CCSDS Standardization of Security Algorithms for Civil Space Missions

Howard Weiss[1]
SPARTA, Inc. (a Parsons Company), Columbia, MD, 21046, USA

The Consultative Committee for Space Data Systems (CCSDS) Security Working Group has published several security guidelines for use within CCSDS. Recognizing the need to establish algorithmic standards, the working group set out to determine the need for cryptographic and authentication algorithms for the civil space community. Tradeoff analyses were performed to determine optimal algorithms for use with both space and ground infrastructures. As a result of those tradeoff analyses, the working group has made recommendations for the use of both cryptographic and authentication algorithms which will be published as a CCSDS Recommendation Blue Book. In this manner, all national space agencies compliant with the CCSDS recommendation can potentially interoperate with each other and can take advantage of cost savings through the use of international standards. Within CCSDS, the standardized algorithms will also form the basis of further security standards such as space data link, network layer, and application layer security. For confidentiality, a single algorithm (AES) using counter mode has been selected because of its ability to be efficiently implemented in hardware. However, authenticated encryption is highly encouraged for all missions using AES in Galois/Counter Mode (AES/GCM). For authentication, multiple algorithms have been selected to allow mission planners the ability to use shared-secret message authentication codes (MACs), cryptographic MACs, or digital signatures – depending on their individual mission's needs and profiles. For shared-secret MAC, HMAC has been specified. For cryptographic MACs, CMAC is the standard. And for digital signature, RSA Digital Signature has been specified.

I. Introduction

Historically, security has not been high on the list of worries for planners and mission architects of civil space missions. They were most interested in designing, building, flying, and obtaining data from their spacecraft. Most of these spacecraft are of a scientific nature and the general mindset was that there was little or no threat to these types of missions - unlike the high threat that is more typical of military missions. But with time and increased global network connectivity, the threat against civil space missions has grown immensely. National policy makers, national space agencies, and mission planners are now keenly aware of, and concerned with overall civil mission security. These concerns include ground system security, command security/authentication, and downlink privacy/confidentiality.

In response to the growing threat, the Consultative Committee for Space Data Systems (CCSDS) chartered the Security Working Group (SecWG) under its Systems Engineering Area (SEA) directorate. The SecWG is made up of members from various national space agencies (e.g., NASA, ESA, UK Space Agency, DLR, CNES, ASI) and is responsible for writing CCSDS security guidance documents, CCSDS security recommendations (standards), and providing advice and guidance to other CCSDS working groups. As a direct result of SecWG actions, all CCSDS standards documents must include a mandatory security section to ensure that the working group developing the standard has paid close attention to security.

This paper will discuss the development of the CCSDS algorithm standards[1], the algorithms chosen, what they are used for, and future work planned within the CCSDS Security Working Group.

[1] Technical Director; Argotek Operation; SPARTA, Inc (a Parsons Company); 7110 Samuel Morse Drive, Columbia, MD 20146 USA.

II. General Overview

Given that there is a heightened threat of attack against all types of electronic systems, space and ground systems are not immune. While in many cases sophisticated equipment, large amounts of power, and large antennas are required to mount an attack to compromise a spacecraft, the cost of such equipment has been drastically reduced making such attacks more viable. While deep-space missions still require the use of a 70 meter dish, low earth orbit spacecraft (making up the bulk of the potential targets) can be reached with much smaller dishes (e.g., 12 meter or smaller) with relatively low power levels. For more information regarding threats against civil space missions, consult the CCSDS Green Book, written by the Security Working Group, entitled *Security Threats against Space Systems*.[13]

As a result, it is in the best interests of all mission planners to ensure that spacecraft and associated ground systems are protected against attack and the data transmitted from space-to-ground and ground-to-space is protected.

The CCSDS algorithm standardization effort is a result of the increasing interconnection of ground networks; the movement towards *joy-sticking* of instruments by principal investigators; the decreasing costs for hardware potentially allowing cheap *rogue* ground stations to be established; and national trends towards enhancing mission security. The recommended algorithms establish a set of common denominators among all missions for implementing information security services.

