

# OpenSSL Pre 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 0.9.8zf – 0.9.8zh.....	2
OpenSSL 0.9.8c – 0.9.8ze.....	3
OpenSSL 0.9.8 – 0.9.8b.....	4
OpenSSL 0.9.7m.....	5
OpenSSL 0.9.7k & 0.9.7l.....	6
OpenSSL 0.9.7 – 0.9.7j.....	7
OpenSSL 0.9.5 – 0.9.6m.....	8
OpenSSL 0.9.1c – 0.9.4.....	9
License.....	9

# OpenSSL 0.9.8zf – 0.9.8zh

Version 0.9.8zf released 19-March-2015

Version 0.9.8zg released 11-June-2015

Version 0.9.8zh released 3-December-2015

DHE-RSA-AES256-SHA	SSLv3Kx=DH	Au=RSAEnc=AES(256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3Kx=DH	Au=DSEnc=AES(256)	Mac=SHA1
AES256-SHA	SSLv3Kx=RSAAu=RSAEnc=AES(256)		Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3Kx=DH	Au=RSAEnc=3DES(168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3Kx=DH	Au=DSEnc=3DES(168)	Mac=SHA1
DES-CBC3-SHA	SSLv3Kx=RSAAu=RSAEnc=3DES(168)		Mac=SHA1
DHE-RSA-AES128-SHA	SSLv3Kx=DH	Au=RSAEnc=AES(128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3Kx=DH	Au=DSEnc=AES(128)	Mac=SHA1
AES128-SHA	SSLv3Kx=RSAAu=RSAEnc=AES(128)		Mac=SHA1
IDEA-CBC-SHA	SSLv3Kx=RSAAu=RSAEnc=IDEA(128)		Mac=SHA1
RC4-SHA	SSLv3Kx=RSAAu=RSAEnc=RC4(128)		Mac=SHA1
RC4-MD5	SSLv3Kx=RSAAu=RSAEnc=RC4(128)		Mac=MD5
EDH-RSA-DES-CBC-SHA	SSLv3Kx=DH	Au=RSAEnc=DES(56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3Kx=DH	Au=DSEnc=DES(56)	Mac=SHA1
DES-CBC-SHA	SSLv3Kx=RSAAu=RSAEnc=DES(56)		Mac=SHA1

# OpenSSL 0.9.8c – 0.9.8ze

Version 0.9.8c released 5-September-2006  
Version 0.9.8d released 28-September-2006  
Version 0.9.8e released 23-February-2007  
Version 0.9.8f released 11-October-2007  
Version 0.9.8g released 19-October-2007  
Version 0.9.8h released 25-May-2008  
Version 0.9.8i released 15-September-2008  
Version 0.9.8j released 7-January-2009  
Version 0.9.8k released 25-March-2009  
Version 0.9.8m released 25-February-2010  
Version 0.9.8n released 24-March-2010  
Version 0.9.8o released 1-June-2010  
Version 0.9.8p released 16-November-2010  
Version 0.9.8q released 2-December-2010

Version 0.9.8l was never released

Version 0.9.8r released 8-February-2011  
Version 0.9.8s released 4-January-2012  
Version 0.9.8t released 18-January-2012  
Version 0.9.8u released 12-March-2012  
Version 0.9.8v released 19-April-2012  
Version 0.9.8w released 24-April-2012  
Version 0.9.8x released 10-May-2012  
Version 0.9.8y released 5-February-2013  
Version 0.9.8za released 5-June-2014  
Version 0.9.8zb released 6-August-2014  
Version 0.9.8zc released 15-October-2014  
Version 0.9.8zd released 8-January-2015  
Version 0.9.8ze released 15-January-2015

DHE-RSA-AES256-SHA	SSLv3Kx=DH	Au=RSAEnc=AES (256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3Kx=DH	Au=DSSEnc=AES (256)	Mac=SHA1
AES256-SHA	SSLv3Kx=RSA	Au=RSAEnc=AES (256)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3Kx=DH	Au=RSAEnc=3DES (168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3Kx=DH	Au=DSSEnc=3DES (168)	Mac=SHA1
DES-CBC3-SHA	SSLv3Kx=RSA	Au=RSAEnc=3DES (168)	Mac=SHA1
DES-CBC3-MD5	SSLv2Kx=RSA	Au=RSAEnc=3DES (168)	Mac=MD5
DHE-RSA-AES128-SHA	SSLv3Kx=DH	Au=RSAEnc=AES (128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3Kx=DH	Au=DSSEnc=AES (128)	Mac=SHA1
AES128-SHA	SSLv3Kx=RSA	Au=RSAEnc=AES (128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=SHA1
IDEA-CBC-MD5	SSLv2Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=MD5
RC2-CBC-MD5	SSLv2Kx=RSA	Au=RSAEnc=RC2 (128)	Mac=MD5
RC4-SHA	SSLv3Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=SHA1
RC4-MD5	SSLv3Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-MD5	SSLv2Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
EDH-RSA-DES-CBC-SHA	SSLv3Kx=DH	Au=RSAEnc=DES (56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3Kx=DH	Au=DSSEnc=DES (56)	Mac=SHA1
DES-CBC-SHA	SSLv3Kx=RSA	Au=RSAEnc=DES (56)	Mac=SHA1
DES-CBC-MD5	SSLv2Kx=RSA	Au=RSAEnc=DES (56)	Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3Kx=DH (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3Kx=DH (512)	Au=DSSEnc=DES (40)	Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3Kx=RSA (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv3Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv2Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export

