# End to End Encryption in Chat Application

# CNS Project Report

## Phase III


Submitted by:

**Amit G. Patil (19104004)**

**Sanjoli Goyal (19104007)**

**Muskan Jain (19104010)**

**Manu Singh Bist (19104041)**

**Batch: B11**

**Faculty Name: Ms Kavita Pandey**

**Department of CSE/IT**

**Jaypee Institute of Information Technology University, Noida**

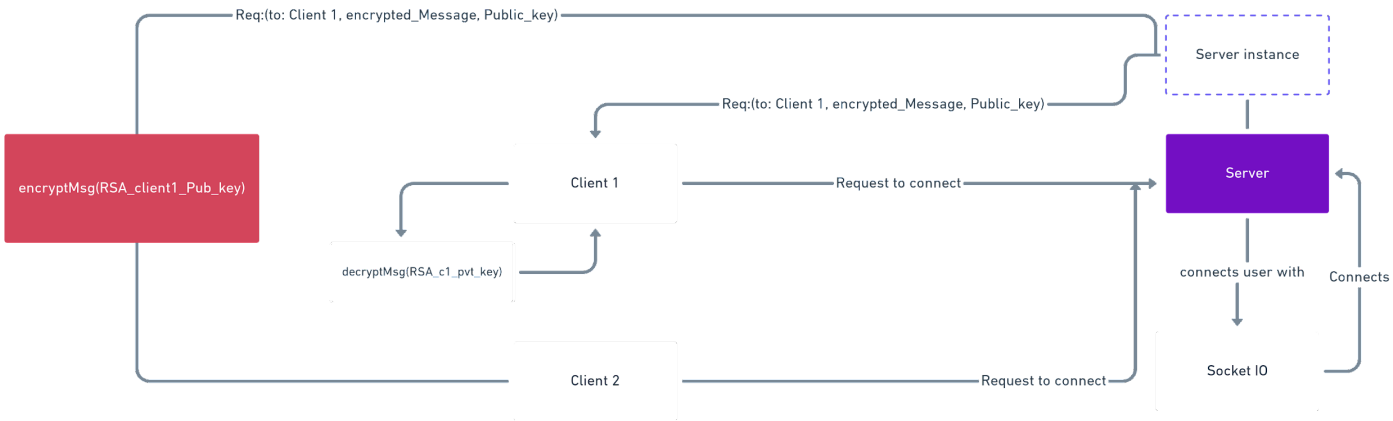

**December 2021**

# Declaration

We hereby declare that this submission is our own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text. We accept the use of the material presented in this report for Education/Research/Teaching purpose by the faculty.

| | | | |
|---|---|---|---|
| | | | |
| Amit Patil | Sanjoli Goyal | Muskan Jain | Manu Singh Bist |
| 11 Nov 2021<br>Mumbai | 11 Nov 2021<br>Hathras | 11 Nov 2021<br>Meerut | 1 Nov 2021<br>Noida |

- ## Architecture Of App




For higher resolution refer here **:** [Link]

- ## Methodology

1. **Generating the keys**
   a. Select two large prime numbers, x and y. The prime numbers need to be large so that they will be difficult for someone to figure out.
   b. Calculate n =x *y.
   c. Calculate the totient function; $\phi((n) = (x-1)(y-1)$
   d. Select an integer e, such that e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n,e)makes up the public key.

   **Note:** Two integers are coprime if the only positive integer that divides them is 1.

   e. Calculate d such that $e.d = 1 \bmod \phi(n)$.

   d can be found using the extended euclidean algorithm. The pair (n,d) makes up the private key.

2. **Encryption**
   Given a plaintext P, represented as a number, the ciphertext C is calculated as:
   $C=P^e \bmod n$

3. **Decryption**
   Using the private key (n,d), the plaintext can be found using:
   $P=C^d \bmod n$

