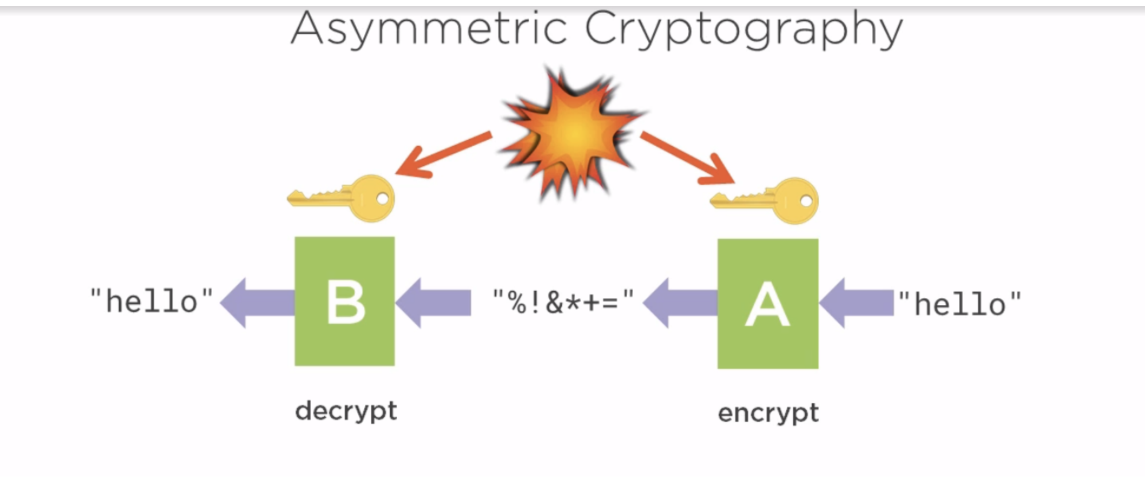
Shell Scripting - Module 8

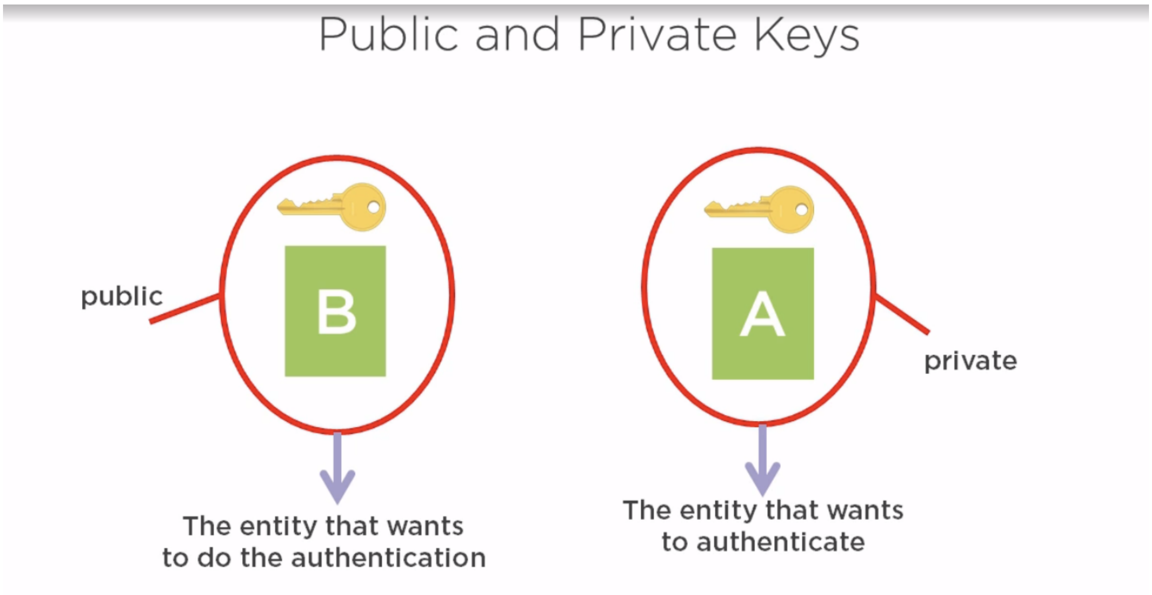
SSH

What is SSH ?

- **SSH used for secure remote command line access.**
- **Enables cryptographic handshake.**
- **Authenticates server securely and exchanges encryption key.**

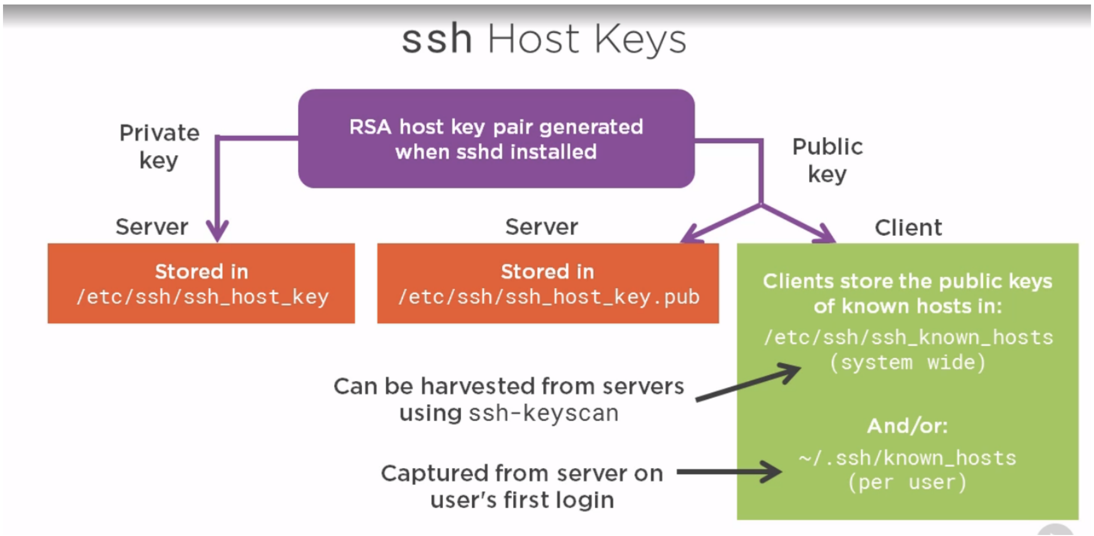


- **Public key and Private key plays vital role in encryption and decryption.**



When you sent " Hello" to server it will be encrypted by Key A and for Decryption it will not use the same key (Key B) Refer Image.

- **SSH host keys**



ssh Host Keys

RSA host key pair generated when sshd installed

Private key

Public key

Server

Stored in /etc/ssh/ssh_host_key

Server

Stored in /etc/ssh/ssh_host_key.pub

Client

Clients store the public keys of known hosts in:

/etc/ssh/ssh_known_hosts (system wide)

And/or:

~/.ssh/known_hosts (per user)

Can be harvested from servers using ssh-keyscan

Captured from server on user's first login

Why using SSH is secure ?

- **Well when you connect to a server using ssh there is a fancy cryptographic handshake which authenticates the server.**
- **Then it securely exchange the encryption key which is used to encrypt all the traffic between the client and server.**
- **SSH uses Asymmetric Cryptography (which means key used for encryption and Decryption is different)**
- **We spoke about 2 keys in that one would be acting as public key and other one would be acting as private key.**
- **Private key is ment to be kept secret**
- **Public key can be shared among others.**
- **Also there is a fancy algorithm called "diffie hellman" that makes these 2 keys to share the information secretly.**