OMAC Test Vectors

Tetsu Iwata Kaoru Kurosawa

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

December 20, 2002

Abstract

In this paper, we present test vectors for OMAC, One-key CBC MAC, proposed by the authors. Test vectors are given for implementations in which the underlying block cipher is the AES, for 128-, 192- and 256-bit keys.

1 Introduction

In this paper, we present test vectors for OMAC, One-key CBC MAC, proposed by the authors. Test vectors are given for implementations in which the underlying block cipher is the AES, for 128-, 192- and 256-bit keys.

See [4] for a specification of OMAC, and [3, 1] for a specification of the AES.

2 Test Vectors

We consider OMAC which uses AES as the underlying block cipher. It takes a message $M \in \{0,1\}^*$ and returns a string in $\{0,1\}^{128}$ as a tag. The key of the OMAC is just the key of AES.

We present 4 examples for each of the allowed key sizes (128-, 192-, and 256-bit keys). Therefore 12 examples are given in total. All strings are expressed in hexadecimal notation.

As a key of AES, we used the following values.

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

These values are taken from [2].

The messages which we used are the first 0-(the empty string), 16-, 40-, and 64-bytes of

```
6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710
```

This is also taken from [2].

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

2.1 OMAC-AES-128

2.1.1 Test Vector for the Empty String

K	`2b7e151628aed2a6abf7158809cf4f3c`
Msg	⟨empty string⟩
Tag	`f6bc6a41f4f84593809e59b719299cfe`

2.1.2 Test Vector for 16-Byte Message

K	`2b7e151628aed2a6abf7158809cf4f3c`
Msg	`6bc1bee22e409f96e93d7e117393172a`
Tag	`070a16b46b4d4144f79bdd9dd04a287c`

2.1.3 Test Vector for 40-Byte Message

K	`2b7e151628aed2a6abf7158809cf4f3c`

Msg	`6bc1bee22e409f96e93d7e117393172a`
	`ae2d8a571e03ac9c9eb76fac45af8e51`
	`30c81c46a35ce411`

Tag	`23fdaa0831cd314491ce4b25acb6023b`

2.1.4 Test Vector for 64-Byte Message

K	2b7e151628aed2a6abf7158809cf4f3c
Msg	6bc1bee22e409f96e93d7e117393172a ae2d8a571e03ac9c9eb76fac45af8e51 30c81c46a35ce411e5fbc1191a0a52ef f69f2445df4f9b17ad2b417be66c3710
Tag	51f0bebf7e3b9d92fc49741779363cfe

2.2 OMAC-AES-192

2.2.1 Test Vector for the Empty String

K	8e73b0f7da0e6452c810f32b809079e5 62f8ead2522c6b7b
Msg	⟨empty string⟩
Tag	149f579df2129d45a69266898f55aeb2

2.2.2 Test Vector for 16-Byte Message

K	8e73b0f7da0e6452c810f32b809079e5 62f8ead2522c6b7b
Msg	6bc1bee22e409f96e93d7e117393172a
Tag	9e99a7bf31e710900662f65e617c5184

2.2.3 Test Vector for 40-Byte Message

K	8e73b0f7da0e6452c810f32b809079e5 62f8ead2522c6b7b
Msg	6bc1bee22e409f96e93d7e117393172a ae2d8a571e03ac9c9eb76fac45af8e51 30c81c46a35ce411
Tag	b35e2d1b73aed49b78bdbdfe61f646df

2.2.4 Test Vector for 64-Byte Message

K	8e73b0f7da0e6452c810f32b809079e5 62f8ead2522c6b7b
Msg	6bc1bee22e409f96e93d7e117393172a ae2d8a571e03ac9c9eb76fac45af8e51 30c81c46a35ce411e5fbc1191a0a52ef f69f2445df4f9b17ad2b417be66c3710
Tag	a1d5df0eed790f794d77589659f39a11

2.3 OMAC-AES-256

2.3.1 Test Vector for the Empty String

K	`603deb1015ca71be2b73aef0857d7781`
	`1f352c073b6108d72d9810a30914dff4`
Msg	⟨empty string⟩
Tag	`47fbde71866eae6080355b5fc7ff704c`

2.3.2 Test Vector for 16-Byte Message

K	`603deb1015ca71be2b73aef0857d7781`
	`1f352c073b6108d72d9810a30914dff4`
Msg	`6bc1bee22e409f96e93d7e117393172a`
Tag	`28a7023f452e8f82bd4bf28d8c37c35c`

2.3.3 Test Vector for 40-Byte Message

K	`603deb1015ca71be2b73aef0857d7781`
	`1f352c073b6108d72d9810a30914dff4`
Msg	`6bc1bee22e409f96e93d7e117393172a`
	`ae2d8a571e03ac9c9eb76fac45af8e51`
	`30c81c46a35ce411`
Tag	`f018e6053611b34bc872d6b7ff24749f`

2.3.4 Test Vector for 64-Byte Message

K	`603deb1015ca71be2b73aef0857d7781`
	`1f352c073b6108d72d9810a30914dff4`
Msg	`6bc1bee22e409f96e93d7e117393172a`
	`ae2d8a571e03ac9c9eb76fac45af8e51`
	`30c81c46a35ce411e5fbc1191a0a52ef`
	`f69f2445df4f9b17ad2b417be66c3710`
Tag	`e1992190549f6ed5696a2c056c315410`

Acknowledgement

The authors would like to thank Eisuke Kuroda and Yuki Ohira of Ibaraki University for implementing OMAC and checking the test vectors.

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] T. Iwata and K. Kurosawa. OMAC: One-Key CBC MAC. Cryptology ePrint Archive, Report 2002/180, November 25, 2002, `http://eprint.iacr.org/`.