

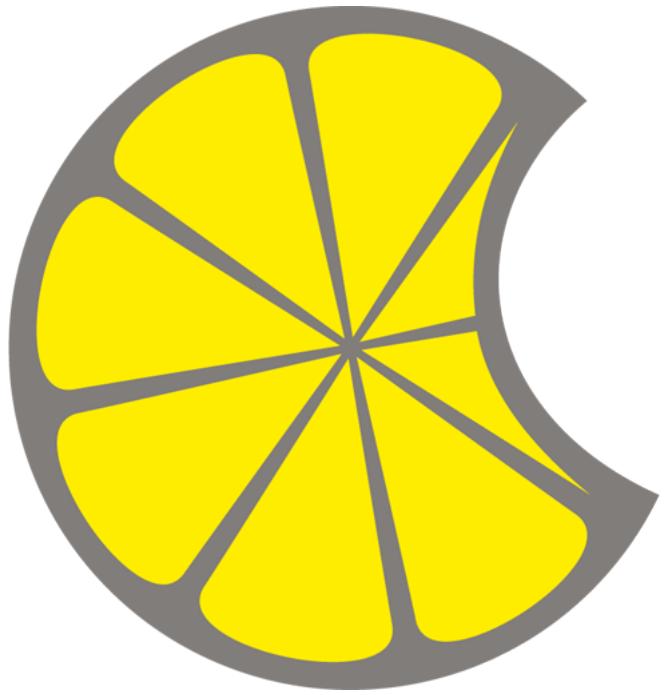


Peculiar SSH(1)

#bsidesljubljana!



@leyrer



@MacLemon



Raise your hand!

Peculiar SSH(1)

From Zero to Hero*ine

| 4:00 - | 6:00

SSH beginners' workshop

Prerequisites

We won't cover these anymore...

`~/.ssh/config`

public-key authentication

Ed25519 or RSA

Port Forwardings

`scp(1)`, `sftp(1)`

Crypto Config

kex, mac, key, cipher, cipher-auth

SSH(1)

SSH(1)

Works on
my machine!
101%

Peculiar SSH

```
tar cf - ./files | xz | pv | \  
ssh $host cat ">" files.tar.xz
```

```
tar cf - ./files | xz | pv | \  
ssh box cat ">" files.tar.xz
```

```
tar cf - ./files | xz | pv | \
ssh -o "Compression no" box \
cat ">" files.tar.xz
```

16MiB 0:00:26 [123KiB/s] [<=>]