- **Results**

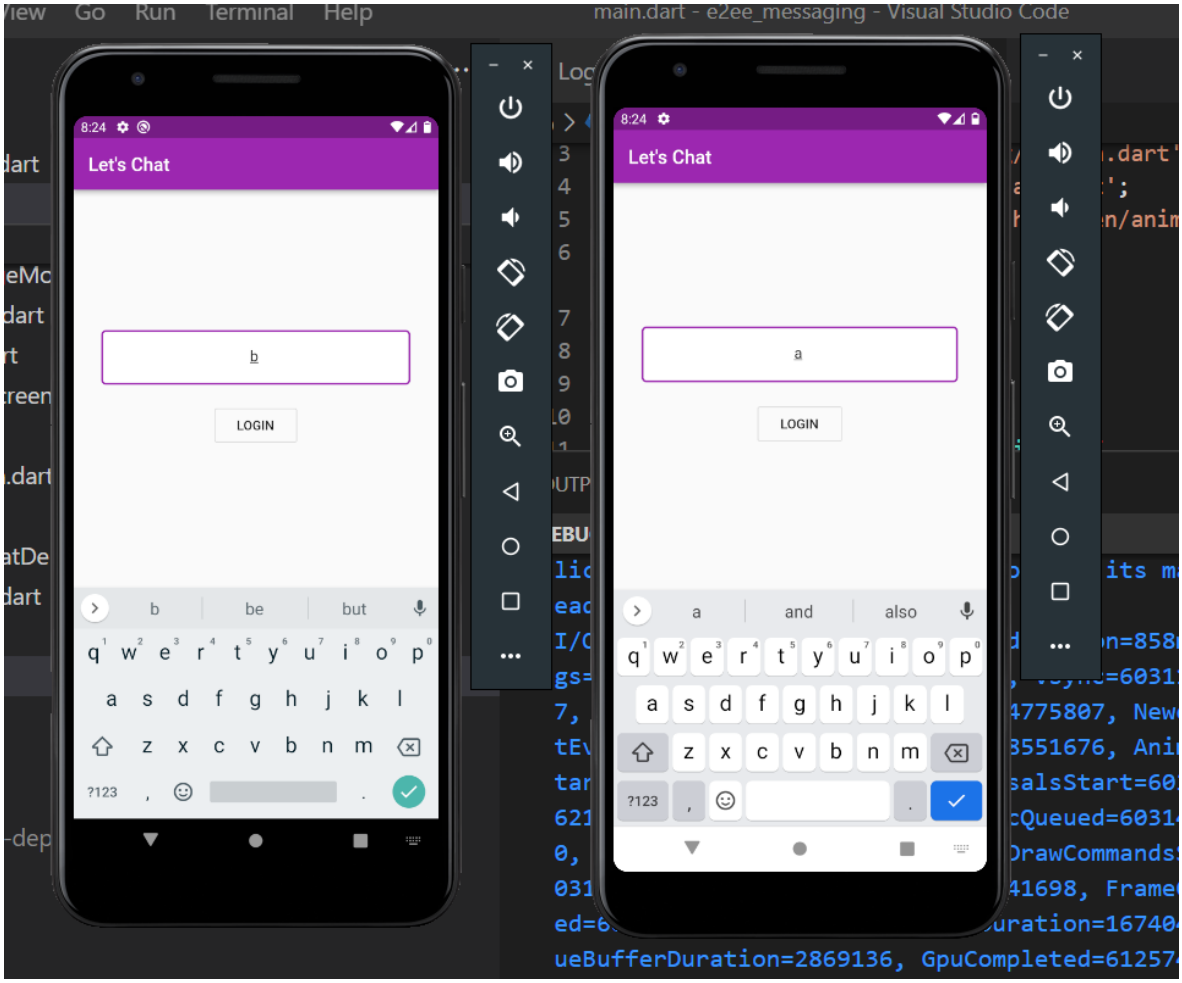
## Project Link:

