

ISO/IEC 18033-1:2005-02 (E)

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

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Terms and definitions	1
3	The nature of encryption	4
3.1	The purpose of encryption	4
3.2	Symmetric and asymmetric ciphers	4
3.3	Key management	5
4	The use and properties of encryption	5
4.1	Asymmetric ciphers	5
4.2	Block ciphers	5
4.2.1	Modes of operation	5
4.2.2	Message Authentication Codes (MACs)	6
4.3	Stream ciphers	6
5	Object identifiers	6
Bibliography		8