

ISO/IEC 18033-2:2006-05 (E)

Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers

Contents	Page
1	Scope 1
2	Normative references 1
3	Definitions 2
4	Symbols and notation 7
5	Mathematical conventions 8
5.1	Functions and algorithms 8
5.2	Bit strings and octet strings 9
5.3	Finite Fields 10
5.4	Elliptic curves 12
6	 14
6.1	Cryptographic hash functions 14
6.2	Key derivation functions 15
6.3	MAC algorithms 16
6.4	Block ciphers 16
6.5	Symmetric ciphers 17
7	Asymmetric ciphers 19
7.1	Plaintext length 20
7.2	The use of labels 21
7.3	Ciphertext format 21
7.4	Encryption options 21
7.5	Method of operation of an asymmetric cipher 22
7.6	Allowable asymmetric ciphers 22
8	Generic hybrid ciphers 22
8.1	Key encapsulation mechanisms 23
8.2	Data encapsulation mechanisms 24
8.3	HC 25
9	Constructions of data encapsulation mechanisms 26
9.1	DEM1 26
9.2	DEM2 27
9.3	DEM3 28
10	ElGamal-based key encapsulation mechanisms 30
10.1	Concrete groups 30
10.2	ECIES-KEM 32
10.3	PSEC-KEM 34
10.4	ACE-KEM 36
11	RSA-based asymmetric ciphers and key encapsulation mechanisms 39
11.1	RSA key generation algorithms 39
11.2	RSA Transform 40
11.3	RSA encoding mechanisms 40
11.4	RSAs 42
11.5	RSA-KEM 44

12	Ciphers based on modular squaring	45
Cryptographic transformations 12.1 HIME key generation algorithms		45
12.2	HIME encoding mechanisms	46
12.3	HIME(R)	48
Annex A (normative) ASN.1 syntax for object identifiers		51
Annex B (informative) Security considerations		61
B.1	MAC algorithms	61
B.2	Block ciphers	62
B.3	Symmetric ciphers	62
B.4	Asymmetric ciphers	63
B.5	Key encapsulation mechanisms	65
B.6	Data encapsulation mechanisms	66
B.7	Security of HC	68
B.8	Intractability assumptions related to concrete groups	68
B.9	Security of ECIES-KEM	69
B.10	Security of PSEC-KEM	71
B.11	Security of ACE-KEM	71
B.12	The RSA inversion problem	72
B.13	Security of RSAES	73
B.14	Security of RSA-KEM	73
B.15	Security of HIME(R)	74
Annex C (informative) Test vectors		75
C.1	Test vectors for DEM1	75
C.2	Test vectors for ECIES-KEM	76
C.3	Test vectors for PSEC-KEM	83
C.4	Test vectors for ACE-KEM	91
C.5	Test vectors for RSAES	100
C.6	Test vectors for RSA-KEM	105
C.7	Test vectors for HC	109
C.8	Test vectors for HIME(R)	112
Bibliography		123