

A Report On

Cryptographic Secure Messaging System Using AES

Submitted by

Name	Entry Number
ARINDAM SAL	2024JCS2041
AYAN SHIL	2024JCS2048

1. Introduction & Goal of the Assignment

This assignment implements a secure messaging application that ensures confidentiality, integrity, message freshness, and username privacy using Advanced Encryption Standard (AES) encryption in CBC mode. We use password-derived keys to secure client-server communication, enabling safe message storage and retrieval by encrypting usernames and messages.

The following figure demonstrates the flow of messages and key generation. The sender uses a password to derive a key using PBKDF2, which, combined with a random Initialization Vector (IV), encrypts both the username and message content before sending it to the receiver.

Representation:

- **Sender (A) → Receiver (B)**
 - **Key Derivation (PBKDF2):** Converts password to key
 - **AES-CBC Mode:** Encrypts messages with confidentiality
 - **IV (Initialization Vector):** Unique per message for replay protection

2. Implementation Features

This section highlights the implementation features, with code snippets demonstrating each feature's fulfilment of assignment requirements.

2.1 Password-Derived Encryption Key (Using PBKDF2)

- The password is converted into a secure key using PBKDF2. This function generates a key using a salt to add entropy.

```
def derive_key(password, salt):  
    return PBKDF2(password, salt, dkLen=AES_KEY_SIZE)
```

2.2 AES Encryption with Random IV for Confidentiality

- AES encryption is performed in CBC mode, with a unique 16-byte IV for each message, ensuring each encrypted output remains distinct.

```
iv = get_random_bytes(AES_BLOCK_SIZE)  
cipher = AES.new(key, AES.MODE_CBC, iv)
```

2.3 Integrity and Replay Prevention with Random IVs

- A unique, random IV is generated for each message, preventing replay attacks and ensuring identical messages have unique encrypted outputs.

```
iv = get_random_bytes(AES_BLOCK_SIZE)
```

2.4 Socket-Based Client-Server Communication

- The client and server communicate over a secure socket, transferring encrypted messages and usernames.

```
with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:  
    s.connect((SERVER_IP, SERVER_PORT))  
    s.sendall(str(data_packet).encode())
```

2.5 Database Storage(SQLite3) for Encrypted Messages

- Each message is securely stored in an SQLite database, along with encrypted usernames, IVs, and salts.
- Additional admin features:
 - Admin can delete individual messages or clear the entire database.
 - Admin can decrypt messages if the correct password is provided.

```
def store_message(user_id, message, iv_user, iv_message, salt_user,  
salt_message):  
    conn = sqlite3.connect("messages.db")  
    # ... SQL insertion of encrypted message data ...
```

3. Security Objectives

This section describes how the implementation achieves the assignment's security objectives.

3.1 Confidentiality

- The encryption ensures that only intended recipients with the correct password can decrypt and read messages.
- **Screenshot:** Encrypted message in the database.

```
Enter Username: arindamsl
Enter Password:
Enter Message: Test1
Message sent securely!

Enter Username: ayanshil
Enter Password:
Enter Message: Hii
Message sent securely!
```

```
PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS
```

```
PS C:\Users\Arindam Sal\Desktop\IITD Data base\Semester-1\OIS-COL759\Assignment\Assignment-3\SecureMessagingApp> python server/server.py
Welcome Admin!
Enter Master Password to Start the Server:
Server started. Waiting for messages...
No messages received. Type 'exit' to stop or press Enter to check for new messages:

ID | Encrypted Username | Encrypted Message | Timestamp
1 | b'\x01\x0a\x0f4up\x07r\x0bf1\x09\x0f5\x08e\x0b2\x0fb\x0ea' | b'\x0a\x08av\x08\x0cf\x0d1\x0a3f\x0c05\x0c5\x0d8\x0e' | 2024-11-12 22:26:15.588214
2 | b'\x01\x0f\x0f42p\x0a1\x0a2r\x0f2\x0f0\x0d0\x0e0\x0e' | b'\x0e\x0f0f\x0f0d0\x085\x0a0\x0f7f\x0a0a1\x0b09\x0d0a' | 2024-11-12 22:26:59.315764
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit:
[]
```

3.2 Integrity

- The AES-CBC mode ensures that tampered messages fail to decrypt correctly, preserving the integrity of each message.