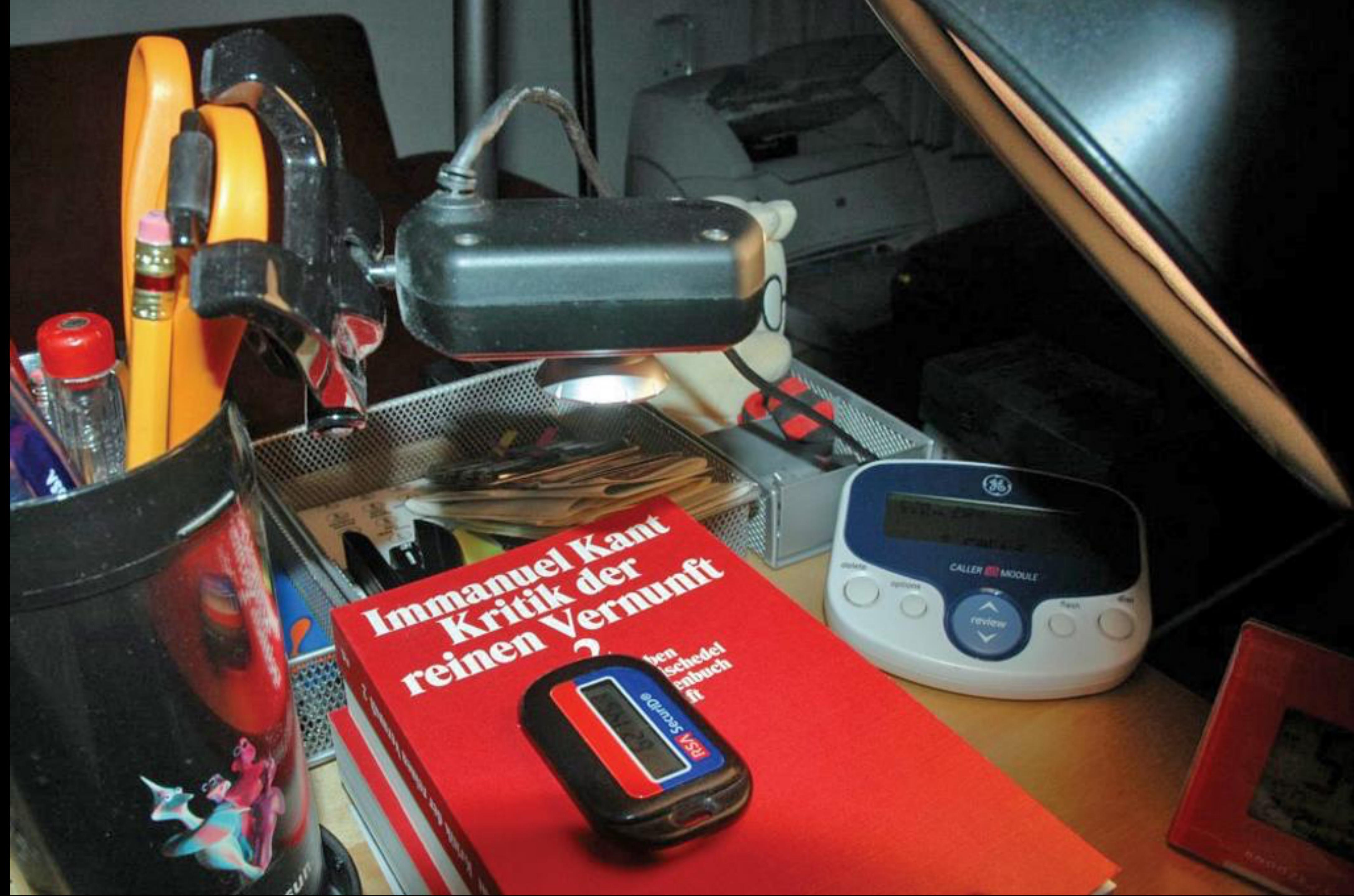
```
yes BSides | pv | \
ssh box "cat > /dev/null"
```

Two-Factor Authentication

Pictures of RSA Tokens

on Webcams

(Google Image Search)