Client App : https://github.com/Mystic-Trooper/E2EE-Messaging

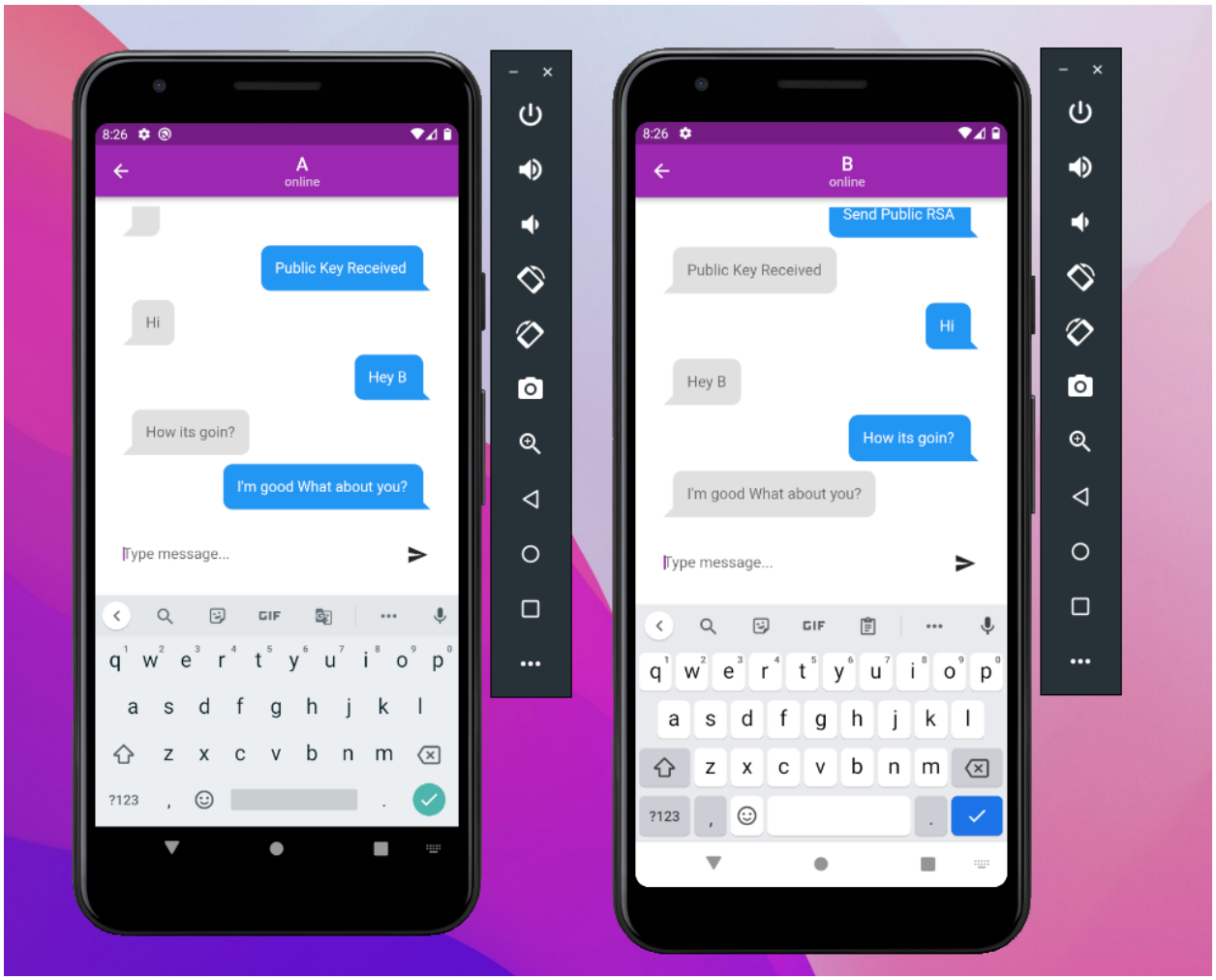
Server App: https://github.com/Mystic-Trooper/E2EE-Messaging-server

## Screenshots

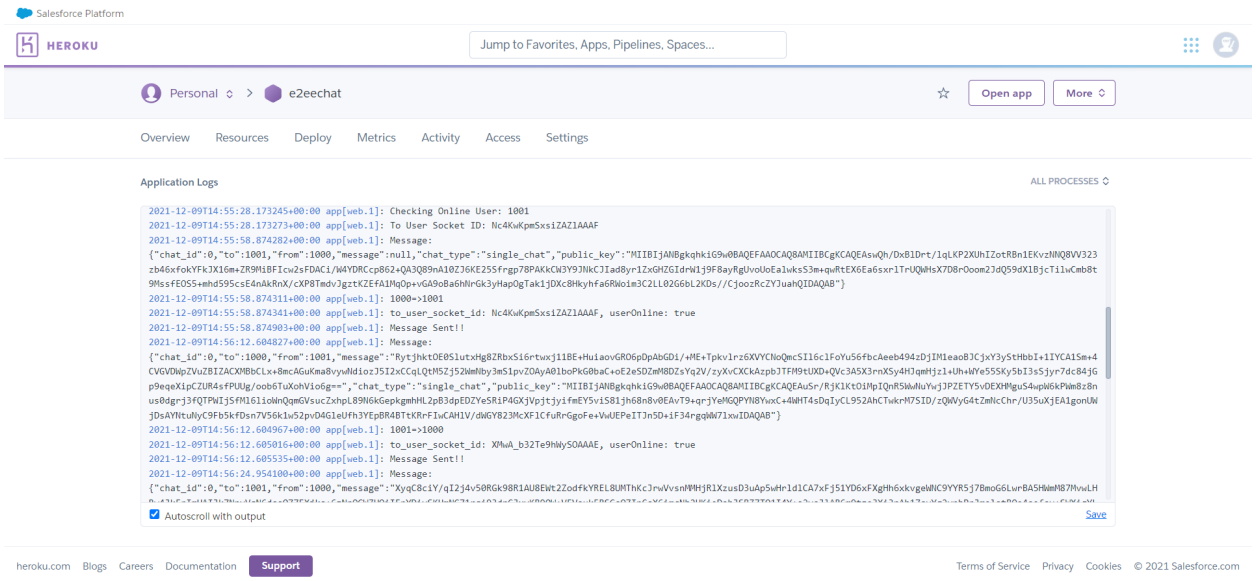
Register users and check for online status



