Programming Assignment using OpenSSL

Group Size: 2 (Alice and Bob)

Note: While generating keys and files, prefix the filenames with either "**Alice**" or "**Bob**", depending on the entity you are representing. This prevents confusion and avoids overwriting existing files.

Part A: Authentication Using RSA

1. **Key Generation:**
   - Alice and Bob will each generate a 2048-bit RSA public-private key pair.
   - The private key on each system must be protected with a secure passphrase.
2. **Public Key Sharing:**
   - Alice and Bob will exchange(via secure email, google chat, etc..) their RSA public keys.
3. **Signature and Verification:**
   - Each participant will create a text file containing their roll number and then generate a signature on it using their private key.
   - The generated signature will then be shared with the other participant.
   - Upon receiving the signature, each participant will verify it using the sender's shared public key to authenticate.

Part B: Key Exchange Using Diffie-Hellman (DFH)

1. **Parameter Generation:**
   - Alice will generate the Diffie-Hellman (DFH) parameters.
   - The DFH parameters will be encrypted using Bob’s RSA public key and shared securely.
2. **Parameter Decryption:**
   - Bob will decrypt the received DFH parameters using his private RSA key.
3. **Key Pair Generation:**
   - Both participants will independently generate DFH key pairs based on the shared parameters.

4. **Shared Secret Computation:**
    - Alice and Bob will exchange their DFH public keys and compute a shared secret.
5. **AES Key Derivation:**
    - The DFH shared secret will be used to derive a symmetric AES key.

Part C: Secure File Sharing Using AES

1. **File Encryption:**
    - Alice will encrypt a text file using the AES key derived in Part B.
2. **File Transmission:**
    - The encrypted file will be shared with Bob.
3. **File Decryption:**
    - Bob will decrypt the file using the shared AES key to retrieve the original content.

Note:

- All cryptographic operations must be implemented using OpenSSL.
- Sharing files (keys, signatures, etc…) will be done via email, google chat.
- A 10% penalty will be applied for each day the submission is late.

What to deliver:

- A report (Name: ***<Group_Number>_Asg_OpenSSL.pdf***) with **all the steps mentioned in detail with screenshots**.
- Mention the Name of the group members and group number at the top of your report.
- If you use LLM's (ChatGPT, DeepSeek etc…), then mention the respective screenshots in your report.
- Add the Anti-Plag Statement in the end of your report

Anti-Plag Statement

We certify that this assignment/report is the result of our collaborative work, based on our collective study and research. All sources, including books, articles, software, datasets, reports, and communications, have been properly acknowledged. This work has not been previously submitted for assessment in any other course unless specific permission was granted by all involved instructors.

We also acknowledge the use of AI tools, such as LLMs (e.g., ChatGPT), for assistance in refining this assignment, if used. We have ensured that their usage complies with the academic integrity policies of this course. We pledge to uphold the principles of honesty, integrity, and responsibility at CSE@IITH.

Additionally, we understand our duty to report any violations of academic integrity by others if we become aware of them.

Names <Roll Nos>:

Date:

Signatures: <keep your initials here>