08686 1

SecurID®

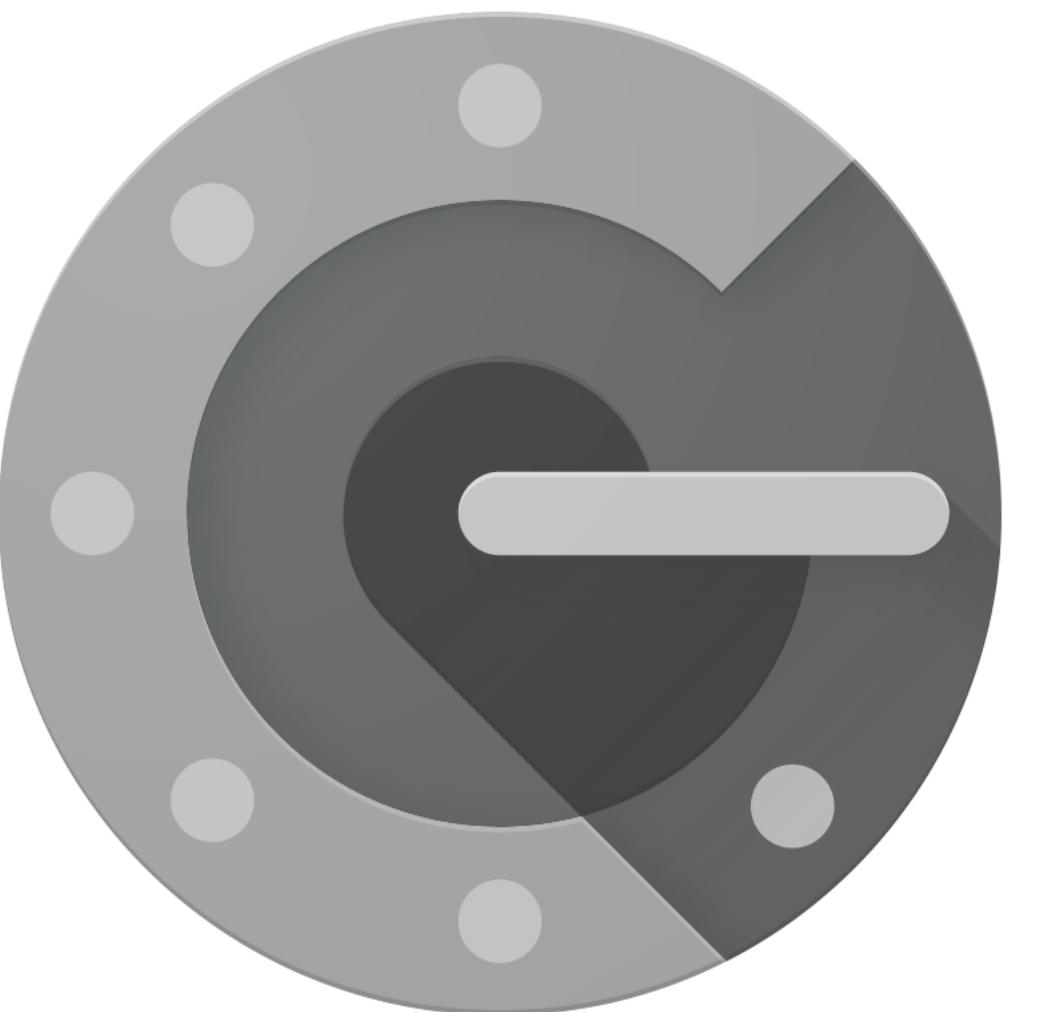


52126244



Secured by RSA

Time base One-Time Pads



```
apt-get install google-authenticator  
Debian flavored Tux
```

*BSD Ports:

graphics/libqrencode

security/pam_google_authenticator

Beastie

```
auth optional /usr/local/lib/  
pam_google_authenticator.so  
/etc/pam.d/sshd
```

```
AuthenticationMethods \
    publickey,keyboard-interactive
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

/etc/ssh/sshd_config

```
$ google-authenticator
```

Live Demo

/ google-authenticator



Multi

Factor Authentication

multiple public keys

```
AuthenticationMethods \
    publickey,publickey
```

/etc/ssh/sshd_config

```
IdentityFile ~/.ssh/foo
```

```
IdentityFile ~/.ssh/bar
```

```
IdentityFile ~/.ssh/baz
```

~/.ssh/ssh_config

```
-i ~/.ssh/foo \
-i ~/.ssh/bar \
-i ~/.ssh/baz
```

interactive

```
AuthenticationMethods \  
    publickey,publickey,keyboard-interactive
```

/etc/ssh/sshd_config

/ multiple public keys



Bastion Hosts

Live Demo

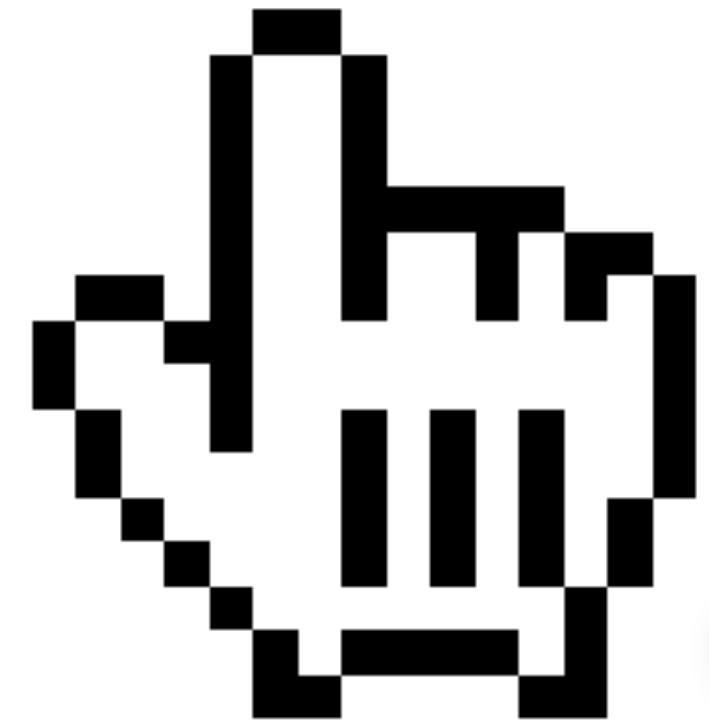
/ Bastion Hosts

HostKey rotation

OpenSSH 6.8+

/etc/sshd_config

