OpenSSL 1.0.2 Cipher Suite Lists

by

Michael Talbot

Introduction

I have put together this list of the various cipher suites that have been and are being used by OpenSSL so that there is a quick and easy reference for people to use. This way you can look up the list that goes with the version of OpenSSL you are using and compare it to other versions (this can be handy if you only know the version number but don't have access to generate the cipher list – such as when using shared web hosting). All of the lists have been created with the command "`openssl ciphers -v`" except for version 0.9.1c where the command used was "`ssleay ciphers -v`". Most of the old versions are only of historical interest but it can be useful to see when various ciphers were added or removed. I will be adding new entries to the list when I can so that it remains up-to-date.

Note

I have no connection with the OpenSSL Project and have produced this document on my own without their involvement. The OpenSSL Project has no responsibility for the accuracy of this information as I have generated these lists without their help.

Table of Contents

OpenSSL 1.0.2g – 1.0.2k

Version 1.0.2g released 1-March-2016

Version 1.0.2h released 3-May-2016

Version 1.0.2i released 22-Sep-2016

Version 1.0.2j released 26-Sep-2016

Version 1.0.2k released 26-Jan-2017

ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(256)	Mac=AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac=SHA384
ECDHE-RSA-AES256-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac=SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)	Mac=SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(256)	Mac=SHA1
SRP-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(256)	Mac=SHA1
DH-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(256)	Mac=AEAD
DH-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA256
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA256
DH-RSA-AES256-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA256
DH-DSS-AES256-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA256
DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA1
DH-RSA-AES256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA1
DH-DSS-AES256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA1
DHE-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(256)	Mac=SHA1
DHE-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(256)	Mac=SHA1
DH-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(256)	Mac=SHA1
DH-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(256)	Mac=SHA1
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AESGCM(256)	Mac=AEAD
ECDH-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AESGCM(256)	Mac=AEAD
ECDH-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AES(256)	Mac=SHA384
ECDH-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(256)	Mac=SHA384
ECDH-RSA-AES256-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=AES(256)	Mac=SHA1
ECDH-ECDSA-AES256-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(256)	Mac=SHA1
AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
AES256-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA256
AES256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA1
CAMELLIA256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(256)	Mac=SHA1
PSK-AES256-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(256)	Mac=SHA1
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
ECDHE-ECDSA-AES128-GCM-	TLSv1.2	Kx=ECDH	Au=ECDS	Enc=AESGCM(128)	Mac=AEAD

