

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

## Information security - Encryption algorithms - Part 1: General

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols and abbreviated terms .....	5
5	Nature of encryption .....	5
5.1	Purpose of encryption .....	5
5.2	Symmetric and asymmetric encryption systems .....	6
5.3	Key management .....	6
6	Use and properties of encryption .....	6
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
7	Object identifiers .....	8
Annex A (informative)	Criteria for submission of encryption systems for possible inclusion Annex B (informative) Criteria for the deletion of encryption systems from Annex C (informative) Attacks on encryption algorithms .....	15
Bibliography .....		18