Published date: 09.08.2010
Last Update: 23.02.2011
Author: Adrian F. Dimcev, contact@carbonwind.net

**Work in progress** Known limitations:there are active/expired drafts mentioning additional cipher suites with TBD cipher suite codes. Currently these are not included into the doc, this is on the todo list.

# SSL/TLS Cipher Suites Lists

[SSL/TLS Cipher Suites Lists 1](#_Toc269221049)

[1. Main Table 2](#_Toc269221050)

[2. Meaning 10](#_Toc269221051)

[3. Extra Cipher Suites 11](#_Toc269221052)

[4. References 14](#_Toc269221053)

[5. Extra References 15](#_Toc269221080)

### 1. Main Table

Table 1

| No | Cipher Suite | Hex Value | SSL 2.0 | SSL 3.0 | TLS 1.0 | TLS 1.1 | TLS 1.2 | RFC | Draft | FIPS\* [26](#_26._FIPS_PUB)[27](#_27._Guidelines_for) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | SSL\_CK\_RC4\_128\_WITH\_MD5(SSL2\_RC4\_128\_WITH\_MD5) | 0x010080 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5(SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5) | 0x020080 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5(SSL2\_RC2\_128\_CBC\_WITH\_MD5) | 0x030080 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5(SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5) | 0x040080 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_IDEA\_128\_CBC\_WITH\_MD5(SSL2\_IDEA\_128\_CBC\_WITH\_MD5) | 0x050080 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5(SSL2\_DES\_64\_CBC\_WITH\_MD5) | 0x060040 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5(SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5) | 0x0700C0 | n | - | - | - | - | Draft Last Update: Feb. 9th, 1995 [1](#_1._Draft,_SSL) | No |
|  | SSL\_CK\_RC4\_64\_WITH\_MD5 | 0x080080 | s | - | - | - | - | ? | No |
|  | TLS\_NULL\_WITH\_NULL\_NULL(SSL\_NULL\_WITH\_NULL\_NULL) | 0x0000 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_WITH\_NULL\_MD5(SSL\_RSA\_WITH\_NULL\_MD5) | 0x0001 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_WITH\_NULL\_SHA(SSL\_RSA\_WITH\_NULL\_SHA) | 0x0002 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5(SSL\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5) | 0x0003 | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_RSA\_WITH\_RC4\_128\_MD5(SSL\_RSA\_WITH\_RC4\_128\_MD5) | 0x0004 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_WITH\_RC4\_128\_SHA(SSL\_RSA\_WITH\_RC4\_128\_SHA) | 0x0005 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5(SSL\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5) | 0x0006 | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_RSA\_WITH\_IDEA\_CBC\_SHA(SSL\_RSA\_WITH\_IDEA\_CBC\_SHA) | 0x0007 | - | n | n | n | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA(SSL\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA) | 0x0008 | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_RSA\_WITH\_DES\_CBC\_SHA(SSL\_RSA\_WITH\_DES\_CBC\_SHA) | 0x0009 | - | n | n | n | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA(SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA) | 0x000A | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA(SSL\_DH\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA) | 0x000B | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_DH\_DSS\_WITH\_DES\_CBC\_SHA(SSL\_DH\_DSS\_WITH\_DES\_CBC\_SHA) | 0x000C | - | n | n | n | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_DH\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA(SSL\_DH\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA) | 0x000D | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA(SSL\_DH\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA) | 0x000E | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_DH\_RSA\_WITH\_DES\_CBC\_SHA(SSL\_DH\_RSA\_WITH\_DES\_CBC\_SHA) | 0x000F | - | n | n | n | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_DH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA(SSL\_DH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA) | 0x0010 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA(SSL\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA) | 0x0011 | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA(SSL\_DHE\_DSS\_WITH\_DES\_CBC\_SHA) | 0x0012 | - | n | n | n | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA(SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA) | 0x0013 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA(SSL\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA) | 0x0014 | - | n | n | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA(SSL\_DHE\_RSA\_WITH\_DES\_CBC\_SHA) | 0x0015 | - | n | n | n | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA(SSL\_ DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA) | 0x0016 | - | n | n | n | n | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5(SSL\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5) | 0x0017 | - | disc | depr | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5(SSL\_DH\_anon\_WITH\_RC4\_128\_MD5) | 0x0018 | - | disc | depr | depr | c | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA(SSL\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA) | 0x0019 | - | disc | depr | x | x | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_DH\_anon\_WITH\_DES\_CBC\_SHA(SSL\_DH\_anon\_WITH\_DES\_CBC\_SHA) | 0x001A | - | disc | depr | depr | depr | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5469 February 2009 [19](#_19._DES_and) | No |
|  | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA(SSL\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA) | 0x001B | - | disc | depr | depr | c | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt)RFC 2246 January 1999 [3](#_3._The_TLS)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | SSL\_FORTEZZA\_KEA\_WITH\_NULL\_SHA | 0X001C | - | n | - | - | - | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt) | No |