Decrypted messages and chat screens




Encrypted exchange of message through socket server




# Socket disconnect

```
2021-12-09T14:58:48.610808+00:00 heroku[router]: at=info method=GET path="/socket.io/?from=1000&EIO=3&transport=websocket" host=e2eechat.herokuapp.com request_id=41c858a4-51ee-4a31-9e3d-f923e25f9ec6 fwd="106.193.224.179" dyno=web.1 connect=0ms service=226465ms status=101 bytes=129 protocol=https
2021-12-09T14:58:48.607105+00:00 app[web.1]: Disconnected XMwA_b32Te9hWySOAAAE
2021-12-09T14:58:48.607303+00:00 app[web.1]: Deleting user with socket id: XMwA_b32Te9hWySOAAAE
2021-12-09T14:58:48.607371+00:00 app[web.1]: Deleting User: 1000
2021-12-09T14:58:48.607540+00:00 app[web.1]: Map(1) { '1001' => { socket_id: 'Nc4KwKpmSxsiZAZ1AAAF' } }
2021-12-09T14:58:48.607581+00:00 app[web.1]: Online Users: 1
2021-12-09T14:58:50.328439+00:00 heroku[router]: at=info method=GET path="/socket.io/?from=1001&EIO=3&transport=websocket" host=e2eechat.herokuapp.com request_id=ba9ed824-c1d3-4b9c-b34c-e6ac92ab256d fwd="106.193.224.179" dyno=web.1 connect=0ms service=220649ms status=101 bytes=129 protocol=https
2021-12-09T14:58:50.326857+00:00 app[web.1]: Disconnected Nc4KwKpmSxsiZAZ1AAAF
2021-12-09T14:58:50.326982+00:00 app[web.1]: Deleting user with socket id: Nc4KwKpmSxsiZAZ1AAAF
2021-12-09T14:58:50.327056+00:00 app[web.1]: Deleting User: 1001
2021-12-09T14:58:50.327127+00:00 app[web.1]: Map(0) {}
2021-12-09T14:58:50.327166+00:00 app[web.1]: Online Users: 0
```

# Socket establish

```
2021-12-09T14:51:17.520795+00:00 heroku[router]: at=info method=GET path="/socket.io/?from=1001&EIO=3&transport=websocket" host=e2eechat.herokuapp.com request_id=d55d66b5-d962-43e3-8ccc-c24059c20960 fwd="106.193.224.179" dyno=web.1 connect=0ms service=202976ms status=101 bytes=129 protocol=https
2021-12-09T14:55:02.147212+00:00 app[web.1]: ------------------------------------
2021-12-09T14:55:02.147305+00:00 app[web.1]: Connected => Socket ID XMwA_b32Te9hWySOAAAE, User: {"from":"1000","EIO":"3","transport":"websocket"}
2021-12-09T14:55:02.147452+00:00 app[web.1]: Map(1) { '1000' => { socket_id: 'XMwA_b32Te9hWySOAAAE' } }
2021-12-09T14:55:02.147517+00:00 app[web.1]: Online Users: 1
2021-12-09T14:55:09.680219+00:00 app[web.1]: ------------------------------------
2021-12-09T14:55:09.680231+00:00 app[web.1]: Connected => Socket ID Nc4KwKpmSxsiZAZ1AAAF, User: {"from":"1001","EIO":"3","transport":"websocket"}
2021-12-09T14:55:09.680335+00:00 app[web.1]: Map(2) {
2021-12-09T14:55:09.680335+00:00 app[web.1]:   '1000' => { socket_id: 'XMwA_b32Te9hWySOAAAE' },
2021-12-09T14:55:09.680336+00:00 app[web.1]:   '1001' => { socket_id: 'Nc4KwKpmSxsiZAZ1AAAF' }
2021-12-09T14:55:09.680336+00:00 app[web.1]: }
2021-12-09T14:55:09.680352+00:00 app[web.1]: Online Users: 2
2021-12-09T14:55:20.293993+00:00 app[web.1]: checking if user is online
2021-12-09T14:55:20.294034+00:00 app[web.1]: Checking Online User: 1000
```

