

# ISO 20215:2015-08 (E)

## Space data and information transfer systems - CCSDS cryptographic algorithms

---

<b>Contents</b>	<b>Page</b>
<b>1 INTRODUCTION.....</b>	<b>1-1</b>
1.1 PURPOSE OF THIS RECOMMENDED STANDARD .....	1-1
1.2 SCOPE.....	1-1
1.3 APPLICABILITY.....	1-2
1.4 RATIONALE.....	1-2
1.5 DOCUMENT STRUCTURE .....	1-2
1.6 NOMENCLATURE .....	1-2
1.7 REFERENCES .....	1-3
<b>2 OVERVIEW .....</b>	<b>2-1</b>
2.1 GENERAL OVERVIEW.....	2-1
2.2 ENCRYPTION OVERVIEW .....	2-1
2.3 AUTHENTICATION/INTEGRITY OVERVIEW .....	2-2
2.4 AUTHENTICATED ENCRYPTION.....	2-3
<b>3 ENCRYPTION ALGORITHMS.....</b>	<b>3-1</b>
3.1 ALGORITHM AND MODE.....	3-1
3.2 CRYPTOGRAPHIC KEY SIZE .....	3-1
3.3 ALGORITHM MODE OF OPERATION.....	3-1
3.4 AUTHENTICATED ENCRYPTION.....	3-1
<b>4 AUTHENTICATION ALGORITHMS .....</b>	<b>4-1</b>
4.1 OVERVIEW .....	4-1
4.2 CCSDS HASH MESSAGE BASED AUTHENTICATION .....	4-1
4.3 CIPHER-BASED AUTHENTICATION.....	4-2
4.4 DIGITAL SIGNATURE BASED AUTHENTICATION .....	4-2
<b>ANNEX A SECURITY, SANA, AND PATENT CONSIDERATIONS (INFORMATIVE) .....</b>	<b>A-1</b>
<b>ANNEX B INFORMATIVE REFERENCES (INFORMATIVE) .....</b>	<b>B-1</b>
<b>ANNEX C ABBREVIATIONS AND ACRONYMS (INFORMATIVE).....</b>	<b>C-1</b>