|  | SSL\_FORTEZZA\_KEA\_WITH\_FORTEZZA\_CBC\_SHA | 0x001D | - | n | - | - | - | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt) | No |
|  | SSL\_FORTEZZA\_KEA\_WITH\_RC4\_128\_SHA | 0x001E | - | n | - | - | - | Draft Last Update: Nov. 18th, 1996 [2](#_2._draft-freier-ssl-version3-02.txt) | No |
|  | TLS\_KRB5\_WITH\_DES\_CBC\_SHA | 0x001E | - | s | n | n | ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_9._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001F | - | s | n | n | ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_RC4\_128\_SHA | 0x0020 | - | s | n | n | ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_IDEA\_CBC\_SHA | 0x0021 | - | s | n | n | ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_DES\_CBC\_MD5 | 0x0022 | - | s | n | n | depr ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_MD5 | 0x0023 | - | s | n | n | ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_RC4\_128\_MD5 | 0x0024 | - | s | n | n | ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_WITH\_IDEA\_CBC\_MD5 | 0x0025 | - | s | n | n | depr ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_EXPORT\_WITH\_DES\_CBC\_40\_SHA | 0x0026 | - | s | n | x | x ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_EXPORT\_WITH\_RC2\_CBC\_40\_SHA | 0x0027 | - | s | n | x | x ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_EXPORT\_WITH\_RC4\_40\_SHA | 0x0028 | - | s | n | x | x ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_EXPORT\_WITH\_DES\_CBC\_40\_MD5 | 0x0029 | - | s | n | x | x ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x002A | - | s | n | x | x ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_KRB5\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x002B | - | s | n | x | x ? | RFC 2712 October 1999 [4](#_4.__Addition)RFC 4346 April 2006 [10](#_10._The_Transport) | No |
|  | TLS\_PSK\_WITH\_NULL\_SHA | 0x002C | - | ? | n | n | n | RFC 4785 January 2007 [13](#_13._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_NULL\_SHA | 0x002D | - | ? | n | n | n | RFC 4785 January 2007 [13](#_13._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_NULL\_SHA | 0x002E | - | ? | n | n | n | RFC 4785 January 2007 [13](#_13._Pre-Shared_Key) | No |
|  | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0030 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0031 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | - | s | n | n | c | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0036 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0037 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | - | s | n | n | n | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | - | s | n | n | c | RFC 3268 June 2002 [5](#_5._Advanced_Encryption)RFC 4346 April 2006 [10](#_10._The_Transport)RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_WITH\_NULL\_SHA256 | 0x003B | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003C | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x003D | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_DSS\_WITH\_AES\_128\_CBC\_SHA25 | 0x003E | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003F | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 | 0x0040 | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0042 | - | ? | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0043 | - | ? | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_MD5(SSL\_RSA\_EXPORT1024\_WITH\_RC4\_56\_MD5) | 0x0060 | - | s | s | x ? | x ? | ? | No |
|  | TLS\_RSA\_EXPORT1024\_WITH\_RC2\_56\_MD5(SSL\_RSA\_EXPORT1024\_WITH\_RC2\_CBC\_56\_MD5) | 0x0061 | - | s | s | x ? | x ? | ? | No |
|  | TLS \_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA(SSL\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA) | 0x0062 | - | s | s | x ? | x ? | Draft Last Update: July 19, 2001 [5](#_5.__draft-ietf-tls-56-bit-ciphersui) | No |
|  | TLS \_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA(SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA) | 0x0063 | - | s | s | x ? | x ? | Draft Last Update: July 19, 2001 [5](#_5.__draft-ietf-tls-56-bit-ciphersui) | No |
|  | TLS \_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA(SSL\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA) | 0x0064 | - | s | s | x ? | x ? | Draft Last Update: July 19, 2001 [5](#_5.__draft-ietf-tls-56-bit-ciphersui) | No |
|  | TLS \_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA(SSL\_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA) | 0x0065 | - | s | s | x ? | x ? | Draft Last Update: July 19, 2001 [5](#_5.__draft-ietf-tls-56-bit-ciphersui) | No |
|  | TLS \_DHE\_DSS\_WITH\_RC4\_128\_SHA(SSL\_DHE\_DSS\_WITH\_RC4\_128\_SHA) | 0x0066 | - | s | s | s | ? | Draft Last Update: July 19, 2001 [5](#_5.__draft-ietf-tls-56-bit-ciphersui) | No |
|  | TLS\_NTRU\_NSS\_WITH\_RC4\_128\_SHA | 0x0061 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher) | No |
|  | TLS\_NTRU\_NSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0062 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher) | No |
|  | TLS\_NTRU\_NSS\_WITH\_AES\_128\_CBC\_SHA | 0x0063 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher) | No |
|  | TLS\_NTRU\_NSS\_WITH\_AES\_256\_CBC\_SHA | 0x0064 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher) | No |
|  | TLS\_NTRU\_RSA\_WITH\_RC4\_128\_SHA | 0x0065 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher)Extra [28](#_28._CyaSSL_source)[30](#_30._Security_Innovation)[31](#_31._CyaSSL_Extensions) | No |
|  | TLS\_NTRU\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0066 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher)Extra [28](#_28._CyaSSL_source)[30](#_30._Security_Innovation)[31](#_31._CyaSSL_Extensions) | No |
|  | TLS\_NTRU\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0067 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher)Extra [28](#_28._CyaSSL_source)[30](#_30._Security_Innovation)[31](#_31._CyaSSL_Extensions) | No |
