TMAC Test Vectors

Submission to NIST

July 24, 2002

Kaoru Kurosawa

Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
+81-294-38-5135 office
+81-294-38-5135 fax
kurosawa@cis.ibaraki.ac.jp

and

Tetsu Iwata

Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
+81-294-38-5266 office
iwata@cis.ibaraki.ac.jp

TMAC Test Vectors

Kaoru Kurosawa and Tetsu Iwata

Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
{kurosawa, iwata}@cis.ibaraki.ac.jp

Abstract. In this paper, we present test vectors for TMAC, Two-Key CBC Message Authentication Code proposed by the authors. The test vectors are given for implementations in which the underlying block cipher is Rijndael, for 128, 192 and 256 bit keys.

1 Introduction

In this paper, we present test vectors for TMAC, Two-Key CBC Message Authentication Code proposed by the authors. The test vectors are given for implementations in which the underlying block cipher is Rijndael, for 128, 192 and 256 bit keys. See [4] for a specification of TMAC, and [3, 1] for a specification of Rijndael.

2 Test Vectors

All strings are expressed in hexadecimal notation. We present 24 examples for TMAC with Rijndael as the underlying block cipher: 8 examples are given for each of the allowed key sizes (128, 192, and 256 bits). TMAC uses two keys, K_1 and K_2, where K_1 is used as a key of Rijndael. We used K_1 such that

$$K_1 = \begin{cases} \texttt{2b7e151628aed2a6abf7158809cf4f3c} & \text{for 128 bit key,} \\ \texttt{8e73b0f7da0e6452c810f32b809079e5} \\ \texttt{62f8ead2522c6b7b} & \text{for 192 bit key, and} \\ \texttt{603deb1015ca71be2b73aef0857d7781} \\ \texttt{1f352c073b6108d72d9810a30914dff4} & \text{for 256 bit key.} \end{cases}$$

These values are taken from [2].

We used K_2 such that

$$K_2 = \begin{cases} \texttt{000102030405060708090a0b0c0d0e0f}, \text{ and} \\ \texttt{f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff}. \end{cases}$$

The messages which we used are the first 0, 16, 40, and 64 bytes of

6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710

This is also taken from [2]. Note that, for each K_1, there are eight combinations of two K_2's and four messages.

In what follows, the message is denoted by "Msg" and the output is denoted by "Tag."

2.1 TMAC-AES-128

Test Vectors for the Empty String

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 000102030405060708090a0b0c0d0e0f
Msg ⟨empty string⟩
Tag 4c08220c79d9191022dc6674874ceaf8

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg ⟨empty string⟩
Tag 10188a5b5c45e61980fb1522a7fbfff9

Test Vectors for 16 Byte Message

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
Tag 6c3076442eead2741dd08057a2f51f44

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
Tag 7de51936b6be2b46fb5665cbb763992e

Test Vectors for 40 Byte Message

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411
Tag b656b827eabdf8e5d7f460e9f5100769

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411
Tag 01134f8efe7c1f6e288a0868b25440a8

Test Vectors for 64 Byte Message

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
Tag 07aa2747781f841879218ca8e6a7a3db

K_1 2b7e151628aed2a6abf7158809cf4f3c
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
Tag e262051676b73dc06cc3d34973e8d0fe

2.2 TMAC-AES-192

Test Vectors for the Empty String

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 000102030405060708090a0b0c0d0e0f
Msg ⟨empty string⟩
Tag 09aa07477468e56f850c577c39b5e095

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg ⟨empty string⟩
Tag a1bdcf836dfe669f32af3da04600d07e

Test Vectors for 16 Byte Message

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
Tag 275546ed5f9bc5d4468029af259dba4d

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
Tag 4b37cf17046ccbbb3fdc0271b68c2e96

Test Vectors for 40 Byte Message

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411
Tag 750d69ef72e5ee9de8a1ec1b961ec093

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411
Tag 2daec77528de8c2b27b7a923bccb2cf5

Test Vectors for 64 Byte Message

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
Tag 3197b08265b5d4016af0273eb1b11d65

K_1 8e73b0f7da0e6452c810f32b809079e5
62f8ead2522c6b7b
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
Tag a9e5ede6366364b34be1deb036821fb5

2.3 TMAC-AES-256

Test Vectors for the Empty String

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 000102030405060708090a0b0c0d0e0f
Msg ⟨empty string⟩
Tag 3ca4c401accc469502d6eb9fbe1dc48b

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg ⟨empty string⟩
Tag 8c6c871e4923f23d6a9a995b820e8574

Test Vectors for 16 Byte Message

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
Tag 031b585bf5108a462e42fe48a0d1e0a1

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
Tag c35d2efdee829cb0a49386deb5c9ecef

Test Vectors for 40 Byte Message

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411
Tag 8d4889ac80d32677c25695dafaf61090

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411
Tag d5a2b0d78a85a298b7a7ab2b91c89df9

Test Vectors for 64 Byte Message

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 000102030405060708090a0b0c0d0e0f
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
Tag bacbfafc54dea13de2bb983d0f5eea7f

K_1 603deb1015ca71be2b73aef0857d7781
1f352c073b6108d72d9810a30914dff4
K_2 f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
Msg 6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
Tag 47a9d0f579765bf05b2073e61313066b

References

1. FIPS Publication 197. Advanced Encryption Standard (AES). Available at http://csrc.nist.gov/encryption/aes/.
2. NIST Special Publication 800-38A. Recommendation for block cipher modes of operation. Available at http://csrc.nist.gov/encryption/modes/.
3. J. Daemen and V. Rijmen. The Design of Rijndael. Springer-Verlag, 2002.
4. K. Kurosawa and T. Iwata. TMAC: Two-Key CBC MAC. Submitted to NIST, June 21, 2002. Available at http://csrc.nist.gov/encryption/modes/ and Cryptology ePrint Archive, Report 2002/092, http://eprint.iacr.org/.