Stylized ssh negotiation

This is a simplified representation of what happens when you logon to an ssh server using a password.

Note: secrets are *red*

Client

Server

ssh_host_key.pub=”yhnu”
ssh_host_key.priv=”qazw”
/etc/passwd

Can we talk? →

← Yes. Here is my public key: “yhnu”

ssh_host_key.pub=“yhnu”

Client generates a random
secret session key.
key_session = “edcr”

Client encrypts *key_session* with the server's public key.
Encrypt(key=ssh_host_key.pub, msg=*”edcr”*) => “rfvt”

Here is a session key only you can decrypt “rfvt” →

Server decrypts session key.
Decrypt(key=*ssh_host_key.priv*, “rfvt”) => *“edcr”*
key_session=”edcr”

We have a secret shared by client and server (*key_session=”edcr”*)

Encrypt(key=*session_key*, msg=*”user1/pass123”*)
=> “udsepnoeuhwbd”

Here is my logon info “udsepnoeuhwbd” →

Decrypt(key=*session_key*,msg=”udsepnoeuhwbd”)
=> *“user1/pass123”*