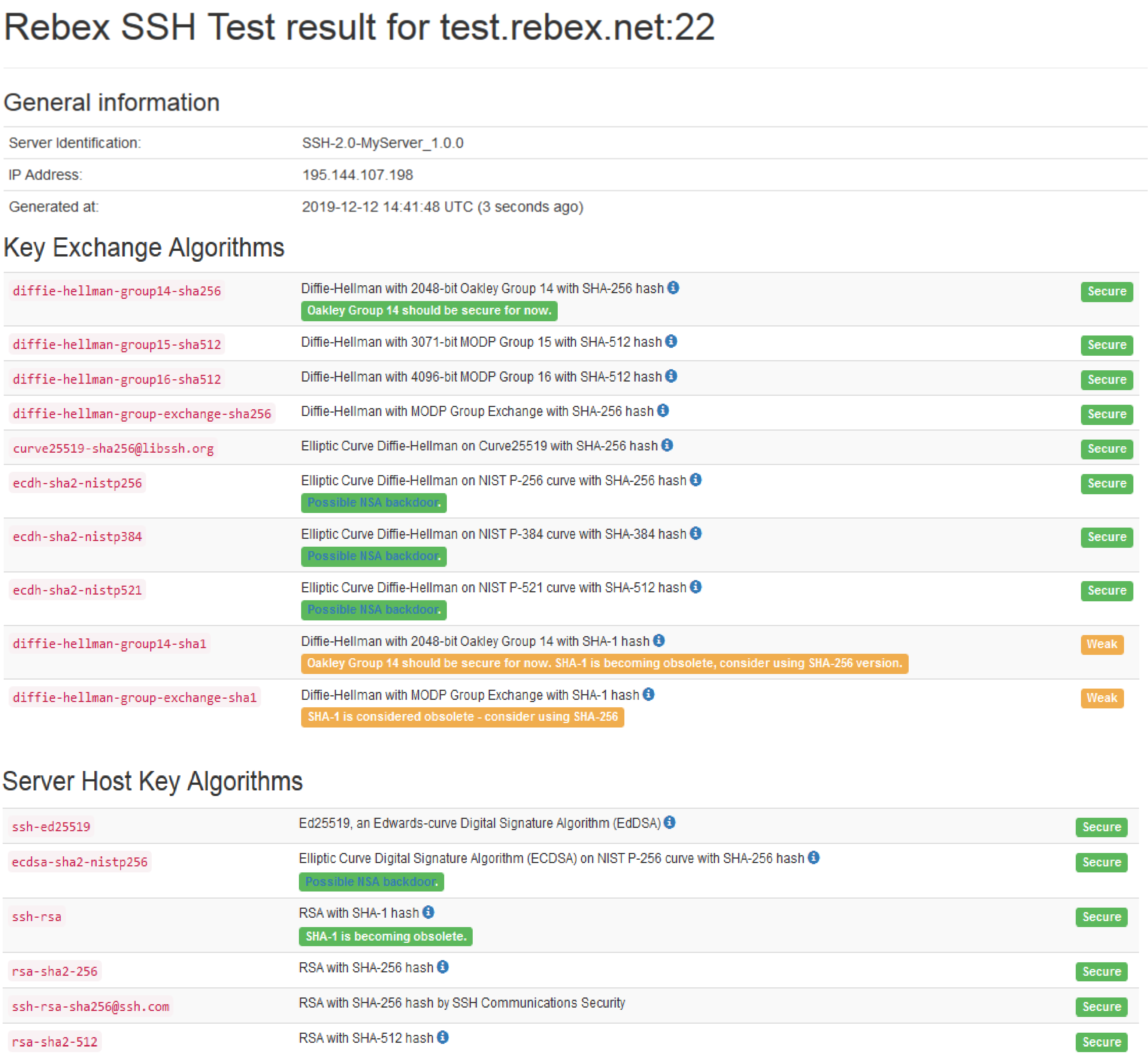
https://sshcheck.com/server/test.rebex.net/

