Basic SFTP

- Client ‘A’ and Server ‘B’ on first connect do a **Diffie-Hellman Key exchange**.
- For the rest of the term of ‘A’, always used above established key for communications with ‘B’.
- The large primes for above DH Key Exchange are generated using the **Miller-Rabin Primimality Test**.
- The client then provides a command line interface with four different commmands:
    - **newlogin** - Create a newlogin takes input a username and password
    - **login** - Login into server takes input a username and password
    - **getfile** - Retrieve a file from the server
    - **logout** - exit the logged in session
    - **quit** - exit and close the client
- The login requests are encrypted using a **Caesar-Cipher**.
- The passwords are stored on the server using **SHA1-Digest**.

Protocol Messages during data

- **Each message/packet has the below components:**

Field	Purpose
opcode	opcode for a message
s_addr	source address
d_addr	destination address
buf	Contains a plaintext message (for example some part of a transmitted file)
ID	The identifier of a user
q	A prime
password	Password chosen by the user

Field	Purpose
status	SUCCESSFUL or UNSUCCESSFUL for successful or unsuccessful result
file	The file which will be transmitted by the server to the client
dummy	dummy variable is used when necessary

- **Opcodes for each Packet**

Opcode	Message	Description
10	LOGINCREAT	a login create request to the server by the client
20	LOGINREPLY	an acknowledgment for successful login create request
30	AUTHREQUEST	a request for accessing service from the server
40	AUTHREPLY	successful/unsuccessful authentication from the client
50	SERVICEREQUEST	service requested to the server by a client
60	SERVICEDONE	File transfer will take place only if the file is in the server

References

- Miller-Rabin Primes