Commands and software uploaded to a spacecraft must be authenticated to ensure that they are sent by only those individuals or control centers that are authorized to send software or commands. It must be assured that the software and commands received are exactly the same as was sent, with no (intentional or un-intentional) errors which, if not discovered, could result in a mission catastrophe. There may also be times when software and commands sent to the spacecraft require confidentiality as well as authentication to ensure increased security.

Likewise, engineering and scientific data sent by a spacecraft to the ground must be protected by confidentiality to ensure privacy. For example, an earth observing satellite whose data is to be analyzed by contracted principal investigators should be the only ones to have access to the data until it has been publically released. There may also be times that the downlink data also requires authentication/integrity to ensure its authenticity (that no one is trying to spoof the ground system) and its correctness.

A. Cryptography Overview

Confidentiality is defined as the *assurance that information is not disclosed to unauthorized entities or processes*. In other words, those who are not authorized are prevented from obtaining the information. Confidentiality can be accomplished by various mechanisms such as physical locks (e.g., on drawers, doors, cabinets), guards (e.g., to prevent entrance to a building or a room), or gates (e.g., to prevent entrance to a facility such as a control center). However, for communications systems, there are only two mechanisms that can be effectively employed to provide confidentiality: transmission through a physically protected medium (e.g., wire or fiber encased in a tamper resistant conduit), or cryptography.

For the CCSDS space environment, cryptography must be used to provide confidentiality of information since the data is sent via radio. For the ground environment, within a facility, the previously discussed mechanisms may suffice. But cryptography is needed for the transfer over ground networks between facilities. Cryptography employs mathematical algorithms to obscure the meaning of information. In this way, cryptography provides confidentiality because only those who possess the decryption key are able to view and use the encrypted data.

In space missions, confidentiality is employed to ensure non-disclosure of information as it traverses the ground network, as it is transmitted between the ground and the spacecraft, between the spacecraft and the ground, and even on-board a spacecraft.

B. Authentication/Integrity Overview

Authentication algorithms provide the basis for implementing authentication and integrity services. Authentication is used to uniquely identify a person or an entity. It may also be used to identify a "role" that a person has taken (e.g., the controller of instrument X). It may also be applied to uniquely identify a workstation or a group of workstations making up a control center. In this way, anything received which is claimed to have been sent from an individual (e.g., John Smith), an individual acting in a role (e.g., John Smith acting as the instrument X controller), or a facility (e.g., the mission control center) can be authenticated as actually having been sent by/from the claimed identity. The receiver is assured that the claimed identity of the source of the data is authentic and the data itself has not been altered or modified in transit without authorization or notification.

Undetected data modification or corruption of data is a major concern. It could affect the integrity/correctness of data received either on the ground from the spacecraft or on the spacecraft from the ground (i.e., what was transmitted is exactly what is received or any unauthorized modifications are detected and flagged). Modified or corrupted commands transmitted to the spacecraft could result in a catastrophic loss of mission. Modified or corrupted payload data from the spacecraft may result in erratic or incorrect science. Modified or corrupted telemetry (e.g., housekeeping or engineering data) might be reacted upon resulting in a catastrophic event (e.g., telemetry incorrectly indicates high onboard temperatures resulting in controller actions that could harm the spacecraft). The spacecraft/instrument must have the ability to recognize and discard unauthorized or corrupted commands and software uploads.

There are various algorithms that can be used to implement authentication services. A mission could use a shared-secret hash-based algorithm. Alternatively, it could use a cipher-based algorithm using, for example AES, to provide authentication. Finally, a digital signature-based algorithm could be used which not only provides authentication, but also employs public key certificates enabling a key management solution.

There is no one right way to implement authentication for all missions and hence the CCSDS algorithms standard has allowed for all three types of authentication algorithms to be employed as missions see fit.

C. Authenticated Encryption Overview

Authenticated encryption is a cipher mode which provides the simultaneous data services of confidentiality, integrity, and authenticity. Authenticated encryption is also known as Authenticated Encryption with Associated Data (AEAD).

