Robust Distributed Symmetric-key Encryption

Alex Castro, Steve Chang,
Garrett Christian, and Rachel Litscher

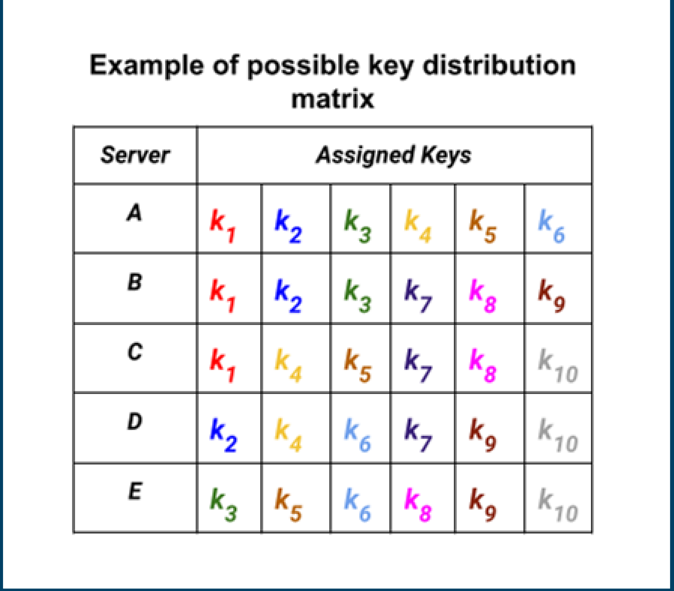
What Our Group Worked on

- Based on Professor Wang’s paper: *“Robust distributed symmetric-key encryption”*
- Implemented the scheme in C++
- Found parallel improvements using OpenMP and C++ threads
- Dockerized the application, ran on different environments, and on Google Cloud

What is Distributed Symmetric-key Encryption

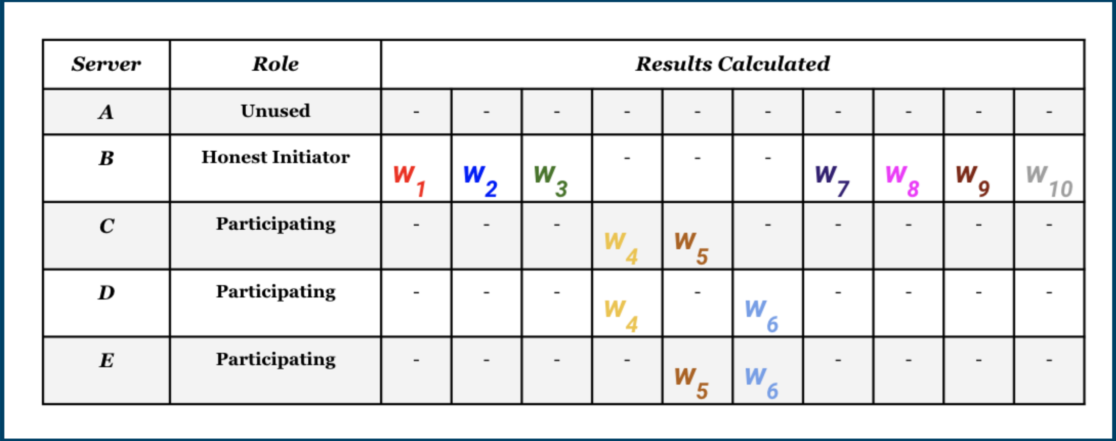
- A full set of keys are split between N servers
- Each machine holds a partial key set
- A secret is generated using the full key set
- Machines work together using their partial key sets to encrypt and decrypt messages
- No set of machines less than the *T* threshold can reconstruct the secret alone

What Makes Professor Wang’s Robust



Example of possible key distribution matrix

Server	*Assigned Keys*					
A	k_1	k_2	k_3	k_4	k_5	k_6
B	k_1	k_2	k_3	k_7	k_8	k_9
C	k_1	k_4	k_5	k_7	k_8	k_{10}
D	k_2	k_4	k_6	k_7	k_9	k_{10}
E	k_3	k_5	k_6	k_8	k_9	k_{10}



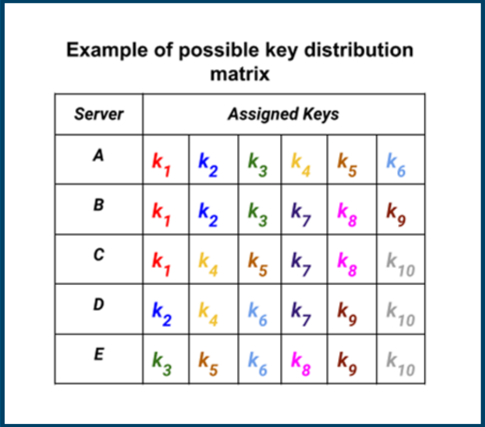
Server	***Role***	***Results Calculated***									
A	**Unused**	-	-	-	-	-	-	-	-	-	-
B	**Honest Initiator**	w_1	w_2	w_3	-	-	-	w_7	w_8	w_9	w_{10}
C	**Participating**	-	-	-	w_4	w_5	-	-	-	-	-
D	**Participating**	-	-	-	w_4	-	w_6	-	-	-	-
E	**Participating**	-	-	-	-	w_5	w_6	-	-	-	-

Different Roles in the Scheme

- Dealer: supplies the omega table and partial keys to the DiSE Servers
- Client: begins either a encryption or decryption transaction
- DiSE Server: waits to be contacted by one of the other roles
- Honest Initiator: random DiSE Server chosen by the client who manages the transaction
- Participant: contacted by the Honest Initiator to create the partial *w*'s for either encryption or decryption