3.3 Message Freshness and Replay Attack Prevention

- Each message has a unique IV, ensuring identical messages appear differently in encrypted form, preventing replay attacks.

```

Enter Username: arindamsal
Enter Password:
Enter Message: Hello world
Message sent securely!

Enter Username: arindamsal
Enter Password:
Enter Message: Hello world
Message sent securely!

PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS
python +v [] ... ^ x

Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 1
Enter Password:
Decrypted Username: arindamsal
Decrypted Message: Hello world

ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\xf0\x9d\xcf\x7c\xdf\xaf\x0a\x18\r\xf4' | b':\x08{s8\x98\xf4\x08\xcb'\xebQ[4\xf5\xfe' | 2024-11-12 22:30:30.385707
2 | b'g:\x08\x08\x08/\xf6\x0a\x19\x030f\xcf\x02' | b'-[\xeb-\j\x04R0\x0bIn\x967:.' | 2024-11-12 22:30:58.332645
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 2
Enter Password:
Decrypted Username: arindamsal
Decrypted Message: Hello world

ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\xf0\x9d\xcf\x7c\xdf\xaf\x0a\x18\r\xf4' | b':\x08{s8\x98\xf4\x08\xcb'\xebQ[4\xf5\xfe' | 2024-11-12 22:30:30.385707
2 | b'g:\x08\x08\x08/\xf6\x0a\x19\x030f\xcf\x02' | b'-[\xeb-\j\x04R0\x0bIn\x967:.' | 2024-11-12 22:30:58.332645
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit:

```

3.4 Username Privacy

- Usernames are encrypted separately and stored with a fixed length (16 bytes max), ensuring privacy.
- **Screenshot:** Encrypted usernames stored in the database

```
ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\xf0\xfa\x94\x18\x18\x18\x18\x18\x18\x18\x18' | b'\x08{s&\xf4\xcb'\xebQ[4\xfe" | 2024-11-12 22:30:30.385707
2 | b'g\x86\x86\x86\x86\x86\x86\x86\x86' | b'|\xeb-\x04Ro\x8bIn\x967:)' | 2024-11-12 22:30:58.332645
```

3.5 Extra Layer of Security

- A master password protects sensitive operations on the server, like message deletion or database reset, adding an extra layer of security.
- **Screenshot:** Prompt for master password before performing admin actions

```
PS C:\Users\Arindam Sal\Desktop\IITD Data base\Semester-1\CNS-COL759\Assignment\Assignment-3\SecureMessagingApp> python server/server.py
Welcome Admin!
Enter Master Password to Start the Server:
Server started. Waiting for messages...

ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\xf0\xfa\x94\x18\x18\x18\x18\x18\x18\x18\x18' | b'\x08{s&\xf4\xcb'\xebQ[4\xfe" | 2024-11-12 22:30:30.385707
2 | b'g\x86\x86\x86\x86\x86\x86\x86\x86' | b'|\xeb-\x04Ro\x8bIn\x967:)' | 2024-11-12 22:30:58.332645
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: █
```

4. Environment Setup & Running the Application

Details on dependencies and the commands to set up and run the application.

4.1. Dependencies

- **Pythonpackages:** Need to Install required packages(`pycryptodome==3.14.1`, `sqlite3` etc) at both client and server sides:

```
pip install -r client/requirements.txt
```

```
pip install -r server/requirements.txt
```

4.2. Commands

- **Running the Server:** `python server/serevr.py`
- **Running the client:** `python client/client.py`

4.3. Master password: `admin007`

5. Testing Strategy

Each test case below verifies different aspects of the application.

5.1. Basic Message Encryption and Decryption

- Ensures the message encrypts and decrypts successfully.
- Screenshot:** Encrypted and decrypted messages match.

```
Enter Username: ayanshil
Enter Password:
Enter Message: This is a trial message....
Message sent securely!

PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS
PS C:\Users\Arindam Sal\Desktop\IITD Data base\Semester-1\QIS-COL759\Assignment\Assignment-3\SecureMessagingApp> python server/server.py
Welcome Admin!
Enter Master Password to Start the Server:
Server started. Waiting for messages...
No messages received. Type 'exit' to stop or press Enter to check for new messages:

ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\x04\x03*\x12\x15\x04\x03\x08\x94\x02' | b'\x06\xcc9\xfe\x878\x08P\x08\x09\x10\x19\x0cf\x10\xad\x05\xba\x05U\x14\x02HA\xdc*\xb8' | 2024-11-12 22:38:00.363052
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 1
Enter Password:
Decrypted Username: ayanshil
Decrypted Message: This is a trial message....
```