# Heroku Logs

```
2021-12-09T14:51:17.520795+00:00 heroku[router]: at=info method=GET path="/socket.io/?from=1001&EIO=3&transport=websocket" host=e2eechat.herokuapp.com request_id=d55d66b5-d962-43e3-8ccc-c24059c20960 fwd="106.193.224.179" dyno=web.1 connect=0ms service=202976ms status=101 bytes=129 protocol=https
```

```
2021-12-09T14:55:02.147212+00:00 app[web.1]:
----------------------------------------
2021-12-09T14:55:02.147305+00:00 app[web.1]: Connected => Socket ID
XMwA_b32Te9hWySOAAAE, User: {"from":"1000","EIO":"3","transport":"websocket"}
2021-12-09T14:55:02.147452+00:00 app[web.1]: Map(1) { '1000' => { socket_id:
'XMwA_b32Te9hWySOAAAE' } }
2021-12-09T14:55:02.147517+00:00 app[web.1]: Online Users: 1
2021-12-09T14:55:09.680219+00:00 app[web.1]:
----------------------------------------
2021-12-09T14:55:09.680231+00:00 app[web.1]: Connected => Socket ID
Nc4KwKpmSxsiZAZlAAAF, User: {"from":"1001","EIO":"3","transport":"websocket"}
2021-12-09T14:55:09.680335+00:00 app[web.1]: Map(2) {
2021-12-09T14:55:09.680335+00:00 app[web.1]:   '1000' => { socket_id:
'XMwA_b32Te9hWySOAAAE' },
2021-12-09T14:55:09.680336+00:00 app[web.1]:   '1001' => { socket_id:
'Nc4KwKpmSxsiZAZlAAAF' }
2021-12-09T14:55:09.680336+00:00 app[web.1]: }
2021-12-09T14:55:09.680352+00:00 app[web.1]: Online Users: 2
2021-12-09T14:55:20.293993+00:00 app[web.1]: checking if user is online
2021-12-09T14:55:20.294034+00:00 app[web.1]: Checking Online User: 1000
2021-12-09T14:55:20.294064+00:00 app[web.1]: To User Socket ID:
XMwA_b32Te9hWySOAAAE
2021-12-09T14:55:28.173218+00:00 app[web.1]: checking if user is online
2021-12-09T14:55:28.173245+00:00 app[web.1]: Checking Online User: 1001
2021-12-09T14:55:28.173273+00:00 app[web.1]: To User Socket ID:
Nc4KwKpmSxsiZAZlAAAF
2021-12-09T14:55:58.874282+00:00 app[web.1]: Message:
{"chat_id":0,"to":1001,"from":1000,"message":null,"chat_type":"single_chat","pu
blic_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAswQh/DxBlDrt/lqLKP2XUhIZ
otRBn1EKvzNNQ8VV323zb46xfokYFkJX16m+ZR9MiBFIcw2sFDACi/W4YDRCcp862+QA3Q89nA10ZJ6
KE25Sfrgp78PAKkCW3Y9JNkCJIad8yr1ZxGHZGIdrW1j9F8ayRgUvoUoEalwksS3m+qwRtEX6Ea6sxr
lTrUQWHsX7D8rOoom2JdQ59dXlBjcTilwCmb8t9MssfEOS5+mhd595csE4nAkRnX/cXP8TmdvJgztKZ
EfA1MqOp+vGA9oBa6hNrGk3yHapOgTak1jDXc8Hkyhfa6RWoim3C2LL02G6bL2KDs//CjoozRcZYJua
hQIDAQAB"}
2021-12-09T14:55:58.874311+00:00 app[web.1]: 1000=>1001
2021-12-09T14:55:58.874341+00:00 app[web.1]: to_user_socket_id:
Nc4KwKpmSxsiZAZlAAAF, userOnline: true
2021-12-09T14:55:58.874903+00:00 app[web.1]: Message Sent!!
```

