Thursday, 15 April 2021

NETWORK SECURITY AND CRYPTOGRAPHY

IMPLEMENTATION / readme OF ASSIGNMENT 2:

- Used make command on Mac terminal in order to build the program.
- After that in order to implement the code please refer the **screenshot-1** , ./client_new/main or ./client
- As the flow diagram suggests , we have to ask the server for the parameters the client will pause it 's execution and wait for the server parameters.
- After getting server's parameter[or only public key can also be send] just for the acknowledgment I am displaying that on the terminal.
- After that the execution at server's side is paused and will wait for encrypted secret key , client signature and client public key for further processing.
- At client side we need to enter the text and cipher key and S-AES will be implemented on it **screenshot-2** .[please refer S-AES for readme content of that algorithm].
- At client side now we have to enter the parameters for client side , that is two prime numbers **screenshot-3**.
- If these prime numbers are not prime , then code will straight away call exit(1) and terminates code.
- After that it will show all possible values of e and d . I am using the first value from the array for e and d in all cases at both server's side and client side.
- Client signature is created and can be scene at **screenshot-4**.
- At client side again it will follow the flow chart and will generate the encrypted secret key , as seen in **screenshot-4.**
- After that all of these content will be transmitted to server using tcp-ip system calls , as done for transmission of parameters of server before[please refer **tcp-ip**].
- Now the server will resume it 's execution after this fairly long pause waiting for encrypted secret key , client signature and client public key.
- At server side after screenshot-1 we need to ask parameters from user before server faces the fairly long pause waiting for content.

- After getting all the content server follows the flow diagram and calculates secret key .
- After that using s-aes calculates the message and then the digest and digital signature as well.
- Digital signature then will be compared with the one generated at client side , then it shows verified if both are same otherwise unverified.
- Another set of output is generated which can be scene from a1,a2.
- Functions used encrypt - is used in any type of encryption using rsa.
- Functions used decrypt - is used in any type of decryption using rsa.
- Other functions are just supporting functions in the algorithms that does minute help or described in readme S-AES.