Appendix C. Cipher Suite Definitions

Cipher Suite Key Cipher Mac Exchange

TLS_NULL_WITH_NULL_NULL NULL NULL NULL TLS_RSA_WITH_NULL_MD5 RSA NULL MD5 TLS_RSA_WITH_NULL_SHA RSA NULL SHA TLS_RSA_WITH_NULL_SHA256 RSA NULL SHA256 TLS_RSA_WITH_RC4_128_MD5 RSA RC4_128 MD5 TLS_RSA_WITH_RC4_128_SHA RSA RC4_128 SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA RSA 3DES_EDE_CBC SHA TLS_RSA_WITH_AES_128_CBC_SHA RSA AES_128_CBC SHA TLS_RSA_WITH_AES_256_CBC_SHA RSA AES_256_CBC SHA TLS_RSA_WITH_AES_128_CBC_SHA256 RSA AES_128_CBC SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 RSA AES_256_CBC SHA256 TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA DH_DSS 3DES_EDE_CBC SHA TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA DH_RSA 3DES_EDE_CBC SHA TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA DHE_DSS 3DES_EDE_CBC SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA DHE_RSA 3DES_EDE_CBC SHA TLS_DH_anon_WITH_RC4_128_MD5 DH_anon RC4_128 MD5 TLS_DH_anon_WITH_3DES_EDE_CBC_SHA DH_anon 3DES_EDE_CBC SHA TLS_DH_DSS_WITH_AES_128_CBC_SHA DH_DSS AES_128_CBC SHA TLS_DH_RSA_WITH_AES_128_CBC_SHA DH_RSA AES_128_CBC SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA DHE_DSS AES_128_CBC SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA DHE_RSA AES_128_CBC SHA TLS_DH_anon_WITH_AES_128_CBC_SHA DH_anon AES_128_CBC SHA TLS_DH_DSS_WITH_AES_256_CBC_SHA DH_DSS AES_256_CBC SHA TLS_DH_RSA_WITH_AES_256_CBC_SHA DH_RSA AES_256_CBC SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA DHE_DSS AES_256_CBC SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA DHE_RSA AES_256_CBC SHA TLS_DH_anon_WITH_AES_256_CBC_SHA DH_anon AES_256_CBC SHA TLS_DH_DSS_WITH_AES_128_CBC_SHA256 DH_DSS AES_128_CBC SHA256 TLS_DH_RSA_WITH_AES_128_CBC_SHA256 DH_RSA AES_128_CBC SHA256 TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 DHE_DSS AES_128_CBC SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 DHE_RSA AES_128_CBC SHA256 TLS_DH_anon_WITH_AES_128_CBC_SHA256 DH_anon AES_128_CBC SHA256 TLS_DH_DSS_WITH_AES_256_CBC_SHA256 DH_DSS AES_256_CBC SHA256 TLS_DH_RSA_WITH_AES_256_CBC_SHA256 DH_RSA AES_256_CBC SHA256 TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 DHE_DSS AES_256_CBC SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 DHE_RSA AES_256_CBC SHA256 TLS_DH_anon_WITH_AES_256_CBC_SHA256 DH_anon AES_256_CBC SHA256

```
Key      IV   Block
```

Cipher	Type	Material	Size	Size
NULL	Stream	0	0	N/A
RC4_128	Stream	16	0	N/A
3DES_EDE_CBC	Block	24	8	8
AES_128_CBC	Block	16	16	16
AES_256_CBC	Block	32	16	16

MAC	Algorithm	mac_length	mac_key_length
NULL	N/A	0	0
MD5	HMAC-MD5	16	16
SHA	HMAC-SHA1	20	20
SHA256	HMAC-SHA256	32	32

Type Indicates whether this is a stream cipher or a block cipher running in CBC mode.

Key Material The number of bytes from the key_block that are used for generating the write keys.

IV Size The amount of data needed to be generated for the initialization vector. Zero for stream ciphers; equal to the block size for block ciphers (this is equal to SecurityParameters.record_iv_length).

Block Size The amount of data a block cipher enciphers in one chunk; a block cipher running in CBC mode can only encrypt an even multiple of its block size.