Rebex SSH Test result for test.rebex.net:22



Rebex SSH Test result for test.rebex.net:22

General information

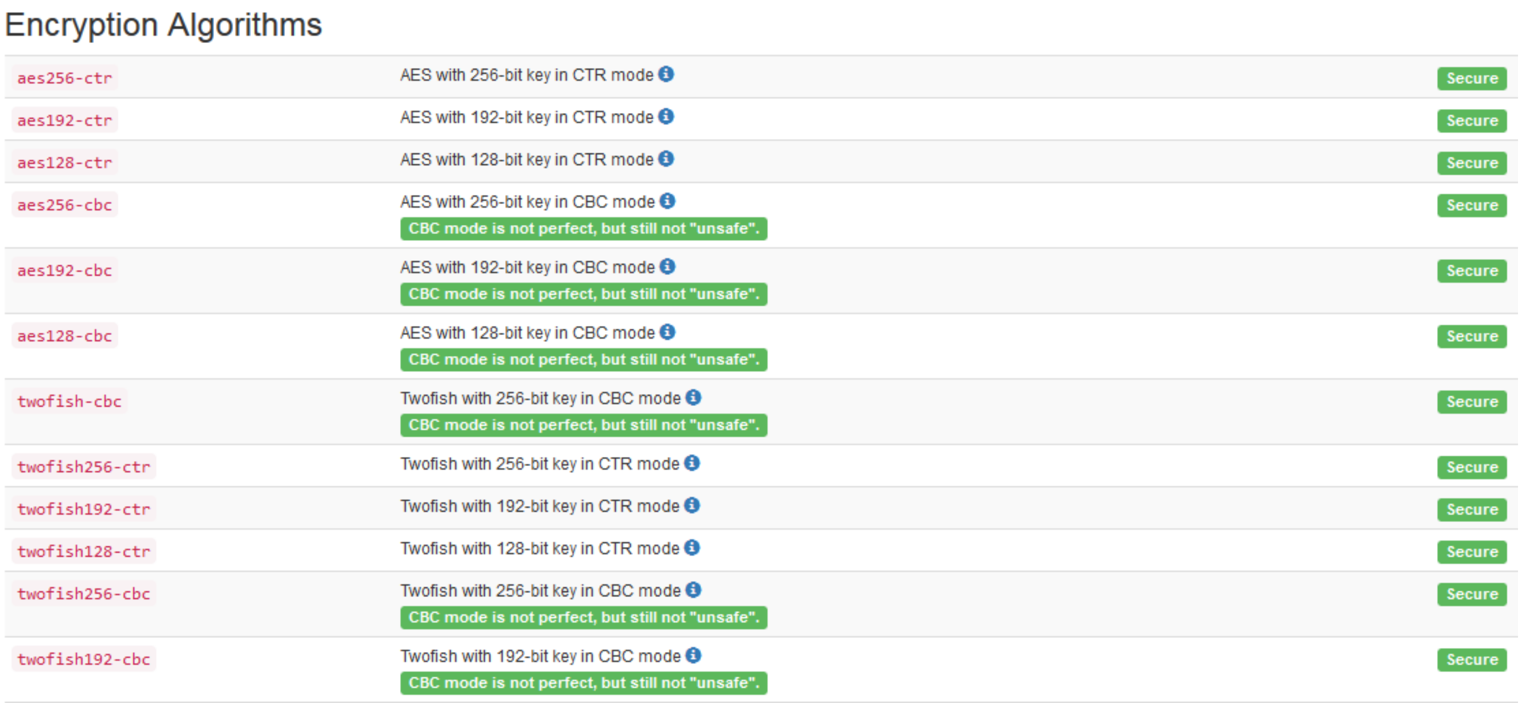
Server Identification:	SSH-2.0-MyServer_1.0.0
IP Address:	195.144.107.198
Generated at:	2019-12-12 14:41:48 UTC (3 seconds ago)

Key Exchange Algorithms

`diffie-hellman-group14-sha256`	Diffie-Hellman with 2048-bit Oakley Group 14 with SHA-256 hash Oakley Group 14 should be secure for now.	Secure
`diffie-hellman-group15-sha512`	Diffie-Hellman with 3071-bit MODP Group 15 with SHA-512 hash	Secure
`diffie-hellman-group16-sha512`	Diffie-Hellman with 4096-bit MODP Group 16 with SHA-512 hash	Secure
`diffie-hellman-group-exchange-sha256`	Diffie-Hellman with MODP Group Exchange with SHA-256 hash	Secure
`curve25519-sha256@libssh.org`	Elliptic Curve Diffie-Hellman on Curve25519 with SHA-256 hash	Secure
`ecdh-sha2-nistp256`	Elliptic Curve Diffie-Hellman on NIST P-256 curve with SHA-256 hash Possible NSA backdoor.	Secure
`ecdh-sha2-nistp384`	Elliptic Curve Diffie-Hellman on NIST P-384 curve with SHA-384 hash Possible NSA backdoor.	Secure
`ecdh-sha2-nistp521`	Elliptic Curve Diffie-Hellman on NIST P-521 curve with SHA-512 hash Possible NSA backdoor.	Secure
`diffie-hellman-group14-sha1`	Diffie-Hellman with 2048-bit Oakley Group 14 with SHA-1 hash Oakley Group 14 should be secure for now. SHA-1 is becoming obsolete, consider using SHA-256 version.	Weak
`diffie-hellman-group-exchange-sha1`	Diffie-Hellman with MODP Group Exchange with SHA-1 hash SHA-1 is considered obsolete - consider using SHA-256	Weak