```
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
# HostKey /etc/ssh/ssh_host_dsa_key
# HostKey /etc/ssh/ssh_host_ed25519_key
```



/etc/sshd_config

```
HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
# HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

/etc/sshd_config

HostKey /etc/ssh/ssh_host_rsa_2017_key

HostKey /etc/ssh/ssh_host_rsa_2018_key

HostKey /etc/ssh/ssh_host_ed25519_2017_key

HostKey /etc/ssh/ssh_host_ed25519_2018_key

sshd_config

```
# HostKey /etc/ssh/ssh_host_ed25519_2017_key  
HostKey /etc/ssh/ssh_host_ed25519_2018_key
```

```
# HostKey /etc/ssh/ssh_host_rsa_2017_key  
HostKey /etc/ssh/ssh_host_rsa_2018_key
```

UpdateHostKeys

`~/.ssh/config`

```
Host *
  UpdateHostKeys ask
    ~/.ssh/config
```

/ HostKey rotation

Legacy Systems

Host **vintagebox**

KexAlgorithms +diffie-hellman-group1-sha1

Ciphers +3des-cbc

PubkeyAcceptedKeyTypes +ssh-rsa

SSH 7.4p1

Bye bye SSHv1
SSH server

open

hosts2.ns

[mobile]

```
1 No exact OS matches for SShost  
3 Nmap run  
3 # SSHNUKE  
4 Connecting  
4 Attempting to exploit SSHv1 CRC32... successful.  
1 Resetting root password to "210H0101", successful.  
1 System open: Access Level <9> 0H0101  
3 # ssh 10.2.2.2 -l root <9>  
3 root@10.2.2.2's password:  
3 RRF=CONTROL>adisablegrid nodes 21 - 48  
Warning: Disabling nodes 21-48 will disconnect sector 11 (27 nodes)  
Warning: Are you sure? (y/n) y  
ARE YOU SURE? (y/n) y  
Grid Node 21 offline...  
Grid Node 22 offline...  
Grid Node 23 offline...  
.....
```

ALERT

ERROR : EMERGENCY SYSTEM FAILURE

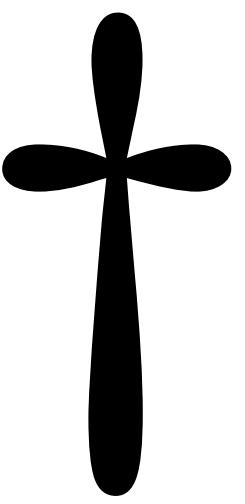
Bye bye 3des-cbc
SSH client

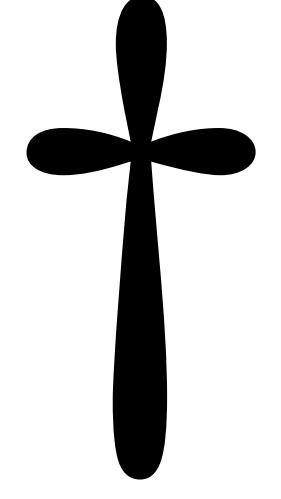
Bye bye
pre-authentication
compression
SSH server

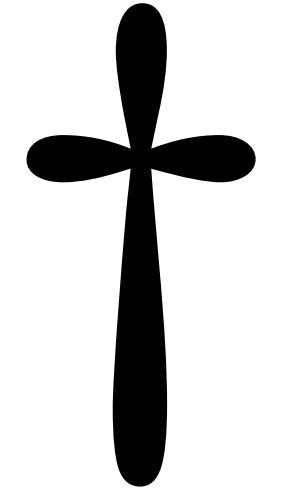
The *Future*...

OpenSSH 7.5+

SSH v.1 protocol



RC4, Blowfish 
RIPE-MD160

RSA < 1.024bits 

privilege separation required

sshd

OpenSSL ≥ 1.0.1

You have been warned!

