Problem Statement

Cryptography Simulation with mbedTLS/OpenSSL
Library Usage and User Interaction

Unique Idea Brief (Solution)

Developing a cryptography simulation for securing communication with functions for key generation encrypting, decrypting data, digital signatures etc.

Features Offered

- Cryptographic Algorithms
    - Symmetric Encryption: AES
    - Asymmetric Encryption: RSA
    - Hashing Algorithms:SHA-384, MD5
    - Message Authentication Codes (MACs): HMAC (Hash-based Message Authentication Code)

- Public Key Infrastructure (PKI):
    - Certificate Generation: Creation of X.509 certificates.
    - Certificate Signing Requests (CSRs): Generation and handling of CSRs.
    - Certificate Authority (CA) Operations:
    - Certificate Validation:

- Digital Signatures:
  - Signing and verifying data with digital signatures.
- Key Management
  - Generation, storage, and management of cryptographic keys.
- Data Integrity:
  - Using cryptographic hashes and HMACs to ensure data integrity.

Process flow

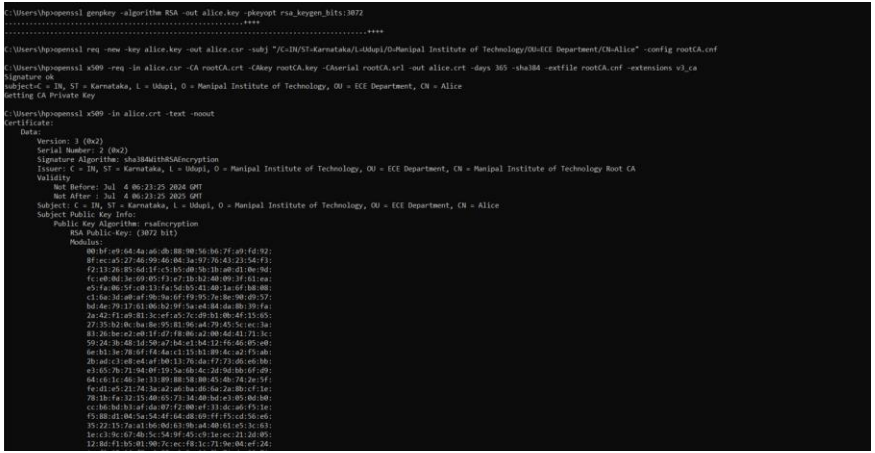
Exercise 1: Creating digital certificates

1. Self Signed root certificate(rootCA.crt) is created with RSA key size of 3072 with SHA384 and serial number as 01
   - Generate the RSA Private Key (3072 bits)
   - Generate the Self-Signed Root Certificate
   - Generate the Root Certificate using the Configuration File:

2. RSA keypair of size 3072 with SHA384 for “Alice” and sign with root CA and serial number as 02
   - Generate Alice's Private Key
   - Generate Alice's Certificate Signing Request (CSR)
   - Sign Alice's CSR with Root CA

3. RSA keypair of size 3072 with SHA384 for “Bob” and sign with root CA and set serial number 03

- Generate RSA Key for Bob
- Create a CSR for Bob
- Set the Serial Number for Bob's Certificate
- Sign Bob's CSR with the Root CA and Set the Serial Number