5.2. Maximum Username Length (16 Bytes)

- Verifies that usernames with exactly 16 bytes are encrypted and stored correctly.
- Screenshot:** Showing storage of 16-byte username.

```
Enter Username: abcdabdcabdcabdc
Enter Password:
Enter Message: 16 bit username length
Message sent securely!

Enter Username: []

PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS
PS C:\Users\Arindam Sal\Desktop\IITD Data base\Semester-1\QIS-COL759\Assignment\Assignment-3\SecureMessagingApp> python server/server.py
Welcome Admin!
Enter Master Password to Start the Server:
Server started. Waiting for messages...

ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\x04\x03*\x12\x15\x04\x03\x08\x94\x02' | b'\x06\xcc9\xfe\x878\x08P\x08\x09\x10\x19\x0cf\x10\xad\x05\xba\x05U\x14\x02HA\xdc*\xb8' | 2024-11-12 22:38:00.363052
2 | b'\x070\x93\x06\x01\x05\xfb\xfe\x09\x0e\x07'\x1e\x02\x08\x05j\x08j\x0e1\x009\x0f3\xcc\x08eh\x06\xfe' | b'\x91.\xc5\xa2$-\xa0\x11$ \x02e\x06-dh\x00\xff)\x06Ksy\x0eb\x0ea\x181\x08K*d\xfb8' | 2024-11-12 22:40:42.647723
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 2
Enter Password:
Decrypted Username: abcdabdcabdcabdc
Decrypted Message: 16 bit username length
```

5.3. Replay Attack Prevention

- Ensures unique IV for each identical message, preventing replays.
- **Screenshot:** Encrypted output differs for identical messages.

```
Enter Username: arindamsal
Enter Password:
Enter Message: Hello world
Message sent securely!

Enter Username: arindamsal
Enter Password:
Enter Message: Hello world
Message sent securely!
```

PROBLEMS DEBUG CONSOLE TERMINAL PORTS

```
python + v [ ] [X] ... ^ X

Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 1
Enter Password:
Decrypted Username: arindamsal
Decrypted Message: Hello world

ID | Encrypted Username | Encrypted Message | Timestamp
---|---|---|---
1 | b'\xafa\x94l\xc2\xc7-df\xcf\xaf\xaf\xaf\xaf\xaf' | b':\x08{s8\x98\xf4\xcb'\xeb0[4xf5\xfe' | 2024-11-12 22:30:30.385707
2 | b'g_\xae\x8e\xdb/\xf6\x8a\x19\xa30f'\xcf\xfd' | b'-|\xeb-\j\xcd4r0\x8bln\x967:)' | 2024-11-12 22:30:58.332645
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 2
Enter Password:
Decrypted Username: arindamsal
Decrypted Message: Hello world

ID | Encrypted Username | Encrypted Message | Timestamp
---|---|---|---
1 | b'\xafa\x94l\xc2\xc7-df\xcf\xaf\xaf\xaf\xaf\xaf' | b':\x08{s8\x98\xf4\xcb'\xeb0[4xf5\xfe' | 2024-11-12 22:30:30.385707
2 | b'g_\xae\x8e\xdb/\xf6\x8a\x19\xa30f'\xcf\xfd' | b'-|\xeb-\j\xcd4r0\x8bln\x967:)' | 2024-11-12 22:30:58.332645
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 
```

5.4. Invalid Password for Decryption

- Checks that decryption fails with an incorrect password.
- **Screenshot:** Failed decryption message.

```
Enter Username: abcdabcdabcdabcd
Enter Password:
Enter Message: 16 bit username length
Message sent securely!

Enter Username: [ ]

PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS

1 | b'\x05\x04\x03*11\x12\x15\x041\x03\x0c0k\x94\x02' | b'\xae\xcc9\xfe\x878\x08p\x0e0k\x091\x1eM\x191\x0cF\x10\x0ad\x06\x0ba\x05U\x141\x0b2H4\x0dc'\x08' | 2024-11-12 22:38:00.363052
2 | b'\xc\x878\x93\x06\x01\x05\x0f0\x0e\x09' \xc1e\x02\x02EL8\x05j\x081\x0e0Y\x0f3\x0cc\x08eh\x06\x0fe' | b'\x91.\x0c5\x0a25-\x0a0\x115\x02e\x096-df\x00\xff')\x06kcsy\x0aeb\x0ea\x181\x0e0k'd\x0f8' | 2024-11-12 22:40:42.647723
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 2
Enter Password:
Decrypted Username: abcdabcdabcdabcd
Decrypted Message: 16 bit username length

ID | Encrypted Username | Encrypted Message | Timestamp

1 | b'\x05\x04\x03*11\x12\x15\x041\x03\x0c0k\x04\x02' | b'\xae\xcc9\xfe\x878\x08p\x0e0k\x091\x1eM\x191\x0cF\x10\x0ad\x06\x0ba\x05U\x141\x0b2H4\x0dc'\x08' | 2024-11-12 22:38:00.363052
2 | b'\xc\x878\x93\x06\x01\x05\x0f0\x0e\x09' \xc1e\x02\x02EL8\x05j\x081\x0e0Y\x0f3\x0cc\x08eh\x06\x0fe' | b'\x91.\x0c5\x0a25-\x0a0\x115\x02e\x096-df\x00\xff')\x06kcsy\x0aeb\x0ea\x181\x0e0k'd\x0f8' | 2024-11-12 22:40:42.647723
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 2
Enter Password:
Decryption failed. Invalid password.
```