SHA256			A		
ECDHE-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=SHA256
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA256
ECDHE-RSA-AES128-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=SHA1
ECDHE-ECDSA-AES128-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA1
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac=SHA1
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(128)	Mac=SHA1
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac=SHA1
DH-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=AEAD
DH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA256
DH-RSA-AES128-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA256
DH-DSS-AES128-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA256
DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA1
DH-RSA-AES128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA1
DH-DSS-AES128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA1
DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)	Mac=SHA1
DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)	Mac=SHA1
DH-RSA-SEED-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=SEED(128)	Mac=SHA1
DH-DSS-SEED-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=SEED(128)	Mac=SHA1
DHE-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(128)	Mac=SHA1
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(128)	Mac=SHA1
DH-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(128)	Mac=SHA1
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AESGCM(128)	Mac=AEAD
ECDH-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AESGCM(128)	Mac=AEAD
ECDH-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AES(128)	Mac=SHA256
ECDH-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(128)	Mac=SHA256
ECDH-RSA-AES128-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=AES(128)	Mac=SHA1
ECDH-ECDSA-AES128-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(128)	Mac=SHA1
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA256
AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA1
SEED-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=SHA1
CAMELLIA128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=IDEA(128)	Mac=SHA1
PSK-AES128-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(128)	Mac=SHA1
ECDHE-RSA-RC4-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=RC4(128)	Mac=SHA1
ECDHE-ECDSA-RC4-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=RC4(128)	Mac=SHA1
ECDH-RSA-RC4-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=RC4(128)	Mac=SHA1
ECDH-ECDSA-RC4-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=RC4(128)	Mac=SHA1
RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1
RC4-MD5	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=MD5
PSK-RC4-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=RC4(128)	Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=3DES(168)	Mac=SHA1
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=3DES(168)	Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac=SHA1
SRP-RSA-3DES-EDE-CBC-	SSLv3	Kx=SRP	Au=RSA	Enc=3DES(168)	Mac=SHA1

```
SHA
SRP-3DES-EDE-CBC-SHA   SSLv3   Kx=SRP        Au=SRP  Enc=3DES(168)     Mac=SHA1
EDH-RSA-DES-CBC3-SHA   SSLv3   Kx=DH         Au=RSA  Enc=3DES(168)     Mac=SHA1
EDH-DSS-DES-CBC3-SHA   SSLv3   Kx=DH         Au=DSS  Enc=3DES(168)     Mac=SHA1
DH-RSA-DES-CBC3-SHA    SSLv3   Kx=DH/RSA     Au=DH   Enc=3DES(168)     Mac=SHA1
DH-DSS-DES-CBC3-SHA    SSLv3   Kx=DH/DSS     Au=DH   Enc=3DES(168)     Mac=SHA1
ECDH-RSA-DES-CBC3-SHA  SSLv3   Kx=ECDH/RSA   Au=ECDH Enc=3DES(168)     Mac=SHA1
ECDH-ECDSA-DES-CBC3-SHASSLv3   Kx=ECDH/ECDSA Au=ECDH Enc=3DES(168)     Mac=SHA1
DES-CBC3-SHA           SSLv3   Kx=RSA        Au=RSA  Enc=3DES(168)     Mac=SHA1
PSK-3DES-EDE-CBC-SHA   SSLv3   Kx=PSK        Au=PSK  Enc=3DES(168)     Mac=SHA1
```