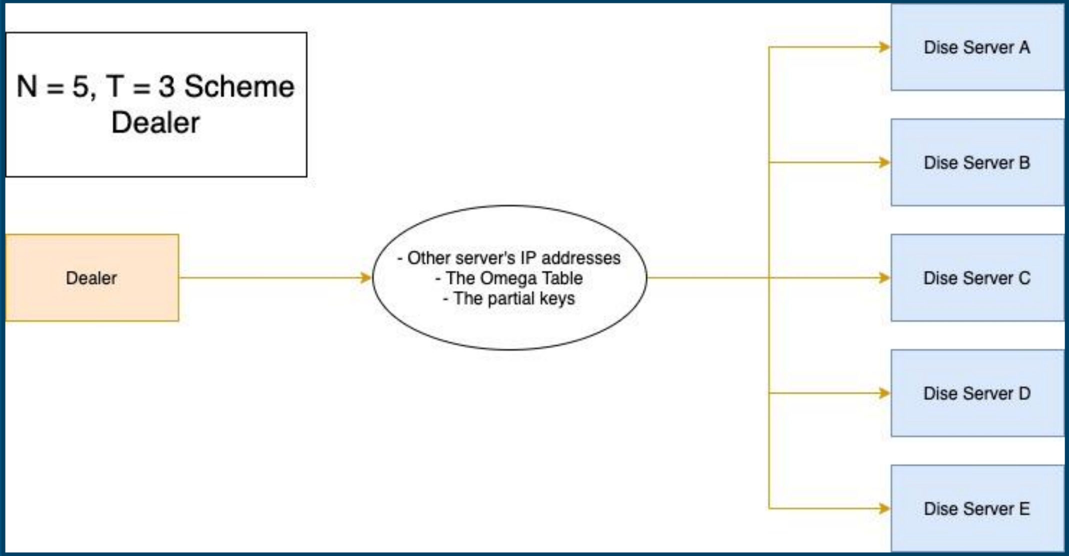
Dealer Flow

- Generate key list and populates the omega matrix
- Send data assigned to each server to the corresponding server in parallel



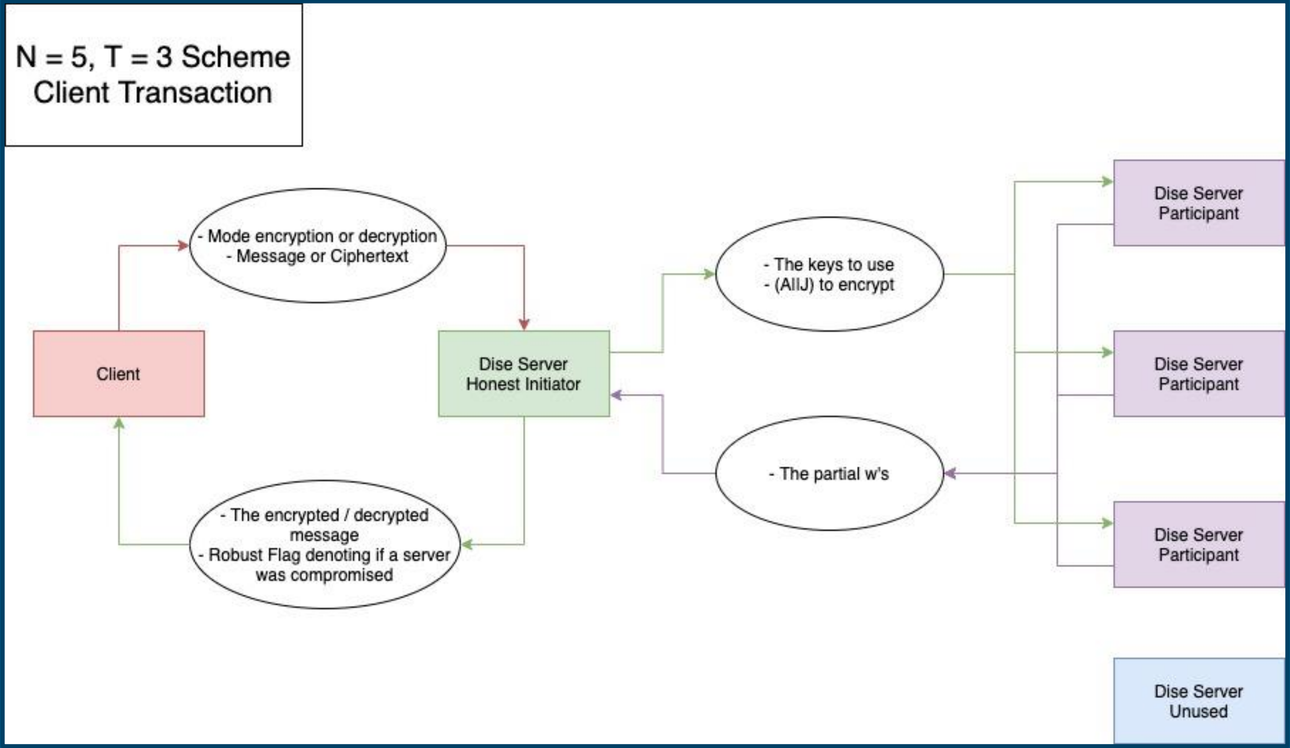
Example of possible key distribution matrix

Server	*Assigned Keys*					
A	k_1	k_2	k_3	k_4	k_5	k_6
B	k_1	k_2	k_3	k_7	k_8	k_9
C	k_1	k_4	k_5	k_7	k_8	k_{10}
D	k_2	k_4	k_6	k_7	k_9	k_{10}
E	k_3	k_5	k_6	k_8	k_9	k_{10}