In general, authenticated encryption can be performed by combining an encryption algorithm with an authentication algorithm as long as both are known to be secure against attack. It has been shown that encrypting data and then applying a message authentication code (MAC) to the ciphertext implies security against an adaptive chosen ciphertext attack.

Several authenticated encryption modes have been developed such as “Counter Mode with CBC-MAC” (CCM), and “Galois/Counter Mode (GCM).” CCM has become a mandatory component of the IEEE 802.11i standard. GCM has been adopted for use with IEEE 802.1AE, IETF IPsec, SSH, and TLS/SSL.

More details on the selected algorithm and modes will be provided in subsequent sections of this paper.

D. Algorithm Surveys

In order to arrive at a set of standard algorithms for confidentiality and authentication, CCSDS published two survey documents: a confidentiality algorithms survey and an authentication algorithms survey.

For the confidentiality algorithms survey[2], thirteen algorithms were compared and evaluated. A single confidentiality algorithm was selected: the Advanced Encryption Algorithm (AES) based on the Rijndael algorithm which was submitted to the International competition for the selection of AES. Moreover, it was determined that the counter mode of operation would be optimal for use in the space environment. Furthermore, authenticated encryption is optionally recommended using the AES Galois Counter Mode (AES/GCM).

In the authentication/integrity survey[3], three sets of algorithms were compared and evaluated: three digital signature algorithms, seven hash-based message authentication codes (MAC) and hashes, and three encryption-based message authentication codes.

For digital signature based authentication, initially the Digital Signature Algorithm (DSA) was selected as the standard. However, later it was determined that with the expiration of the RSA patents that the RSA Digital Signature Algorithm was in more general use and would be a better selection.

For hash-based authentication, HMAC using SHA-256 is recommended although other hash algorithms may be used in place of SHA-256 (e.g., SHA-512, RIPEMD-160).

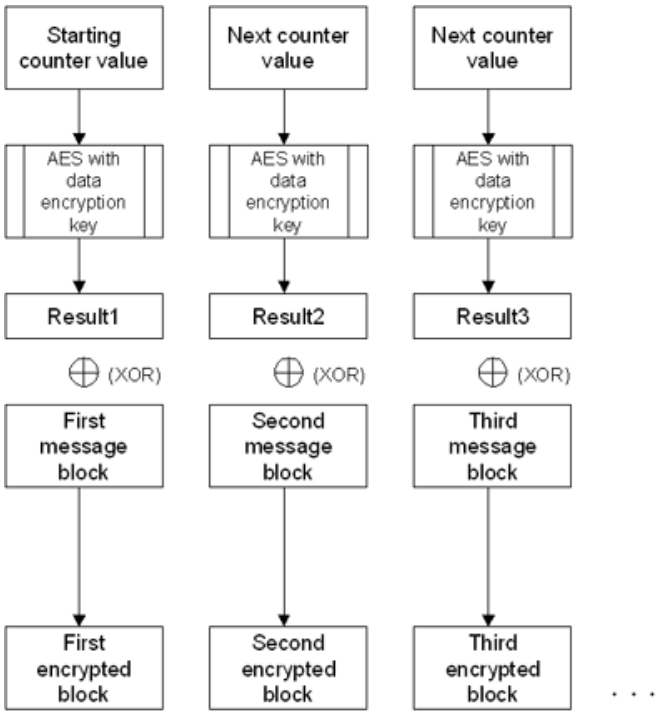
Finally, for encryption-based authentication, the Cipher-based Message Authentication Code (CMAC) was selected using the AES algorithm and a minimum 128-bit key length. Galois Message Authentication Code (GMAC) may be used as an alternative.

More details on the selected algorithms will be provided in subsequent sections of this paper.

