

# ISO/IEC 10118-1:2016-10 (E)

## Information technology - Security techniques - Hash-functions - Part 1: General

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Symbols and abbreviated terms .....</b>	<b>2</b>
<b>4.1</b>	<b>General symbols .....</b>	<b>2</b>
<b>4.2</b>	<b>Symbols specific to this document .....</b>	<b>3</b>
<b>4.3</b>	<b>Coding conventions .....</b>	<b>3</b>
<b>5</b>	<b>Requirements .....</b>	<b>3</b>
<b>6</b>	<b>General model for hash-functions .....</b>	<b>3</b>
<b>6.1</b>	<b>General .....</b>	<b>3</b>
<b>6.2</b>	<b>Hashing operation .....</b>	<b>4</b>
<b>6.2.1</b>	<b>General .....</b>	<b>4</b>
<b>6.2.2</b>	<b>Step 1 (padding) .....</b>	<b>4</b>
<b>6.2.3</b>	<b>Step 2 (splitting) .....</b>	<b>4</b>
<b>6.2.4</b>	<b>Step 3 (iteration) .....</b>	<b>4</b>
<b>6.2.5</b>	<b>Step 4 (output transformation) .....</b>	<b>4</b>
<b>6.3</b>	<b>Use of the general model .....</b>	<b>5</b>
<b>Annex A (normative)</b>	<b>Padding methods .....</b>	<b>6</b>
<b>Annex B (normative)</b>	<b>Criteria for submission of hash-functions for possible inclusion in Annex C</b>	
	<b>(informative) Security considerations .....</b>	<b>10</b>
<b>Bibliography .....</b>		<b>12</b>