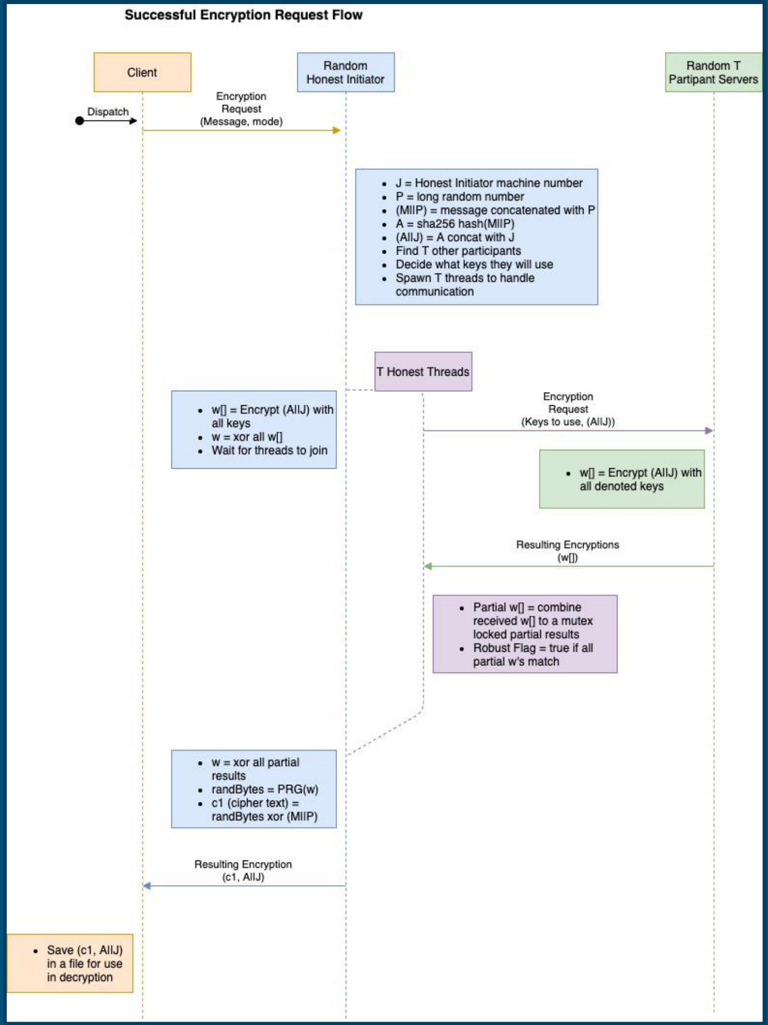
N = 5, T = 3 Scheme Dealer

Transaction Communication Overview



Encryption Flow

- Client Hits a random Server to be Honest Initiator
- Honest Init creates M||P and A||J
- Asks random T to create partial W's



Successful Encryption Request Flow

Client

Random Honest Initiator

Random T Partipant Servers

Dispatch

Encryption Request (Message, mode)

- J = Honest Initiator machine number
- P = long random number
- (M||P) = message concatenated with P
- A = sha256 hash(M||P)
- (A||J) = A concat with J
- Find T other participants
- Decide what keys they will use
- Spawn T threads to handle communication

T Honest Threads

- w[] = Encrypt (A||J) with all keys
- w = xor all w[]
- Wait for threads to join

Encryption Request (Keys to use, (A||J))

- w[] = Encrypt (A||J) with all denoted keys

Resulting Encryptions (w[])

- Partial w[] = combine received w[] to a mutex locked partial results
- Robust Flag = true if all partial w's match

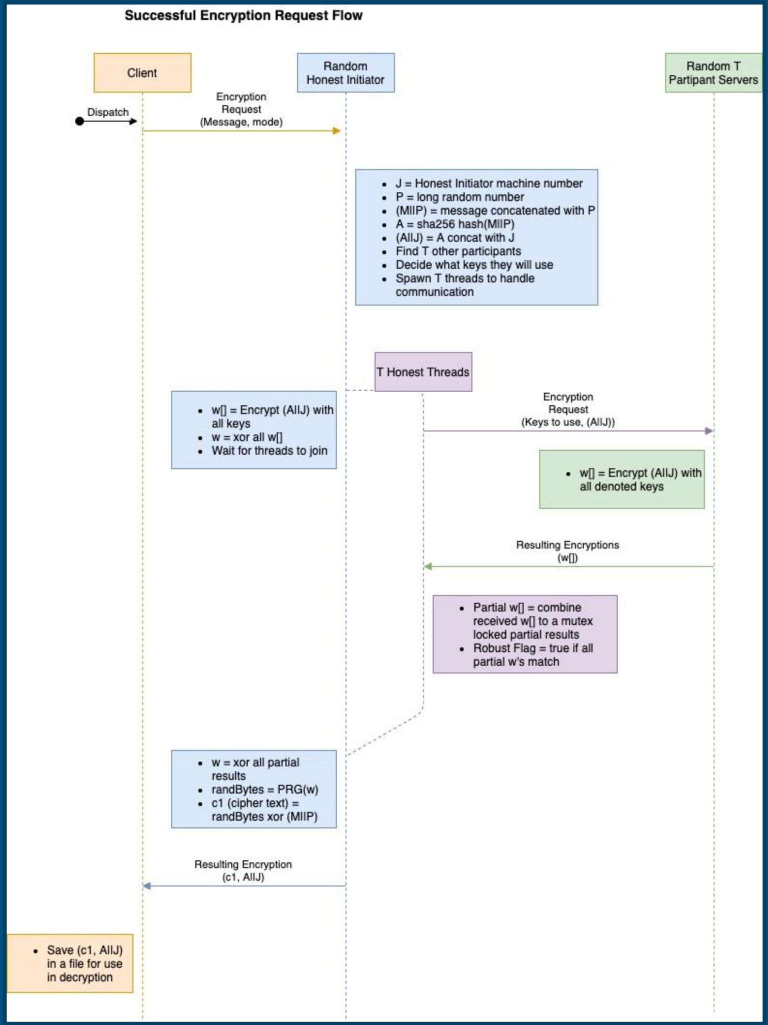
- w = xor all partial results
- randBytes = PRG(w)
- c1 (cipher text) = randBytes xor (M||P)

Resulting Encryption (c1, A||J)

- Save (c1, A||J) in a file for use in decryption

Encryption Flow

- Honest Initiator checks robustness
- Uses a pseudo-random number generator with the final W as seed
- xors final w with the message
- Client saves (C1, A||J)



Successful Encryption Request Flow

Client

Random Honest Initiator

Random T Partipant Servers

Dispatch

Encryption Request (Message, mode)

- J = Honest Initiator machine number
- P = long random number
- (MllP) = message concatenated with P
- A = sha256 hash(MllP)
- (AllJ) = A concat with J
- Find T other participants
- Decide what keys they will use
- Spawn T threads to handle communication

T Honest Threads

- w[] = Encrypt (AllJ) with all keys
- w = xor all w[]
- Wait for threads to join

Encryption Request (Keys to use, (AllJ))

- w[] = Encrypt (AllJ) with all denoted keys

Resulting Encryptions (w[])

- Partial w[] = combine received w[] to a mutex locked partial results
- Robust Flag = true if all partial w's match

