

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

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

---

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

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