Cheatography

SSH Working Cheat Sheet

by Vasiq Mz (vasiqmz) via cheatography.com/39007/cs/12167/

Symmetric Encryption

Same key is used for encryption and decryption

Also used to encrypt the entire SSH session but not the authentication

This key is created using Key Exchange Algorithm - Diffie Hellman

The keys are session based so it can only be used for the current session

Asymmetric Encryption

Uses public-private key pair

Public Key is known to everyone and is used to encrypt data

Private Key is only known to the key owner and used to perform decryption

SSH uses this encryption technique to come up with a private key or symmetric key used for session-based encryption

SSH Connection - Stage 1

Server checks for supported Protocol version

Both parties then negotiates a session key using a Diffie-Hellman algorithm (explained separately)

The session key is used to encrypt the entire session

The public-private key pair used here is separate then the SSH keys generated above

SSH Connection - Stage 2

SSH key pair based authentication

Client sends the Key ID to the SSH Server

Server check the key ID in its authorized keys file

If matching public key is present, then server generates a random number and uses the public key to encrypt it

The client then uses it's private key to decrypt the generated random number and reveal the original number

The client combines the decrypted number with the shared session key used to encrypt the session, and calculates the MD5 hash of it

The client send the MD5 hash to the server, to which the server then compares it with it's own calculated MD5 hash

If the client & server's MD5 hash matches then the user is authenticated

By **Vasiq Mz** (vasiqmz)
cheatography.com/vasiqmz/

Published 23rd June, 2017.
Last updated 23rd June, 2017.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com