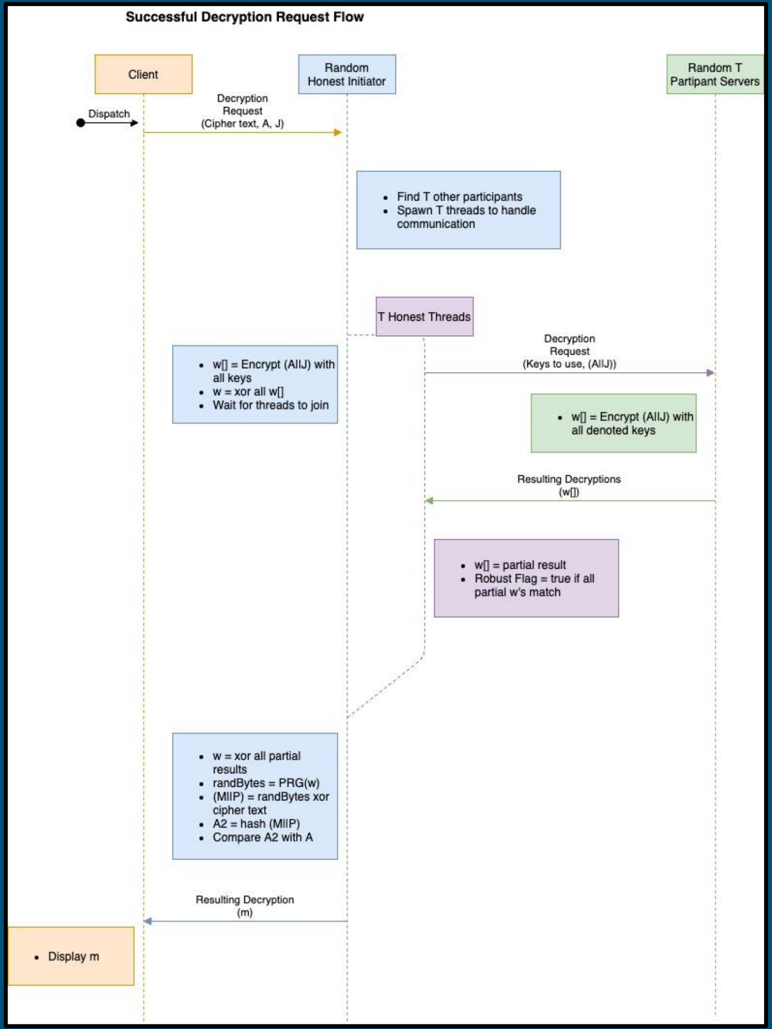
- w = xor all partial results
- randBytes = PRG(w)
- c1 (cipher text) = randBytes xor (MllP)

Resulting Encryption (c1, AllJ)

- Save (c1, AllJ) in a file for use in decryption

Decryption Flow

- Client sends (C1, A||J) to random Honest Initiator
- Performs encryption steps in reverse
- Key difference is that it checks the hash of M||P with the provided A



Successful Decryption Request Flow

Client

Random Honest Initiator

Random T Partipant Servers

Dispatch

Decryption Request (Cipher text, A, J)

- Find T other participants
- Spawn T threads to handle communication

T Honest Threads

- w[] = Encrypt (A||J) with all keys
- w = xor all w[]
- Wait for threads to join

Decryption Request (Keys to use, (A||J))

- w[] = Encrypt (A||J) with all denoted keys

Resulting Decryptions (w[])

- w[] = partial result
- Robust Flag = true if all partial w's match

- w = xor all partial results
- randBytes = PRG(w)
- (M||P) = randBytes xor cipher text
- A2 = hash (M||P)
- Compare A2 with A

Resulting Decryption (m)

- Display m

Roadblocks

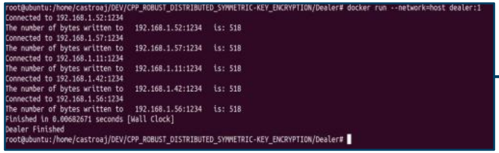
- We were building the application from the ground up
- Had difficulty running the larger case
- Due to version issues, we could not use OpenSSL and Crypto++ for the pseudo-random number generator

DOCKER Running on Different Virtual Machines

- To demonstrate the portability of our application we ran it on multiple types of virtual machines
- Virtual Machines Used:
  - Ubuntu
  - Debian
  - Kali

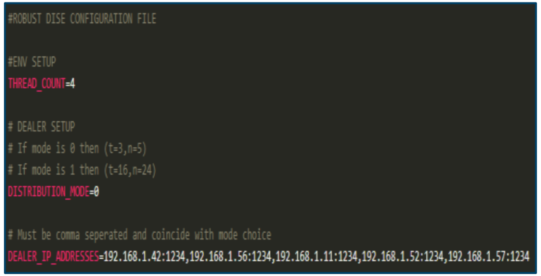
DOCKER Demo of *N 5 T 3 - DEAL*

Dealer

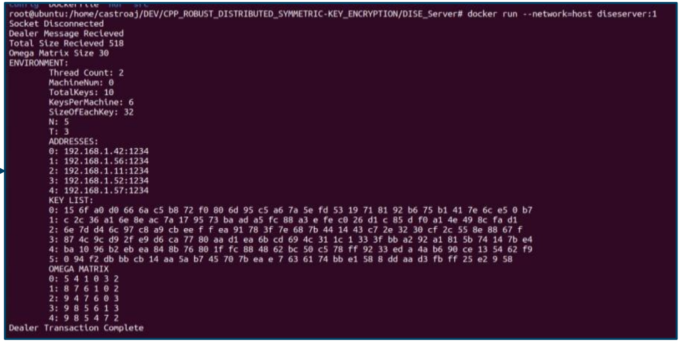


```
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Dealer# docker run --network=host dealer:1
Connected to 192.168.1.52:1234
The number of bytes written to   192.168.1.52:1234   is: 518
Connected to 192.168.1.57:1234
The number of bytes written to   192.168.1.57:1234   is: 518
Connected to 192.168.1.11:1234
The number of bytes written to   192.168.1.11:1234   is: 518
Connected to 192.168.1.42:1234
The number of bytes written to   192.168.1.42:1234   is: 518
Connected to 192.168.1.56:1234
The number of bytes written to   192.168.1.56:1234   is: 518
Finished in 0.00682671 seconds [Wall Clock]
Dealer Finished
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Dealer# 
```

