '67', '250', '219', '76', '189', '198', '128', '133', '219', '189', '155', '219', '241', '67', '207', '219', '15', '128', '128', '198', '219', '250', '67', '198', '164', '219', '207', '189', '198', '232', '128', '219', '207', '128', '128', '198', '219', '164', '146', '103', '219', '232', '67', '198', '219', '268', '128', '219', '241', '67', '198', '24', '146', '103', '155', '219', '155', '146', '180', '67', '164', '221', '269']

Received Cipher 1 = 252

Received Cipher 2 = [189, 219, 67, 250, 219, 76, 189, 198, 128, 133, 219, 189, 155, 219, 241, 67, 207, 219, 15, 128, 128, 198, 219, 250, 67, 198, 164, 219, 207, 189, 198, 232, 128, 219, 207, 128, 128, 198, 219, 164, 146, 103, 219, 232, 67, 198, 219, 268, 128, 219, 241, 67, 198, 24, 146, 103, 155, 219, 155, 146, 180, 67, 164, 221]

K = 217

finding K inverse= 150

the output is [105, 32, 97, 109, 32, 102, 105, 110, 101, 44, 32, 105, 116, 32, 104, 97, 115, 32, 98, 101, 101, 110, 32, 109, 97, 110, 121, 32, 115, 105, 110, 99, 101, 32, 115, 101, 101, 110, 32, 121, 111, 117, 32, 99, 97, 110, 32, 119, 101, 32, 104, 97, 110, 103, 111, 117, 116, 32, 116, 111, 100, 97, 121, 63]

Decrypted Text = i am fine, it has been many since seen you can we hangout today?

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 3

K = 244

generated Cipher 1= 147

generated Cipher 2 = [203, 165, 265, 90, 7, 84, 34, 109, 165, 7, 15, 165, 84, 265, 9, 251, 251]

returned value = 147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269

message text= 147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269

SEND : b'147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269'

This message has been delivered

RECV : viji~147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269

======================================================>start decryption

tempmessage after spliting ['147', '203', '165', '265', '90', '7', '84', '34', '109', '165', '7', '15', '165', '84', '265', '9', '251', '251', '269']

Received Cipher 1 = 147

Received Cipher 2 = [203, 165, 265, 90, 7, 84, 34, 109, 165, 7, 15, 165, 84, 265, 9, 251, 251]

K = 244

finding K inverse= 43

the output is [121, 101, 97, 104, 32, 115, 117, 114, 101, 32, 107, 101, 115, 97, 118, 33, 33]

Decrypted Text = yeah sure kesav!!

RECV : kesav~253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269

======================================================>start decryption

tempmessage after spliting ['253', '179', '95', '134', '57', '53', '74', '53', '53', '134', '175', '120', '238', '134', '263', '238', '238', '134', '120', '179', '36', '134', '154', '15', '134', '37', '134', '200', '137', '134', '53', '158', '134', '179', '36', '242', '134', '36', '263', '36', '154', '116', '134', '200', '116', '154', '196', '238', '269']

Received Cipher 1 = 253

Received Cipher 2 = [179, 95, 134, 57, 53, 74, 53, 53, 134, 175, 120, 238, 134, 263, 238, 238, 134, 120, 179, 36, 134, 154, 15, 134, 37, 134, 200, 137, 134, 53, 158, 134, 179, 36, 242, 134, 36, 263, 36, 154, 116, 134, 200, 116, 154, 196, 238]

K = 21

finding K inverse= 205

the output is [111, 107, 32, 118, 105, 106, 105, 105, 32, 98, 121, 101, 32, 115, 101, 101, 32, 121, 111, 117, 32, 97, 116, 32, 53, 32, 112, 109, 32, 105, 110, 32, 111, 117, 114, 32, 117, 115, 117, 97, 108, 32, 112, 108, 97, 99, 101]

Decrypted Text = ok vijii bye see you at 5 pm in our usual place

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 10

K = 265

generated Cipher 1= 144

generated Cipher 2 = [54, 134, 78, 141, 78, 70, 82, 134, 141, 93, 141, 118, 141, 62, 118, 106, 106, 141, 146, 134, 141, 74, 122, 134, 82, 134]

returned value = 144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269

message text= 144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269

SEND : b'144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269'

This message has been delivered

RECV : viji~144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269

======================================================>start decryption

tempmessage after spliting ['144', '54', '134', '78', '141', '78', '70', '82', '134', '141', '93', '141', '118', '141', '62', '118', '106', '106', '141', '146', '134', '141', '74', '122', '134', '82', '134', '269']

Received Cipher 1 = 144

Received Cipher 2 = [54, 134, 78, 141, 78, 70, 82, 134, 141, 93, 141, 118, 141, 62, 118, 106, 106, 141, 146, 134, 141, 74, 122, 134, 82, 134]