2021-12-09T14:56:12.604827+00:00 app[web.1]: Message:
{"chat_id":0,"to":1000,"from":1001,"message":"RytjhktOE0SlutxHg8ZRbxSi6rtwxj11B
E+HuiaovGRO6pDpAbGDi/+ME+Tpkvlrz6XVYCNoQmcSIl6clFoYu56fbcAeeb494zDjIM1eaoBJCjxY
3yStHbbI+1IYCA1Sm+4CVGVDWpZVuZBIZACXMBbCLx+8mcAGuKma8vywNdiozJ5I2xCCqLQtM5Zj52W
mNby3mS1pvZOAyA0lboPkG0baC+oE2eSDZmM8DZsYq2V/zyXvCXCkAzpbJTFM9tUXD+QVc3A5X3rnXS
y4HJqmHjzl+Uh+WYe55SKy5bI3sSjyr7dc84jGp9eqeXipCZUR4sfPUUg/oob6TuXohVio6g=="," ch
at_type":"single_chat","public_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAuSr/RjKlKtOiMpIQnR5WwNuYwjJPZETY5vDEXHMguS4wpW6kPWm8z8nus0dgrj3fQTPWIjSfMl6li
oWnQqmGVsucZxhpL89N6kGepkgmhHL2pB3dpEDZYeSRiP4GXjVpjtjyifmEY5viS81jh68n8v0EAvT9
+qrjYeMGQPYN8YwxC+4WHT4sDqIyCL952AhCTwkrM7SID/zQWVyG4tZmNcChr/U35uXjEA1gonUWjDs
AYNtuNyC9Fb5kfDsn7V56k1w52pvD4GleUfh3YEpBR4BTtKRrFIwCAHlV/dWGY823McXFlCfuRrGgoF
e+VwUEPeITJn5D+iF34rgqWW7lxwIDAQAB"}
2021-12-09T14:56:12.604967+00:00 app[web.1]: 1001=>1000
2021-12-09T14:56:12.605016+00:00 app[web.1]: to_user_socket_id:
XMwA_b32Te9hWySOAAAE, userOnline: true
2021-12-09T14:56:12.605535+00:00 app[web.1]: Message Sent!!
2021-12-09T14:56:24.954100+00:00 app[web.1]: Message:
{"chat_id":0,"to":1001,"from":1000,"message":"XyqC8ciY/qI2j4v50RGk98R1AU8EWt2Zo
dfkYREL8UMThKcJrwVvsnMMHjRlXzusD3uAp5wHrldlCA7xFj51YD6xFXgHh6xkvgeWNC9YYR5j7Bmo
G6LwrBA5HWmM87MvwLHRw4JkErImHAIJk7NnyVqN6dsaQ77EXjks+6zNpOGWZHOiIFnYDivSKUmNG71
rqi93dpCJxvKB9OW+VFVouk5RSGsO7InCsX6imcNh2UKieDohJSBZ7TQ1I4Y+o2yoJlAR6m9tze3Xi3
pAh17syYg2vnhPrJmelatBOe4aefay+SWXigYLoPSQgvRiC+bHK43RU/qaWk2PPOIj0hM2KQ==","ch
at_type":"single_chat","public_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAswQh/DxBlDrt/lqLKP2XUhIZotRBn1EKvzNNQ8VV323zb46xfokYFkJX16m+ZR9MiBFIcw2sFDACi
/W4YDRCcp862+QA3Q89nA10ZJ6KE25Sfrgp78PAKkCW3Y9JNkCJIad8yr1ZxGHZGIdrW1j9F8ayRgUv
oUoEalwksS3m+qwRtEX6Ea6sxrlTrUQWHsX7D8rOoom2JdQ59dXlBjcTilwCmb8t9MssfEOS5+mhd59
5csE4nAkRnX/cXP8TmdvJgztKZEfA1MqOp+vGA9oBa6hNrGk3yHapOgTak1jDXc8Hkyhfa6RWoim3C2
LL02G6bL2KDs//CjoozRcZYJuahQIDAQAB"}
2021-12-09T14:56:24.954197+00:00 app[web.1]: 1000=>1001
2021-12-09T14:56:24.954240+00:00 app[web.1]: to_user_socket_id:
Nc4KwKpmSxsiZAZlAAAF, userOnline: true
2021-12-09T14:56:32.544099+00:00 app[web.1]: Message Sent!!
2021-12-09T14:56:41.047368+00:00 app[web.1]: Message:
{"chat_id":0,"to":1001,"from":1000,"message":"CGAvKBuYr6TFLqkj/VClJACGbQPSuN+Gn
hVdTaQRZ3KYFFJZxJMwPlI+3PbrfoutiQV0+06qHXeqmpo0Y4C/ZShC8onF7OWTmqHf9tYkjETiXjqd
ux9W+vsq34G7Cgu7di/WCO493oixKfu5fmBqq8zRtLnggWJ8Q9ZZjexQ3s+e3rV0/JF/+L6IA6aLlIh
g+GZrCJThlKyVqJMcp0eATnoGk5D57flfgSUK4sfGdqlfU9Ypr1ZIis+FYwAdQAtj3EmDqvNfHoaQnz
tlY6uU8dI8sZ7LRDgeWkpq9aZYJH8geL2SS6t5x5BuZQUxY302thFg9FneA6F0/An5Jp8new==","ch