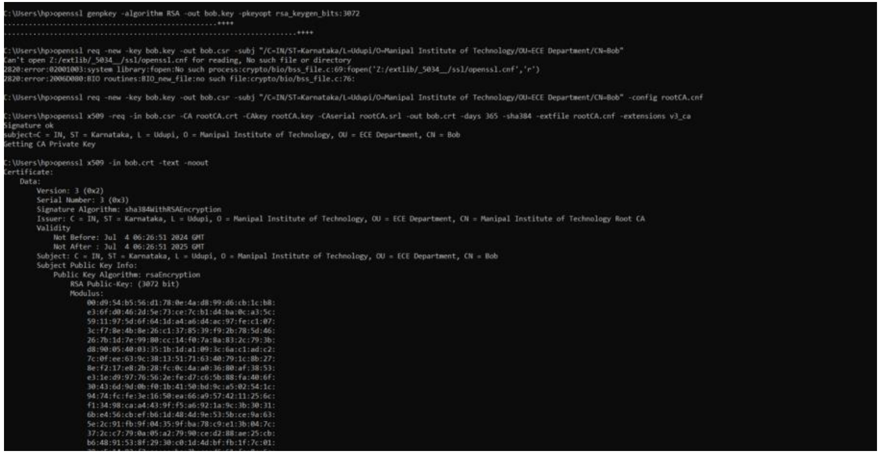


```
C:\Users\hp>openssl genpkey -algorithm RSA -out alice.key -pkeyopt rsa_keygen_bits:3072
..............................................................++++
..................................................................................++++

C:\Users\hp>openssl req -new -key alice.key -out alice.csr -subj "/C=IN/ST=Karnataka/L=Udupi/O=Manipal Institute of Technology/OU=ECE Department/CN=Alice" -config rootCA.cnf

C:\Users\hp>openssl x509 -req -in alice.csr -CA rootCA.crt -CAkey rootCA.key -CAserial rootCA.srl -out alice.crt -days 365 -sha384 -extfile rootCA.cnf -extensions v3_ca
Signature ok
subject=C = IN, ST = Karnataka, L = Udupi, O = Manipal Institute of Technology, OU = ECE Department, CN = Alice
Getting CA Private Key

C:\Users\hp>openssl x509 -in alice.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: C = IN, ST = Karnataka, L = Udupi, O = Manipal Institute of Technology, OU = ECE Department, CN = Manipal Institute of Technology Root CA
        Validity
            Not Before: Jul  4 06:23:25 2024 GMT
            Not After : Jul  4 06:23:25 2025 GMT
        Subject: C = IN, ST = Karnataka, L = Udupi, O = Manipal Institute of Technology, OU = ECE Department, CN = Alice
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (3072 bit)
                Modulus:
                    00:bf:e9:64:4a:a6:db:88:90:56:b6:7f:a9:fd:92:
                    8f:ec:a5:27:46:99:46:04:3a:97:76:43:23:54:f3:
                    f2:13:26:85:6d:1f:c5:b5:d0:5b:1b:a0:d1:0e:9d:
                    fc:e0:0d:3e:69:05:f3:e7:1b:b2:40:09:3f:61:ea:
                    e5:fa:06:5f:c0:13:fa:5d:b5:41:40:1a:6f:b8:08:
                    c1:6a:3d:a0:af:9b:9a:6f:f9:95:7e:8e:90:d9:57:
                    bd:4e:79:17:61:06:b2:9f:5a:e4:84:da:8b:39:fa:
                    2a:42:f1:a9:81:3c:ef:a5:7c:d9:b1:0b:4f:15:65:
                    27:35:b2:0c:ba:8e:95:81:96:a4:79:45:5c:ec:3a:
                    83:26:be:e2:e0:1f:d7:f8:06:a2:00:4d:41:71:3c:
                    59:24:3b:48:1d:50:a7:b4:e1:b4:12:f6:46:05:e0:
                    6e:b1:3e:78:6f:f4:4a:c1:15:b1:89:4c:a2:f5:ab:
                    2b:ad:c3:e8:e4:af:b0:13:76:da:f7:73:d6:e6:bb:
                    e3:65:7b:71:94:0f:19:5a:6b:4c:2d:9d:bb:6f:d9:
                    64:c6:1c:46:3e:33:89:88:58:80:45:4b:74:2e:5f:
                    fe:d1:e5:21:74:3a:a2:a6:ba:d6:6a:2a:8b:cf:1e:
                    78:1b:fa:32:15:40:65:73:34:40:bd:e3:05:0d:b0:
                    cc:b6:bd:b3:af:da:07:f2:00:ef:33:dc:a6:f5:1e:
                    f5:88:d1:04:5a:54:4f:64:d8:69:ff:f5:cd:56:e6:
                    35:22:15:7a:a1:b6:0d:63:9b:a4:40:61:e5:3c:63:
                    1e:c3:9c:67:4b:5c:54:9f:45:c9:1e:ec:21:2d:05:
                    12:8d:f1:b5:01:90:7c:ec:f8:1c:71:9e:04:ef:24:
```



```
C:\Users\hp>openssl genpkey -algorithm RSA -out bob.key -pkeyopt rsa_keygen_bits:3072
.....................................................++++
........................................................................++++

C:\Users\hp>openssl req -new -key bob.key -out bob.csr -subj "/C=IN/ST=Karnataka/L=Udupi/O=Manipal Institute of Technology/OU=ECE Department/CN=Bob"
Can't open Z:/extlib/_5034__/ssl/openssl.cnf for reading, No such file or directory
2820:error:02001003:system library:fopen:No such process:crypto/bio/bss_file.c:69:fopen('Z:/extlib/_5034__/ssl/openssl.cnf','r')
2820:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:76:

C:\Users\hp>openssl req -new -key bob.key -out bob.csr -subj "/C=IN/ST=Karnataka/L=Udupi/O=Manipal Institute of Technology/OU=ECE Department/CN=Bob" -config rootCA.cnf

C:\Users\hp>openssl x509 -req -in bob.csr -CA rootCA.crt -CAkey rootCA.key -CAserial rootCA.srl -out bob.crt -days 365 -sha384 -extfile rootCA.cnf -extensions v3_ca
Signature ok
subject=C = IN, ST = Karnataka, L = Udupi, O = Manipal Institute of Technology, OU = ECE Department, CN = Bob
Getting CA Private Key

C:\Users\hp>openssl x509 -in bob.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: C = IN, ST = Karnataka, L = Udupi, O = Manipal Institute of Technology, OU = ECE Department, CN = Manipal Institute of Technology Root CA
        Validity
            Not Before: Jul  4 06:26:51 2024 GMT
            Not After : Jul  4 06:26:51 2025 GMT
        Subject: C = IN, ST = Karnataka, L = Udupi, O = Manipal Institute of Technology, OU = ECE Department, CN = Bob
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (3072 bit)
                Modulus:
                    00:d9:54:b5:56:d1:78:0e:4a:d8:99:d6:cb:1c:b8:
                    e3:6f:d0:46:2d:5e:73:ce:7c:b1:d4:ba:0c:a3:5c:
                    59:11:97:5d:6f:64:1d:a4:a6:d4:ac:97:fe:c1:07:
                    3c:f7:8e:4b:8e:26:c1:37:85:39:f9:2b:78:5d:46:
                    26:7b:1d:7e:99:80:cc:14:f0:7a:8a:83:2c:79:3b:
                    d8:90:05:40:03:35:1b:1d:a1:09:3c:6a:c1:ad:c2:
                    7c:0f:ee:63:9c:38:13:51:71:63:40:79:1c:8b:27:
                    8e:f2:17:e8:2b:28:fc:0c:4a:a0:36:80:af:38:53:
                    e3:1e:d9:97:76:56:2e:fe:d7:c6:5b:88:fa:40:6f:
                    30:43:6d:9d:0b:f0:1b:41:50:bd:9c:a5:02:54:1c:
                    94:74:fc:fe:3e:16:50:ea:66:a9:57:42:11:25:6c:
                    f1:34:98:ca:a4:43:9f:f5:a6:92:1a:9c:3b:30:31:
                    6b:e4:56:cb:ef:b6:1d:48:4d:9e:53:5b:ce:9a:63:
                    5e:2c:91:fb:9f:04:35:9f:ba:78:c9:e1:3b:04:7c:
                    37:2c:c7:79:0a:05:a2:79:90:ce:d2:88:ae:25:cb:
                    b6:48:91:53:8f:29:30:c0:1d:4d:bf:fb:1f:7c:01:
```

Technologies used

1. OpenSSL Library:

- Cryptographic Algorithms
- X.509 Certificates: Manages digital certificates for authentication and secure communication.

2. Programming Languages:

- C++: Primary language for implementing OpenSSL.

3. Integrated Development Environment (IDE):

- Microsoft Visual Studio: Microsoft Visual Studio provides a comprehensive Integrated Development Environment (IDE) for coding, debugging, and testing the cryptography simulation tool.

Team members and contribution:

Team size- 1
Name: Delisha Carol Dsouza
Contribution: Whole project

Conclusion

Cryptography simulation with OpenSSL libraries provides a comprehensive and versatile platform for exploring and implementing a wide array of cryptographic operations. The simulation tool that makes use of the OpenSSL library offers a useful combination of instruction and real-world application. It offers capabilities including hashing techniques like SHA-256 and MD5, RSA-based digital signatures, encryption and decryption modes like CBC and ECB, and RSA and AES key creation.

Through the use of OpenSSL for cryptography simulation, comprehension and expertise is improved in the field of cybersecurity by gaining real-world experience and practical insights into cryptographic techniques and protocols.