# OpenSSL 0.9.8 – 0.9.8b

Version 0.9.8 released 5-July-2005

Version 0.9.8a released 11-October-2005

Version 0.9.8b released 4-May-2006

DHE-RSA-AES256-SHA	SSLv3 Kx=DH	Au=RSAEnc=AES (256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3 Kx=DH	Au=DSSEnc=AES (256)	Mac=SHA1
AES256-SHA	SSLv3 Kx=RSA	Au=RSAEnc=AES (256)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3 Kx=DH	Au=RSAEnc=3DES (168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3 Kx=DH	Au=DSSEnc=3DES (168)	Mac=SHA1
DES-CBC3-SHA	SSLv3 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=SHA1
DES-CBC3-MD5	SSLv2 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=MD5
DHE-RSA-AES128-SHA	SSLv3 Kx=DH	Au=RSAEnc=AES (128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3 Kx=DH	Au=DSSEnc=AES (128)	Mac=SHA1
AES128-SHA	SSLv3 Kx=RSA	Au=RSAEnc=AES (128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=SHA1
IDEA-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=MD5
RC2-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC2 (128)	Mac=MD5
DHE-DSS-RC4-SHA	SSLv3 Kx=DH	Au=DSSEnc=RC4 (128)	Mac=SHA1
RC4-SHA	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=SHA1
RC4-MD5	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-64-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (64)	Mac=MD5
EXP1024-DHE-DSS-DES-CBC-SHA	SSLv3 Kx=DH (1024)	Au=DSSEnc=DES (56)	Mac=SHA1 export
EXP1024-DES-CBC-SHA	SSLv3 Kx=RSA (1024)	Au=RSAEnc=DES (56)	Mac=SHA1 export
EXP1024-RC2-CBC-MD5	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC2 (56)	Mac=MD5 export
EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH	Au=RSAEnc=DES (56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH	Au=DSSEnc=DES (56)	Mac=SHA1
DES-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=DES (56)	Mac=SHA1
DES-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=DES (56)	Mac=MD5
EXP1024-DHE-DSS-RC4-SHA	SSLv3 Kx=DH (1024)	Au=DSSEnc=RC4 (56)	Mac=SHA1 export
EXP1024-RC4-SHA	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC4 (56)	Mac=SHA1 export
EXP1024-RC4-MD5	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC4 (56)	Mac=MD5 export
EXP-EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=DSSEnc=DES (40)	Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3 Kx=RSA (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export

# OpenSSL 0.9.7m

Released 23-February-2007

DHE-RSA-AES256-SHA	SSLv3Kx=DH	Au=RSAEnc=AES (256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3Kx=DH	Au=DSSEnc=AES (256)	Mac=SHA1
AES256-SHA	SSLv3Kx=RSA	Au=RSAEnc=AES (256)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3Kx=DH	Au=RSAEnc=3DES (168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3Kx=DH	Au=DSSEnc=3DES (168)	Mac=SHA1
DES-CBC3-SHA	SSLv3Kx=RSA	Au=RSAEnc=3DES (168)	Mac=SHA1
DES-CBC3-MD5	SSLv2Kx=RSA	Au=RSAEnc=3DES (168)	Mac=MD5
DHE-RSA-AES128-SHA	SSLv3Kx=DH	Au=RSAEnc=AES (128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3Kx=DH	Au=DSSEnc=AES (128)	Mac=SHA1
AES128-SHA	SSLv3Kx=RSA	Au=RSAEnc=AES (128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=SHA1
RC4-SHA	SSLv3Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=SHA1
RC4-MD5	SSLv3Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
IDEA-CBC-MD5	SSLv2Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=MD5
RC2-CBC-MD5	SSLv2Kx=RSA	Au=RSAEnc=RC2 (128)	Mac=MD5
RC4-MD5	SSLv2Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
EDH-RSA-DES-CBC-SHA	SSLv3Kx=DH	Au=RSAEnc=DES (56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3Kx=DH	Au=DSSEnc=DES (56)	Mac=SHA1
DES-CBC-SHA	SSLv3Kx=RSA	Au=RSAEnc=DES (56)	Mac=SHA1
DES-CBC-MD5	SSLv2Kx=RSA	Au=RSAEnc=DES (56)	Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3Kx=DH (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3Kx=DH (512)	Au=DSSEnc=DES (40)	Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3Kx=RSA (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv3Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv2Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export

