OpenSSL 1.1.0 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 1.1.0 – 1.1.0d

Version 1.1.0 released 25-Aug-2016

Version 1.1.0a released 22-Sep-2016

Version 1.1.0b released 26-Sep-2016

Version 1.1.0c released 10-Nov-2016

Version 1.1.0d released 26-Jan-2017

```
ECDHE-ECDSA-AES256-GCM-TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(256)  Mac=AEAD
SHA384
ECDHE-RSA-AES256-GCM-  TLSv1.2 Kx=ECDH     Au=RSA   Enc=AESGCM(256)  Mac=AEAD
SHA384
DHE-RSA-AES256-GCM-    TLSv1.2 Kx=DH       Au=RSA   Enc=AESGCM(256)  Mac=AEAD
SHA384
ECDHE-ECDSA-CHACHA20-  TLSv1.2 Kx=ECDH     Au=ECDSA Enc=CHACHA20/POLY Mac=AEAD
POLY1305                                            1305(256)
ECDHE-RSA-CHACHA20-    TLSv1.2 Kx=ECDH     Au=RSA   Enc=CHACHA20/POLY Mac=AEAD
POLY1305                                            1305(256)
DHE-RSA-CHACHA20-      TLSv1.2 Kx=DH       Au=RSA   Enc=CHACHA20/POLY Mac=AEAD
POLY1305                                            1305(256)
ECDHE-ECDSA-AES128-GCM-TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(128)  Mac=AEAD
SHA256
ECDHE-RSA-AES128-GCM-  TLSv1.2 Kx=ECDH     Au=RSA   Enc=AESGCM(128)  Mac=AEAD
SHA256
DHE-RSA-AES128-GCM-    TLSv1.2 Kx=DH       Au=RSA   Enc=AESGCM(128)  Mac=AEAD
SHA256
ECDHE-ECDSA-AES256-    TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES(256)     Mac=SHA384
SHA384
ECDHE-RSA-AES256-SHA384TLSv1.2 Kx=ECDH     Au=RSA   Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-SHA256  TLSv1.2 Kx=DH       Au=RSA   Enc=AES(256)     Mac=SHA256
ECDHE-ECDSA-AES128-    TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES(128)     Mac=SHA256
SHA256
ECDHE-RSA-AES128-SHA256TLSv1.2 Kx=ECDH     Au=RSA   Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-SHA256  TLSv1.2 Kx=DH       Au=RSA   Enc=AES(128)     Mac=SHA256
ECDHE-ECDSA-AES256-SHA SSLv3   Kx=ECDH     Au=ECDSA Enc=AES(256)     Mac=SHA1
ECDHE-RSA-AES256-SHA   SSLv3   Kx=ECDH     Au=RSA   Enc=AES(256)     Mac=SHA1
DHE-RSA-AES256-SHA     SSLv3   Kx=DH       Au=RSA   Enc=AES(256)     Mac=SHA1
ECDHE-ECDSA-AES128-SHA SSLv3   Kx=ECDH     Au=ECDSA Enc=AES(128)     Mac=SHA1
ECDHE-RSA-AES128-SHA   SSLv3   Kx=ECDH     Au=RSA   Enc=AES(128)     Mac=SHA1
DHE-RSA-AES128-SHA     SSLv3   Kx=DH       Au=RSA   Enc=AES(128)     Mac=SHA1
RSA-PSK-AES256-GCM-    TLSv1.2 Kx=RSAPSK   Au=RSA   Enc=AESGCM(256)  Mac=AEAD
SHA384
DHE-PSK-AES256-GCM-    TLSv1.2 Kx=DHEPSK   Au=PSK   Enc=AESGCM(256)  Mac=AEAD
SHA384
RSA-PSK-CHACHA20-      TLSv1.2 Kx=RSAPSK   Au=RSA   Enc=CHACHA20/POLY Mac=AEAD
POLY1305                                            1305(256)
DHE-PSK-CHACHA20-      TLSv1.2 Kx=DHEPSK   Au=PSK   Enc=CHACHA20/POLY Mac=AEAD
POLY1305                                            1305(256)
