

Internet Draft  
October 2003  
Expiration Date: March 2004

IPsec Working Group  
S. Moriai  
Sony Computer Entertainment Inc.  
S. Okazaki  
NTT Multimedia Communications Laboratories, Inc.  
A. Kato  
NTT Software Corp.

The Camellia Cipher Algorithm and Its Use With IPsec  
<[draft-ietf-ipsec-ciph-camellia-01.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). 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 obsolete 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-Drafts Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This document is a submission to the IETF Internet Protocol Security (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list ([ipsec@lists.tislabs.com](mailto:ipsec@lists.tislabs.com)) or to the editors.

Distribution of this memo is unlimited.

Abstract

This document describes the use of the Camellia block cipher algorithm in Cipher Block Chaining Mode, with an explicit IV, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).

**1. Introduction**

This document describes the use of the Camellia block cipher algorithm in Cipher Block Chaining Mode, with an explicit IV, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).

Camellia was selected as a recommended cryptographic primitive by

the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [[NESSIE](#)] and included in the list of

Moriai, Okazaki, Kato

[Page 1]

cryptographic techniques for Japanese e-Government systems which were selected by the Japan CRYPTREC (Cryptography Research and Evaluation Committees) [[CRYPTREC](#)]. Camellia has been submitted to other several standardization bodies such as ISO (ISO/IEC 18033) , IETF Transport Layer Security working group [[Camellia-TLS](#)] and S/MIME Mail Security [[Camellia-SMIME](#)] and it is under consideration.

Camellia supports 128-bit block size and 128-, 192-, and 256-bit key lengths, i.e. the same interface specifications as the Advanced Encryption Standard (AES) [[AES](#)].

Camellia was jointly developed by NTT and Mitsubishi Electric Corporation in 2000. It was carefully designed to withstand all known cryptanalytic attacks and even to have a sufficiently large security leeway for use of the next 10-20 years. It has been scrutinized by worldwide cryptographic experts.

Camellia was also designed to have suitability for both software and hardware implementations and to cover all possible encryption applications that range from low-cost smart cards to high-speed network systems. Compared to the AES, Camellia offers at least comparable encryption speed in software and hardware. An optimized implementation of Camellia in assembly language can encrypt on a Pentium III (1.13GHz) at the rate of 471 Mbits per second. In addition, a distinguishing feature is its small hardware design. The current smallest hardware implementation, which includes encryption, decryption, and the key schedule for 128-bit keys, occupies only 8.12K gates using a 0.18um CMOS ASIC library [[Camellia](#)]. This is in the smallest class among all existing 128-bit block ciphers. It perfectly meets one of the current IPsec market requirements, where low power consumption is a mandatory condition.

The remainder of this document specifies the use of Camellia within the context of IPsec ESP. For further information on how the various pieces of ESP fit together to provide security services, please refer to [[ARCH](#)], [[ESP](#)], and [[ROAD](#)].

### **1.1 Specification of Requirements**

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" that appear in this document are to be interpreted as described in [[RFC-2119](#)].

## **2. The Camellia Cipher Algorithm**

All symmetric block cipher algorithms share common characteristics and variables, including mode, key size, weak keys, block size, and rounds. The following sections contain descriptions of the relevant

characteristics of Camellia.

The algorithm specification and object identifiers are described in [Camellia-ID]. The Camellia homepage, <http://info.isl.ntt.co.jp/camellia/>, contains a wealth of information

about camellia, including detailed specification, security analysis, performance figures, reference implementation, test vectors, and intellectual property information.

## **2.1 Mode**

NIST has defined 5 modes of operation for AES and other FIPS-approved ciphers [[MODES](#)]: CBC (Cipher Block Chaining), ECB (Electronic CodeBook), CFB (Cipher FeedBack), OFB (Output FeedBack) and CTR (Counter). The CBC mode is well-defined and well-understood for symmetric ciphers, and is currently required for all other ESP ciphers. This document specifies the use of the Camellia cipher in CBC mode within ESP. This mode requires an Initialization Vector (IV) that is the same size as the block size. Use of a randomly generated IV prevents generation of identical ciphertext from packets which have identical data that spans the first block of the cipher algorithm's block size.

The IV is XOR'd with the first plaintext block before it is encrypted. Then for successive blocks, the previous ciphertext block is XOR'd with the current plaintext, before it is encrypted.

More information on CBC mode can be obtained in [[MODES](#), [CRYPTO-S](#)]. For the use of CBC mode in ESP with 64-bit ciphers, please see [[CBC](#)].

## **2.2 Key Size**

Camellia supports three key sizes: 128 bits, 192 bits, and 256 bits. The default key size is 128 bits, and all implementations **MUST** support this key size. Implementations **MAY** also support key sizes of 192 bits and 256 bits.

Camellia uses a different number of rounds for each of the defined key sizes. When a 128-bit key is used, implementations **MUST** use 18 rounds. When a 192-bit key is used, implementations **MUST** use 24 rounds. When a 256-bit key is used, implementations **MUST** use 24 rounds.

## **2.3 Weak Keys**

At the time of writing this document there are no known weak keys for Camellia.

## **2.4 Block Size and Padding**

Camellia uses a block size of sixteen octets (128 bits).

