ISO/IEC 18033-3:2010-12 (E)

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

Contents

Page

Foreword v

1 Scope 1

2 Terms and definitions 1

3 Symbols 2

4 64-bit block ciphers 3
4.1 Introduction 3
4.2 TDEA 3
4.2.1 The Triple Data Encryption Algorithm 3
4.2.2 TDEA encryption/decryption 3
4.2.3 TDEA keying options 4
4.3 MISTY1 4
4.3.1 The MISTY1 algorithm 4
4.3.2 MISTY1 encryption 4
4.3.3 MISTY1 decryption 5
4.3.4 MISTY1 functions 5
4.3.5 MISTY1 key schedule 10
4.4 CAST-128 11
4.4.1 The CAST-128 algorithm 11
4.4.2 CAST-128 encryption 11
4.4.3 CAST-128 decryption 11
4.4.4 CAST-128 functions 11
4.4.5 CAST-128 key schedule 18
4.5 HIGHT 20
4.5.1 The HIGHT algorithm 20
4.5.2 HIGHT encryption 21
4.5.3 HIGHT decryption 22
4.5.4 HIGHT functions 23
4.5.5 HIGHT key schedule 23

5 128-bit block ciphers 24
5.1 Introduction 24
5.2 AES 24
5.2.1 The AES algorithm 24
5.2.2 AES encryption 24
5.2.3 AES decryption 25
5.2.4 AES transformations 26
5.2.5 AES key schedule 30
5.3 Camellia 32
5.3.1 The Camellia algorithm 32
5.3.2 Camellia encryption 32
5.3.3 Camellia decryption 34
5.3.4 Camellia functions 37
5.3.5 Camellia key schedule 43
5.4 SEED 47
5.4.1 The SEED algorithm 47
5.4.2 SEED encryption 47
5.4.3 SEED decryption 47

5.4.4 SEED functions 48
5.4.5 SEED key schedule 50

Annex A (normative) Description of DES 52

A.1 Introduction 52
A.2 DES encryption 52
A.3 DES decryption 52
A.4 DES functions 52
A.4.1 Initial permutation IP 52
A.4.2 Inverse initial permutation IP-1 54
A.4.3 Function f 54
A.4.4 Expansion permutation E 55
A.4.5 Permutation P 55
A.4.6 S-Boxes 56
A.5 DES key schedule 57

Annex B (normative) Object identifiers 60

Annex C (informative) Algebraic forms of MISTY1 and Camellia S-boxes 62

C.1 Introduction 62
C.2 MISTY1 S-boxes 62
C.2.1 The S-boxes S7 and S9 62
C.2.2 MISTY1 S-box S7 62
C.2.3 MISTY1 S-box S9 62
C.3 Camellia S-boxes 63

Annex D (informative) Test vectors 64

D.1 Introduction 64
D.2 TDEA test vectors 64
D.2.1 TDEA encryption 64
D.2.2 DES encryption and decryption 65
D.3 MISTY1 test vectors 66
D.4 CAST-128 test vectors 67
D.5 HIGHT test vectors 67
D.6 AES test vectors 67
D.6.1 AES encryption 67
D.6.2 Key expansion example 68
D.6.3 Cipher example 70
D.7 Camellia test vectors 73
D.7.1 Introduction 73
D.7.2 Camellia encryption 73
D.8 SEED test vectors 75

Annex E (informative) Feature table 77

Bibliography 78