OpenSSL 1.0.2a – 1.0.2f

Version 1.0.2a released 19-March-2015

Version 1.0.2b released 11-June-2015

Version 1.0.2c released 12-June-2015

Version 1.0.2d released 9-July-2015

Version 1.0.2e released 3-December-2015

Version 1.0.2f released 28-January-2016

```
ECDHE-RSA-AES256-GCM-SHA384    TLSv1.2 Kx=ECDH       Au=RSA   Enc=AESGCM(256)  Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384  TLSv1.2 Kx=ECDH       Au=ECDSA Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384        TLSv1.2 Kx=ECDH       Au=RSA   Enc=AES(256)     Mac=SHA384
ECDHE-ECDSA-AES256-SHA384      TLSv1.2 Kx=ECDH       Au=ECDSA Enc=AES(256)     Mac=SHA384
ECDHE-RSA-AES256-SHA           SSLv3   Kx=ECDH       Au=RSA   Enc=AES(256)     Mac=SHA1
ECDHE-ECDSA-AES256-SHA         SSLv3   Kx=ECDH       Au=ECDSA Enc=AES(256)     Mac=SHA1
SRP-DSS-AES-256-CBC-SHA        SSLv3   Kx=SRP        Au=DSS   Enc=AES(256)     Mac=SHA1
SRP-RSA-AES-256-CBC-SHA        SSLv3   Kx=SRP        Au=RSA   Enc=AES(256)     Mac=SHA1
SRP-AES-256-CBC-SHA            SSLv3   Kx=SRP        Au=SRP   Enc=AES(256)     Mac=SHA1
DH-DSS-AES256-GCM-SHA384       TLSv1.2 Kx=DH/DSS     Au=DH    Enc=AESGCM(256)  Mac=AEAD
DHE-DSS-AES256-GCM-SHA384      TLSv1.2 Kx=DH         Au=DSS   Enc=AESGCM(256)  Mac=AEAD
DH-RSA-AES256-GCM-SHA384       TLSv1.2 Kx=DH/RSA     Au=DH    Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-GCM-SHA384      TLSv1.2 Kx=DH         Au=RSA   Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256          TLSv1.2 Kx=DH         Au=RSA   Enc=AES(256)     Mac=SHA256
DHE-DSS-AES256-SHA256          TLSv1.2 Kx=DH         Au=DSS   Enc=AES(256)     Mac=SHA256
DH-RSA-AES256-SHA256           TLSv1.2 Kx=DH/RSA     Au=DH    Enc=AES(256)     Mac=SHA256
DH-DSS-AES256-SHA256           TLSv1.2 Kx=DH/DSS     Au=DH    Enc=AES(256)     Mac=SHA256
DHE-RSA-AES256-SHA             SSLv3   Kx=DH         Au=RSA   Enc=AES(256)     Mac=SHA1
DHE-DSS-AES256-SHA             SSLv3   Kx=DH         Au=DSS   Enc=AES(256)     Mac=SHA1
DH-RSA-AES256-SHA              SSLv3   Kx=DH/RSA     Au=DH    Enc=AES(256)     Mac=SHA1
DH-DSS-AES256-SHA              SSLv3   Kx=DH/DSS     Au=DH    Enc=AES(256)     Mac=SHA1
DHE-RSA-CAMELLIA256-SHA        SSLv3   Kx=DH         Au=RSA   Enc=Camellia(256)Mac=SHA1
DHE-DSS-CAMELLIA256-SHA        SSLv3   Kx=DH         Au=DSS   Enc=Camellia(256)Mac=SHA1
DH-RSA-CAMELLIA256-SHA         SSLv3   Kx=DH/RSA     Au=DH    Enc=Camellia(256)Mac=SHA1
DH-DSS-CAMELLIA256-SHA         SSLv3   Kx=DH/DSS     Au=DH    Enc=Camellia(256)Mac=SHA1
ECDH-RSA-AES256-GCM-SHA384     TLSv1.2 Kx=ECDH/RSA   Au=ECDH  Enc=AESGCM(256)  Mac=AEAD
ECDH-ECDSA-AES256-GCM-SHA384   TLSv1.2 Kx=ECDH/ECDSA Au=ECDH  Enc=AESGCM(256)  Mac=AEAD
ECDH-RSA-AES256-SHA384         TLSv1.2 Kx=ECDH/RSA   Au=ECDH  Enc=AES(256)     Mac=SHA384
ECDH-ECDSA-AES256-SHA384       TLSv1.2 Kx=ECDH/ECDSA Au=ECDH  Enc=AES(256)     Mac=SHA384
ECDH-RSA-AES256-SHA            SSLv3   Kx=ECDH/RSA   Au=ECDH  Enc=AES(256)     Mac=SHA1
ECDH-ECDSA-AES256-SHA          SSLv3   Kx=ECDH/ECDSA Au=ECDH  Enc=AES(256)     Mac=SHA1
AES256-GCM-SHA384              TLSv1.2 Kx=RSA        Au=RSA   Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                  TLSv1.2 Kx=RSA        Au=RSA   Enc=AES(256)     Mac=SHA256
AES256-SHA                     SSLv3   Kx=RSA        Au=RSA   Enc=AES(256)     Mac=SHA1
CAMELLIA256-SHA                SSLv3   Kx=RSA        Au=RSA   Enc=Camellia(256)Mac=SHA1
PSK-AES256-CBC-SHA             SSLv3   Kx=PSK        Au=PSK   Enc=AES(256)     Mac=SHA1
ECDHE-RSA-AES128-GCM-SHA256    TLSv1.2 Kx=ECDH       Au=RSA   Enc=AESGCM(128)  Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256  TLSv1.2 Kx=ECDH       Au=ECDSA Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256        TLSv1.2 Kx=ECDH       Au=RSA   Enc=AES(128)     Mac=SHA256
```

