Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512
draft-nystrom-smime-hmac-sha-02

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 29, 2005.

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 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 ........................................... 3
2. Conventions used in this document ...................... 3
3. Scheme identifiers ...................................... 3
   3.1 ASN.1 Object Identifiers ............................ 3
   3.2 Algorithm URIs .................................... 4
4. Test vectors ........................................... 4
   4.1 Introduction ....................................... 4
   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. IANA considerations ..................................... 8
6. Security Considerations .................................. 8
7. Acknowledgments ........................................ 9
8. References ............................................. 9
   8.1 Normative references ............................... 9
   8.2 Informative references ............................. 9
   Author’s Address ....................................... 9
   Intellectual Property and Copyright Statements .......... 10
1. Introduction

This document provides test vectors for the HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA384, 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 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:

```plaintext
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.

4.2 Test case 1

Key = 0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b
      0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b (20 bytes)
Data = 4869205468657265                  ("Hi There")

HMAC-SHA-224 = 896fb1128abbdf196832107cd49df33f
               47b4b1169912ba4f53684b22
HMAC-SHA-256 = b0344c61d8db38535ca8afceaf0bf12b
               881dc200c9833da726e9376c2e32c7f7
HMAC-SHA-384 = afd03944d84895626b0825f4ab46907f
               15f9dadbe4101ec682aa034c7cebc59c
               faea9ea9076ede7f4af152e8b2fa9cb6
HMAC-SHA-512 = 87aa7cdea5ef619d4ff0b4241a1d6cb0
               2379f4e2ce4ec2787ad0b30545e17cde
               daa833b7d6b8a702038b274eaaa3f4e4
               be9d914eeb61f1702e696c203a126854

4.3 Test case 2

Test with key shorter than the length of the HMAC output.
4.4 Test case 3

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

Key = aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
\hspace{1cm} (20 bytes)

Data = dddddddddddddddddddddddddddddddddddddddddddddd
\hspace{1cm} (50 bytes)

HMAC-SHA-224 = 7fb3cb3588c6c1f6f6fa9694d7d6ad264
\hspace{1cm} 9365b0c1f65d69d1ec8333ea

HMAC-SHA-256 = 773ea91e36800e46854db8ebd09181a7
\hspace{1cm} 2959098b3ef8c122d9635514ced565fe

HMAC-SHA-384 = 88062608d3e6ad8a0a2ace014c8a86f
\hspace{1cm} 0aa635d947ac9febe83ef4e55966144b
\hspace{1cm} 2a5ab39dc13814b94e3ab6e101a34f27

HMAC-SHA-512 = fa73b0089d56a284efbf0f0756c890be9
\hspace{1cm} b1b5bdd8ee81a3655f83e33b2279d39
\hspace{1cm} bf3e848279a722c806b485a47e67c807
\hspace{1cm} b946a337bee8942674278859e13292fb

4.5 Test case 4

Test with combined length of key and data larger than 64 bytes (= block-size of SHA-224 and SHA-256).
4.6 Test case 5

Test with truncation of output to 128 bits.

Key = 0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c (20 bytes)
Data = 546573742057697468205472756e636174696f6e ("Test With Trunca")
       746966 ("tion")

HMAC-SHA-224 = 0e2aa68a90c8d37c988bcdb9fca6fa8
HMAC-SHA-256 = a3b6167473100ee06e0c796c2955552b
HMAC-SHA-384 = 3abf34c3503b2a23a46efc619baef897
HMAC-SHA-512 = 415fad6271580a531d4179bc891d87a6

4.7 Test case 6

Test with key larger than 128 bytes (= block-size of SHA-384 and SHA-512).
Key = aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa  (131 bytes)
Data = 54657374205573696e67204c61726765  ("Test Using Large")
       72205468616e20426c6f636b2d53697a  ("r Than Block-Siz")
       65204b6579202d2048617368204b6579  ("e Key - Hash Key")
       204669727374  (" First")
HMAC-SHA-224 = 95e9a0db962095adaebe9b2d6f0dbce2
d499f112f2d2b7273fa6870e
HMAC-SHA-256 = 60e431591ee0b67f0d8a26aacbf5b77f
              8e0bc6213728c5140546040f00ee37f54
HMAC-SHA-384 = 4ece084485813e9088d2c63a041bc5b4
              4f9ef1012a2b588f3cd11f05033ac4c6
              0c2ef6ab4030fe8296248df163f44952
HMAC-SHA-512 = 80b24263c7c1a3ebb71493c1dd7be884
              9b46d1f41b4aeec1121b013783f8f352
              6b56d037e05f2598bd0fd2215d6a1e52
              95e64f73f63f0aec8b915a985d786598

4.8 Test case 7

Test with key and data larger than 128 bytes (= block-size of SHA-384 and SHA-512).
5. IANA considerations

This document does not have any actions for IANA.

6. 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.
7. Acknowledgments

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.

8. References

8.1 Normative references


8.2 Informative references


Author’s Address

Magnus Nystrom
RSA Security

Email: magnus@rsasecurity.com
Intellectual Property Statement

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.

Disclaimer of Validity

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.

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.

Acknowledgment

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