

# ISO/IEC 10116:2017-07 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols, abbreviated terms and notation .....	3
4.1	Symbols and abbreviated terms .....	3
4.2	Notation .....	4
5	Requirements .....	4
6	Electronic Codebook (ECB) mode .....	5
6.1	Preliminaries .....	5
6.2	Encryption .....	5
6.3	Decryption .....	5
7	Cipher Block Chaining (CBC) mode .....	6
7.1	Preliminaries .....	6
7.2	Encryption .....	6
7.3	Decryption .....	6
7.4	Avoiding ciphertext expansion .....	7
7.4.1	General .....	7
7.4.2	Three ciphertext stealing variants of CBC .....	7
8	Cipher Feedback (CFB) mode .....	8
8.1	Preliminaries .....	8
8.2	Encryption .....	9
8.3	Decryption .....	10
8.4	Avoiding ciphertext expansion .....	10
9	Output Feedback (OFB) mode .....	11
9.1	Preliminaries .....	11
9.2	Encryption .....	11
9.3	Decryption .....	12
9.4	Avoiding ciphertext expansion .....	12
10	Counter (CTR) mode .....	13
10.1	Preliminaries .....	13
10.2	Encryption .....	13
10.3	Decryption .....	14
10.4	Avoiding ciphertext expansion .....	14
Annex A (normative)	Object identifiers .....	15
Annex B (informative)	Properties of the modes of operation and important security guidance .....	17

<b>Annex C (informative) Figures describing the modes of operation .....</b>	<b>22</b>
<b>Annex D (informative) Numerical examples for the modes of operation .....</b>	<b>27</b>
<b>Bibliography .....</b>	<b>39</b>