# OpenSSL 0.9.7k & 0.9.7l

Version 0.9.7k released 5-September-2006

Version 0.9.7l released 28-September-2006

DHE-RSA-AES256-SHA	SSLv3 Kx=DH	Au=RSAEnc=AES (256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3 Kx=DH	Au=DSSEnc=AES (256)	Mac=SHA1
AES256-SHA	SSLv3 Kx=RSA	Au=RSAEnc=AES (256)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3 Kx=DH	Au=RSAEnc=3DES (168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3 Kx=DH	Au=DSSEnc=3DES (168)	Mac=SHA1
DES-CBC3-SHA	SSLv3 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=SHA1
DES-CBC3-MD5	SSLv2 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=MD5
DHE-RSA-AES128-SHA	SSLv3 Kx=DH	Au=RSAEnc=AES (128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3 Kx=DH	Au=DSSEnc=AES (128)	Mac=SHA1
AES128-SHA	SSLv3 Kx=RSA	Au=RSAEnc=AES (128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=SHA1
IDEA-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=MD5
RC2-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC2 (128)	Mac=MD5
RC4-SHA	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=SHA1
RC4-MD5	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH	Au=RSAEnc=DES (56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH	Au=DSSEnc=DES (56)	Mac=SHA1
DES-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=DES (56)	Mac=SHA1
DES-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=DES (56)	Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=DSSEnc=DES (40)	Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3 Kx=RSA (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export

# OpenSSL 0.9.7 – 0.9.7j

Version 0.9.7 released 31-December-2002

Version 0.9.7a released 19-February-2003

Version 0.9.7b released 10-April-2003

Version 0.9.7c released 30-September-2003

Version 0.9.7d released 17-March-2004

Version 0.9.7e released 25-October-2004

Version 0.9.7f released 22-March-2005

Version 0.9.7g released 11-April-2005

Version 0.9.7h released 11-October-2005

Version 0.9.7i released 15-October-2005

Version 0.9.7j released 4-May-2006

DHE-RSA-AES256-SHA	SSLv3 Kx=DH	Au=RSAEnc=AES (256)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3 Kx=DH	Au=DSSEnc=AES (256)	Mac=SHA1
AES256-SHA	SSLv3 Kx=RSA	Au=RSAEnc=AES (256)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3 Kx=DH	Au=RSAEnc=3DES (168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3 Kx=DH	Au=DSSEnc=3DES (168)	Mac=SHA1
DES-CBC3-SHA	SSLv3 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=SHA1
DES-CBC3-MD5	SSLv2 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=MD5
DHE-RSA-AES128-SHA	SSLv3 Kx=DH	Au=RSAEnc=AES (128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3 Kx=DH	Au=DSSEnc=AES (128)	Mac=SHA1
AES128-SHA	SSLv3 Kx=RSA	Au=RSAEnc=AES (128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=SHA1
IDEA-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=MD5
RC2-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC2 (128)	Mac=MD5
DHE-DSS-RC4-SHA	SSLv3 Kx=DH	Au=DSSEnc=RC4 (128)	Mac=SHA1
RC4-SHA	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=SHA1
RC4-MD5	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-64-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (64)	Mac=MD5
EXP1024-DHE-DSS-DES-CBC-SHA	SSLv3 Kx=DH (1024)	Au=DSSEnc=DES (56)	Mac=SHA1 export
EXP1024-DES-CBC-SHA	SSLv3 Kx=RSA (1024)	Au=RSAEnc=DES (56)	Mac=SHA1 export
EXP1024-RC2-CBC-MD5	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC2 (56)	Mac=MD5 export
EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH	Au=RSAEnc=DES (56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH	Au=DSSEnc=DES (56)	Mac=SHA1
DES-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=DES (56)	Mac=SHA1
DES-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=DES (56)	Mac=MD5
EXP1024-DHE-DSS-RC4-SHA	SSLv3 Kx=DH (1024)	Au=DSSEnc=RC4 (56)	Mac=SHA1 export
EXP1024-RC4-SHA	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC4 (56)	Mac=SHA1 export
EXP1024-RC4-MD5	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC4 (56)	Mac=MD5 export
EXP-EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=DSSEnc=DES (40)	Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3 Kx=RSA (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export