Questions?

More questions...

...over a beverage!

Thanks #bsidesljubljana!

@leyrer

@MacLemon

Debugging

Y U NO CONNECT?

`ssh -G <Host>`

`ls ~/.ssh/config` working?

```
ssh -v <Host>
```

verbosity, up to 3×

SSHecurity Config

`ssh_config(5), sshd_config(5)`

Key Exchange Algorithms

KexAlgorithms

ssh -Q kex
ssh 6.3+

```
$ ssh -Q kex
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

```
$ ssh -Q kex
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

```
$ ssh -Q kex
diffie hellman group1 sha1
diffie hellman group14 sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie hellman group exchange sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

```
$ ssh -Q kex
diffie hellman group1 sha1
diffie hellman group14 sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie hellman group exchange sha1
diffie-hellman-group-exchange-sha256
ecdh sha2 nistp256
ecdh sha2 nistp384
ecdh sha2 nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

```
$ ssh -Q kex
diffie hellman group1 sha1
diffie hellman group14 sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie hellman group exchange sha1
diffie-hellman-group-exchange-sha256
ecdh sha2 nistp256
ecdh sha2 nistp384
ecdh sha2 nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

/etc/ssh/moduli

```
#      $OpenBSD: moduli,v 1.8 2012/08/29 05:06:54 dtucker Exp $
# Time Type Tests Tries Size Generator Modulus
20120821044040 2 6 100 1023 5
D9277DAA27DB131C03B108D41A76B4DA8ACEECCAE73D2E48CEDAAA70B09EF9F04FB020DCF36C51B8E485B26FABE0337E24232BE4F4E693548310244937433FB1A5758195DC73B
84ADEF8237472C46747D79DC0A2CF8A57CE8DBD8F466A20F8551E7B1B824B2E4987A8816D9BC0741C2798F3EBAD3ADEBCC78FCE6A770E2EC9F
20120821044046 2 6 100 1023 2
D9277DAA27DB131C03B108D41A76B4DA8ACEECCAE73D2E48CEDAAA70B09EF9F04FB020DCF36C51B8E485B26FABE0337E24232BE4F4E693548310244937433FB1A5758195DC73B
84ADEF8237472C46747D79DC0A2CF8A57CE8DBD8F466A20F8551E7B1B824B2E4987A8816D9BC0741C2798F3EBAD3ADEBCC78FCE6A7711F2C6B
20120821044047 2 6 100 1023 2
D9277DAA27DB131C03B108D41A76B4DA8ACEECCAE73D2E48CEDAAA70B09EF9F04FB020DCF36C51B8E485B26FABE0337E24232BE4F4E693548310244937433FB1A5758195DC73B
84ADEF8237472C46747D79DC0A2CF8A57CE8DBD8F466A20F8551E7B1B824B2E4987A8816D9BC0741C2798F3EBAD3ADEBCC78FCE6A771225323
20120821045107 2 6 100 1535 5
D1391174233D315398FE2830AC6B2B66BCCD01B0A634899F339B7879F1DB85712E9DC4E4B1C6C8355570C1D2DCB53493DF18175A9C53D1128B592B4C72D97136F5542FEB981CBF
E8012FDD30361F288A42BD5EBB08BAB0A5640E1AC48763B2ABD1945FEE36B2D55E1D50A1C86CED9DD141C4E7BE2D32D9B562A0F8E2E927020E91F58B57EB9ACDDA106A59302D7E
92AD5F6E851A45FA1CFE86029A0F727F65A8F475F33572E2FDAB6073F0C21B8B54C3823DB2EF068927E5D747498F99B86567
20120821045110 2 6 100 1535 5
D1391174233D315398FE2830AC6B2B66BCCD01B0A634899F339B7879F1DB85712E9DC4E4B1C6C8355570C1D2DCB53493DF18175A9C53D1128B592B4C72D97136F5542FEB981CBF
E8012FDD30361F288A42BD5EBB08BAB0A5640E1AC48763B2ABD1945FEE36B2D55E1D50A1C86CED9DD141C4E7BE2D32D9B562A0F8E2E927020E91F58B57EB9ACDDA106A59302D7E
92AD5F6E851A45FA1CFE86029A0F727F65A8F475F33572E2FDAB6073F0C21B8B54C3823DB2EF068927E5D747498F99BA2677
20120821045639 2 6 100 2047 2
DD2047CBDBB6F8E919BC63DE885B34D0FD6E3DB2887D8B46FE249886ACED6B46DFCD5553168185FD376122171CD8927E60120FA8D01F01D03E58281FEA9A1ABE97631C828E4181
5F34FDCDF787419FE13A3137649AA93D2584230DF5F24B5C00C88B7D7DE4367693428C730376F218A53E853B0851BAB7C53C15DA7839CBE1285DB63F6FA45C1BB59FE1C5BB918F
0F8459D7EF60ACFF5C0FA0F3FCAD1C5F4CE4416D4F4B36B05CDCEBE4FB879E95847EFBC6449CD190248843BC7EDB145FBFC4EDBB1A3C959298F08F3BA2CFBE231BBE204BE6F906
209D28BD4820AB3E7BE96C26AE8A809ADD8D1A5A0B008E9570FA4C4697E116B8119892C604293680B09D63
```

/etc/ssh/moduli

