Groupe de travail Réseau
Request for Comments : 4231
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Nystrom, RSA Security

décembre 2005

Identifiants et valeurs d'essai pour HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512

Résumé
Le présent document donne les valeurs d'essais pour les schémas d'authentification de message HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512. Il donne aussi les identifiants d'objet ASN.1 et les identifiants de ressource universels (URI, *Uniform Resource Identifier*) pour identifier l'utilisation de ces schémas dans les protocoles. Les vecteurs d'essais fournis dans ce document peuvent être utilisés pour les essais de conformité.

Table des matières

1. Introduction

Le présent document donne les valeurs d'essais pour les schémas d'authentification de message HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512. Il donne aussi les identifiants d'objet ASN.1 et les URI pour identifier l'usage de ces schémas dans les protocoles qui utilisent les constructions ASN.1 (comme celles construites sur les extensions de messagerie Internet multi objets/sûre (S/MIME, *Secure/Multipurpose Internet Mail Extensions*) [RFC3852]) ou les protocoles fondés sur les constructions XML (comme celles qui sous-tendent les signatures numériques XML [RFC3275]).

HMAC-SHA-224 est la réalisation du code d'authentification de message HMAC [RFC2104] qui utilise la fonction de hachage SHA-224, HMAC-SHA-256 est la réalisation du code d'authentification de message HMAC qui utilise la fonction

de hachage SHA-256, HMAC-SHA-384 est la réalisation du code d'authentification de message HMAC qui utilise la fonction de hachage SHA-384, et HMAC-SHA-512 est la réalisation du code d'authentification de message HMAC qui utilise la fonction de hachage SHA-512. SHA-224, SHA-256, SHA-384, et SHA-512 sont toutes décrites dans [FIPS180-2].

2. Conventions utilisées dans le document

Le mot-clé "DEVRAIT" dans ce document est à interpréter comme décrit dans la [RFC2119].

3. Identifiants de schéma

3.1 Identifiants d'objet ASN.1

Les identifiants d'objet ASN.1 suivants ont été alloués pour ces schémas :

IDENTIFIANT D'OBJET rsadsi ::= {iso(1) member-body(2) us(840) rsadsi(113549)}
IDENTIFIANT D'OBJET digestAlgorithm ::= {rsadsi 2}
IDENTIFIANT D'OBJET id-hmacWithSHA224 ::= {digestAlgorithm 8}
IDENTIFIANT D'OBJET id-hmacWithSHA256 ::= {digestAlgorithm 9}
IDENTIFIANT D'OBJET id-hmacWithSHA384 ::= {digestAlgorithm 10}
IDENTIFIANT D'OBJET id-hmacWithSHA512 ::= {digestAlgorithm 11}

Quand le composant "algorithm" dans une valeur de AlgorithmIdentifier de type ASN.1 (voir par exemple la [RFC3852], Section 10) identifie un de ces schémas, le composant "parameter" DEVRAIT être présent mais avoir le type NULL.

3.2 URI d'algorithme

Les URI suivants ont été alloués pour ces schémas :

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

Comme il est d'usage, dans le contexte de la [RFC3275], l'élément <ds:HMACOutputLength> peut spécifier la longueur tronquée du résultat du schéma.

4. Valeurs d'essais

4.1 Introduction

Les valeurs d'essais dans ce document ont fait l'objet d'une vérifiation croisée par trois mises en œuvre indépendantes. Une mise en œuvre qui fonctionne avec les résultats fournis dans le présent document devrait être interopérable avec les autres mises en œuvre similaires.

Les clés, données, et résumés sont fournis en hexadécimal.

4.2 Cas d'essais 1

Clé = 0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b (20 octets)
Données = 4869205468657265 ("Hi There")

HMAC-SHA-224 = 896fb1128abbdf196832107cd49df33f47b4b1169912ba4f53684b22
HMAC-SHA-256 = b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da726e9376c2e32cff7
HMAC-SHA-384 = afd03944d84895626b0825f4ab46907f15f9dadbe4101ec682aa034c7cebc59c
faea9ea9076ede7f4af152e8b2fa9cb6
HMAC-SHA-512 = 87aa7cdea5ef619d4ff0b4241a1d6cb02379f4e2ce4ec2787ad0b30545e17cde

daa833b7d6b8a702038b274eaea3f4e4be9d914eeb61f1702e696c203a126854

4.3 Cas d'essais 2

Essai avec une clé plus courte que la longueur du résultat HMAC.

Clé = 4a656665 ("Jefe")
Données = 7768617420646f2079612077616e7420 ("what do ya want ")
666f72206e6f7468696e673f ("for nothing?")

HMAC-SHA-224 = a30e01098bc6dbbf45690f3a7e9e6d0f8bbea2a39e6148008fd05e44
HMAC-SHA-256 = 5bdcc146bf60754e6a042426089575c75a003f089d2739839dec58b964ec3843
HMAC-SHA-384 = af45d2e376484031617f78d2b58a6b1b9c7ef464f5a01b47e42ec3736322445e
8e2240ca5e69e2c78b3239ecfab21649
HMAC-SHA-512 = 164b7a7bfcf819e2e395fbe73b56e0a387bd64222e831fd610270cd7ea250554
9758bf75c05a994a6d034f65f8f0e6fdcaeab1a34d4a6b4b636e070a38bce737

4.4 Cas d'essais 3

Essai avec une longueur combinée de clé et données qui est plus longue que 64 octets (= taille de bloc de SHA-224 et SHA-256).