at_type":"single_chat","public_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAswQh/DxBlDrt/lqLKP2XUhIZotRBn1EKvzNNQ8VV323zb46xfokYFkJX16m+ZR9MiBFIcw2sFDACi
/W4YDRCcp862+QA3Q89nA10ZJ6KE25Sfrgp78PAKkCW3Y9JNkCJIad8yr1ZxGHZGIdrW1j9F8ayRgUv
oUoEalwksS3m+qwRtEX6Ea6sxrlTrUQWHsX7D8rOoom2JdQ59dXlBjcTilwCmb8t9MssfEOS5+mhd59
5csE4nAkRnX/cXP8TmdvJgztKZEfA1MqOp+vGA9oBa6hNrGk3yHapOgTak1jDXc8Hkyhfa6RWoim3C2
LL02G6bL2KDs//CjoozRcZYJuahQIDAQAB"}
2021-12-09T14:56:41.047398+00:00 app[web.1]: 1000=>1001
2021-12-09T14:56:41.047426+00:00 app[web.1]: to_user_socket_id:
Nc4KwKpmSxsiZAZlAAAF, userOnline: true
2021-12-09T14:56:41.047925+00:00 app[web.1]: Message Sent!!
2021-12-09T14:56:50.687131+00:00 app[web.1]: Message:
{"chat_id":0,"to":1000,"from":1001,"message":"p3LV8oEf+zhezSALqLutOLgvK+5ffSr7W
qnYipUkGe8Cn2IfG2ikoYV5AN24/R2AUzXyUcBEDEDOsbEeyswOaGQshzjelLptqDf72aQ2cscTiQiz
czbEakkQ3e/Bfd73qvS85Mf0FrQAxWqp/AJbAVbJ+Av0lxPaw5AaJaxlTowYDceRhg7LR4lskAZy9c4
pVWGpRiG0FaHwI3bKHb0CwdLE3+vb1mWHcP+Evs75I3o6ZgJbWVFVnhBCHUyRqUTH2/M8WpyL1EE0IP
khA+oqISr86NOmJmCkoX0pivt68fVMzNxh5nzklgxWtJNNQMpq36j/OqeLZF0rLEYbDqtI7g==","ch
at_type":"single_chat","public_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAuSr/RjKlKtOiMpIQnR5WwNuYwjJPZETY5vDEXHMguS4wpW6kPWm8z8nus0dgrj3fQTPWIjSfMl6li
oWnQqmGVsucZxhpL89N6kGepkgmhHL2pB3dpEDZYeSRiP4GXjVpjtjyifmEY5viS81jh68n8v0EAvT9
+qrjYeMGQPYN8YwxC+4WHT4sDqIyCL952AhCTwkrM7SID/zQWVyG4tZmNcChr/U35uXjEA1gonUWjDs
AYNtuNyC9Fb5kfDsn7V56k1w52pvD4GleUfh3YEpBR4BTtKRrFIwCAHlV/dWGY823McXFlCfuRrGgoF
e+VwUEPeITJn5D+iF34rgqWW7lxwIDAQAB"}
2021-12-09T14:56:50.687250+00:00 app[web.1]: 1001=>1000
2021-12-09T14:56:50.687343+00:00 app[web.1]: to_user_socket_id:
XMwA_b32Te9hWySOAAAE, userOnline: true
2021-12-09T14:56:50.688201+00:00 app[web.1]: Message Sent!!
2021-12-09T14:58:48.610808+00:00 heroku[router]: at=info method=GET
path="/socket.io/?from=1000&EIO=3&transport=websocket"
host=e2eechat.herokuapp.com request_id=41c858a4-51ee-4a31-9e3d-f923e25f9ec6
fwd="106.193.224.179" dyno=web.1 connect=0ms service=226465ms status=101
bytes=129 protocol=https
2021-12-09T14:58:48.607105+00:00 app[web.1]: Disconnected XMwA_b32Te9hWySOAAAE
2021-12-09T14:58:48.607303+00:00 app[web.1]: Deleting user with socket id:
XMwA_b32Te9hWySOAAAE
2021-12-09T14:58:48.607371+00:00 app[web.1]: Deleting User: 1000
2021-12-09T14:58:48.607540+00:00 app[web.1]: Map(1) { '1001' => { socket_id:
'Nc4KwKpmSxsiZAZlAAAF' } }
2021-12-09T14:58:48.607581+00:00 app[web.1]: Online Users: 1

```
2021-12-09T14:58:50.328439+00:00 heroku[router]: at=info method=GET
path="/socket.io/?from=1001&EIO=3&transport=websocket"
host=e2eechat.herokuapp.com request_id=ba9ed824-c1d3-4b9c-b34c-e6ac92ab256d
fwd="106.193.224.179" dyno=web.1 connect=0ms service=220649ms status=101
bytes=129 protocol=https
2021-12-09T14:58:50.326857+00:00 app[web.1]: Disconnected Nc4KwKpmSxsiZAZlAAAF
2021-12-09T14:58:50.326982+00:00 app[web.1]: Deleting user with socket id:
Nc4KwKpmSxsiZAZlAAAF
2021-12-09T14:58:50.327056+00:00 app[web.1]: Deleting User: 1001
2021-12-09T14:58:50.327127+00:00 app[web.1]: Map(0) {}
2021-12-09T14:58:50.327166+00:00 app[web.1]: Online Users: 0
```

