Appendix I
Algorithm Identifier List

Lo Kam Tao Leo
leolo@leolo.org

2nd July 2018

Contents

1 Preface

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

2 Hash algorithm

Identifier	Algorithm name	Remarks
0x0000 - 0x2fff	*Unallocated*	
0x3000	MD2	
0x3001	MD4	
0x3002	MD5	
0x3003 - 0x5000	*Unallocated*	
0x5001	SHA1	
0x5002	SHA224	
0x5003	SHA256	
0x5004	SHA384	
0x5005	SHA512	
0x5005 - 0x500f	*Unallocated*	
0x5010	SHA3-224	
0x5011	SHA3-256	
0x5012	SHA3-384	
0x5013	SHA3-512	
0x5013	SHAKE128, 128bit output	
0x5014	SHAKE128, 64bit output	
0x5015	SHAKE128, 192bit output	
0x5016	SHAKE128, 256bit output	
0x5017	SHAKE256, 256bit output	
0x5018	SHAKE256, 128bit output	
0x5019	SHAKE256, 384bit output	
0x501a	SHAKE256, 512bit output	
0x501b - 0xc000	*Unallocated*	

Identifier	Algorithm name	Remarks
0xc001	CRC32	
0xc002	CRC64	
0xc003 - 0xfdff	*Unallocated*	
0xfe00 - 0xfeff	Implementation specific algorithm	[1]
0xff00 - 0xffff	Reserved for future expansion	

1. Implementations SHOULD use this block of identifiers for algorithm that does not have any identifier allocated to it.

3 Encryption algorithm

Identifier	Cipher Type	Algorithm name	Remarks
0x0000 - 0x4fff		*Unallocated*	
0x5000	BLOCK	Null cipher	[1]
0x5001	STREAM	Null cipher	[1]
0x5002 - 0xae3f		*Unallocated*	
0xae40 - 0xae6f	BLOCK	*Reserved for AES family*	
0xae60 - 0xde4f		*Unallocated*	
0xde50	BLOCK	DES, CBC mode, 56bit key	[3]
0xde51	BLOCK	3DES, CBC mode, key option 1, 168bit key	[3]
0xde52	BLOCK	DES, CBC mode 56bit key with gzip	[3][4]
0xde53	BLOCK	3DES, CBC mode, key option 1, 168bit key with gzip	[3][4]
0xde54	BLOCK	DES, ECB mode, 56bit key	[3]
0xde55	BLOCK	3DES, ECB mode, key option 1, 168bit key	[3]
0xde56	BLOCK	DES, ECB mode 56bit key with gzip	[3][4]
0xde57	BLOCK	3DES, ECB mode, key option 1, 168bit key with gzip	[3][4]
0xde58 - 0xfdff		*Unallocated*	
0xfe00 - 0xfeff		Implementation specific algorithm	[2]
0xff00 - 0xffff		Reserved for future expansion	

1. Null cipher is not recommended to be used as it does not actually encrypt the data. Implementation SHOULD provide warning for using these cipher.

2. Implementations SHOULD use this block of identifiers for algorithm that does not have any identifier allocated to it.

3. Weak cipher, not recommended to be used.

4. The payload is compressed first, then encrypt

3.1 List of encryption mode for block cipher[Wik18]

The list here was retrieved from Wikipedia (CC BY-SA 3.0 licensed) at https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Abbreviation	Name
ECB	Electronic Code Book
CBC	Cipher Block Chaining
PCBC	Propagating Cipher Block Chaining
CFB	Cipher Feedback
OFB	Output Feedback
CTR	Counter

4 Key derivation algorithm

Identifier	Algorithm name	Remarks
`0x0000 - 0xfdff`	*Unallocated*	
`0xfe00 - 0xfeff`	Implementation specific algorithm	[1]
`0xff00 - 0xffff`	Reserved for future expansion	

1. Implementations SHOULD use this block of identifiers for algorithm that does not have any identifier allocated to it.

References

[Wik18] Wikipedia contributors. Block cipher mode of operation — Wikipedia, the free encyclopedia, 2018. [Online; accessed 1-July-2018].