|  | TLS\_NTRU\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0068 | - | ? | s | ? | ? | Draft Last Update: July 3, 2001 [29](#_29._NTRU_Cipher)Extra [28](#_28._CyaSSL_source)[30](#_30._Security_Innovation)[31](#_31._CyaSSL_Extensions) | No |
|  | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x0067 | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x0068 | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x0069 | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x006A | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x006B | - | s | s | s | n | RFC 5246 August 2008 [15](#_13._The_Transport) | Yes |
|  | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA256 | 0x006C | - | s | s | s | c | RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA256 | 0x006D | - | s | s | s | c | RFC 5246 August 2008 [15](#_13._The_Transport) | No |
|  | TLS\_GOSTR341094\_WITH\_28147\_CNT\_IMIT | 0x0080 | - | ? | n | ? | ? | Draft Last Update: December 8, 2008 [24](#_24._draft-chudov-cryptopro-cptls-04) | No |
|  | TLS\_GOSTR341001\_WITH\_28147\_CNT\_IMIT | 0x0081 | - | ? | n | ? | ? | Draft Last Update: December 8, 2008 [24](#_24._draft-chudov-cryptopro-cptls-04) | No |
|  | TLS\_GOSTR341094\_WITH\_NULL\_GOSTR3411 | 0x0082 | - | ? | n | ? | ? | Draft Last Update: December 8, 2008 [24](#_24._draft-chudov-cryptopro-cptls-04) | No |
|  | TLS\_GOSTR341001\_WITH\_NULL\_GOSTR3411 | 0x0083 | - | ? | n | ? | ? | Draft Last Update: December 8, 2008 [24](#_24._draft-chudov-cryptopro-cptls-04) | No |
|  | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0085 | - | ? | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0086 | - | ? | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | - | s | n | n | n | RFC 4132 July 2005 [7](#_6.__Addition)RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_PSK\_WITH\_RC4\_128\_SHA | 0x008A | - | s | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008B | - | s | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x008C | - | s | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x008D | - | s | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_RC4\_128\_SHA | 0x008E | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008F | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x0090 | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x0091 | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_RC4\_128\_SHA | 0x0092 | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0093 | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x0094 | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x0095 | - | ? | n | n | n | RFC 4279 December 2005 [9](#_9._Pre-Shared_Key) | No |
|  | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | - | s | n | ? | ? | RFC 4162 August 2005 [8](#_8.__Addition) | No |
|  | TLS\_DH\_DSS\_WITH\_SEED\_CBC\_SHA | 0x0097 | - | ? | n | ? | ? | RFC 4162 August 2005 [8](#_8.__Addition) | No |
|  | TLS\_DH\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0098 | - | ? | n | ? | ? | RFC 4162 August 2005 [8](#_8.__Addition) | No |
|  | TLS\_DHE\_DSS\_WITH\_SEED\_CBC\_SHA | 0x0099 | - | s | n | ? | ? | RFC 4162 August 2005 [8](#_8.__Addition) | No |
|  | TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA | 0x009A | - | s | n | ? | ? | RFC 4162 August 2005 [8](#_8.__Addition) | No |
|  | TLS\_DH\_ ANON\_WITH\_SEED\_CBC\_SHA | 0x009B | - | s | n | ? | ? | RFC 4162 August 2005 [8](#_8.__Addition) | No |
|  | TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | 0x009C | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | 0x009D | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | 0x009E | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | 0x009F | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DH\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | 0x00A0 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DH\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | 0x00A1 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256 | 0x00A2 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384 | 0x00A3 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DH\_DSS\_WITH\_AES\_128\_GCM\_SHA256 | 0x00A4 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DH\_DSS\_WITH\_AES\_256\_GCM\_SHA384 | 0x00A5 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | Yes |
|  | TLS\_DH\_anon\_WITH\_AES\_128\_GCM\_SHA256 | 0x00A6 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | No |
|  | TLS\_DH\_anon\_WITH\_AES\_256\_GCM\_SHA384 | 0x00A7 | - | x | x | x | n | RFC 5288 August 2008 [16](#_16._AES_Galois) | No |
|  | TLS\_PSK\_WITH\_AES\_128\_GCM\_SHA256 | 0x00A8 | - | x | x | x | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_AES\_256\_GCM\_SHA384 | 0x00A9 | - | x | x | x | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_AES\_128\_GCM\_SHA256 | 0x00AA | - | x | x | x | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_AES\_256\_GCM\_SHA384 | 0x00AB | - | x | x | x | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_AES\_128\_GCM\_SHA256 | 0x00AC | - | x | x | x | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_AES\_256\_GCM\_SHA384 | 0x00AD | - | x | x | x | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA256 | 0x00AE | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA384 | 0x00AF | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_NULL\_SHA256 | 0x00B0 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_PSK\_WITH\_NULL\_SHA384 | 0x00B1 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_AES\_128\_CBC\_SHA256 | 0x00B2 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_AES\_256\_CBC\_SHA384 | 0x00B3 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_NULL\_SHA256 | 0x00B4 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_DHE\_PSK\_WITH\_NULL\_SHA384 | 0x00B5 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_AES\_128\_CBC\_SHA256 | 0x00B6 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_AES\_256\_CBC\_SHA384 | 0x00B7 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_NULL\_SHA256 | 0x00B8 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_PSK\_WITH\_NULL\_SHA384 | 0x00B9 | - | ? | n | n | n | RFC 5487 March 2009 [20](#_20._Pre-Shared_Key) | No |