III. Encryption Algorithms

Based on the results of the encryption algorithm survey, the algorithm chosen for CCSDS to provide confidentiality is the Advanced Encryption Algorithm (AES).[4]

Rijndael was submitted to the United States National Institute of Standards and Technology (NIST) in response to their international competition for a replacement for their Data Encryption Standard (DES) which, based on current technology, was too weak to provide necessary protection. As a result of the competition, Rijndael was chosen as the replacement for DES.



The algorithm has undergone extensive analysis both from government and private sectors. It is key agile allowing the use of 128, 192, and 256-bit key lengths. It can operate in the various "traditional" block cipher modes such as cipher block chaining (CBC) and electronic code book (ECB). It can also operate in counter mode in which the data to be encrypted does not get directly operated on by the algorithm. Rather the algorithm uses a counter to create random bits which are then exclusive OR'd (XOR) with the plaintext data to create ciphertext. As a result, when using counter mode each block of data is independent of any other block of data. This means that when implementing counter mode, encryption can be done in parallel providing a great increase in speed over serial operations. Counter mode also does not require padding which is common when using a block cipher algorithm. Counter Mode is illustrated in Figure 1.

Figure 1. Counter Mode Cipher Mode Operation[14]

While AES can use multiple key lengths, CCSDS determined that the 128-bit length was sufficient for civil space. However, larger key sizes may be used for increased protection.

IV. Authentication/Integrity Algorithms

As was stated in previous sections, rather than standardize on a single authentication/integrity algorithm, CCSDS has standardized on several algorithms – each one for a different authentication algorithm class as previously discussed. The three classes of authentication algorithms are:

- Hash-based,
- Cipher-based, or
- Digital signature-based.

Hash-based authentication uses the properties of hash algorithms to ensure authentication. A hash algorithm accepts an arbitrarily long input stream and produces a fixed size output message authentication code (MAC) called a "hash," a "message digest," or an "integrity check value" (ICV). Each resulting hash is unique for a given input stream. Different input streams will result in different, unique hashes. If only a single bit is changed in a large input stream, the resulting hash will be unique. For example, the Secure Hash Algorithm (SHA-256) may accept a data stream of several megabits and will produce a 256-bit hash which is unique and can only be recalculated given the original input stream. Typically, the hash is transmitted along with the data from a source to a destination. The receiver at the destination recalculates the hash over the received data which is then compared to the transmitted hash to ensure that the transmission did not sustain any errors. To ensure data origin authentication, a "shared secret" (shared between the source and the destination in a secure manner but not transmitted with the data) is

concatenated to the original input data and the hash is calculated over the data and the shared secret. Upon receipt, the receiver concatenates the shared secret to the received data before re-calculating the hash. If the transmitted hash matches the locally calculated hash, authentication and integrity have been achieved.

Cipher-based authentication uses the properties of a block cipher algorithm to achieve authentication and integrity. Using a secret key, the cipher algorithm is used to create a MAC analogous to the one discussed above for the hash-based algorithm. The secret key is analogous to the shared secret previously discussed. Rather than using a hash algorithm, a block cipher algorithm, such as AES, is used.

Digital Signature-based authentication makes use of the properties of asymmetric (public/private key) encryption. Each entity to be authenticated has a public/private key pair associated with it. For example, a ground control center might be an entity that holds a public/private key pair. Public keys can be universally shared and are not protected. But the private key is protected and not shared with anyone.

All commands issued by the control center would be digitally signed using the center's unique private key using a digital signature algorithm. The receiver of the command (e.g., a spacecraft) would use the control center's public key, which was previously shared, cached, or obtained from a key server, to authenticate the digital signature and hence the command. There are three well-known digital signature algorithms: the Digital Signature Algorithm (DSA), the Rivest-Shamir-Adleman (RSA) Digital Signature Algorithm, and Elliptic Curve Digital Signature Algorithm (ECDSA). All three are specified in the Digital Signature Standard (DSS)[9].

