

Network Working Group
Request for Comments: 4231
Category: Standards Track

M. Nystrom
RSA Security
December 2005

Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256,
HMAC-SHA-384, and HMAC-SHA-512

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document provides test vectors for the HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 message authentication schemes. It also provides ASN.1 object identifiers and Uniform Resource Identifiers (URIs) to identify use of these schemes in protocols. The test vectors provided in this document may be used for conformance testing.

Table of Contents

1.	Introduction	2
2.	Conventions Used in This Document	2
3.	Scheme Identifiers	3
3.1.	ASN.1 Object Identifiers	3
3.2.	Algorithm URIs	3
4.	Test Vectors	3
4.1.	Introduction	3
4.2.	Test Case 1	4
4.3.	Test Case 2	4
4.4.	Test Case 3	5
4.5.	Test Case 4	5
4.6.	Test Case 5	6
4.7.	Test Case 6	6
4.8.	Test Case 7	7
5.	Security Considerations	7
6.	Acknowledgements	8
7.	References	8
7.1.	Normative References	8
7.2.	Informative References	8

1. Introduction

This document provides test vectors for the HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 message authentication schemes. It also provides ASN.1 object identifiers and URIs to identify use of these schemes in protocols using ASN.1 constructs (such as those built on Secure/Multipurpose Internet Mail Extensions (S/MIME) [4]) or protocols based on XML constructs (such as those leveraging XML Digital Signatures [5]).

HMAC-SHA-224 is the realization of the HMAC message authentication code [1] using the SHA-224 hash function, HMAC-SHA-256 is the realization of the HMAC message authentication code using the SHA-256 hash function, HMAC-SHA-384 is the realization of the HMAC message authentication code using the SHA-384 hash function, and HMAC-SHA-512 is the realization of the HMAC message authentication code using the SHA-512 hash function. SHA-224, SHA-256, SHA-384, and SHA-512 are all described in [2].

2. Conventions Used in This Document

The key word "SHOULD" in this document is to be interpreted as described in RFC 2119 [3].

3. Scheme Identifiers

3.1. ASN.1 Object Identifiers

The following ASN.1 object identifiers have been allocated for these schemes:

```
rsadsi OBJECT IDENTIFIER ::=
    {iso(1) member-body(2) us(840) rsadsi(113549)}
```

```
digestAlgorithm OBJECT IDENTIFIER ::= {rsadsi 2}
```

```
id-hmacWithSHA224 OBJECT IDENTIFIER ::= {digestAlgorithm 8}
id-hmacWithSHA256 OBJECT IDENTIFIER ::= {digestAlgorithm 9}
id-hmacWithSHA384 OBJECT IDENTIFIER ::= {digestAlgorithm 10}
id-hmacWithSHA512 OBJECT IDENTIFIER ::= {digestAlgorithm 11}
```

When the "algorithm" component in a value of ASN.1 type `AlgorithmIdentifier` (see, e.g., [4], Section 10) identifies one of these schemes, the "parameter" component SHOULD be present but have type `NULL`.

3.2. Algorithm URIs

The following URIs have been allocated for these schemes:

```
http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#hmac-sha-224
http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#hmac-sha-256
http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#hmac-sha-384
http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#hmac-sha-512
```

As usual, when used in the context of [5], the `<ds:HMACOutputLength>` element may specify the truncated length of the scheme output.

4. Test Vectors

4.1. Introduction

The test vectors in this document have been cross-verified by three independent implementations. An implementation that concurs with the results provided in this document should be interoperable with other similar implementations.

Keys, data, and digests are provided in hex.

4.4. Test Case 3

Test with a combined length of key and data that is larger than 64 bytes (= block-size of SHA-224 and SHA-256).

[illegible]

4.8. Test Case 7

Test with a key and data that is larger than 128 bytes (= block-size of SHA-384 and SHA-512).

```

Key =      aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
           aaaaaa                                     (131 bytes)

Data =     54686973206973206120746573742075      ("This is a test u")
           73696e672061206c6172676572207468      ("sing a larger th")
           616e20626c6f636b2d73697a65206b65      ("an block-size ke")
           7920616e642061206c61726765722074      ("y and a larger t")
           68616e20626c6f636b2d73697a652064      ("han block-size d")
           6174612e20546865206b6579206e6565      ("ata. The key nee")
           647320746f2062652068617368656420      ("ds to be hashed ")
           6265666f7265206265696e6720757365      ("before being use")
           642062792074686520484d414320616c      ("d by the HMAC al")
           676f726974686d2e                        ("gorithm.")

HMAC-SHA-224 = 3a854166ac5d9f023f54d517d0b39dbd
               946770db9c2b95c9f6f565d1
HMAC-SHA-256 = 9b09ffa71b942fcb27635fbcd5b0e944
               bfdc63644f0713938a7f51535c3a35e2
HMAC-SHA-384 = 6617178e941f020d351e2f254e8fd32c
               602420feb0b8fb9adccebb82461e99c5
               a678cc31e799176d3860e6110c46523e
HMAC-SHA-512 = e37b6a775dc87dbaa4dfa9f96e5e3ffd
               debd71f8867289865df5a32d20cdc944
               b6022cac3c4982b10d5eeb55c3e4de15
               134676fb6de0446065c97440fa8c6a58

```

5. Security Considerations

This document is intended to provide the identifications and test vectors for the four identified message authentication code schemes to the Internet community. No assertion of the security of these message authentication code schemes for any particular use is intended. The reader is referred to [1] for a discussion of the general security of the HMAC construction.

6. Acknowledgements

The test cases in this document are derived from the test cases in [6], although the keys and data are slightly different.

Thanks to Jim Schaad and Brad Hards for assistance in verifying the results.

7. References

7.1. Normative References

- [1] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
- [2] National Institute of Standards and Technology, "Secure Hash Standard", FIPS 180-2, August 2002, with Change Notice 1 dated February 2004.
- [3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2. Informative References

- [4] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.
- [5] Eastlake 3rd, D., Reagle, J., and D. Solo, "(Extensible Markup Language) XML-Signature Syntax and Processing", RFC 3275, March 2002.
- [6] Cheng, P. and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1", RFC 2202, September 1997.

Author's Address

Magnus Nystrom
RSA Security

EMail: magnus@rsasecurity.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

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/SHE 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 procedures with respect to rights in RFC 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.

Acknowledgement

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