```
#      $OpenBSD: moduli,v 1.13 2015/05/28 00:03:06 dtucker Exp $
# Time          Type Tests Tries Size Generator Modulus
20120821044040 2 6 100 1023 5 D9277DA...
20120821044046 2 6 100 1023 2 6935483...
20120821044047 2 6 100 1023 2 D9277DA...
20120821045107 2 6 100 1535 5 D139117...
20120821045110 2 6 100 1535 5 D139117...
20120821045639 2 6 100 2047 2 DD2047C...
```

/etc/ssh/moduli

```
#      $OpenBSD: moduli,v 1.13 2015/05/28 00:03:06 dtucker Exp $
# Time          Type  Tests Tries Size Generator Modulus
# 20120821044040 2   6   100  1023 5   D9277DA...
# 20120821044046 2   6   100  1023 2   6935483...
# 20120821044047 2   6   100  1023 2   D9277DA...
20120821045107 2   6   100  1535 5   D139117...
20120821045110 2   6   100  1535 5   D139117...
20120821045639 2   6   100  2047 2   DD2047C...
```

```
KexAlgorithms \
    curve25519-sha256, \
    curve25519-sha256@libssh.org, \
    diffie-hellman-group-exchange-sha256, \
    diffie-hellman-group18-sha512, \
    diffie-hellman-group16-sha512, \
    diffie-hellman-group14-sha256
```

Host *

```
KexAlgorithms \
    curve25519-sha256, \
    curve25519-sha256@libssh.org, \
    diffie-hellman-group-exchange-sha256, \
    diffie-hellman-group18-sha512, \
    diffie-hellman-group16-sha512, \
    diffie-hellman-group14-sha256
```

Key Types

PubkeyAcceptedKeyTypes

`ssh -Q key`
ssh 6.3+

```
$ ssh -Q key
ssh-ed25519
ssh-ed25519-cert-v01@openssh.com
ssh-rsa
ssh-dss
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
ssh-rsa-cert-v01@openssh.com
ssh-dss-cert-v01@openssh.com
ecdsa-sha2-nistp256-cert-v01@openssh.com
ecdsa-sha2-nistp384-cert-v01@openssh.com
ecdsa-sha2-nistp521-cert-v01@openssh.com
```

```
$ ssh -Q key
ssh-ed25519
ssh-ed25519-cert-v01@openssh.com
ssh-rsa
ssh-dss
ecdsa sha2 nistp256
ecdsa sha2 nistp384
ecdsa sha2 nistp521
ssh-rsa-cert-v01@openssh.com
ssh-dss cert v01@openssh.com
ecdsa sha2 nistp256 cert v01@openssh.com
ecdsa sha2 nistp384 cert v01@openssh.com
ecdsa sha2 nistp521 cert v01@openssh.com
```

Host *

PubkeyAcceptedKeyTypes

```
ssh-ed25519-cert-v01@openssh.com, \
ssh-ed25519, \
ssh-rsa-cert-v01@openssh.com, \
ssh-rsa
```

Message Authentication

MACs

`ssh -Q mac`
`ssh 6.3+`