5.5. Special Characters in Username and Message

- Confirms that non-ASCII characters encrypt and decrypt correctly.
- **Screenshot:** Display of special characters after decryption.

[illegible]

5.6. Multiple Clients with the Same Password

- Checks that multiple clients can send messages securely.
- **Screenshot:** Shows encrypted messages from different clients.

```
Enter Username: client-1
Enter Password:
Enter Message: client-1 message
Message sent securely!

Enter Username: client-2
Enter Password:
Enter Message: client-2 message
Message sent securely!

Enter Username:
PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS

3 | b'\x1f\x01\x04\x0e90L5n_\x0e\xda\x086w\x12' | b'\x111\x0bmG-\xb05\x09\x07fD\x0a5\xfbf\x0c3f1t;?x0c\x01D\x04"@-\x00\x0eemI0" | 2024-11-12 22:44:32.772391
4 | b'\x02\x0b\x0c*\x0e\xca\xbd\x03'\x12\xcf\x01E"0" | b'E73]H0\xbd\x02\x04[T\x04\x05\x03\x03\x01\x0b\x0c\x09f\x0b\x08\x04\x00\x0a\rq\x0ce)\x088\x0b1' | 2024-11-12 22:46:01.764979
5 | b'\xfdf\x00\x078t>\x01\xdc\x0e\xfbvduv\x04' | b'\x0c\x07:\x0dg\x19\x05\x025\x04\x06)\x06\xfe\x05\x0a-\x17\x01b\xfb0e0D\x0e80\xfb\x0b1'\x03\x0c" | 2024-11-12 22:46:13.213402
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit:
4
Enter Password:
Decrypted Username: client-1
Decrypted Message: client-1 message

ID | Encrypted Username | Encrypted Message | Timestamp
-----
1 | b'\x05\x04\x03*11\x12\x15\x041\x0c3\x0c0k\x04\x02' | b'\x06\x0c9\xfe\x078\x08P\x0e8\x0b1\x010\x0191\x08cf\x10\xad\x06\x0a\x052\x1c14|\x02HA\xdc*\x0e' | 2024-11-12 22:38:00.363052
2 | b'\x070\x03\x06\x01\x05\xfbf\x0c9\x0e\x07"\x1e\x02\x0c2\x0c2EL8\x05j\x08j\x01\x0e0f\x03\x0cc\x08eh\x06\xfe' | b'\x01.\x05\x025-\x0a0\x115\x02e\x06-dh\x00\xff)\x06Ksy\x0eb\x0ea\x181\x0e8k'd\xfe' | 2024-11-12 22:40:42.647723
3 | b'\x1f\x01\x04\x0e90L5n_\x0e\xda\x086w\x12' | b'\x111\x0bmG-\xb05\x09\x07fD\x0a5\xfbf\x0c3f1t;?x0c\x01D\x04"@-\x00\x0eemI0" | 2024-11-12 22:44:32.772391
4 | b'\x02\x0b\x0c*\x0e\xca\xbd\x03'\x12\xcf\x01E"0" | b'E73]H0\xbd\x02\x04[T\x04\x05\x03\x03\x01\x0b\x0c\x09f\x0b\x08\x04\x00\x0a\rq\x0ce)\x088\x0b1' | 2024-11-12 22:46:01.764979
5 | b'\xfdf\x00\x078t>\x01\xdc\x0e\xfbvduv\x04' | b'\x0c\x07:\x0dg\x19\x05\x025\x04\x06)\x06\xfe\x05\x0a-\x17\x01b\xfb0e0D\x0e80\xfb\x0b1'\x03\x0c" | 2024-11-12 22:46:13.213402
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit: 5
Enter Password:
Decrypted Username: client-2
Decrypted Message: client-2 message
```