|  | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256 | 0x00BA | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA256 | 0x00BB | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256 | 0x00BC | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA256 | 0x00BD | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256 | 0x00BE | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA256 | 0x00BF | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256 | 0x00C0 | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA256 | 0x00C1 | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256 | 0x00C2 | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA256 | 0x00C3 | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256 | 0x00C4 | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA256 | 0x00C5 | - | x | x | x | n | RFC 5932 June 2010 [23](#_23._Camellia_Cipher) | No |
|  | TLS\_RSA\_WITH\_HC\_128\_CBC\_MD5 | 0x00FB | - | ? | s | ? | ? | Unknown [28](#_28._CyaSSL_source) | No |
|  | TLS\_RSA\_WITH\_HC\_128\_CBC\_SHA | 0x00FC | - | ? | s | ? | ? | Unknown [28](#_28._CyaSSL_source) | No |
|  | TLS\_RSA\_WITH\_RABBIT\_CBC\_SHA | 0x00FD | - | ? | s | ? | ? | Unknown [28](#_28._CyaSSL_source) | No |
|  | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve)RFC 5430 March 2009 [18](#_18._Suite_B) | Yes |
|  | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve)RFC 5430 March 2009 [18](#_18._Suite_B) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | Yes |
|  | TLS\_ECDH\_anon\_WITH\_NULL\_SHA | 0xC015 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_anon\_WITH\_RC4\_128\_SHA | 0xC016 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC017 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0xC018 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_ECDH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0xC019 | - | s | n | n | n | RFC 4492 May 2006 [12](#_12._Elliptic_Curve) | No |
|  | TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01A | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01B | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01C | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0xC01D | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC01E | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0xC01F | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0xC020 | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC021 | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0xC022 | - | ? | n | n | n ? | RFC 5054 November 2007 [14](#_14._Using_the) | No |
|  | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC023 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic)RFC 5430 March 2009 [18](#_18._Suite_B) | Yes |
|  | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC024 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic)RFC 5430 March 2009 [18](#_18._Suite_B) | Yes |
|  | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC025 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC026 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC027 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC028 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC029 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC02A | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC02B | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic)RFC 5430 March 2009 [18](#_18._Suite_B) | Yes |
|  | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC02C | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic)RFC 5430 March 2009 [18](#_18._Suite_B) | Yes |
|  | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC02D | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC02E | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC02F | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC030 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC031 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC032 | - | x | x | x | n | RFC 5288 August 2008 [17](#_17._TLS_Elliptic) | Yes |
|  | TLS\_ECDHE\_PSK\_WITH\_RC4\_128\_SHA | 0xC033 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 227. | TLS\_ECDHE\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC034 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 228. | TLS\_ECDHE\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0xC035 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 229. | TLS\_ECDHE\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0xC036 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 230. | TLS\_ECDHE\_PSK\_WITH\_AES\_128\_CBC\_SHA256 | 0xC037 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 231. | TLS\_ECDHE\_PSK\_WITH\_AES\_256\_CBC\_SHA384 | 0xC038 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 232. | TLS\_ECDHE\_PSK\_WITH\_NULL\_SHA | 0xC039 | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 233. | TLS\_ECDHE\_PSK\_WITH\_NULL\_SHA256 | 0xC03A | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 234. | TLS\_ECDHE\_PSK\_WITH\_NULL\_SHA384 | 0xC03B | - | ? | n | n | n | RFC 5489 March 2009 [21](#_21._ECDHE_PSK_Cipher) | No |
| 235. | SSL\_RSA\_FIPS\_WITH\_DES\_CBC\_SHA | 0xFEFE(0xFFE1) | - | n | s | - | - | FIPS SSL CipherSuites [25](#_25._FIPS_SSL) | No |
| 236. | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF(0xFFE0) | - | n | s | - | - | FIPS SSL CipherSuites [25](#_25._FIPS_SSL) | No |
| 237. | TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV \*\* | 0x00FF | s | s | n | n | n | RFC 5746 February 2010 [22](#_22._Transport_Layer) | - |

