

# Contents

<b>1</b>	<b>Preface</b>	<b>1</b>
<b>2</b>	<b>Hash algorithm</b>	<b>1</b>
<b>3</b>	<b>Encryption algorithm</b>	<b>2</b>
<b>4</b>	<b>Key derivation algorithm</b>	<b>2</b>

Copyright (c) 2018, LO Kam Tao Leo All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 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
0000 - fdff	<i>Unallocated</i>	
fe00 - feff	Implementation specific algorithm	[1]
ff00 - ffff	Reserved for future expansion	

1. Implementations MAY 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
0000 - 4fff		<i>Unallocated</i>	
5000	BLOCK	Null cipher	[1]
5001	STREAM	Null cipher	[1]
5002 - fdff		<i>Unallocated</i>	
fe00 - frff		Implementation specific algorithm	[2]
ff00 - ffff		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 MAY use this block of identifiers for algorithm that does not have any identifier allocated to it.

## 4 Key derivation algorithm

Identifier	Algorithm name	Remarks
0000 - fdff	<i>Unallocated</i>	
fe00 - feff	Implementation specific algorithm	[1]
ff00 - ffff	Reserved for future expansion	

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