

# ISO/IEC 18033-1:2021-09 (E)

## Information security - 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>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>5</b>
<b>5</b>	<b>Nature of encryption .....</b>	<b>5</b>
5.1	Purpose of encryption .....	5
5.2	Symmetric and asymmetric encryption systems .....	6
5.3	Key management .....	6
<b>6</b>	<b>Use and properties of encryption .....</b>	<b>6</b>
6.1	General .....	6
6.2	Asymmetric encryption systems .....	7
6.3	Block ciphers .....	7
6.3.1	General .....	7
6.3.2	Modes of operation .....	7
6.3.3	Message authentication codes (MACs) .....	7
6.4	Stream ciphers .....	8
6.5	Identity-based encryption systems .....	8
6.6	Homomorphic encryption systems .....	8
<b>7</b>	<b>Object identifiers .....</b>	<b>8</b>
<b>Annex A (informative)</b>	<b>Criteria for submission of encryption systems for possible inclusion Annex</b>	
<b>B (informative)</b>	<b>Criteria for the deletion of encryption systems from Annex C</b>	
<b>(informative)</b>	<b>Attacks on encryption algorithms .....</b>	<b>15</b>
<b>Bibliography .....</b>		<b>18</b>