\* Applicable only for TLS 1.0, TLS 1.1 and TLS 1.2
\*\* Not a cipher suite

### 2. Meaning

Table 2

|  |  |
| --- | --- |
| Value | Meaning |
| - | not applicable |
| s | not “native”, seen implemented |
| n | “native” cipher suite |
| c | special case possible usage |
| x | usage disallowed |
| depr | deprecated |
| disc | discouraged |
| ? | unknown status |

The situation of some ADH ciphers is a little ambiguous, for example TLS 1.0 RFC 2246 deprecates some ADH cipher suites.
But RFC 3268 adds AES ADH suites to TLS 1.0 which are not considered deprecated.
RFC 4132 adds (ADH) Camellia cipher suites to TLS 1.0, but makes no mention about the ADH ones.
Sames with RFC 4162 which adds SEED cipher suites to TLS 1.0.
TLS 1.1 RFC 4346 lists some ADH cipher suites as deprecated, however makes no mention about AES ADH ones, just lists them.
RFC 4492 adds ECC ADH cipher suites, but does not particularly make any reference about them.
TLS 1.2 RFC 5246 finally lists the AES ADH cipher along with the others, labeling the mode as “of limited use”, however the status of the ECC ADH ones is not clear(these are not listed in this RFC).
Furthermore, RFC 5288 adds some AES-GCM ADH cipher suites, but does not particularly make any reference about them.
Also RFC 5932 adds new Camellia ADH cipher suites(listing the “old” ones too), but does not particularly make any reference about them.
The Rabbit and CH-128 based cipher suites were not associated with any draft or RFC, such a document being not found, instead they were linked to CyaSSL source code file mentioning them.