Clé aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa (20 octets)
Données = ddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
ddddddddddddddddddddddddddddddddddddddddddd (50 octets)

HMAC-SHA-224 = 7fb3cb3588c6c1f6ffa9694d7d6ad2649365b0c1f65d69d1ec8333ea
HMAC-SHA-256 = 773ea91e36800e46854db8ebd09181a72959098b3ef8c122d9635514ced565fe
HMAC-SHA-384 = 88062608d3e6ad8a0aa2ace014c8a86f0aa635d947ac9febe83ef4e55966144b
2a5ab39dc13814b94e3ab6e101a34f27
HMAC-SHA-512 = fa73b0089d56a284efb0f0756c890be9b1b5dbdd8ee81a3655f83e33b2279d39
bf3e848279a722c806b485a47e67c807b946a337bee8942674278859e13292fb

4.5 Cas d'essais 4

Essai avec une longueur combinée de clé et données qui est plus longue que 64 octets (= taille de bloc de SHA-224 et SHA-256).

Clé = 0102030405060708090a0b0c0d0e0f10111213141516171819 (25 octets)
Données = cdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcd
cdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcd (50 octets)

HMAC-SHA-224 = 6c11506874013cac6a2abc1bb382627cec6a90d86efc012de7afec5a
HMAC-SHA-256 = 82558a389a443c0ea4cc819899f2083a85f0faa3e578f8077a2e3ff46729665b
HMAC-SHA-384 = 3e8a69b7783c25851933ab6290af6ca77a9981480850009cc5577c6e1f573b4e
6801dd23c4a7d679ccf8a386c674cffb
HMAC-SHA-512 = b0ba465637458c6990e5a8c5f61d4af7e576d97ff94b872de76f8050361ee3db
a91ca5c11aa25eb4d679275cc5788063a5f19741120c4f2de2adebeb10a298dd

4.6 Cas d'essais 5

Essai avec troncature du résultat à 128 bits.

Clé = 0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c (20 octets)
Données = 546573742057697468205472756e6361 ("Test With Trunca")
74696f6e ("tion")

HMAC-SHA-224 = 0e2aea68a90c8d37c988bcdb9fca6fa8
HMAC-SHA-256 = a3b6167473100ee06e0c796c2955552b
HMAC-SHA-384 = 3abf34c3503b2a23a46efc619baef897

HMAC-SHA-512 = 415fad6271580a531d4179bc891d87a6

4.7 Cas d'essais 6

Essai avec une clé de plus de 128 octets (= taille de bloc de SHA-384 et SHA-512).

```
Clé =          aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaa                    (131 octets)
Données = 5465737420557369e67204c61726765  ("Test Using Large")
               72205468616e20426c6f636b2d53697a  ("r Than Block-Siz")
               65204b6579202d2048617368204b6579  ("e Key - Hash Key")
               204669727374              (" First")
```

```
HMAC-SHA-224 = 95e9a0db962095adaebe9b2d6f0dbce2d499f112f2d2b7273fa6870e
HMAC-SHA-256 = 60e431591ee0b67f0d8a26aacbf5b77f8e0bc6213728c5140546040f0ee37f54
HMAC-SHA-384 = 4ece084485813e9088d2c63a041bc5b44f9ef1012a2b588f3cd11f05033ac4c6
               0c2ef6ab4030fe8296248df163f44952
HMAC-SHA-512 = 80b24263c7c1a3ebb71493c1dd7be8b49b46d1f41b4aeec1121b013783f8f352
               6b56d037e05f2598bd0fd2215d6a1e5295e64f73f63f0aec8b915a985d786598
```

4.8 Cas d'essais 7

Essai avec une clé et des données de plus de 128 octets (= taille de bloc de SHA-384 et SHA-512).

```
Clé =          aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
               aaaaaa                    (131 octets)
Données = 5468697320697320612074657374207 5  ("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 = 3a854166ac5d9f023f54d517d0b39dbd946770db9c2b95c9f6f565d1
HMAC-SHA-256 = 9b09ffa71b942fcb27635fbcd5b0e944bfdc63644f0713938a7f51535c3a35e2
HMAC-SHA-384 = 6617178e941f020d351e2f254e8fd32c602420feb0b8fb9adccebb82461e99c5
               a678cc31e799176d3860e6110c46523e
HMAC-SHA-512 = e37b6a775dc87dbaa4dfa9f96e5e3ffddebd71f8867289865df5a32d20cdc944
               b6022cac3c4982b10d5eeb55c3e4de15134676fb6de0446065c97440fa8c6a58
```

5. Considérations sur la sécurité

Ce document est destiné à fournir l'identification et les valeurs d'essai pour les quatre schémas de code d'authentification de message identifiés pour la communauté de l'Internet. Aucune assertion de la sécurité de ces schémas de code d'authentification de message n'est faite pour un usage particulier. Le lécteur se réfèrera à la [RFC2104] pour une discussion de la sécurité générale des constructions HMAC.

6 Remerciements

Les cas d'essai dans ce document sont dérivés des cas d'essais de la [RFC2202], bien que les clés et les données soient légèrement différentes.

Merci à Jim Schaad et Brad Hards pour leur assistance à la vérification des résultats.

7. Références

7.1 Références normatives

[FIPS180-2] National Institute of Standards and Technology, "Secure Hash Standard", FIPS 180-2, août 2002, avec avis de changement n° 1 de février 2004.

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

9.2 Références pour information

[RFC2202] P. Cheng et R. Glenn, "Cas d'essai pour HMAC-MD5 et HMAC-SHA-1", septembre 1997. *(Information)*

[RFC3275] D. Eastlake 3rd , J. Reagle, D. Solo, "Syntaxe et traitement de signature en langage de balisage extensible (XML)", mars 2002. *(D.S.)*

[RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. *(Obsolète, voir la* RFC5652)

Adresse de l'auteur

Magnus Nystrom
RSA Security
mél : magnus@rsasecurity.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.