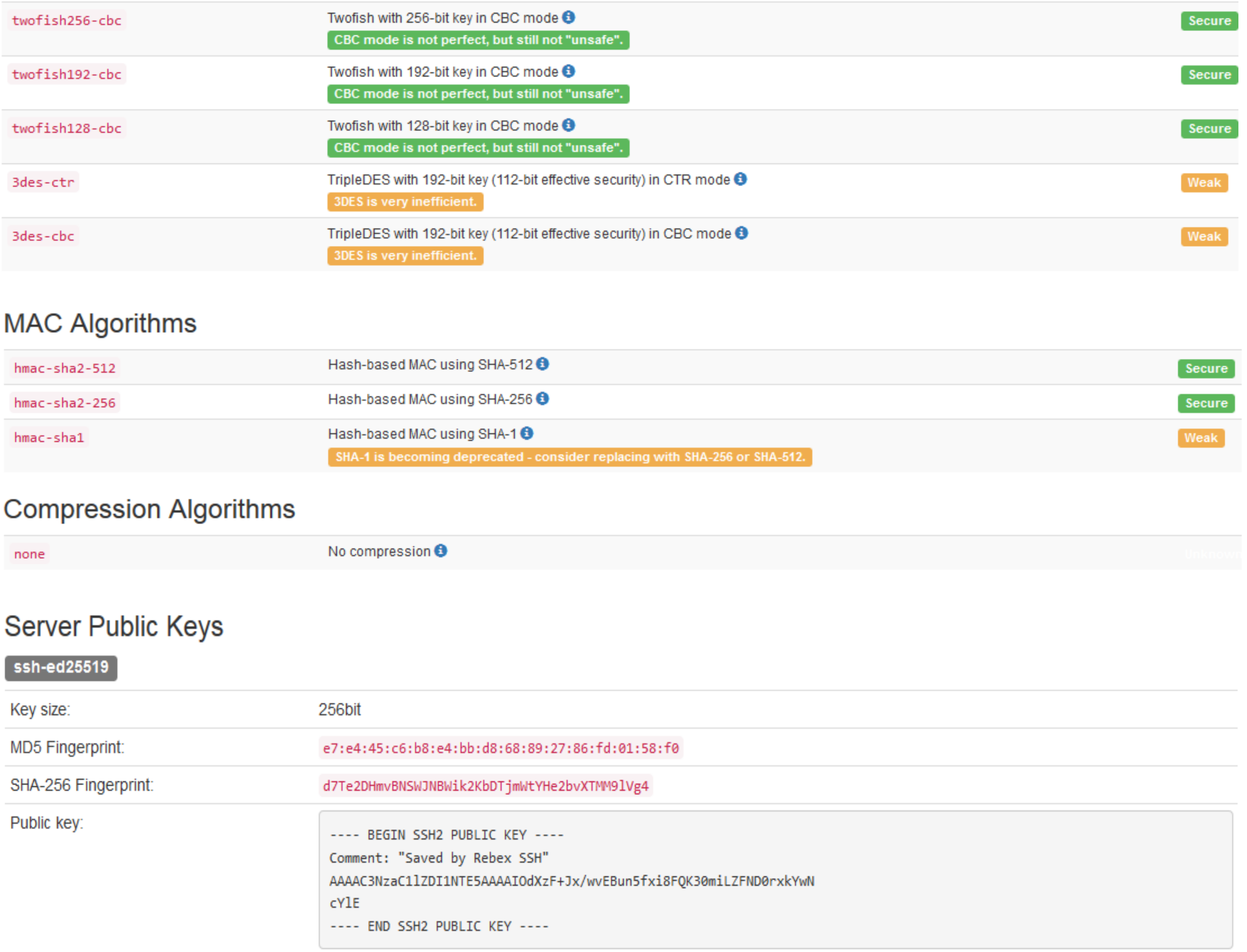
Server Host Key Algorithms

`ssh-ed25519`	Ed25519, an Edwards-curve Digital Signature Algorithm (EdDSA)	Secure
`ecdsa-sha2-nistp256`	Elliptic Curve Digital Signature Algorithm (ECDSA) on NIST P-256 curve with SHA-256 hash Possible NSA backdoor.	Secure
`ssh-rsa`	RSA with SHA-1 hash SHA-1 is becoming obsolete.	Secure
`rsa-sha2-256`	RSA with SHA-256 hash	Secure
`ssh-rsa-sha256@ssh.com`	RSA with SHA-256 hash by SSH Communications Security	Secure
`rsa-sha2-512`	RSA with SHA-512 hash	Secure



Encryption Algorithms

aes256-ctr	AES with 256-bit key in CTR mode	Secure
aes192-ctr	AES with 192-bit key in CTR mode	Secure
aes128-ctr	AES with 128-bit key in CTR mode	Secure
aes256-cbc	AES with 256-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
aes192-cbc	AES with 192-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
aes128-cbc	AES with 128-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
twofish-cbc	Twofish with 256-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
twofish256-ctr	Twofish with 256-bit key in CTR mode	Secure
twofish192-ctr	Twofish with 192-bit key in CTR mode	Secure
twofish128-ctr	Twofish with 128-bit key in CTR mode	Secure
twofish256-cbc	Twofish with 256-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
twofish192-cbc	Twofish with 192-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure



twofish256-cbc	Twofish with 256-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
twofish192-cbc	Twofish with 192-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure

twofish128-cbc	Twofish with 128-bit key in CBC mode CBC mode is not perfect, but still not "unsafe".	Secure
3des-ctr	TripleDES with 192-bit key (112-bit effective security) in CTR mode 3DES is very inefficient.	Weak
3des-cbc	TripleDES with 192-bit key (112-bit effective security) in CBC mode 3DES is very inefficient.	Weak

MAC Algorithms

hmac-sha2-512	Hash-based MAC using SHA-512	Secure
hmac-sha2-256	Hash-based MAC using SHA-256	Secure
hmac-sha1	Hash-based MAC using SHA-1 SHA-1 is becoming deprecated - consider replacing with SHA-256 or SHA-512.	Weak

Compression Algorithms

none	No compression	Unknown

Server Public Keys

ssh-ed25519

Key size:	256bit
MD5 Fingerprint:	e7:e4:45:c6:b8:e4:bb:d8:68:89:27:86:fd:01:58:f0
SHA-256 Fingerprint:	d7Te2DHmvBNSWJNBWik2KbDTjmWtYHe2bvXTMM9lVg4

Public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Saved by Rebex SSH"
AAAAC3NzaC1lZDI1NTE5AAAAIOdXzF+Jx/wvEBun5fxi8FQK30miLZFND0rxkYwN
cYlE
---- END SSH2 PUBLIC KEY ----
```

ecdsa-sha2-nistp256

Key size:	256bit
MD5 Fingerprint:	`3d:f0:7e:e0:b5:cf:6f:60:94:66:79:96:d3:2e:81:a4`
SHA-256 Fingerprint:	`OzvpQxRUzSfV9F/ECMXbQ7B7zbK0aTngrhFCBUno65c`

Public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Saved by Rebex SSH"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLZcZopPvkxY
ERubWeSrWOSHpxJdR14WFVES/Q3hFguTn6L+0EANqYcbRXhGBUV6SjR7SaxZACXS
xOzgCtG4kwc=
---- END SSH2 PUBLIC KEY ----
```

rsa-sha2-512

Key size:	2048bit
MD5 Fingerprint:	`03:61:c4:98:f1:ff:7d:23:97:51:07:13:88:b8:c5:55`
SHA-256 Fingerprint:	`FFMFsBkaSJbqAeiMb+4c2OJI765czqp6ArYO0GznBJo`