### 3. Extra Cipher Suites

Apart from the cipher suites listed above, IANA’s Transport Layer Security (TLS) Parameters, section TLS Cipher Suite Registry, mentions some reserved values. Some of these values are already present in the above table. Possible other values can be seen bellow. Probably some suites numbers were not registered or have been modified, or are quite meaningless as writing.

Table 3, ECC Cipher Suites for TLS
draft-03 gives a hint that some values (47-4C) correspond to cipher suites which are known to have been implemented.
<http://tools.ietf.org/html/draft-ietf-tls-ecc-00#section-10>
<http://tools.ietf.org/html/draft-ietf-tls-ecc-01#section-5>
<http://tools.ietf.org/html/draft-ietf-tls-ecc-03>

|  |  |
| --- | --- |
| Cipher Suite | Hex Value |
| TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0x0047 |
| TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0x0048 |
| TLS\_ECDH\_ECDSA\_WITH\_DES\_CBC\_SHA | 0x0049 |
| TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x004A |
| TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0x004B |
| TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0x004C |
| TLS\_ECDH\_ECDSA\_EXPORT\_WITH\_RC4\_40\_SHA | 0x004B |
| TLS\_ECDH\_ECDSA\_EXPORT\_WITH\_RC4\_56\_SHA | 0x004C |
| TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0x004D |
| TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0x004E |
| TLS\_ECDH\_RSA\_WITH\_DES\_CBC\_SHA | 0x004F |
| TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0050 |
| TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0051 |
| TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0052 |
| TLS\_ECDH\_RSA\_EXPORT\_WITH\_RC4\_40\_SHA | 0x0053 |
| TLS\_ECDH\_RSA\_EXPORT\_WITH\_RC4\_56\_SHA | 0x0054 |
| TLS\_ECDH\_anon\_NULL\_WITH\_SHA | 0x0055 |
| TLS\_ECDH\_anon\_WITH\_RC4\_128\_SHA | 0x0056 |
| TLS\_ECDH\_anon\_WITH\_DES\_CBC\_SHA | 0x0057 |
| TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0058 |
| TLS\_ECDH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0059 |
| TLS\_ECDH\_anon\_EXPORT\_WITH\_RC4\_40\_SHA | 0x005A |
| TLS\_ECDH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x005B |
| TLS\_ECDH\_anon\_EXPORT\_WITH\_RC4\_40\_SHA | 0x005C |

Table 4, Using SRP for TLS Authentication
<http://tools.ietf.org/html/draft-ietf-tls-srp-02>

|  |  |
| --- | --- |
| Cipher Suite | Hex Value |
| TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0050 |
| TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0051 |
| TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0052 |
| TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0x0053 |
| TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0054 |
| TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0055 |
| TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0x0056 |
| TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0057 |
| LS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0058 |

Table 5, Addition of MISTY1 to TLS
<http://tools.ietf.org/id/draft-ietf-tls-misty1-01.txt>

|  |  |
| --- | --- |
| Cipher Suite | Hex Value |
| TLS\_RSA\_WITH\_MISTY1\_CBC\_SHA | 0x003B |
| TLS\_DH\_DSS\_WITH\_MISTY1\_CBC\_SHA | 0x003C |
| TLS\_DH\_RSA\_WITH\_MISTY1\_CBC\_SHA | 0x003D |
| TLS\_DHE\_DSS\_WITH\_MISTY1\_CBC\_SHA | 0x003E |
| TLS\_DHE\_RSA\_WITH\_MISTY1\_CBC\_SHA | 0x003F |
| TLS\_DH\_anon\_WITH\_MISTY1\_CBC\_SHA | 0x004A |

Table 5, TLS Extension for SEED and HAS-160
<http://tools.ietf.org/html/draft-ietf-tls-seedhas-00>

|  |  |
| --- | --- |
| Cipher Suite | Hex Value |
| TLS\_RSA\_WITH\_SEED\_CBC\_MD5 | 0x002C |
| TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x002D |
| TLS\_RSA\_WITH\_SEED\_CBC\_HAS160 | 0x002E |

