Create two directories: alice and bob. The action to be carried out by Alice should be done in her directory. Same goes for Bob. Sending the file from one user to another is same as copying from directory of one user to another.

Confidentiality

1. Alice creates a random key of size 128 bits and stores it in file **symm.key**. This key will be used for the purpose of encrypting and decrypting data using symmetric ciphers.
2. Alice creates a file **plain.txt**, adds some dummy data to the file.
3. Alice encrypts the contents of **plain.txt** to **cipher.txt** using AES-128 algorithm in CBC mode. Use **symm.key** for the purpose of encryption.
4. Alice creates a 2048 bit RSA private key. Store in file **alicepriv.key**.
5. Alice extracts the public key from **alicepriv.key** and store in file **alicepub.key**.
6. Repeat step 4 and 5 to create private and public key of Bob. **bobpriv.key** and **bobpub.key**. Alice and Bob exchange their public keys.
7. Alice sends **cipher.txt** to Bob.
8. Alice encrypts **symm.key** using the public key of Bob. Store in **symm.enc.key**.
9. Bob decrypts **symm.enc.key** using his private key and stores the output in **symm.dec.key**.
10. Bob decrypts **cipher.txt** using **symm.dec.key** and stores the output in **cipher.dec.txt**. The **cipher.dec.txt** and **plain.txt** should have same contents.

Integrity Check

11. Alice computes sha-512 hash on **plain.txt** and store in **hash.txt**.
12. Alice verifies the hash.
13. Make minor changes to **plain.txt** and check that verification of hash now fails.

Authentication check

14. Alice computes MAC on **plain.txt** using sha-512 and store in **plain.mac**.
15. Alice verifies the MAC.
16. Make minor changes to **plain.txt** and check that verification of MAC now fails.

Digital Signature

17. Alice creates sha-512 hash on **plain.txt** and signs it using her private key. Store signed hash in file **hash.sign**.
18. Alice sends **plain.txt** and **hash.sign** to Bob.
19. Bob verifies the signature using the public key of Alice.
20. Check that the verification fails if the file **plain.txt** is modified.