Dealer Configuration File

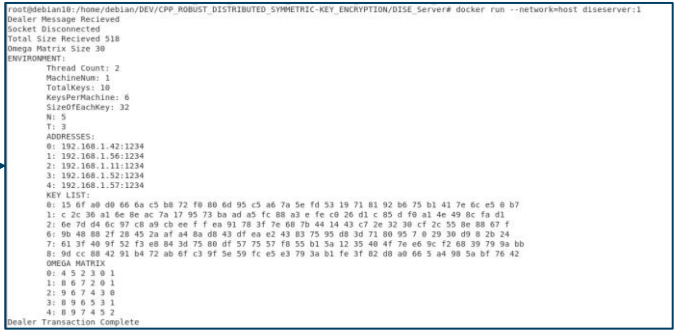


```
#ROBUST DISE CONFIGURATION FILE

#ENV SETUP
THREAD_COUNT=4

# DEALER SETUP
# If mode is 0 then (t=3,n=5)
# If mode is 1 then (t=16,n=24)
DISTRIBUTION_MODE=0

# Must be comma seperated and coincide with mode choice
DEALER_IP_ADDRESSES=192.168.1.42:1234,192.168.1.56:1234,192.168.1.11:1234,192.168.1.52:1234,192.168.1.57:1234
```



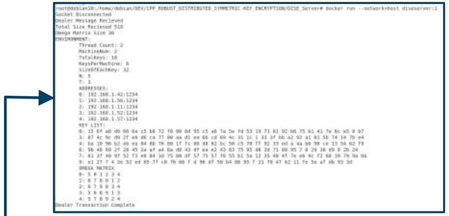
```
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/DISE_Server# docker run --network=host diseserver:1
Socket Disconnected
Dealer Message Recieved
Total Size Recieved 518
Omega Matrix Size 30
ENVIRONMENT:
        Thread Count: 2
        MachineNum: 0
        TotalKeys: 10
        KeysPerMachine: 6
        SizeOfEachKey: 32
        N: 5
        T: 3
        ADDRESSES:
        0: 192.168.1.42:1234
        1: 192.168.1.56:1234
        2: 192.168.1.11:1234
        3: 192.168.1.52:1234
        4: 192.168.1.57:1234
        KEY LIST:
        0: 15 6f a0 d0 66 6a c5 b8 72 f0 80 6d 95 c5 a6 7a 5e fd 53 19 71 81 92 b6 75 b1 41 7e 6c e5 0 b7
        1: c 2c 36 a1 6e 8e ac 7a 17 95 73 ba ad a5 fc 88 a3 e fe c0 26 d1 c 85 d f0 a1 4e 49 8c fa d1
        2: 6e 7d d4 6c 97 c8 a9 cb ee f f ea 91 78 3f 7e 68 7b 44 14 43 c7 2e 32 30 cf 2c 55 8e 88 67 f
        3: 87 4c 9c d9 2f e9 d6 ca 77 80 aa d1 ea 6b cd 69 4c 31 1c 1 33 3f bb a2 92 a1 81 5b 74 14 7b e4
        4: ba 10 96 b2 eb ea 84 8b 76 80 1f fc 88 48 62 bc 50 c5 78 ff 92 33 ed a 4a b6 90 ce 13 54 62 f9
        5: 0 94 f2 db bb cb 14 aa 5a b7 45 70 7b ea e 7 63 61 74 bb e1 58 8 dd aa d3 fb ff 25 e2 9 58
        OMEGA MATRIX
        0: 5 4 1 0 3 2
        1: 8 7 6 1 0 2
        2: 9 4 7 6 0 3
        3: 9 8 5 6 1 3
        4: 9 8 5 4 7 2
Dealer Transaction Complete
```

MACHINE 0 - Ubuntu // IP: 192.168.1.42:1234



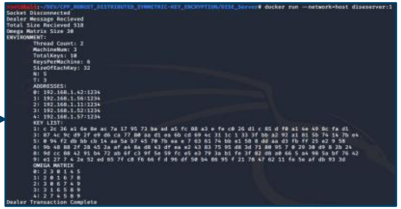
```
root@debian10:/home/debian/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/DISE_Server# docker run --network=host diseserver:1
Dealer Message Recieved
Socket Disconnected
Total Size Recieved 518
Omega Matrix Size 30
ENVIRONMENT:
        Thread Count: 2
        MachineNum: 1
        TotalKeys: 10
        KeysPerMachine: 6
        SizeOfEachKey: 32
        N: 5
        T: 3
        ADDRESSES:
        0: 192.168.1.42:1234
        1: 192.168.1.56:1234
        2: 192.168.1.11:1234
        3: 192.168.1.52:1234
        4: 192.168.1.57:1234
        KEY LIST:
        0: 15 6f a0 d0 66 6a c5 b8 72 f0 80 6d 95 c5 a6 7a 5e fd 53 19 71 81 92 b6 75 b1 41 7e 6c e5 0 b7
        1: c 2c 36 a1 6e 8e ac 7a 17 95 73 ba ad a5 fc 88 a3 e fe c0 26 d1 c 85 d f0 a1 4e 49 8c fa d1
        2: 6e 7d d4 6c 97 c8 a9 cb ee f f ea 91 78 3f 7e 68 7b 44 14 43 c7 2e 32 30 cf 2c 55 8e 88 67 f
        6: 9b 48 88 2f 28 45 2a af a4 8a d8 43 df ea e2 43 83 75 95 d8 3d 71 80 95 7 0 29 30 d9 8 2b 24
        7: 61 3f 40 9f 52 f3 e8 84 3d 75 80 df 57 75 57 f8 55 b1 5a 12 35 40 4f 7e e6 9c f2 68 39 79 9a bb
        8: 9d cc 88 42 91 b4 72 ab 6f c3 9f 5e 59 fc e5 e3 79 3a b1 fe 3f 82 d8 a0 66 5 a4 98 5a bf 76 42
        OMEGA MATRIX
        0: 4 5 2 3 0 1
        1: 8 6 7 2 0 1
        2: 9 6 7 4 3 0
        3: 8 9 6 5 3 1
        4: 8 9 7 4 5 2
Dealer Transaction Complete
```

