OpenSSL 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

Introduction.....1
OpenSSL 1.0.0r – 1.0.0t.....2
OpenSSL 1.0.0n – 1.0.0q.....3
OpenSSL 1.0.0 – 1.0.0m.....5
License.....6

OpenSSL 1.0.0r – 1.0.0t

Version 1.0.0r released 19-March-2015

Version 1.0.0s released 11-June-2015

Version 1.0.0t released 3-December-2015

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
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
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
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-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-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
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
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
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
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-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
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
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
DES-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=DES(56)	Mac=SHA1

OpenSSL 1.0.0n – 1.0.0q

Version 1.0.0n released 6-August-2014

Version 1.0.0o released 15-October-2014

Version 1.0.0p released 8-January-2015

Version 1.0.0q released 15-January-2015

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
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
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
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-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-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
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
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
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
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-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
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
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
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-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

OpenSSL 1.0.0 – 1.0.0m

Version 1.0.0 released 29-March-2010

Version 1.0.0a released 1-June-2010

Version 1.0.0b released 16-November-2010

Version 1.0.0c released 2-December-2010

Version 1.0.0d released 8-February-2011

Version 1.0.0e released 6-September-2011

Version 1.0.0f released 4-January-2012

Version 1.0.0g released 18-January-2012

Version 1.0.0h released 12-March-2012

Version 1.0.0i released 19-April-2012

Version 1.0.0j released 10-May-2012

Version 1.0.0k released 5-February-2013

Version 1.0.0l released 6-January-2014

Version 1.0.0m released 5-June-2014

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
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
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
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-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-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
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
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
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
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
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
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
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-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
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
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-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