# **REPORT**

### **Problem Statement:**

Cryptography Simulation with mbedTLS/OpenSSL Library Usage and User Interaction.

Team Name Team Size

Adventurers 2 (TWO)

Team Member 1 Team Member 2

Karthikeyan A Sri Ganesh R

**College Name:** Sairam Group of Institutions

# **Topics:**

- 1. Created Digital Certificates.
- 2. Implemented CryptoWrapper.
- 3. Secured the custom protocol.

#### 1. CREATED DIGITAL CERTIFICATES:

Name	Date modified	Туре	Size
📮 alice	25-06-2024 09:04	Security Certificate	2 KB
alice.csr	25-06-2024 09:03	CSR File	2 KB
alice.key	18-06-2024 08:47	KEY File	3 KB
🧓 bob	25-06-2024 09:04	Security Certificate	2 KB
bob.csr	25-06-2024 09:04	CSR File	2 KB
bob.key	18-06-2024 08:50	KEY File	3 KB
□ rootCA	18-06-2024 08:27	Security Certificate	2 KB
rootCA.key	18-06-2024 08:26	KEY File	3 KB

# 2. IMPLEMENTED "CryptoWrapper":

All 5 unit test cases have passed.

```
testHMAC PASSED!
The plaintext is the same - This is a secret plaintext that we want to protect testSymmetricEncryption PASSED!
Error in finalizing digest verify at verifyMessageRsa3072Pss testRsaSigning PASSED!
testDh PASSED!
Error in checking host at checkCertificate
Error in verifying store context at checkCertificate testCertificateChecking PASSED!
```

### 3. SECURED THE CUSTOM PROTOCOL:

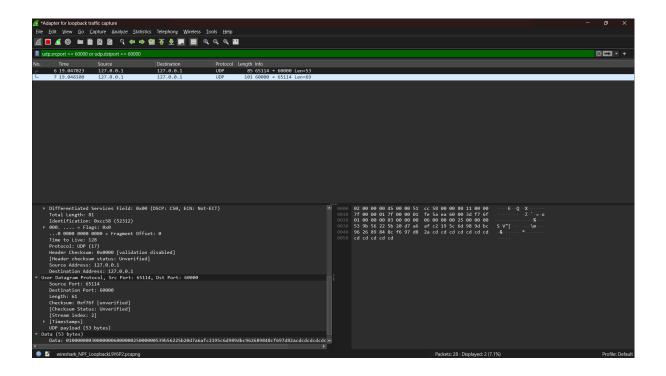
# Starting the server:

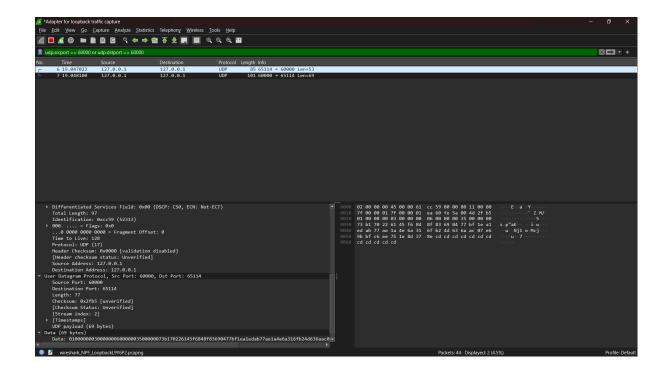
```
udp_party\x64\Debug>udp_party -port 60000 -key alice.key -pwd alice -cert alice.crt
-root rootCA.crt -peer Bob.com
Server: Starting listening...
```

# Starting the client:

```
udp_party\x64\Debug>udp_party -ip 127.0.0.1 -port 60000 -key bob.key -pwd bobkey -cert bob.crt -root rootCA.crt -peer Alice.com
Session started with Alice.com
Received response:"HI! I'M ELIZA. WHAT'S YOUR PROBLEM?"
```

#### View Packets from wire shark:





\*\* Wireshark capture has been attached to github repo in both Insecure Channel (before implementation) and Secured Channel (after implementation) folders. \*\*