Public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Saved by Rebex SSH"
AAAAB3NzaC1yc2EAAAABJQAAAQEAkRM6RxDdi3uAGogR3nsQMpmt43X4WnwgMzs8
VkwUCqikewxqk4U7EyUSOUeT3CoUNOtywrkNbH83e6/yQgzc3M8i/eDzYtXaNGcK
yLfy3Ci6XOwiLLOx1z2AGvvTXln1RXtve+Tn1RTr1BhXVh2cUYbiuVtTWqbEgErT
20n4GWD4wv7FhkDbLXNi8DX07F9v7+jH67i0kyGm+E3rE+SaCMRo3zXE6VO+ijcm
9HdVxfltQwOYLfuPXM2t5aUSfa96KJcA0I4RCMzA/8Dl9hXGfbWdbD2hK1ZQ1pLv
vpNPPyKKjPZcMpOznprbg+jIlsZMWIHt7mq2OJXSdruhRrGzZw==
---- END SSH2 PUBLIC KEY ----
```

ssh-rsa-sha256@ssh.com

Key size:	2048bit
MD5 Fingerprint:	`03:61:c4:98:f1:ff:7d:23:97:51:07:13:88:b8:c5:55`
SHA-256 Fingerprint:	`FFMFsBkaSJbqAeiMb+4c2OJI765czqp6ArYO0GznBJo`

Public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Saved by Rebex SSH"
AAAAB3NzaC1yc2EAAAABJQAAAQEAkRM6RxDdi3uAGogR3nsQMpmt43X4WnwgMzs8
VkwUCqikewxqk4U7EyUSOUeT3CoUNOtywrkNbH83e6/yQgzc3M8i/eDzYtXaNGcK
yLfy3Ci6XOwiLLOx1z2AGvvTXln1RXtve+Tn1RTr1BhXVh2cUYbiuVtTWqbEgErT
20n4GWD4wv7FhkDbLXNi8DX07F9v7+jH67i0kyGm+E3rE+SaCMRo3zXE6VO+ijcm
9HdVxfltQwOYLfuPXM2t5aUSfa96KJcA0I4RCMzA/8Dl9hXGfbWdbD2hK1ZQ1pLv
vpNPPyKKjPZcMpOznprbg+jIlsZMWIHt7mq2OJXSdruhRrGzZw==
---- END SSH2 PUBLIC KEY ----
```

rsa-sha2-256

Key size:	2048bit
MD5 Fingerprint:	`03:61:c4:98:f1:ff:7d:23:97:51:07:13:88:b8:c5:55`
SHA-256 Fingerprint:	`FFMFsBkaSJbqAeiMb+4c2OJI765czqp6ArYO0GznBJo`

Public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Saved by Rebex SSH"
AAAAB3NzaC1yc2EAAAABJQAAAQEAkRM6RxDdi3uAGogR3nsQMpmt43X4WnwgMzs8
VkwUCqikewxqk4U7EyUSOUeT3CoUNOtywrkNbH83e6/yQgzc3M8i/eDzYtXaNGcK
yLfy3Ci6XOwiLLOx1z2AGvvTXln1RXtve+Tn1RTr1BhXVh2cUYbiuVtTWqbEgErT
20n4GWD4wv7FhkDbLXNi8DX07F9v7+jH67i0kyGm+E3rE+SaCMRo3zXE6VO+ijcm
9HdVxfltQwOYLfuPXM2t5aUSfa96KJcA0I4RCMzA/8Dl9hXGfbWdbD2hK1ZQ1pLv
vpNPPyKKjPZcMpOznprbg+jIlsZMWIHt7mq2OJXSdruhRrGzZw==
---- END SSH2 PUBLIC KEY ----
```

ssh-rsa

Key size:	2048bit
MD5 Fingerprint:	`03:61:c4:98:f1:ff:7d:23:97:51:07:13:88:b8:c5:55`
SHA-256 Fingerprint:	`FFMFsBkaSJbqAeiMb+4c2OJI765czqp6ArYO0GznBJo`

Public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Saved by Rebex SSH"
AAAAB3NzaC1yc2EAAAABJQAAAQEAkRM6RxDdi3uAGogR3nsQMpmt43X4WnwgMzs8
VkwUCqikewxqk4U7EyUSOUeT3CoUNOtywrkNbH83e6/yQgzc3M8i/eDzYtXaNGcK
yLfy3Ci6XOwiLLOx1z2AGvvTXln1RXtve+Tn1RTr1BhXVh2cUYbiuVtTWqbEgErT
20n4GWD4wv7FhkDbLXNi8DX07F9v7+jH67i0kyGm+E3rE+SaCMRo3zXE6VO+ijcm
9HdVxfltQwOYLfuPXM2t5aUSfa96KJcA0I4RCMzA/8Dl9hXGfbWdbD2hK1ZQ1pLv
vpNPPyKKjPZcMpOznprbg+jIlsZMWIHt7mq2OJXSdruhRrGzZw==
---- END SSH2 PUBLIC KEY ----
```