K = 265

finding K inverse= 67

the output is [121, 101, 115, 32, 115, 117, 114, 101, 32, 44, 32, 105, 32, 119, 105, 108, 108, 32, 98, 101, 32, 116, 104, 101, 114, 101]

Decrypted Text = yes sure , i will be there

2.ON CLIENT SIDE [KESAV]

C:\Real-Time-Secure-Chat-Application>python client.py

good

010010000100010101011001

message in decimal: 4736345

messege in ASCii : [72, 69, 89]

726989

6

7

[72698, 9]

cipher is [2316460, 138676]

[0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1]

from RSA: [2316460, 138676]

plain back: [72698, 9]

textt: [72, 69, 89]

HEY

Plain back: HEY

Successfully connected to server

SEND: b'kesav'

RECV : SERVER~kesav added to the chat~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

RECV : viji~45,3,47,63,135,140,218,233,81,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 45,3,47,63,135,140,218,233,81,269

======================================================>start decryption

tempmessage after spliting ['45', '3', '47', '63', '135', '140', '218', '233', '81', '269']

Received Cipher 1 = 45

Received Cipher 2 = [3, 47, 63, 135, 140, 218, 233, 81]

K = 44

finding K inverse= 214

the output is [104, 105, 32, 107, 101, 115, 97, 118]

Decrypted Text = hi kesav

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 12

K = 37

generated Cipher 1= 120

generated Cipher 2 = [82, 240, 230, 230, 72, 108, 62, 119, 156, 119]

returned value = 120,82,240,230,230,72,108,62,119,156,119,269

message text= 120,82,240,230,230,72,108,62,119,156,119,269

SEND : b'120,82,240,230,230,72,108,62,119,156,119,269'

This message has been delivered

RECV : kesav~120,82,240,230,230,72,108,62,119,156,119,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 120,82,240,230,230,72,108,62,119,156,119,269

======================================================>start decryption

tempmessage after spliting ['120', '82', '240', '230', '230', '72', '108', '62', '119', '156', '119', '269']

Received Cipher 1 = 120

Received Cipher 2 = [82, 240, 230, 230, 72, 108, 62, 119, 156, 119]

K = 37

finding K inverse= 80

the output is [104, 101, 108, 108, 111, 32, 118, 105, 106, 105]

Decrypted Text = hello viji

RECV : viji~202,167,186,54,10,148,2,82,10,21,186,87,171,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 202,167,186,54,10,148,2,82,10,21,186,87,171,269

======================================================>start decryption

tempmessage after spliting ['202', '167', '186', '54', '10', '148', '2', '82', '10', '21', '186', '87', '171', '269']

Received Cipher 1 = 202

Received Cipher 2 = [167, 186, 54, 10, 148, 2, 82, 10, 21, 186, 87, 171]

K = 118

finding K inverse= 57

the output is [104, 111, 119, 32, 97, 114, 101, 32, 121, 111, 117, 63]

Decrypted Text = how are you?

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 251

K = 217

generated Cipher 1= 252

generated Cipher 2 = [189, 219, 67, 250, 219, 76, 189, 198, 128, 133, 219, 189, 155, 219, 241, 67, 207, 219, 15, 128, 128, 198, 219, 250, 67, 198, 164, 219, 207, 189, 198, 232, 128, 219, 207, 128, 128, 198, 219, 164, 146, 103, 219, 232, 67, 198, 219, 268, 128, 219, 241, 67, 198, 24, 146, 103, 155, 219, 155, 146, 180, 67, 164, 221]

returned value = 252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269

message text= 252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269

SEND : b'252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269'

This message has been delivered

RECV : kesav~252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 252,189,219,67,250,219,76,189,198,128,133,219,189,155,219,241,67,207,219,15,128,128,198,219,250,67,198,164,219,207,189,198,232,128,219,207,128,128,198,219,164,146,103,219,232,67,198,219,268,128,219,241,67,198,24,146,103,155,219,155,146,180,67,164,221,269

======================================================>start decryption

tempmessage after spliting ['252', '189', '219', '67', '250', '219', '76', '189', '198', '128', '133', '219', '189', '155', '219', '241', '67', '207', '219', '15', '128', '128', '198', '219', '250', '67', '198', '164', '219', '207', '189', '198', '232', '128', '219', '207', '128', '128', '198', '219', '164', '146', '103', '219', '232', '67', '198', '219', '268', '128', '219', '241', '67', '198', '24', '146', '103', '155', '219', '155', '146', '180', '67', '164', '221', '269']

Received Cipher 1 = 252

Received Cipher 2 = [189, 219, 67, 250, 219, 76, 189, 198, 128, 133, 219, 189, 155, 219, 241, 67, 207, 219, 15, 128, 128, 198, 219, 250, 67, 198, 164, 219, 207, 189, 198, 232, 128, 219, 207, 128, 128, 198, 219, 164, 146, 103, 219, 232, 67, 198, 219, 268, 128, 219, 241, 67, 198, 24, 146, 103, 155, 219, 155, 146, 180, 67, 164, 221]