One algorithm for each authentication class has been standardized by CCSDS. It is left to individual missions to determine which algorithm class to use and subsequently, which algorithm. For example, a mission might utilize AES for encryption. To save storage and to reduce the amount of software that would have to be flight certified, reuse of AES for authentication makes a lot of sense and therefore they might use CMAC for authentication. On the other hand, if a mission does not implement confidentiality, it might choose to use a "lighter weight" authentication algorithm such as one that is hash-based rather than one that is cryptographic-based.

A. Hash-based Authentication

CCSDS has chosen the Hash-based Message Authentication Code (HMAC) algorithm. This is a keyed hash algorithm which is specified in NIST Federal Information Processing Standard (FIPS) 198-1[7]. The HMAC reference does not specify a hash algorithm for use in HMAC. CCSDS requires the use of the Secure Hash Algorithm (SHA-256) resulting in 256-bit hashes. However, CCSDS allows the use the many other strong hash functions available. For example SHA-384, SHA-512, or RIPEMD-160 are alternative hash algorithms that could be substituted for SHA-256. Because of potential attacks, the use of SHA-1 is discouraged. The Secure Hash Algorithm is specified in FIPS 180-2[11]. The HMAC algorithm is illustrated in Figure 2.

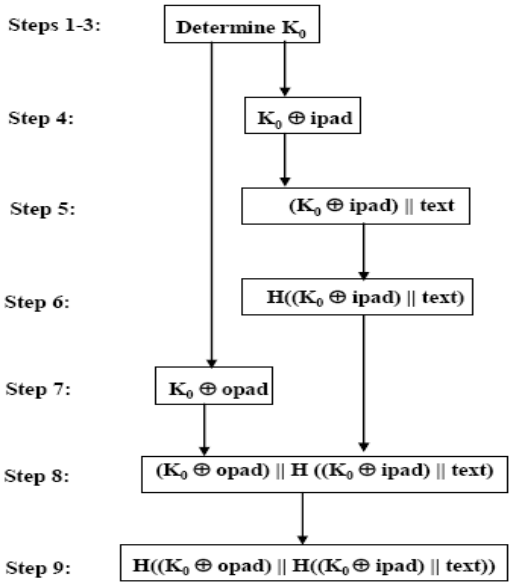


Figure 2. HMAC Algorithm[7]

HMAC had originally been specified with a final truncation step which reduced the size of the resultant MAC. The intent was to both hide some bits if they were to be transmitted and to reduce the transmission overhead. However, there is controversy over whether the hiding of bits is a good or a bad thing. As a result, in the CCSDS standard, truncation is not a mandatory function. However, if a mission has extremely constrained communications links, truncation may optionally be performed to help reduce the communications overhead. NIST recommends that a MAC not be truncated more than half of its original size.[8]

B. Cipher-based Authentication

CCSDS has chosen the Cipher-based Message Authentication Code (CMAC)[10] algorithm for cipher-based authentication. CMAC can use AES or the Triple Data Encryption Algorithm (TDEA), however CCSDS has specified the use of the AES algorithm. CMAC, utilizing the AES algorithm, supports multiple key sizes: 128-bit, 192-bit, and 256-bit. CCSDS has specified that missions use a 128-bit key, but larger key sizes may be chosen for stronger security. The resultant MAC will be at least 128 bits in length. The CMAC algorithm is illustrated in Figure 3.