MACHINE 1- Debian // IP: 192.168.1.56:1234



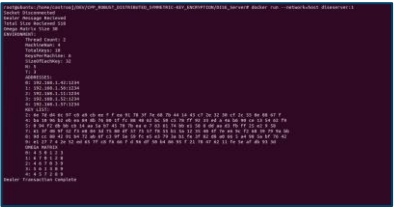
```
root@debian10:/home/debian/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/DISE_Server# docker run --network=host diseserver:1
Socket Disconnected
Dealer Message Recieved
Total Size Recieved 518
Omega Matrix Size 30
ENVIRONMENT:
        Thread Count: 2
        MachineNum: 2
        TotalKeys: 10
        KeysPerMachine: 6
        SizeOfEachKey: 32
        N: 5
        T: 3
        ADDRESSES:
        0: 192.168.1.42:1234
        1: 192.168.1.56:1234
        2: 192.168.1.11:1234
        3: 192.168.1.52:1234
        4: 192.168.1.57:1234
        KEY LIST:
        0: 15 6f a0 d0 66 6a c5 b8 72 f0 80 6d 95 c5 a6 7a 5e fd 53 19 71 81 92 b6 75 b1 41 7e 6c e5 0 b7
        3: 87 4c 9c d9 2f e9 d6 ca 77 80 aa d1 ea 6b cd 69 4c 31 1c 1 33 3f bb a2 92 a1 81 5b 74 14 7b e4
        4: ba 10 96 b2 eb ea 84 8b 76 80 1f fc 88 48 62 bc 50 c5 78 ff 92 33 ed a 4a b6 90 ce 13 54 62 f9
        6: 9b 48 88 2f 28 45 2a af a4 8a d8 43 df ea e2 43 83 75 95 d8 3d 71 80 95 7 0 29 30 d9 8 2b 24
        7: 61 3f 40 9f 52 f3 e8 84 3d 75 80 df 57 75 57 f8 55 b1 5a 12 35 40 4f 7e e6 9c f2 68 39 79 9a bb
        9: e1 27 7 4 2e 52 ed 85 7f c8 f6 66 f d 96 df 50 b4 86 95 f 21 78 47 62 11 fe 5e af db 93 3d
        OMEGA MATRIX
        0: 5 0 1 2 3 4
        1: 8 7 6 0 1 2
        2: 6 7 9 0 3 4
        3: 5 6 8 9 1 3
        4: 5 7 8 9 2 4
Dealer Transaction Complete
```

MACHINE 2- Debian // IP:192.168.1.11:1234



```
root@kali:~/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/DISE_Server# docker run --network=host diseserver:1
Socket Disconnected
Dealer Message Recieved
Total Size Recieved 518
Omega Matrix Size 30
ENVIRONMENT:
        Thread Count: 2
        MachineNum: 3
        TotalKeys: 10
        KeysPerMachine: 6
        SizeOfEachKey: 32
        N: 5
        T: 3
        ADDRESSES:
        0: 192.168.1.42:1234
        1: 192.168.1.56:1234
        2: 192.168.1.11:1234
        3: 192.168.1.52:1234
        4: 192.168.1.57:1234
        KEY LIST:
        1: c 2c 36 a1 6e 8e ac 7a 17 95 73 ba ad a5 fc 88 a3 e fe c0 26 d1 c 85 d f0 a1 4e 49 8c fa d1
        3: 87 4c 9c d9 2f e9 d6 ca 77 80 aa d1 ea 6b cd 69 4c 31 1c 1 33 3f bb a2 92 a1 81 5b 74 14 7b e4
        5: 0 94 f2 db bb cb 14 aa 5a b7 45 70 7b ea e 7 63 61 74 bb e1 58 8 dd aa d3 fb ff 25 e2 9 58
        6: 9b 48 88 2f 28 45 2a af a4 8a d8 43 df ea e2 43 83 75 95 d8 3d 71 80 95 7 0 29 30 d9 8 2b 24
        8: 9d cc 88 42 91 b4 72 ab 6f c3 9f 5e 59 fc e5 e3 79 3a b1 fe 3f 82 d8 a0 66 5 a4 98 5a bf 76 42
        9: e1 27 7 4 2e 52 ed 85 7f c8 f6 66 f d 96 df 50 b4 86 95 f 21 78 47 62 11 fe 5e af db 93 3d
        OMEGA MATRIX
        0: 2 3 0 1 4 5
        1: 2 0 1 6 7 8
        2: 3 0 6 7 4 9
        3: 3 1 6 5 8 9
        4: 2 7 4 5 8 9
Dealer Transaction Complete
```

MACHINE 3 - Kali // IP: 192.168.1.52:1234

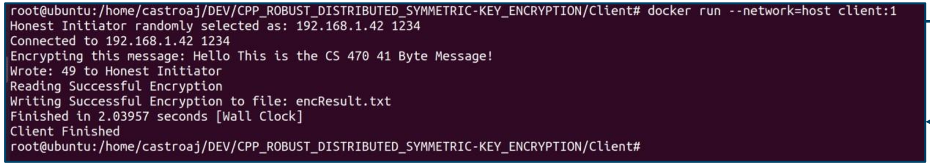


```
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/DISE_Server# docker run --network=host diseserver:1
Socket Disconnected
Dealer Message Recieved
Total Size Recieved 518
Omega Matrix Size 30
ENVIRONMENT:
        Thread Count: 2
        MachineNum: 4
        TotalKeys: 10
        KeysPerMachine: 6
        SizeOfEachKey: 32
        N: 5
        T: 3
        ADDRESSES:
        0: 192.168.1.42:1234
        1: 192.168.1.56:1234
        2: 192.168.1.11:1234
        3: 192.168.1.52:1234
        4: 192.168.1.57:1234
        KEY LIST:
        2: 6e 7d d4 6c 97 c8 a9 cb ee f f ea 91 78 3f 7e 68 7b 44 14 43 c7 2e 32 30 cf 2c 55 8e 88 67 f
        4: ba 10 96 b2 eb ea 84 8b 76 80 1f fc 88 48 62 bc 50 c5 78 ff 92 33 ed a 4a b6 90 ce 13 54 62 f9
        5: 0 94 f2 db bb cb 14 aa 5a b7 45 70 7b ea e 7 63 61 74 bb e1 58 8 dd aa d3 fb ff 25 e2 9 58
        7: 61 3f 40 9f 52 f3 e8 84 3d 75 80 df 57 75 57 f8 55 b1 5a 12 35 40 4f 7e e6 9c f2 68 39 79 9a bb
        8: 9d cc 88 42 91 b4 72 ab 6f c3 9f 5e 59 fc e5 e3 79 3a b1 fe 3f 82 d8 a0 66 5 a4 98 5a bf 76 42
        9: e1 27 7 4 2e 52 ed 85 7f c8 f6 66 f d 96 df 50 b4 86 95 f 21 78 47 62 11 fe 5e af db 93 3d
        OMEGA MATRIX
        0: 4 5 0 1 2 3
        1: 6 7 0 1 2 8
        2: 4 6 7 0 3 9
        3: 5 6 1 3 8 9
        4: 4 5 7 2 8 9
Dealer Transaction Complete
```