ECDHE-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA256
ECDHE-RSA-AES128-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=SHA1
ECDHE-ECDSA-AES128-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA1
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac=SHA1
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(128)	Mac=SHA1
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac=SHA1
DH-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=AEAD
DH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA256
DH-RSA-AES128-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA256
DH-DSS-AES128-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA256
DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA1
DH-RSA-AES128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA1
DH-DSS-AES128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA1
DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)	Mac=SHA1
DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)	Mac=SHA1
DH-RSA-SEED-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=SEED(128)	Mac=SHA1
DH-DSS-SEED-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=SEED(128)	Mac=SHA1
DHE-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(128)	Mac=SHA1
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(128)	Mac=SHA1
DH-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(128)	Mac=SHA1
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AESGCM(128)	Mac=AEAD
ECDH-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AESGCM(128)	Mac=AEAD
ECDH-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AES(128)	Mac=SHA256
ECDH-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(128)	Mac=SHA256
ECDH-RSA-AES128-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=AES(128)	Mac=SHA1
ECDH-ECDSA-AES128-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(128)	Mac=SHA1
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA256
AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA1
SEED-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=SHA1
CAMELLIA128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=IDEA(128)	Mac=SHA1
PSK-AES128-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(128)	Mac=SHA1
ECDHE-RSA-RC4-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=RC4(128)	Mac=SHA1
ECDHE-ECDSA-RC4-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=RC4(128)	Mac=SHA1
ECDH-RSA-RC4-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=RC4(128)	Mac=SHA1
ECDH-ECDSA-RC4-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=RC4(128)	Mac=SHA1
RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1
RC4-MD5	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=MD5
PSK-RC4-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=RC4(128)	Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=3DES(168)	Mac=SHA1
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=3DES(168)	Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=3DES(168)	Mac=SHA1
SRP-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=3DES(168)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH	Au=RSA	Enc=3DES(168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH	Au=DSS	Enc=3DES(168)	Mac=SHA1
DH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=3DES(168)	Mac=SHA1
DH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=3DES(168)	Mac=SHA1
ECDH-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=3DES(168)	Mac=SHA1
ECDH-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=3DES(168)	Mac=SHA1
DES-CBC3-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=3DES(168)	Mac=SHA1

PSK-3DES-EDE-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=3DES(168)	Mac=SHA1
EDH-RSA-DES-CBC-SHA	SSLv3	Kx=DH	Au=RSA	Enc=DES(56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3	Kx=DH	Au=DSS	Enc=DES(56)	Mac=SHA1
DH-RSA-DES-CBC-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=DES(56)	Mac=SHA1
DH-DSS-DES-CBC-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=DES(56)	Mac=SHA1
DES-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=DES(56)	Mac=SHA1

OpenSSL 1.0.2

Released 22-January-2015

ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(256)	Mac=AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac=SHA384
ECDHE-RSA-AES256-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac=SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)	Mac=SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(256)	Mac=SHA1
SRP-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(256)	Mac=SHA1
DH-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(256)	Mac=AEAD
DH-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA256
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA256
DH-RSA-AES256-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA256
DH-DSS-AES256-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA256
DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA1
DH-RSA-AES256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA1
DH-DSS-AES256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA1
DHE-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(256)	Mac=SHA1
DHE-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(256)	Mac=SHA1
DH-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(256)	Mac=SHA1
DH-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(256)	Mac=SHA1
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AESGCM(256)	Mac=AEAD
ECDH-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AESGCM(256)	Mac=AEAD
ECDH-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AES(256)	Mac=SHA384
ECDH-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(256)	Mac=SHA384
ECDH-RSA-AES256-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=AES(256)	Mac=SHA1
ECDH-ECDSA-AES256-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(256)	Mac=SHA1

AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
AES256-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA256
AES256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA1
CAMELLIA256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(256)	Mac=SHA1
PSK-AES256-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(256)	Mac=SHA1
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(128)	Mac=AEAD
ECDHE-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=SHA256
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA256
ECDHE-RSA-AES128-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=SHA1
ECDHE-ECDSA-AES128-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA1
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac=SHA1
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(128)	Mac=SHA1
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac=SHA1
DH-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=AEAD
DH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA256
DH-RSA-AES128-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA256
DH-DSS-AES128-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA256
DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA1
DH-RSA-AES128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA1
DH-DSS-AES128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA1
DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)	Mac=SHA1
DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)	Mac=SHA1
DH-RSA-SEED-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=SEED(128)	Mac=SHA1
DH-DSS-SEED-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=SEED(128)	Mac=SHA1
DHE-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(128)	Mac=SHA1
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(128)	Mac=SHA1
DH-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(128)	Mac=SHA1
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AESGCM(128)	Mac=AEAD
ECDH-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AESGCM(128)	Mac=AEAD
ECDH-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH/RSA	Au=ECDH	Enc=AES(128)	Mac=SHA256
ECDH-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(128)	Mac=SHA256
ECDH-RSA-AES128-	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=AES(128)	Mac=SHA1

SHA						
ECDH-ECDSA-AES128-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=AES(128)	Mac=SHA1	
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=AEAD	
AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA256	
AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA1	
SEED-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=SHA1	
CAMELLIA128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(128)	Mac=SHA1	
IDEA-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=IDEA(128)	Mac=SHA1	
PSK-AES128-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(128)	Mac=SHA1	
ECDHE-RSA-RC4-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=RC4(128)	Mac=SHA1	
ECDHE-ECDSA-RC4-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=RC4(128)	Mac=SHA1	
ECDH-RSA-RC4-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=RC4(128)	Mac=SHA1	
ECDH-ECDSA-RC4-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=RC4(128)	Mac=SHA1	
RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1	
RC4-MD5	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=MD5	
PSK-RC4-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=RC4(128)	Mac=SHA1	
ECDHE-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=3DES(168)	Mac=SHA1	
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=3DES(168)	Mac=SHA1	
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac=SHA1	
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=3DES(168)	Mac=SHA1	
SRP-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=3DES(168)	Mac=SHA1	
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH	Au=RSA	Enc=3DES(168)	Mac=SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH	Au=DSS	Enc=3DES(168)	Mac=SHA1	
DH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=3DES(168)	Mac=SHA1	
DH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=3DES(168)	Mac=SHA1	
ECDH-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH/RSA	Au=ECDH	Enc=3DES(168)	Mac=SHA1	
ECDH-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH	Enc=3DES(168)	Mac=SHA1	
DES-CBC3-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=3DES(168)	Mac=SHA1	
PSK-3DES-EDE-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=3DES(168)	Mac=SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	Kx=DH	Au=RSA	Enc=DES(56)	Mac=SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	Kx=DH	Au=DSS	Enc=DES(56)	Mac=SHA1	
DH-RSA-DES-CBC-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=DES(56)	Mac=SHA1	
DH-DSS-DES-CBC-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=DES(56)	Mac=SHA1	
DES-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=DES(56)	Mac=SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	Kx=DH(512)	Au=RSA	Enc=DES(40)	Mac=SHA1	export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	Kx=DH(512)	Au=DSS	Enc=DES(40)	Mac=SHA1	export
EXP-DH-RSA-DES-CBC-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=DES(40)	Mac=SHA1	export
EXP-DH-DSS-DES-CBC-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=DES(40)	Mac=SHA1	export
EXP-DES-CBC-SHA	SSLv3	Kx=RSA(512)	Au=RSA	Enc=DES(40)	Mac=SHA1	export
EXP-RC2-CBC-MD5	SSLv3	Kx=RSA(512)	Au=RSA	Enc=RC2(40)	Mac=MD5	export
EXP-RC4-MD5	SSLv3	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export

License