## Code

### Pseudo Code RSA Algo

```
int x = 61, int y = 53;
int n = x * y;
// n = 3233.

// compute the totient, phi
int phi = (x - 1) * (y - 1);
// phi = 3120.

int e = findCoprime(phi);
// find an 'e' which is > 1 and is a co-prime of phi.
// e = 17 satisfies the current values.

// Using the extended euclidean algorithm, find 'd' which satisfies
// this equation:
d = (1 mod(phi)) / e;
// d = 2753 for the example values.

public_key = (e = 17, n = 3233);
private_key = (d = 2753, n = 3233);

// Given the plaintext P=123, the ciphertext C is :
```

```
C = (123 ^ 17) % 3233 = 855;
// To decrypt the ciphertext C:
P = (855 ^ 2753) % 3233 = 123;
```

### Web Socket

- **Add individual user connection to socket**
  - onEachUserConnection(socket)
- **Receives message from client 1 and resent it to client2**
  - singleChatHandler(socket, chat_message)
- **If user request to leave chat**
  - onDisconnect(socket)
- **Internal function to remove user state**
  - removeUserWithSocketIdFromMap(socket_id)
- **Acknowledge user socket connection request**
  - sendBackToClient(socket,event,message)

## Output

Video link : video_demo_cns_e2ee.mp4

# ● Conclusions

In this report,, a secure mobile chat application was developed.The proposed architecture for a secure mobile chat application provides confidentiality, integrity and privacy for users who want to send text messages to each other without the need for extra hardware or physical tokens. Users can be confident that nobody, even not the provider of the service, can read their messages. Even in the case that a mobile phone reaches the wrong hands, no readable information can be extracted from the physical memory of the phone.

The major Challenges we face

1. Local environment linking between arm and x86.
2. Exchange of RSA keys between clients

- ## References


[1] Nirvan Tyagi, Ian Miers and Thomas Ristenpart, “Traceback for End-to-End Encrypted Messaging”, Published:06 November 2019, Available: https://dl.acm.org/doi/pdf/10.1145/3319535.3354243

[2] Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican and Kevin Milner, “On Ends-to-Ends Encryption Asynchronous Group Messaging with Strong Security Guarantees”,Published:15 October 2018, Available: https://dl.acm.org/doi/pdf/10.1145/3243734.3243747

[3] Paul Rosler, Christian Mainka, Jorg Schwenk, “More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema”, Published: 09 July 2018, Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8406614

[4] Wei Bai, Michael Pearson, Patrick Gage Kelley and Michelle L. Mazurek, “Improving Non-Experts’ Understanding of End-to-End Encryption: An Exploratory Study” , Published: IEEE 2020, Available:https://eusec20.cs.uchicago.edu/eusec20-Bai.pdf

[5] Michael Schliep and Nicholas Hopper, End-to-End Secure Mobile Group Messaging with Conversation Integrity and Deniability, published: November 11, 2019, available: https://dl.acm.org/doi/pdf/10.1145/3338498.3358644.

[6] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz and Melanie Volkamer, “Finally Johnny Can Encrypt. But Does This Make Him Feel More Secure?” , published: August 2018, Available: https://dl.acm.org/doi/10.1145/3230833.3230859

[7] Puneet Kumar Aggarwal, P.S. Grover, and Laxmi Ahuja, “Security Aspect in Instant Mobile Messaging Applications,” published:23 August 2018 . Available: https://ieeexplore.ieee.org/document/8443844 .