MACHINE 4 - Ubuntu // IP: 192.168.1.57:1234

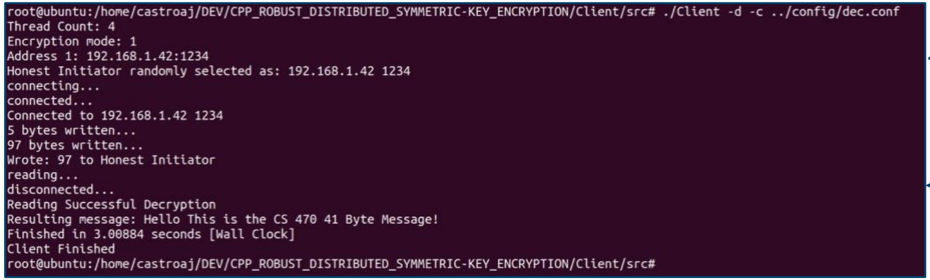
DOCKER Demo of *N 5 T 3 - ENC / DEC*

Client - Encryption Request

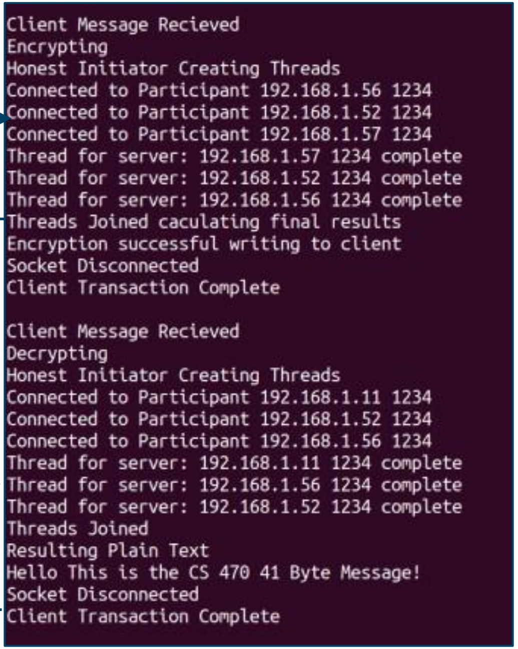


```
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Client# docker run --network=host client:1
Honest Initiator randomly selected as: 192.168.1.42 1234
Connected to 192.168.1.42 1234
Encrypting this message: Hello This is the CS 470 41 Byte Message!
Wrote: 49 to Honest Initiator
Reading Successful Encryption
Writing Successful Encryption to file: encResult.txt
Finished in 2.03957 seconds [Wall Clock]
Client Finished
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Client#
```

Client - Decryption Request



```
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Client/src# ./Client -d -c ../config/dec.conf
Thread Count: 4
Encryption mode: 1
Address 1: 192.168.1.42:1234
Honest Initiator randomly selected as: 192.168.1.42 1234
connecting...
connected...
Connected to 192.168.1.42 1234
5 bytes written...
97 bytes written...
Wrote: 97 to Honest Initiator
reading...
disconnected...
Reading Successful Decryption
Resulting message: Hello This is the CS 470 41 Byte Message!
Finished in 3.00884 seconds [Wall Clock]
Client Finished
root@ubuntu:/home/castroaj/DEV/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Client/src#
```



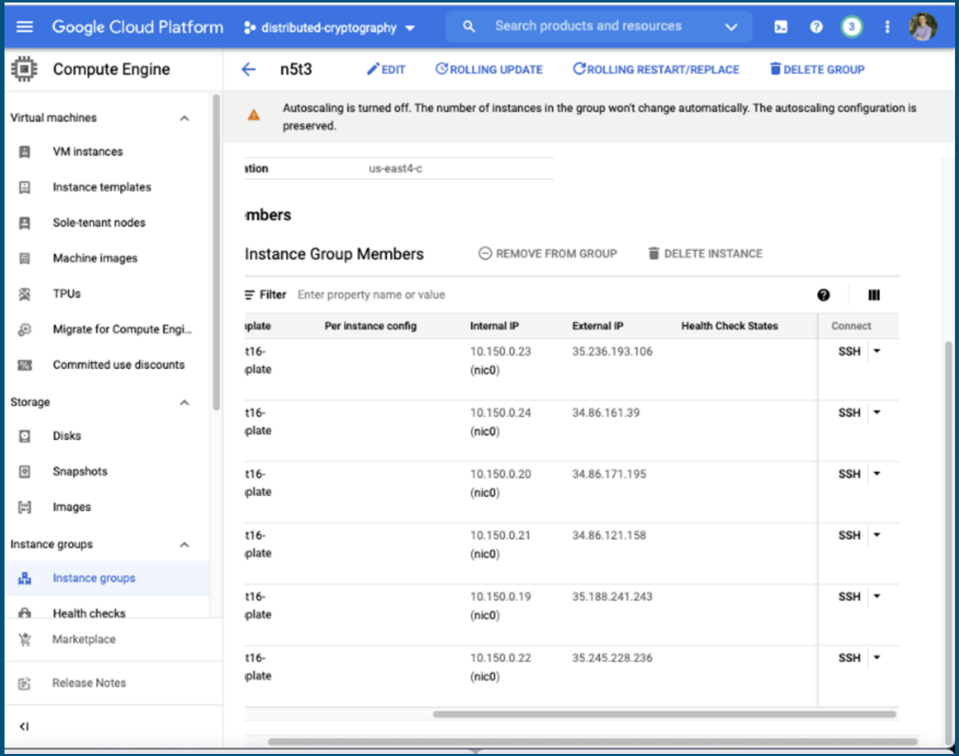
```
Client Message Recieved
Encrypting
Honest Initiator Creating Threads
Connected to Participant 192.168.1.56 1234
Connected to Participant 192.168.1.52 1234
Connected to Participant 192.168.1.57 1234
Thread for server: 192.168.1.57 1234 complete
Thread for server: 192.168.1.52 1234 complete
Thread for server: 192.168.1.56 1234 complete
Threads Joined caculating final results
Encryption successful writing to client
Socket Disconnected
Client Transaction Complete

Client Message Recieved
Decrypting
Honest Initiator Creating Threads
Connected to Participant 192.168.1.11 1234
Connected to Participant 192.168.1.52 1234
Connected to Participant 192.168.1.56 1234
Thread for server: 192.168.1.11 1234 complete
Thread for server: 192.168.1.56 1234 complete
Thread for server: 192.168.1.52 1234 complete
Threads Joined
Resulting Plain Text
Hello This is the CS 470 41 Byte Message!
Socket Disconnected
Client Transaction Complete
```