Padding is required by the algorithms to maintain a 16-octet (128-bit) blocksize. Padding **MUST** be added, as specified in [[ESP](#)], such that the data to be encrypted (which includes the ESP Pad Length

and Next Header fields) has a length that is a multiple of 16 octets.

Because of the algorithm specific padding requirement, no additional padding is required to ensure that the ciphertext terminates on a

4-octet boundary (i.e. maintaining a 16-octet blocksize guarantees that the ESP Pad Length and Next Header fields will be right aligned within a 4-octet word). Additional padding MAY be included, as specified in [ESP], as long as the 16-octet blocksize is maintained.

## **2.6 Performance**

Performance figures of Camellia are available at <http://info.isl.ntt.co.jp/camellia/>. It also includes performance comparison with the AES cipher and other AES finalists. [NESSIE] project has reported performance of Optimized Implementations independently.

## **3. ESP Payload**

Camellia was designed to follow the same API as the AES cipher. Therefore, any consideration related to ESP payload is the same as that of the AES cipher. Details can be found in [AES-IPSEC].

## **4. Interaction with IKE**

Camellia was designed to follow the same API as the AES cipher. Therefore, this section defines only Phase 1 Identifier and Phase 2 Identifier. Any other consideration related to interaction with IKE is the same as that of the AES cipher. Details can be found in [AES-IPSEC].

### **4.1 Phase 1 Identifier**

For Phase 1 negotiations, IANA has assigned an Encryption Algorithm ID of (TBD) for CAMELLIA-CBC.

### **4.2 Phase 2 Identifier**

For Phase 2 negotiations, IANA has assigned an ESP Transform Identifier of [TBD] for ESP\_CAMELLIA.

## **5. Security Considerations**

Implementations are encouraged to use the largest key sizes they can when taking into account performance considerations for their particular hardware and software configuration. Note that encryption necessarily impacts both sides of a secure channel, so such consideration must take into account not only the client side, but the server as well. However, a key size of 128 bits is considered secure for the foreseeable future.

No security problem has been found on Camellia [CRYPTREC][NESSIE].

## **6. 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.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

## 7. References

- [AES] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001.  
<http://csrc.nist.gov/publications/fips/fips197/fips-197.{ps,pdf}>.
- [AES-IPSEC] Frankel, S., S. Kelly, and R. Glenn, "The AES Cipher Algorithm and Its Use With IPsec," [RFC 3602](#), September, 2003.
- [ARCH] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.
- [Camellia] Aoki, K, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms," September, 2001, <http://info.isl.ntt.co.jp/camellia/CRYPTREC/2001/01eeval.pdf>.
- [Camellia-ID] Nakajima, J. and S. Moriai, "A Description of the Camellia Encryption Algorithm," [draft-nakajima-camellia-02.txt](#), July, 2001.
- [Camellia-TLS] Moriai, S., "Addition of the Camellia Encryption

Algorithm to TLS," [draft-ietf-tls-camellia-03.txt](#),  
June, 2003.

[Camellia-SMIME]

Moriai, Okazaki, Kato

[Page 5]

Moriai, S. and Kato, A., "Use of the Camellia Encryption Algorithm in CMS",  
[draft-ietf-smime-camellia-05.txt](#), August 2003.

- [CBC] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms," [RFC 2451](#), November 1998.
- [CRYPTO-S] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1995, ISBN 0-471-12845-7.
- [CRYPTREC] Information-technology Promotion Agency (IPA), Japan, CRYPTREC.  
<http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html>.
- [DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP," [RFC 2407](#), November 1998.
- [ESP] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [IKE] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.
- [MODES] Symmetric Key Block Cipher Modes of Operation,  
<http://www.nist.gov/modes/>.
- [NESSIE] The NESSIE project (New European Schemes for Signatures, Integrity and Encryption),  
<http://www.cosic.esat.kuleuven.ac.be/nessie/>.
- [RFC-2026] Bradner, S., "The Internet Standards Process -- Revision 3", [RFC2026](#), October 1996.
- [RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC-2119](#), March 1997.
- [ROAD] Thayer, R., N. Doraswamy and R. Glenn, "IP Security Document Roadmap", [RFC 2411](#), November 1998.

## **8. Authors' Addresses**

Shiho Moriai  
Sony Computer Entertainment Inc.  
Phone: +81-3-6438-7523  
FAX: +81-3-6438-8629  
Email: [camellia@isl.ntt.co.jp](mailto:camellia@isl.ntt.co.jp) (Camellia team)  
[shiho@rd.scei.sony.co.jp](mailto:shiho@rd.scei.sony.co.jp) (Shiho Moriai)

Satomi Okazaki  
NTT Multimedia Communications Laboratories, Inc.  
250 Cambridge Avenue, Suite 300

Moriai, Okazaki, Kato

[Page 6]

Palo Alto, CA 94306, USA  
Phone: +1-650-833-3631  
FAX: +1-650-326-1878  
Email: satomi@nttmcl.com

Akihiro Kato  
NTT Software Corporation  
Phone: +81-45-212-7404  
FAX: +81-45-212-7410  
Email: akato@po.ntts.co.jp

## **9. Full Copyright Statement**

Copyright (C) The Internet Society (1998). 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 assigns.

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 MERCHANT ABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

