

# ISO/IEC 18033-3 :2005-07 (E)

Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers

---

## Contents

	Page
Foreword .....	v
Introduction.....	vi
<b>1 Scope .....</b>	<b>1</b>
<b>2 Terms and definitions .....</b>	<b>1</b>
<b>3 Symbols.....</b>	<b>2</b>
<b>4 64-bit block ciphers.....</b>	<b>2</b>
<b>4.1 TDEA.....</b>	<b>3</b>
4.1.1 TDEA encryption/decryption.....	3
4.1.2 TDEA keying options .....	3
<b>4.2 MISTY1.....</b>	<b>3</b>
4.2.1 MISTY1 encryption .....	3
4.2.2 MISTY1 decryption .....	4
4.2.3 MISTY1 functions .....	4
4.2.4 MISTY1 key schedule .....	9
<b>4.3 CAST-128.....</b>	<b>10</b>
4.3.1 CAST-128 encryption .....	10
4.3.2 CAST-128 decryption .....	10
4.3.3 CAST-128 functions .....	10
4.3.4 CAST-128 key schedule .....	17
<b>5 128-bit block ciphers.....</b>	<b>20</b>
<b>5.1 AES.....</b>	<b>20</b>
5.1.1 AES encryption.....	20
5.1.2 AES decryption.....	21
5.1.3 AES transformations.....	21
5.1.4 AES key schedule.....	26
<b>5.2 Camellia.....</b>	<b>27</b>
5.2.1 Camellia encryption .....	27
5.2.2 Camellia decryption .....	29
5.2.3 Camellia functions.....	32
5.2.4 Camellia key schedule .....	38
<b>5.3 SEED.....</b>	<b>42</b>
5.3.1 SEED encryption .....	42
5.3.2 SEED decryption .....	42
5.3.3 SEED functions.....	43
5.3.4 SEED key schedule .....	46
<b>Annex A (normative) Description of DES.....</b>	<b>47</b>
<b>A.1. DES encryption.....</b>	<b>47</b>
<b>A.2. DES decryption.....</b>	<b>47</b>
<b>A.3. DES functions .....</b>	<b>47</b>
A.3.1 Initial permutation $IP$ .....	47
A.3.2 Inverse initial permutation $IP^{-1}$ .....	48
A.3.3 Function $f$ .....	49
A.3.4 Expansion permutation $E$ .....	49
A.3.5 Permutation $P$ .....	50
A.3.6 S-Boxes .....	50
<b>A.4. DES key schedule (KS).....</b>	<b>51</b>
<b>Annex B (normative) ASN.1 module .....</b>	<b>53</b>
<b>Annex C (informative) Algebraic forms of MISTY1 and Camellia S-boxes .....</b>	<b>55</b>
<b>C.1 MISTY1 S-boxes.....</b>	<b>55</b>

- C.1.1 MISTY1 S-box  $S_7$  ..... 55**
- C.1.2 MISTY1 S-box  $S_9$  ..... 55**
- C.2 Camellia S-box ..... 55**
- Annex D (informative) Test vectors ..... 57**
- D.1 TDEA test vectors ..... 57**
- D.1.1 TDEA encryption ..... 57**
- D.1.2 DES encryption and decryption ..... 58**
- D.2 MISTY1 test vectors ..... 59**
- D.3 CAST-128 test vectors ..... 60**
- D.4 AES test vectors ..... 60**
- D.4.1 AES encryption ..... 60**
- D.4.2 Key expansion example ..... 61**
- D.4.3 Cipher example ..... 63**
- D.5 Camellia test vectors ..... 65**
- D.5.1 Camellia encryption ..... 65**
- D.6 SEED test vectors ..... 68**
- Annex E (informative) Feature table ..... 70**
- Bibliography ..... 71**