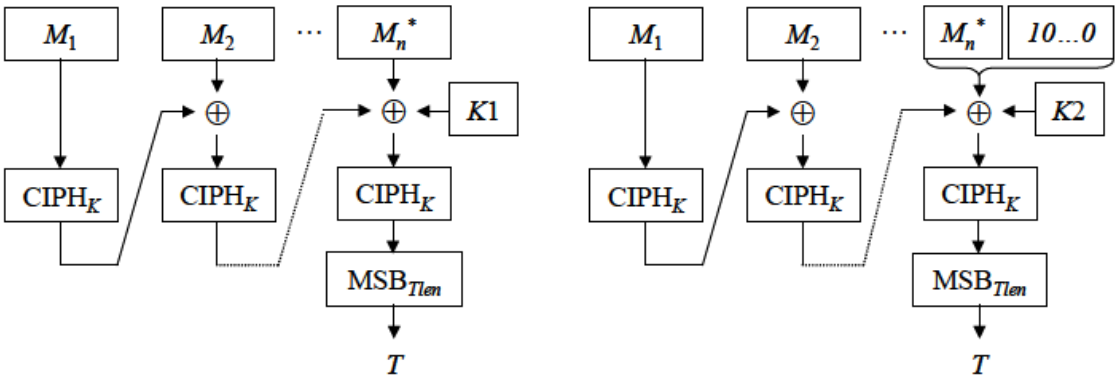


Figure 3. CMAC Algorithm[10]

For operational or design reasons, the Galois Message Authentication Code (GMAC)[6] may be used in place of CMAC. This is especially useful when an authenticated encryption implementation is used for authentication-only.

C. Digital Signature-based Authentication

CCSDS has chosen the RSA Digital Signature Algorithm[9] for digital signature-based authentication. RSA is extremely well known and widely used to provide authentication and integrity for applications such as electronic mail.

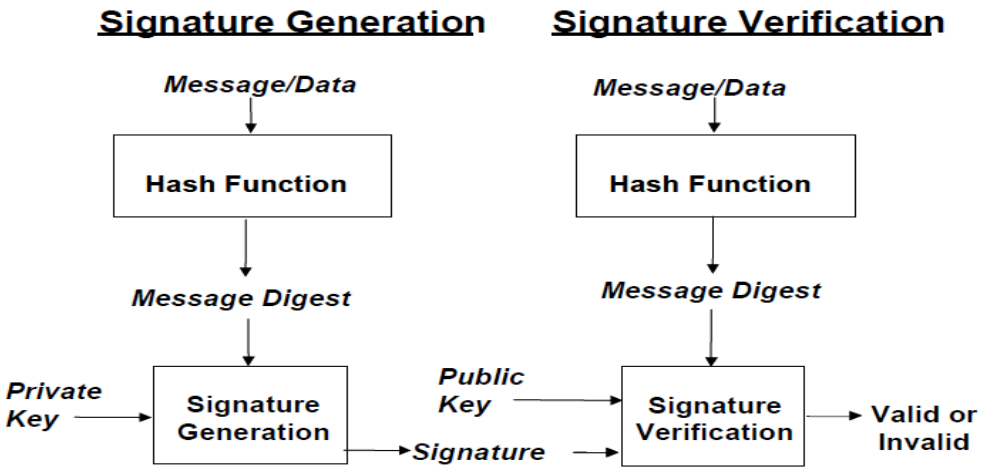


Figure 4. Digital Signature Process[9]

The RSA algorithm may be used with three different modulus sizes: 1024, 2048, and 3072 bits. CCSDS has chosen to use a minimum modulus of 2048 bits. CCSDS also allows the use of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). A generalized illustration of the digital signature process is shown in Figure 4.

The use of digital signature authentication is predicated on the ability to generate and share asymmetric key pairs. Private keys are held by the key owner and are never shared. But the public keys are shared either directly in a peer-to-peer manner, they can be stored and retrieved from a public key server, or they can be locally cached.

For spacecraft without the ability to contact a key server to obtain public keys, a public key cache can be pre-loaded prior to launch or public keys may be uploaded after launch. Public key certificates, containing the public keys of other spacecraft and ground control centers, could be pre-loaded onboard the spacecraft prior to launch, or uploaded when on-orbit.

V. Conclusion

This paper has discussed the development of CCSDS security algorithm standards. Both confidentiality and authentication/integrity algorithms have been discussed.

At the moment, CCSDS has taken the first step in specifying these algorithms but has not yet issued any standards regarding how or where these algorithms should be used. The intent is that there will be additional standards developed employing these algorithms.

Currently, the most advanced development is a link layer security standard for use with the existing CCSDS link layer protocols: telecommand (TC), telemetry (TM), and Advanced Orbiting Systems (AOS). The protocol creates a security "shim" that specifies a standard way to use security services with the existing CCSDS link layer protocols. The security protocol does not require any changes to be made to the existing protocols. This work is being performed by the Space Data Link Security Working Group which is co-chartered by the CCSDS Systems Engineering and Space Link Area directorates.