Table 6, Kerberos Cipher Suites in Transport Layer Security (TLS)
<http://tools.ietf.org/html/draft-ietf-tls-kerb-01>

|  |  |
| --- | --- |
| Cipher Suite | Hex Value |
| TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0070 |
| TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_MD5 | 0x0071 |
| TLS\_KRB5\_WITH\_RC4\_128\_SHA | 0x0072 |
| TLS\_KRB5\_WITH\_RC4\_128\_MD5 | 0x0073 |
| TLS\_KRB5\_WITH\_DES\_CBC\_SHA | 0x0074 |
| TLS\_KRB5\_WITH\_DES\_CBC\_MD5 | 0x0075 |
| TLS\_KRB5\_WITH\_AES\_128\_CBC\_SHA | 0x0076 |
| TLS\_KRB5\_WITH\_AES\_256\_CBC\_SHA | 0x0077 |
| TLS\_KRB5\_WITH\_NULL\_SHA | 0x0078 |
| TLS\_KRB5\_WITH\_NULL\_MD5 | 0x0079 |

### 4. References

### 1. Draft, SSL 0.2 Protocol Specification<http://www.mozilla.org/projects/security/pki/nss/ssl/draft02.html>

### 2. draft-freier-ssl-version3-02.txt, The SSL Protocol Version 3.0<http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt>

### 3. The TLS Protocol Version 1.0<http://www.ietf.org/rfc/rfc2246.txt>

### 4. Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc2712.txt>

### 5. draft-ietf-tls-56-bit-ciphersuites-01.txt 56-bit, Export Cipher Suites For TLS<http://tools.ietf.org/html/draft-ietf-tls-56-bit-ciphersuites-01>

### 6. Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc3268.txt>

### 7. Addition of Camellia Cipher Suites to Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc4132.txt>

### 8. Addition of SEED Cipher Suites to Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc4162.txt>

### 9. Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc4279.txt>

### 10. The Transport Layer Security (TLS) Protocol Version 1.1<http://www.ietf.org/rfc/rfc4346.txt>

### 12. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc4492.txt>

### 13. Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc4785.txt>

### 14. Using the Secure Remote Password (SRP) Protocol for TLS Authentication<http://www.ietf.org/rfc/rfc5054.txt>

### 15. The Transport Layer Security (TLS) Protocol Version 1.2<http://www.ietf.org/rfc/rfc5246.txt>

### 16. AES Galois Counter Mode (GCM) Cipher Suites for TLS<http://www.ietf.org/rfc/rfc5288.txt>

### 17. TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)<http://www.ietf.org/rfc/rfc5289.txt>

### 18. Suite B Profile for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc5430.txt>

### 19. DES and IDEA Cipher Suites for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc5469.txt>

### 20. Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode<http://www.ietf.org/rfc/rfc5487.txt>

### 21. ECDHE\_PSK Cipher Suites for Transport Layer Security (TLS)<http://www.ietf.org/rfc/rfc5489.txt>

### 22. Transport Layer Security (TLS) Renegotiation Indication Extension<http://www.ietf.org/rfc/rfc5746.txt>

### 23. Camellia Cipher Suites for TLS<http://www.ietf.org/rfc/rfc5932.txt>

### 24. draft-chudov-cryptopro-cptls-04 GOST 28147-89 Cipher Suites for Transport Layer Security (TLS)<http://tools.ietf.org/html/draft-chudov-cryptopro-cptls-04>

### 25. FIPS SSL CipherSuites<http://www.mozilla.org/projects/security/pki/nss/ssl/fips-ssl-ciphersuites.html>

### 26. FIPS PUB 140-2<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf> <http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf> <http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf> <http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf> <http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf>

### 27. Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations

### <http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>

### 28. CyaSSL source code<https://github.com/cyassl/cyassl/blob/master/include/cyassl_int.h>

### 29. NTRU Cipher Suites for TLS

<http://tools.ietf.org/html/draft-ietf-tls-ntru-00>

### 30. Security Innovation CyaSSL+NTRU<http://securityinnovation.com/products/encryption/cyassl.shtml>

### 31. CyaSSL Extensions Reference<http://www.yassl.com/yaSSL/Docs_CyaSSL_Extensions_Reference.html>

### 5. Extra References

* Transport Layer Security (TLS) Parameters, <http://www.iana.org/assignments/tls-parameters/tls-parameters.xml>
* SSL/TLS Timeline, <http://www.carbonwind.net/blog/post/A-quickie-for-a-Friday-e28093-a-SSLTLS-timeline.aspx>
* SSL & TLS Specifications, <http://www7b.biglobe.ne.jp/~k-west/SSLandTLS/index-e.html>