

Network Working Group  
Housley  
Request for Comments: 3874  
Security  
Category: Informational  
2004

R.  
Vigil  
September

## A 224-bit One-way Hash Function: SHA-224

### Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (2004).

### Abstract

This document specifies a 224-bit one-way hash function, called SHA-224. SHA-224 is based on SHA-256, but it uses a different initial value and the result is truncated to 224 bits.

### 1. Introduction

This document specifies a 224-bit one-way hash function, called SHA-224. The National Institute of Standards and Technology (NIST) announced the FIPS 180-2 Change Notice on February 28, 2004 which specifies the SHA-224 one-way hash function. One-way hash functions are also known as message digests. SHA-224 is based on SHA-256, the 256-bit one-way hash function already specified by NIST [SHA2]. Computation of a SHA-224 hash value is two steps. First, the SHA-256 hash value is computed, except that a different initial value is used. Second, the resulting 256-bit hash value is truncated to 224 bits.

NIST is developing guidance on cryptographic key management, and NIST recently published a draft for comment [NISTGUIDE]. Five security levels are discussed in the guidance: 80, 112, 128, 192, and 256 bits of security. One-way hash functions are available for all of these levels except one. SHA-224 fills this void. SHA-224 is a one-way hash function that provides 112 bits of security, which is the generally accepted strength of Triple-DES [3DES].

This document makes the SHA-224 one-way hash function specification available to the Internet community, and it publishes the object identifiers for use in ASN.1-based protocols.

Housley  
1]

Informational

[Page

RFC 3874  
2004

A 224-bit One-way Hash Function: SHA-224 September

### 1.1. Usage Considerations

Since SHA-224 is based on SHA-256, roughly the same amount of effort is consumed to compute a SHA-224 or a SHA-256 digest message digest value. Even though SHA-224 and SHA-256 have roughly equivalent computational complexity, SHA-224 is an appropriate choice for a one-way hash function that provides 112 bits of security. The use of a different initial value ensures that a truncated SHA-256 message digest value cannot be mistaken for a SHA-224 message digest value computed on the same data.

Some usage environments are sensitive to every octet that is transmitted. In these cases, the smaller (by 4 octets) message digest value provided by SHA-224 is important.

These observations lead to the following guidance:

- \* When selecting a suite of cryptographic algorithms that all offer 112 bits of security strength, SHA-224 is an appropriate choice for one-way hash function.
- \* When terseness is not a selection criteria, the use of SHA-256 is a preferred alternative to SHA-224.

### 1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [STDWORDS].

## 2. SHA-224 Description

SHA-224 may be used to compute a one-way hash value on a message whose length less than  $2^{64}$  bits.

SHA-224 makes use of SHA-256 [SHA2]. To compute a one-way hash value, SHA-256 uses a message schedule of sixty-four 32-bit words, eight 32-bit working variables, and produces a hash value of eight

32-bit words.

The function is defined in the exact same manner as SHA-256, with the following two exceptions:

First, for SHA-224, the initial hash value of the eight 32-bit working variables, collectively called H, shall consist of the following eight 32-bit words (in hex):

Housley	Informational	[Page
2]		
RFC 3874	A 224-bit One-way Hash Function: SHA-224	September
2004		

H_0 = c1059ed8	H_4 = ffc00b31
H_1 = 367cd507	H_5 = 68581511
H_2 = 3070dd17	H_6 = 64f98fa7
H_3 = f70e5939	H_7 = befa4fa4

Second, SHA-224 simply makes use of the first seven 32-bit words in the SHA-256 result, discarding the remaining 32-bit words in the SHA-256 result. That is, the final value of H is used as follows, where || denotes concatenation:

H\_0 || H\_1 || H\_2 || H\_3 || H\_4 || H\_5 || H\_6

### 3. Test Vectors

This section includes three test vectors. These test vectors can be used to test implementations of SHA-224.

#### 3.1. Test Vector #1

Let the message to be hashed be the 24-bit ASCII string "abc", which is equivalent to the following binary string:

01100001 01100010 01100011

The SHA-224 hash value (in hex):

23097d22 3405d822 8642a477 bda255b3 2aadbce4 bda0b3f7 e36c9da7

#### 3.2. Test Vector #2

Let the message to be hashed be the 448-bit ASCII string "abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq".

The SHA-224 hash value is (in hex):

75388b16 512776cc 5dba5da1 fd890150 b0c6455c b4f58b19 52522525



Internet community. No independent assertion of the security of this one-way hash function is intended by the author for any particular use. However, as long as SHA-256 provides the expected security, SHA-224 will also provide its expected level of security.

## 6. References

### 6.1. Normative References

- [SHA2] Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, 1 August 2002.
- [STDWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Housley	Informational	[Page
4]		
RFC 3874	A 224-bit One-way Hash Function: SHA-224	September
2004		

### 6.2. Informative References

- [3DES] American National Standards Institute. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation. 1998.
- [CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.
- [NISTGUIDE] National Institute of Standards and Technology. Second Draft: "Key Management Guideline, Part 1: General Guidance." June 2002. [<http://csrc.nist.gov/encryption/kms/guideline-1.pdf>]
- [X.208-88] CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.
- [X.209-88] CCITT Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

## 7. Acknowledgments

Many thanks to Jim Schaad for generating the test vectors. A second implementation by Brian Gladman was used to confirm that the test vectors are correct.

8. Author's Address

Russell Housley  
Vigil Security, LLC  
918 Spring Knoll Drive  
Herndon, VA 20170  
USA

EEmail: housley@vigilsec.com

Housley  
5]

Informational

[Page

RFC 3874  
2004

A 224-bit One-way Hash Function: SHA-224

September

9. Full Copyright Statement

Copyright (C) The Internet Society (2004).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an

"AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/S HE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE

INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to

pertain to the implementation or use of the technology described in

this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has

made any independent effort to identify any such rights.  
Information  
on the IETF's procedures with respect to rights in IETF Documents  
can  
be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any  
assurances of licenses to be made available, or the result of an  
attempt made to obtain a general license or permission for the use  
of  
such proprietary rights by implementers or users of this  
specification can be obtained from the IETF on-line IPR repository  
at  
<http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention  
any  
copyrights, patents or patent applications, or other proprietary  
rights that may cover technology that may be required to implement  
this standard. Please address the information to the IETF at  
ietf-  
[ipr@ietf.org](mailto:ipr@ietf.org).

#### Acknowledgement

Funding for the RFC Editor function is currently provided by the  
Internet Society.