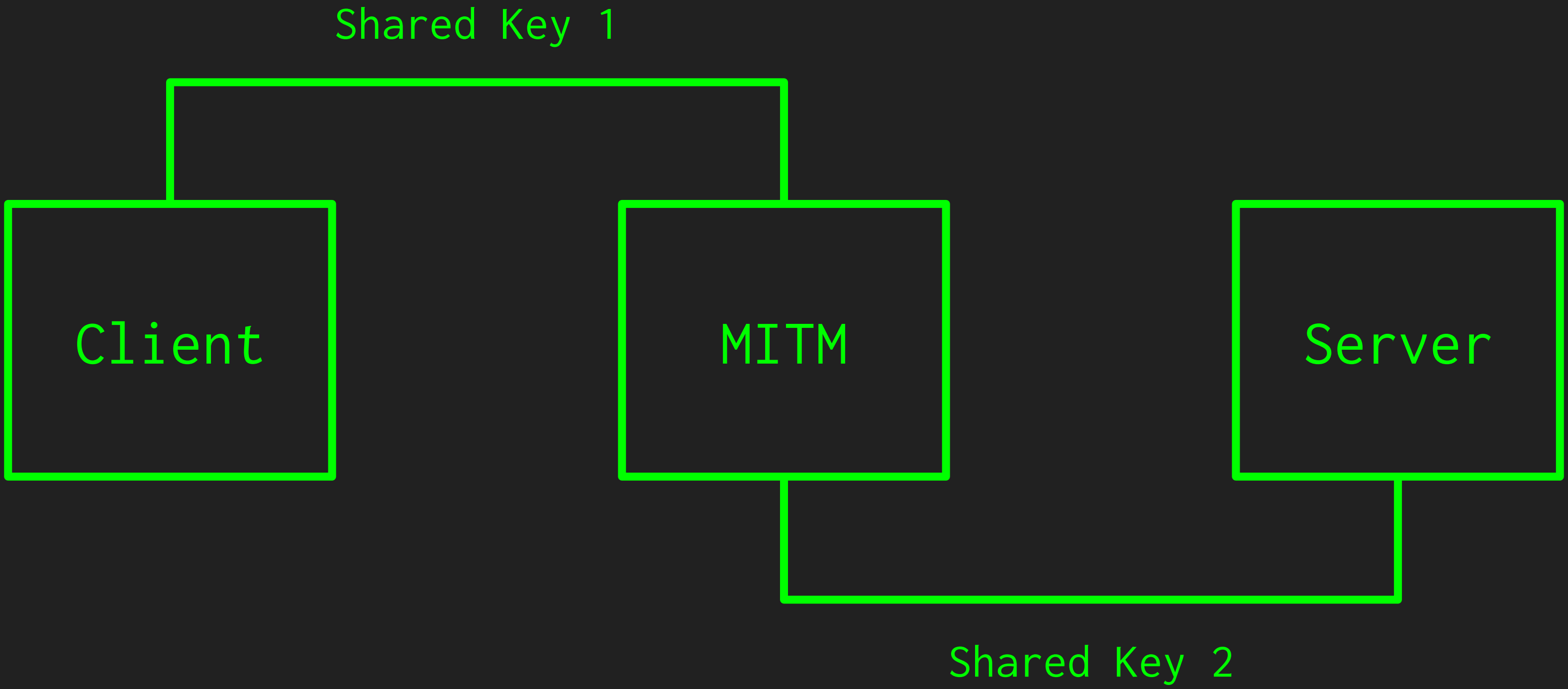
```
> MITM attack

> Host: stdlinux.cse.ohio-state.edu
> Protocol: SSHv2

> Victim IP: 10.0.2.4
> Gateway IP: 10.0.2.2

> Python 2.7.14
> Libraries: scapy, pycryptodome, sshpubkey
> diffie-hellman-group-exchange-sha256

> Client --> SSH version --> Server
> Client <-- SSH version <-- Server

> Client --> Algorithms --> Server
> Client <-- Algorithms <-- Server
> ssh-rsa (signature)
> aes128-ctr (encryption)
> umac-64@openssh.com (mac)
> Client --> min, n, max --> Server

> Client <-- p, g <-- Server

> Client --> e --> Server

> Client <-- server public key, f, signature <-- Server
> signature = RSA( server_private_key, HASH )
> HASH = SHA256( client_ssh_ver | server_ssh_ver | client_algs |
server_algs | server_public_key | min | n | max | p | g | e | f |
shared_key )
```



Shared Key 1

Client

MITM

Server

Shared Key 2

```
> mitm.py
> ARP poisoning

> sniffer.py
> Capture, modify, and forward packets
```