# OpenSSL 0.9.5 – 0.9.6m

Version 0.9.5 released 28-February-2000

Version 0.9.5a released 1-April-2000

Version 0.9.6 released 24-september-2000

Version 0.9.6a released 5-April-2001

Version 0.9.6b released 9-July-2001

Version 0.9.6c released 21-December-2001

Version 0.9.6d released 9-May-2002

Version 0.9.6e released 30-July-2002

Version 0.9.6f released 8-August-2002

Version 0.9.6g released 9-August-2002

Version 0.9.6h released 5-December-2002

Version 0.9.6i released 19-February-2003

Version 0.9.6j released 10-April-2003

Version 0.9.6k released 30-September-2003

Version 0.9.6l released 4-November-2003

Version 0.9.6m released 17-March-2004

EDH-RSA-DES-CBC3-SHA	SSLv3 Kx=DH	Au=RSAEnc=3DES (168)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3 Kx=DH	Au=DSSEnc=3DES (168)	Mac=SHA1
DES-CBC3-SHA	SSLv3 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=SHA1
DES-CBC3-MD5	SSLv2 Kx=RSA	Au=RSAEnc=3DES (168)	Mac=MD5
DHE-DSS-RC4-SHA	SSLv3 Kx=DH	Au=DSSEnc=RC4 (128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=SHA1
RC4-SHA	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=SHA1
RC4-MD5	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
IDEA-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=IDEA (128)	Mac=MD5
RC2-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC2 (128)	Mac=MD5
RC4-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (128)	Mac=MD5
RC4-64-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (64)	Mac=MD5
EXP1024-DHE-DSS-RC4-SHA	SSLv3 Kx=DH (1024)	Au=DSSEnc=RC4 (56)	Mac=SHA1 export
EXP1024-RC4-SHA	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC4 (56)	Mac=SHA1 export
EXP1024-DHE-DSS-DES-CBC-SHA	SSLv3 Kx=DH (1024)	Au=DSSEnc=DES (56)	Mac=SHA1 export
EXP1024-DES-CBC-SHA	SSLv3 Kx=RSA (1024)	Au=RSAEnc=DES (56)	Mac=SHA1 export
EXP1024-RC2-CBC-MD5	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC2 (56)	Mac=MD5 export
EXP1024-RC4-MD5	SSLv3 Kx=RSA (1024)	Au=RSAEnc=RC4 (56)	Mac=MD5 export
EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH	Au=RSAEnc=DES (56)	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH	Au=DSSEnc=DES (56)	Mac=SHA1
DES-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=DES (56)	Mac=SHA1
DES-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=DES (56)	Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=DSSEnc=DES (40)	Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3 Kx=RSA (512)	Au=RSAEnc=DES (40)	Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC2 (40)	Mac=MD5 export
EXP-RC4-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC4 (40)	Mac=MD5 export



# OpenSSL 0.9.1c – 0.9.4

Version 0.9.1c released 23-December-1998

Version 0.9.2b released 22-March-1999

Version 0.9.3 released 25-May-1999

Version 0.9.3a released 29-May-1999

Version 0.9.4 released 9-August-1999

EDH-RSA-DES-CBC3-SHA	SSLv3 Kx=DH	Au=RSAEnc=3DES (168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3 Kx=DH	Au=DSSEnc=3DES (168) Mac=SHA1
DES-CBC3-SHA	SSLv3 Kx=RSA	Au=RSAEnc=3DES (168) Mac=SHA1
IDEA-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=IDEA (128) Mac=SHA1
RC4-SHA	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128) Mac=SHA1
RC4-MD5	SSLv3 Kx=RSA	Au=RSAEnc=RC4 (128) Mac=MD5
EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH	Au=RSAEnc=DES (56) Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH	Au=DSSEnc=DES (56) Mac=SHA1
DES-CBC-SHA	SSLv3 Kx=RSA	Au=RSAEnc=DES (56) Mac=SHA1
DES-CBC3-MD5	SSLv2 Kx=RSA	Au=RSAEnc=3DES (168) Mac=MD5
IDEA-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=IDEA (128) Mac=MD5
RC2-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC2 (128) Mac=MD5
RC4-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (128) Mac=MD5
RC4-64-MD5	SSLv2 Kx=RSA	Au=RSAEnc=RC4 (64) Mac=MD5
DES-CBC-MD5	SSLv2 Kx=RSA	Au=RSAEnc=DES (56) Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=RSAEnc=DES (40) Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3 Kx=DH (512)	Au=DSSEnc=DES (40) Mac=SHA1 export
EXP-DES-CBC-SHA	SSLv3 Kx=RSA (512)	Au=RSAEnc=DES (40) Mac=SHA1 export
EXP-RC2-CBC-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC2 (40) Mac=MD5 export
EXP-RC4-MD5	SSLv3 Kx=RSA (512)	Au=RSAEnc=RC4 (40) Mac=MD5 export
EXP-RC2-CBC-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC2 (40) Mac=MD5 export
EXP-RC4-MD5	SSLv2 Kx=RSA (512)	Au=RSAEnc=RC4 (40) Mac=MD5 export

## License



This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/>.