

# ISO/IEC 18033-1:2015-08 (E)

## Information technology - Security techniques - Encryption algorithms - Part 1: General

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>3</b>	<b>Symbols and abbreviated terms .....</b>	<b>5</b>
<b>3.1</b>	<b>Symbols .....</b>	<b>5</b>
<b>3.2</b>	<b>Abbreviated terms .....</b>	<b>5</b>
<b>4</b>	<b>The nature of encryption .....</b>	<b>5</b>
<b>4.1</b>	<b>The purpose of encryption .....</b>	<b>5</b>
<b>4.2</b>	<b>Symmetric and asymmetric ciphers .....</b>	<b>6</b>
<b>4.3</b>	<b>Key management .....</b>	<b>6</b>
<b>5</b>	<b>The use and properties of encryption .....</b>	<b>6</b>
<b>5.1</b>	<b>Asymmetric ciphers .....</b>	<b>6</b>
<b>5.2</b>	<b>Block ciphers .....</b>	<b>7</b>
<b>5.2.1</b>	<b>General .....</b>	<b>7</b>
<b>5.2.2</b>	<b>Modes of operation .....</b>	<b>7</b>
<b>5.2.3</b>	<b>Message Authentication Codes (MACs) .....</b>	<b>7</b>
<b>5.3</b>	<b>Stream ciphers .....</b>	<b>7</b>
<b>5.4</b>	<b>Identity-based mechanisms .....</b>	<b>8</b>
<b>6</b>	<b>Object identifiers .....</b>	<b>8</b>
<b>Annex A (normative)</b>	<b>Criteria for submission of ciphers for possible inclusion in this International Standard .....</b>	<b>9</b>
<b>Annex B (normative)</b>	<b>Criteria for the deletion of ciphers from this International Standard .....</b>	<b>13</b>
<b>Annex C (informative)</b>	<b>Attacks on encryption algorithms .....</b>	<b>14</b>
<b>Bibliography .....</b>		<b>16</b>