

SFTP Explained

FTP (File Transport Protocol) is a well known and widely used protocol for moving data over the internet.

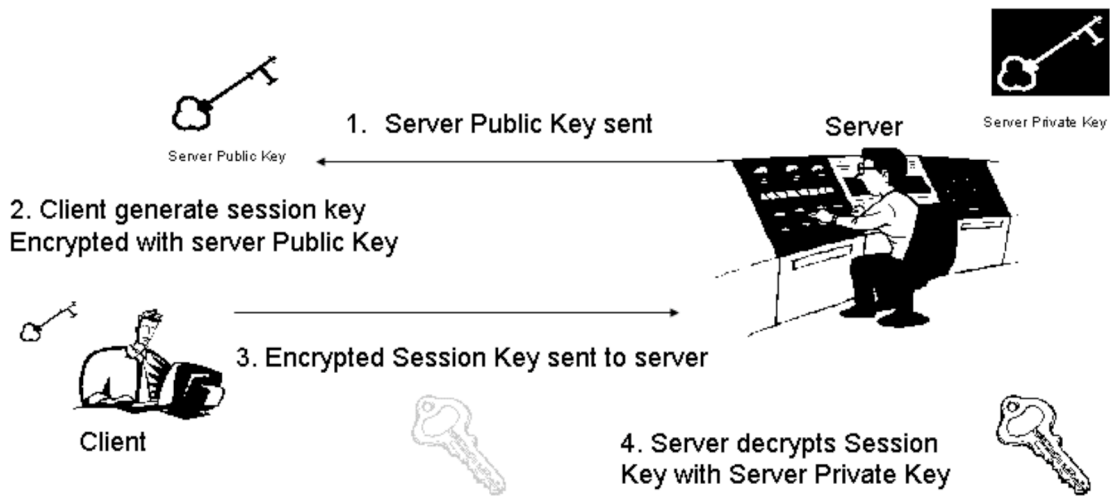
FTP however does not have any security. The packets of data are sent in clear text and hence can be “eaves dropped” by anyone “listening” to the connection. FTP caters only for password authentication which can be easily overcome.

Built into the SSH protocol suite is a companion protocol called Secure FTP (SFTP). The SFTP protocol works identically to FTP; however it also uses encryption (making the data impossible to read by a 3rd party) and authentication (ensuring the recipient/sender is who they claim to be).

The Authentication/encryption Method it uses is best explained by the following 2 diagrams:

This is the 1st Step Used to set up Encryption

SSH 2 Transport Layer established 1st before main body of data is sent



Public Private Key Principal

- Anyone can have your public key
- Only you should have your private key
- Data encrypted with a public key can only be decrypted with the corresponding private key !

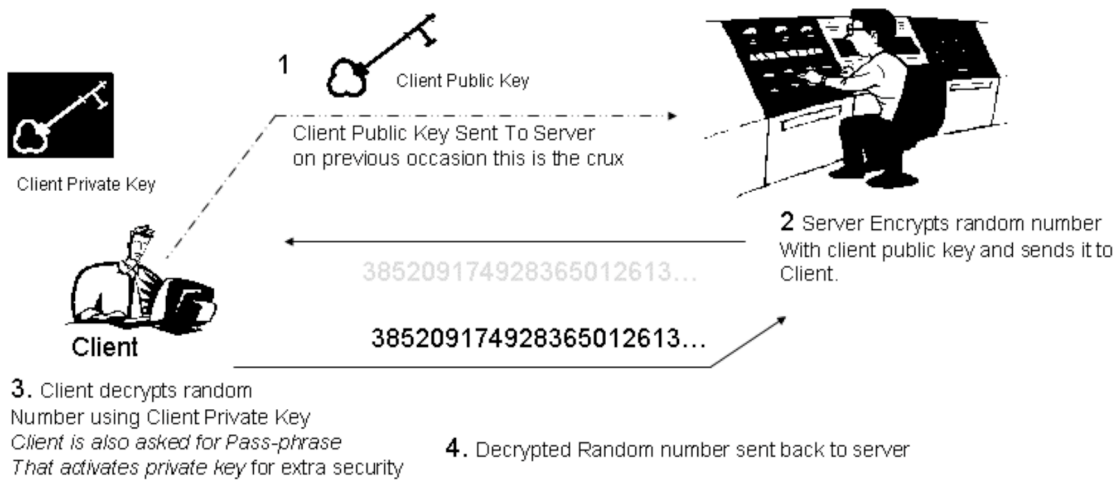
5. ALL FURTHER DATA TRANSMISSION IS ENCRYPTED WITH SESSION KEY

every new session has a new key !

This is the 2nd Step where the Client is Authenticated

SSH 2 Authentication Layer established 2nd Used for main body of data
Is The Client Really The Client and not a 3rd Party?

Public Key Authentication Method



Public Private Key Principal

- Anyone can have your public key
- Only you should have your private key
- Data encrypted with a public key can only be decrypted with the corresponding private key !

5. Server compares the 2 Random numbers
If they equal then the connection is allowed