The CCSDS Security Working Group is also studying upper layer security such as network and application layer. The ground work has begun to define a CCSDS profile for the use of the IP Security (IPsec) protocol for those missions using the Internet Protocol. The Working Group has examined the many options that IPsec has to offer and have created a baseline of those options that will be supported and which will not be supported in the CCSDS profile. The profile will be written as a CCSDS *adaptation* profile standard Blue Book.

Along the same lines the CCSDS Security Working Group has written a key management overview document and is currently writing a key management standard. The key management overview provides introductory information about key management for mission planners. The key management standard document will set standards for the various types of key management for use by missions.

Much work remains to be done in CCSDS security but headway is being made to help secure civil space missions.

Appendix A
Acronym List

AES	Advanced Encryption Standard
AOS	Advanced Orbiting Systems
CBC	Cipher block chaining
CCSDS	Consultative Committee for Space Data Systems
CMAC	Cipher-based Message Authentication Code
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECB	Electronic code book
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Hash-based Message Authentication Code
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPsec	IP Security Protocol
MAC	Message Authentication Code
NIST	National Institute for Standards and Technology
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TC	Telecommand
TLS	Transport Layer Security
TM	Telemetry
XOR	Exclusive OR

Appendix B
Glossary[12]

Authentication	The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.
Cipher text	Data produced through the use of encipherment. The semantic content of the resulting data is not available.
Digital Signature	Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.
Encryption	The cryptographic transformation of data (see cryptography) to produce ciphertext.
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: (1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and (2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Message Authentication Code	A cryptographic checksum that results from passing data through a message authentication algorithm.

Acknowledgments

This paper is based on the work performed by the CCSDS Security Working group made up of members from NASA, ESA, DLR, UK Space Agency, CNES, and ASI. The author would like to thank the working group for all of its hard work in creating, writing, and reviewing the algorithms standard. The author would also like to thank the NASA standards program for financial, programmatic, and moral support.

References

1. CCSDS, "CCSDS Cryptographic Algorithms," Draft Recommended Standard, CCSDS 353.0-R-1, November 2011.
2. CCSDS, "Encryption Algorithm Trade Survey," Green Book, Issue 1, March 2008.
3. CCSDS, "Authentication/Integrity Algorithm Issues Survey," Green Book, Issue 1, March 2008.
4. NIST, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Special Publication 197. Gaithersburg, Maryland: NIST, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
5. Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," National Institute of Standards and Technology Special Publication 800-38A. Gaithersburg, Maryland: NIST, 2001. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
6. Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," National Institute of Standards and Technology Special Publication 800-38D. Gaithersburg, Maryland: NIST, November 2007. http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
7. NIST, "The Keyed Hash Message Authentication Code," Federal Information Processing Standard 198-1 (FIPS-198-1), U.S. National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf, July 2008.
8. Dang, Q, "Recommendation for Applications using Approved Hash Algorithms," SP 800-107, http://csrc.nist.gov/publications/nistpubs/800-107/NIST-SP-800-107.pdf, February 2009.
9. NIST, "Digital Signature Standard," Federal Information Processing Standard 186-3, U.S. National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, June 2009.
10. Dworkin, M., "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," NIST Special Publication 800-38B, National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf, May 2005.
11. NIST, "Secure Hash Standard," Federal Information Processing Standard 180-2, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf, August 2002.
12. CCSDS, "Information Security Glossary of Terms," Draft Information Report, Green Book, CCSDS 350.8-G-1, November 2011.
13. CCSDS, "Security Threats against Space Missions," Information Report, Green Book, CCSDS 350.1-G-1, October 2006.
14. Microsoft TechNet, "Wi-Fi Protected Access 2 Data Encryption and Integrity," http://technet.microsoft.com/en-us/library/bb878096.aspx, The Cable Guy – August 2005.