5.7. Empty Message

- Ensures that empty messages are encrypted and stored without errors.
- **Screenshot:** Show encrypted empty message.

```
Enter Username: clientX
Enter Password:
Enter Message:
Message sent securely!

Enter Username:
PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS

1 | b'\x05\x04\x03*11\x12\x15\x041\x0c3\x0c0k\x04\x02' | b'\x06\x0c9\xfe\x078\x08P\x0e8\x0b1\x010\x0191\x08cf\x10\xad\x06\x0a\x052\x1c14|\x02HA\xdc*\x0e' | 2024-11-12 22:38:00.363052
2 | b'\x070\x03\x06\x01\x05\xfbf\x0c9\x0e\x07"\x1e\x02\x0c2\x0c2EL8\x05j\x08j\x01\x0e0f\x03\x0cc\x08eh\x06\xfe' | b'\x01.\x05\x025-\x0a0\x115\x02e\x06-dh\x00\xff)\x06Ksy\x0eb\x0ea\x181\x0e8k'd\xfe' | 2024-11-12 22:40:42.647723
3 | b'\x1f\x01\x04\x0e90L5n_\x0e\xda\x086w\x12' | b'\x111\x0bmG-\xb05\x09\x07fD\x0a5\xfbf\x0c3f1t;?x0c\x01D\x04"@-\x00\x0eemI0" | 2024-11-12 22:44:32.772391
4 | b'\x02\x0b\x0c*\x0e\xca\xbd\x03'\x12\xcf\x01E"0" | b'E73]H0\xbd\x02\x04[T\x04\x05\x03\x03\x01\x0b\x0c\x09f\x0b\x08\x04\x00\x0a\rq\x0ce)\x088\x0b1' | 2024-11-12 22:46:01.764979
5 | b'\xfdf\x00\x078t>\x01\xdc\x0e\xfbvduv\x04' | b'\x0c\x07:\x0dg\x19\x05\x025\x04\x06)\x06\xfe\x05\x0a-\x17\x01b\xfb0e0D\x0e80\xfb\x0b1'\x03\x0c" | 2024-11-12 22:46:13.213402
6 | b'\xfaf\x0b1\x08\x04f\x0a(=\x0c' | b'\x08f\x01\x0cf\x0da\x0c\x03\x0bb6\x1c6\x08P.\x0f' | 2024-11-12 22:48:28.014332
Enter Message ID to view, 'delete <ID>' to delete a message, 'drop table' to delete all messages, or 'exit' to quit:
6
Enter Password:
Decrypted Username: clientX
Decrypted Message: [Empty Message]
```

5.8. Username Exceeds 16 Bytes

- Verifies that usernames longer than 16 bytes are rejected.
- **Screenshot:** Error message for username length limit.

```
Enter Username: ahcdabdcdbcdabdcdbcd
Enter Password:
Enter Message: Username Exceeds 16 Bytes
Error: Username cannot exceed 16 bytes in UTF-8. Please use a shorter username.
Enter Username:
PROBLEMS  DEBUG CONSOLE  TERMINAL  PORTS
```


5.9. Empty Password

- Checks that an empty password triggers an error.
- **Screenshot:** Error message for empty password.

```
Enter Username: userY
Enter Password:
Error: Attention!! Password cannot be empty. Please enter a valid Password.
Enter Username: 
```

PROBLEMS DEBUG CONSOLE TERMINAL PORTS

6. Empty Username

- Verifies that empty usernames are rejected.
- **Screenshot:** Error message for empty username.

```
Enter Username:
Error: Attention!! Username cannot be empty. Please enter a valid username.
Please enter a username that is 16 bytes or less.
Enter Username: 
```

PROBLEMS DEBUG CONSOLE TERMINAL PORTS

7. Server is Down

- Client fails to send message
- **Screenshot:** Handling when the server is down.

```
Enter Username: userZ
Enter Password:
Enter Message: Check server
OOPS!! Server Down. Message not sent.
```

```
Enter Username: 
```

PROBLEMS DEBUG CONSOLE TERMINAL PORTS

PS C:\Users\Arindam_Sa\\Desktop\IITD Data base\Semester-1\OIS-COL759\Assignment\Assignment-3\SecureMessagingApp>

6. Future Scope & Conclusion

6.1. Conclusion: This assignment effectively demonstrates secure message encryption, with additional features to enhance confidentiality, integrity, and replay protection in a simulated client-server setup. By ensuring encrypted storage of messages and adding a master password for server operations, this application lays a foundation for real-world secure communication systems.

6.2. Future Scope: Future improvements could include:

- Implementing a more robust key exchange protocol.
- Enhancing password security with multi-factor authentication.
- Adding message forwarding or deletion timestamps for better traceability.