Honest Initiator
Contacts: 192.168.1.11

192.168.1.52

192.168.1.56

DOCKER Running on Google Cloud



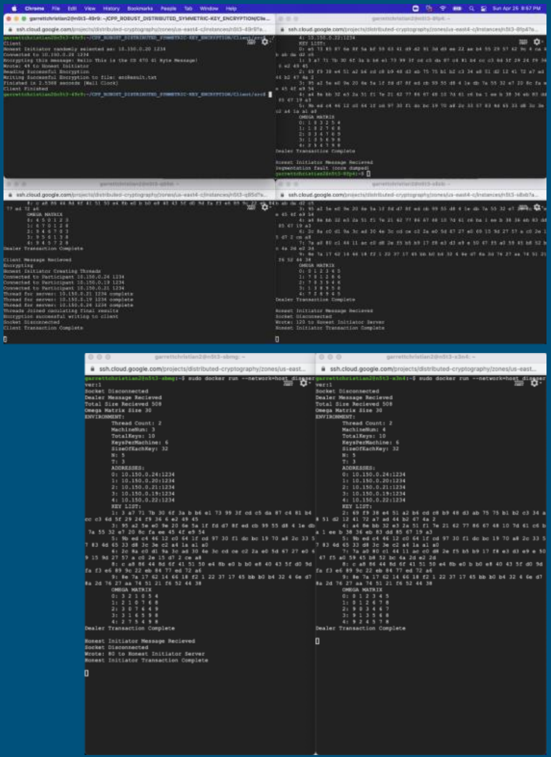
Autoscaling is turned off. The number of instances in the group won't change automatically. The autoscaling configuration is preserved.

ation us-east4-c

mbers

Instance Group Members

plate	Per instance config	Internal IP	External IP	Health Check States	Connect
t16- plate		10.150.0.23 (nic0)	35.236.193.106		SSH
t16- plate		10.150.0.24 (nic0)	34.86.161.39		SSH
t16- plate		10.150.0.20 (nic0)	34.86.171.195		SSH
t16- plate		10.150.0.21 (nic0)	34.86.121.158		SSH
t16- plate		10.150.0.19 (nic0)	35.188.241.243		SSH
t16- plate		10.150.0.22 (nic0)	35.245.228.236		SSH



Chrome File Edit View History Bookmarks People Tab Window Help
garrettchristian2@n5t3-49r9: ~/CPP_ROBUST_DISTRIBUTED_SYMMETRIC-KEY_ENCRYPTION/Clie...
ssh.cloud.google.com/projects/distributed-cryptography/zones/us-east4-c/instances/n5t3-49r9?a...
garrettchristian2@n5t3-sbmg: ~
ssh.cloud.google.com/projects/distributed-cryptography/zones/us-east...

```
Client
Honest Initiator randomly selected as: 10.150.0.20 1234
Connected to 10.150.0.20 1234
Encrypting this message: Hello This is the CS 470 41 Byte Message!
Wrote: 49 to Honest Initiator
Reading Successful Encryption
Writing Successful Encryption to file: encResult.txt
Finished in 2.5308 seconds (Wall Clock)
Client Finished
```

```
garrettchristian2@n5t3-sbmg:~$ sudo docker run --network=host disser
ver:1
Socket Disconnected
Dealer Message Recieved
Total Size Recieved 508
Omega Matrix Size 30
ENVIRONMENT:
        Thread Count: 2
        MachineNum: 3
        TotalKeys: 10
        KeysPerMachine: 6
        SizeOfEachKey: 32
        N: 5
        T: 3
        ADDRESSES:
        0: 10.150.0.24:1234
        1: 10.150.0.20:1234
        2: 10.150.0.21:1234
        3: 10.150.0.19:1234
        4: 10.150.0.22:1234
        KEY LIST:
        1: 3 a7 71 7b 30 6f 3a b b6 e1 73 99 3f cd c5 da 87 c4 81 b4
cc c3 6d 5f 29 24 f9 36 6 e2 49 45
        3: 95 a2 5e e0 9e 20 6e 5a 1f fd d7 8f ed cb 99 55 d8 4 1e db
 7a 55 32 e7 20 8c fa ee 45 4f e9 54
        5: 9b ed c4 46 12 c0 64 1f cd 97 30 f1 dc bc 19 70 a8 2c 33 5
7 83 4d 65 33 d8 3c 3e c2 a4 1a a1 a0
        6: 2c 8a c0 d1 9a 3c ad 30 4e 3c cd ce c2 2a e0 5d 67 27 e0 6
9 15 9d 27 57 a c0 2e 15 d7 2 ce a8
        8: c a8 86 44 8d 6f 41 51 50 e4 8b e0 b b0 e8 40 43 5f d0 9d
fa f3 e6 89 9c 22 eb 84 77 ed 72 a6
        9: 8e 7a 17 62 14 66 18 f2 1 22 37 17 45 bb b0 b4 32 4 6e d7
8a 2d 76 27 aa 74 51 21 f6 52 44 38
        OMEGA MATRIX
        0: 3 2 1 0 5 4
        1: 2 1 0 7 6 8
        2: 3 0 7 6 4 9
        3: 3 1 6 5 9 8
        4: 2 7 5 4 9 8
Dealer Transaction Complete

Honest Initiator Message Recieved
Socket Disconnected
Wrote: 80 to Honest Initiator Server
Honest Initiator Transaction Complete
```

Live Local Host Demo (N=5, T= 3)

Thank You!