

The AES-XCBC-PRF-128 Algorithm for  
the Internet Key Exchange Protocol (IKE)

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 (2004). All Rights Reserved.

Abstract

Some implementations of IP Security (IPsec) may want to use a pseudo-random function derived from the Advanced Encryption Standard (AES). This document describes such an algorithm, called AES-XCBC-PRF-128.

1. Introduction

[AES-XCBC-MAC] describes a method to use the Advanced Encryption Standard (AES) as a message authentication code (MAC) whose output is 96 bits long. While 96 bits is considered appropriate for a MAC, it is too short to be useful as a long-lived pseudo-random (PRF) in either IKE version 1 or version 2. Both versions of IKE use the PRF to create keys in a fashion that is dependent on the length of the output of the PRF. Using a PRF that has 96 bits of output creates keys that are easier to attack with brute force than a PRF that uses 128 bits of output.

Fortunately, there is a very simple method to use much of [AES-XCBC-MAC] as a PRF whose output is 128 bits: omit the step that truncates the 128-bit value to 96 bits.

## 2. The AES-XCBC-PRF-128 Algorithm

The AES-XCBC-PRF-128 algorithm is identical to [AES-XCBC-MAC] except that the truncation step in section 4.3 of [AES-XCBC-MAC] is *\*not\** performed. That is, there is no processing after section 4.2 of [AES-XCBC-MAC].

The test vectors in section 4.6 can be used for AES-XCBC-PRF-128, but only those listed as "AES-XCBC-MAC", not "AES-XCBC-MAC-96".

## 3. Security Considerations

The security provided by AES-XCBC-MAC-PRF is based upon the strength of AES. At the time of this writing, there are no known practical cryptographic attacks against AES or AES-XCBC-MAC-PRF.

As is true with any cryptographic algorithm, part of its strength lies in the security of the key management mechanism, the strength of the associated secret key, and upon the correctness of the implementations in all of the participating systems. [AES-XCBC-MAC] contains test vectors to assist in verifying the correctness of the AES-XCBC-MAC-PRF code. The test vectors all show the full MAC value before it is truncated to 96 bits. The PRF makes use of the full MAC value, not the truncated one.

## 4. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

## 5. References

### 5.1. Normative References

[AES-XCBC-MAC] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

## 6. Author's Address

Paul Hoffman  
VPN Consortium  
127 Segre Place  
Santa Cruz, CA 95060 USA

EMail: paul.hoffman@vpnc.org

## 7. Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

## Acknowledgement

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

