# ISO/IEC 10116:2006-02 (E)

## Information technology - Security techniques - Modes of operation for an n-bit block cipher

## Contents

Page


Foreword ..... vii

1 Scope ..... 1

2 Normative references ..... 1

3 Terms and definitions ..... 2

4 Symbols (and abbreviated terms) ..... 3

5 Requirements ..... 5

6 Electronic Codebook (ECB) mode ..... 6
6.1 Preliminaries ..... 6
6.2 Encryption ..... 6
6.3 Decryption ..... 6

7 Cipher Block Chaining (CBC) mode ..... 6
7.1 Preliminaries ..... 6
7.2 Encryption ..... 7
7.3 Decryption ..... 7

8 Cipher Feedback (CFB) mode ..... 8
8.1 Preliminaries ..... 8
8.2 Encryption ..... 8
8.3 Decryption ..... 9

9 Output Feedback (OFB) mode ..... 10
9.1 Preliminaries ..... 10
9.2 Encryption ..... 10
9.3 Decryption ..... 11

10 Counter (CTR) mode ..... 11
10.1 Preliminaries ..... 11
10.2 Encryption ..... 12
10.3 Decryption ..... 12

Annex A (normative) Object identifiers ..... 14

Annex B (informative) Properties of the modes of operation ..... 16

B.1 Properties of the Electronic Codebook (ECB) mode of operation ..... 16
B.2 Properties of the Cipher Block Chaining (CBC) mode of operation ..... 17
B.3 Properties of the Cipher Feedback (CFB) mode of operation ..... 18
B.4 Properties of the Output Feedback (OFB) mode of operation ..... 20
B.5 Properties of the Counter (CTR) mode of operation ..... 21

Annex C (informative) Figures describing the modes of operation ..... 23

Annex D (informative) Examples for the Modes of Operation ..... 26

D.1 General ..... 26
D.2 Triple Data Encryption Algorithm ..... 26
D.2.1 ECB Mode ..... 27
D.2.2 CBC Mode ..... 29
D.2.3 CFB Mode ..... 31
D.2.4 OFB Mode ..... 34
D.2.5 Counter Mode ..... 35
D.3 Advanced Encryption Standard ..... 36
D.3.1 ECB Mode ..... 36
D.3.2 CBC Mode ..... 37
D.3.3 CFB Mode ..... 38
D.3.4 OFB Mode ..... 39
D.3.5 Counter Mode ..... 40

Bibliography ..... 41

Figures C.1 The Cipher Block Chaining (CBC) mode of operation with m = 1 ..... 23

C.2 The Cipher Block Chaining (CBC) mode of operation ..... 23
C.3 The Cipher Feedback (CFB) mode of operation ..... 24
C.4 The Output Feedback (OFB) mode of operation ..... 24
C.5 The Counter (CTR) mode of operation ..... 25