K = 217

finding K inverse= 150

the output is [105, 32, 97, 109, 32, 102, 105, 110, 101, 44, 32, 105, 116, 32, 104, 97, 115, 32, 98, 101, 101, 110, 32, 109, 97, 110, 121, 32, 115, 105, 110, 99, 101, 32, 115, 101, 101, 110, 32, 121, 111, 117, 32, 99, 97, 110, 32, 119, 101, 32, 104, 97, 110, 103, 111, 117, 116, 32, 116, 111, 100, 97, 121, 63]

Decrypted Text = i am fine, it has been many since seen you can we hangout today?

RECV : viji~147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 147,203,165,265,90,7,84,34,109,165,7,15,165,84,265,9,251,251,269

======================================================>start decryption

tempmessage after spliting ['147', '203', '165', '265', '90', '7', '84', '34', '109', '165', '7', '15', '165', '84', '265', '9', '251', '251', '269']

Received Cipher 1 = 147

Received Cipher 2 = [203, 165, 265, 90, 7, 84, 34, 109, 165, 7, 15, 165, 84, 265, 9, 251, 251]

K = 244

finding K inverse= 43

the output is [121, 101, 97, 104, 32, 115, 117, 114, 101, 32, 107, 101, 115, 97, 118, 33, 33]

Decrypted Text = yeah sure kesav!!

elgammel encryption

=======================================>start el\_gammal encrypting

k generating must be between 0 ,q is generated 238

K = 21

generated Cipher 1= 253

generated Cipher 2 = [179, 95, 134, 57, 53, 74, 53, 53, 134, 175, 120, 238, 134, 263, 238, 238, 134, 120, 179, 36, 134, 154, 15, 134, 37, 134, 200, 137, 134, 53, 158, 134, 179, 36, 242, 134, 36, 263, 36, 154, 116, 134, 200, 116, 154, 196, 238]

returned value = 253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269

message text= 253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269

SEND : b'253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269'

This message has been delivered

RECV : kesav~253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269~EE60C649ED93AA5E~2~269,15,199,166~582313,5,347069,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 253,179,95,134,57,53,74,53,53,134,175,120,238,134,263,238,238,134,120,179,36,134,154,15,134,37,134,200,137,134,53,158,134,179,36,242,134,36,263,36,154,116,134,200,116,154,196,238,269

======================================================>start decryption

tempmessage after spliting ['253', '179', '95', '134', '57', '53', '74', '53', '53', '134', '175', '120', '238', '134', '263', '238', '238', '134', '120', '179', '36', '134', '154', '15', '134', '37', '134', '200', '137', '134', '53', '158', '134', '179', '36', '242', '134', '36', '263', '36', '154', '116', '134', '200', '116', '154', '196', '238', '269']

Received Cipher 1 = 253

Received Cipher 2 = [179, 95, 134, 57, 53, 74, 53, 53, 134, 175, 120, 238, 134, 263, 238, 238, 134, 120, 179, 36, 134, 154, 15, 134, 37, 134, 200, 137, 134, 53, 158, 134, 179, 36, 242, 134, 36, 263, 36, 154, 116, 134, 200, 116, 154, 196, 238]

K = 21

finding K inverse= 205

the output is [111, 107, 32, 118, 105, 106, 105, 105, 32, 98, 121, 101, 32, 115, 101, 101, 32, 121, 111, 117, 32, 97, 116, 32, 53, 32, 112, 109, 32, 105, 110, 32, 111, 117, 114, 32, 117, 115, 117, 97, 108, 32, 112, 108, 97, 99, 101]

Decrypted Text = ok vijii bye see you at 5 pm in our usual place

RECV : viji~144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269~F82B33721ABF312E~2~269,15,199,166~1449359,11,1048931,

elgamal decryption

content copy message=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-==- 144,54,134,78,141,78,70,82,134,141,93,141,118,141,62,118,106,106,141,146,134,141,74,122,134,82,134,269

======================================================>start decryption

tempmessage after spliting ['144', '54', '134', '78', '141', '78', '70', '82', '134', '141', '93', '141', '118', '141', '62', '118', '106', '106', '141', '146', '134', '141', '74', '122', '134', '82', '134', '269']

Received Cipher 1 = 144

Received Cipher 2 = [54, 134, 78, 141, 78, 70, 82, 134, 141, 93, 141, 118, 141, 62, 118, 106, 106, 141, 146, 134, 141, 74, 122, 134, 82, 134]

K = 265

finding K inverse= 67

the output is [121, 101, 115, 32, 115, 117, 114, 101, 32, 44, 32, 105, 32, 119, 105, 108, 108, 32, 98, 101, 32, 116, 104, 101, 114, 101]

Decrypted Text = yes sure , i will be there