```
strings /usr/sbin/sshd | \
grep "mac" | \
grep -v "[ :%]" | \
head -1 | tr ',', '\n'
```

```
$ ssh -Q mac
```

```
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
umac-64@openssh.com
umac-128@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

```
$ ssh -Q mac
```

```
hmac-sha1  
hmac-sha1-96  
hmac-sha2-256  
hmac-sha2-512  
hmac-md5  
hmac-md5-96  
hmac-ripemd160  
hmac-ripemd160@openssh.com  
umac-64@openssh.com  
umac-128@openssh.com  
hmac-sha1-ctm@openssh.com  
hmac-sha1-96-ctm@openssh.com  
hmac-sha2-256-ctm@openssh.com  
hmac-sha2-512-ctm@openssh.com  
hmac-md5-ctm@openssh.com  
hmac-md5-96-ctm@openssh.com  
hmac-ripemd160-ctm@openssh.com  
umac-64-ctm@openssh.com  
umac-128-ctm@openssh.com
```

```
$ ssh -Q mac
```

```
hmac-sha1  
hmac-sha1-96  
hmac-sha2-256  
hmac-sha2-512  
hmac-md5  
hmac-md5-96  
hmac-ripemd160  
hmac-ripemd160@openssh.com  
umac-64@openssh.com  
umac-128@openssh.com  
hmac-sha1-ctm@openssh.com  
hmac-sha1-96-ctm@openssh.com  
hmac-sha2-256-ctm@openssh.com  
hmac-sha2-512-ctm@openssh.com  
hmac-md5-ctm@openssh.com  
hmac-md5-96-ctm@openssh.com  
hmac-ripemd160-ctm@openssh.com  
umac-64-ctm@openssh.com  
umac-128-ctm@openssh.com
```

```
Host *
  MACs \
    hmac-sha2-512-etm@openssh.com, \
    hmac-sha2-256-etm@openssh.com, \
    hmac-ripemd160-etm@openssh.com, \
    umac-128-etm@openssh.com, \
    hmac-sha2-512, \
    hmac-sha2-256, \
    hmac-ripemd160@openssh.com, \
    hmac-ripemd160, \
    umac-128@openssh.com
```

Symmetric ciphers

ssh -Q cipher
ssh 6.3+

```
$ ssh -Q cipher
```

```
3des-cbc  
blowfish-cbc  
cast128-cbc  
arcfour  
arcfour128  
arcfour256  
aes128-cbc  
aes192-cbc  
aes256-cbc  
rijndael-cbc@lysator.liu.se  
aes128-ctr  
aes192-ctr  
aes256-ctr  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

```
$ ssh -Q cipher  
3des-cbc  
blowfish-cbc  
cast128-cbc  
arcfour  
arcfour128  
arcfour256  
aes128-cbc  
aes192-cbc  
aes256-cbc  
rijndael-cbc@lysator.liu.se  
aes128-ctr  
aes192-ctr  
aes256-ctr  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

```
$ ssh -Q cipher  
3des-cbc  
blowfish-cbc  
cast128-cbc  
arcfour  
arcfour128  
arcfour256  
aes128-cbc  
aes192-cbc  
aes256-cbc  
rijndael-cbc@lysator.liu.se  
aes128-ctr  
aes192-ctr  
aes256-ctr  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

```
$ ssh -Q cipher  
3des-cbc  
blowfish-cbc  
cast128-cbc  
arcfour  
arcfour128  
arcfour256  
aes128-cbc  
aes192-cbc  
aes256-cbc  
rijndael-cbc@lysator.liu.se  
aes128-ctr  
aes192-ctr  
aes256-ctr  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

Host *

Ciphers

chacha20-poly1305@openssh.com,

aes256-gcm@openssh.com,

aes128-gcm@openssh.com,

aes256-ctr,

aes192-ctr,

aes128-ctr

```
ssh -Q cipher-auth
```

```
$ ssh -Q cipher-auth  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```


Client Hardening

CVE-2016-0777

CVE-2016-0778

```
# Prevent client bug CVE-2016-0777, CVE-2016-0778
```

```
Host *
```

```
    UseRoaming no
```

```
~/.ssh/config
```