ECDHE-PSK-CHACHA20-    TLSv1.2 Kx=ECDHEPSK Au=PSK   Enc=CHACHA20/POLY Mac=AEAD
POLY1305                                            1305(256)
AES256-GCM-SHA384      TLSv1.2 Kx=RSA      Au=RSA   Enc=AESGCM(256)  Mac=AEAD
PSK-AES256-GCM-SHA384  TLSv1.2 Kx=PSK      Au=PSK   Enc=AESGCM(256)  Mac=AEAD
PSK-CHACHA20-POLY1305  TLSv1.2 Kx=PSK      Au=PSK   Enc=CHACHA20/POLY Mac=AEAD
                                                    1305(256)
RSA-PSK-AES128-GCM-    TLSv1.2 Kx=RSAPSK   Au=RSA   Enc=AESGCM(128)  Mac=AEAD
SHA256
DHE-PSK-AES128-GCM-    TLSv1.2 Kx=DHEPSK   Au=PSK   Enc=AESGCM(128)  Mac=AEAD
SHA256
```

```
AES128-GCM-SHA256       TLSv1.2 Kx=RSA       Au=RSA   Enc=AESGCM(128)  Mac=AEAD
PSK-AES128-GCM-SHA256   TLSv1.2 Kx=PSK       Au=PSK   Enc=AESGCM(128)  Mac=AEAD
AES256-SHA256           TLSv1.2 Kx=RSA       Au=RSA   Enc=AES(256)     Mac=SHA256
AES128-SHA256           TLSv1.2 Kx=RSA       Au=RSA   Enc=AES(128)     Mac=SHA256
ECDHE-PSK-AES256-CBC-   TLSv1   Kx=ECDHEPSK  Au=PSK   Enc=AES(256)     Mac=SHA384
SHA384
ECDHE-PSK-AES256-CBC-   SSLv3   Kx=ECDHEPSK  Au=PSK   Enc=AES(256)     Mac=SHA1
SHA
SRP-RSA-AES-256-CBC-SHASSLv3   Kx=SRP       Au=RSA   Enc=AES(256)     Mac=SHA1
SRP-AES-256-CBC-SHA     SSLv3   Kx=SRP       Au=SRP   Enc=AES(256)     Mac=SHA1
RSA-PSK-AES256-CBC-     TLSv1   Kx=RSAPSK    Au=RSA   Enc=AES(256)     Mac=SHA384
SHA384
DHE-PSK-AES256-CBC-     TLSv1   Kx=DHEPSK    Au=PSK   Enc=AES(256)     Mac=SHA384
SHA384
RSA-PSK-AES256-CBC-SHA  SSLv3   Kx=RSAPSK    Au=RSA   Enc=AES(256)     Mac=SHA1
DHE-PSK-AES256-CBC-SHA  SSLv3   Kx=DHEPSK    Au=PSK   Enc=AES(256)     Mac=SHA1
AES256-SHA              SSLv3   Kx=RSA       Au=RSA   Enc=AES(256)     Mac=SHA1
PSK-AES256-CBC-SHA384   TLSv1   Kx=PSK       Au=PSK   Enc=AES(256)     Mac=SHA384
PSK-AES256-CBC-SHA      SSLv3   Kx=PSK       Au=PSK   Enc=AES(256)     Mac=SHA1
ECDHE-PSK-AES128-CBC-   TLSv1   Kx=ECDHEPSK  Au=PSK   Enc=AES(128)     Mac=SHA256
SHA256
ECDHE-PSK-AES128-CBC-   SSLv3   Kx=ECDHEPSK  Au=PSK   Enc=AES(128)     Mac=SHA1
SHA
SRP-RSA-AES-128-CBC-SHASSLv3   Kx=SRP       Au=RSA   Enc=AES(128)     Mac=SHA1
SRP-AES-128-CBC-SHA     SSLv3   Kx=SRP       Au=SRP   Enc=AES(128)     Mac=SHA1
RSA-PSK-AES128-CBC-     TLSv1   Kx=RSAPSK    Au=RSA   Enc=AES(128)     Mac=SHA256
SHA256
DHE-PSK-AES128-CBC-     TLSv1   Kx=DHEPSK    Au=PSK   Enc=AES(128)     Mac=SHA256
SHA256
RSA-PSK-AES128-CBC-SHA  SSLv3   Kx=RSAPSK    Au=RSA   Enc=AES(128)     Mac=SHA1
DHE-PSK-AES128-CBC-SHA  SSLv3   Kx=DHEPSK    Au=PSK   Enc=AES(128)     Mac=SHA1
AES128-SHA              SSLv3   Kx=RSA       Au=RSA   Enc=AES(128)     Mac=SHA1
PSK-AES128-CBC-SHA256   TLSv1   Kx=PSK       Au=PSK   Enc=AES(128)     Mac=SHA256
PSK-AES128-CBC-SHA      SSLv3   Kx=PSK       Au=PSK   Enc=AES(128)     Mac=SHA1
```

License