

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

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

---

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