

Network Working Group
Internet Draft
March 2005
Expiration Date: June 2005

A. Kato
NTT Software Corporation
S. Moriai
Sony Computer Entertainment Inc.
M. Kanda
Nippon Telegraph and Telephone Corporation
March 2005

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

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [section 3 of RFC 3667](#). By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with [RFC 3668](#).

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 obsoleted 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/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This document may not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

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

1. Introduction

Camellia was selected as a recommended cryptographic primitive by

Kato, Moriai, Kanda

[Page 1]

Internet-Draft

The Use of Camellia with IPsec

March 2005

the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [[NESSIE](#)] and included in the list of cryptographic techniques for Japanese e-Government systems, which were selected by the Japan CRYPTREC (Cryptography Research, Evaluation Committees) [[CRYPTREC](#)]. Camellia has been submitted to other several standardization bodies such as ISO (ISO/IEC 18033) and IETF S/MIME Mail Security Working Group [[Camellia-CMS](#)].

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. 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. Camellia has a Feistel structure, which is different from AES. It is rich for the IPsec community that has block cipher in which was well verified by the cryptographic expert with another structure. In addition, a distinguishing feature is its small hardware design.

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.

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

Kato, Moriai, Kanda

[Page 2]

Internet-Draft

The Use of Camellia with IPsec

March 2005

[\[Camellia-Desc\]](#).

[2.1. Mode](#)

NIST has defined 5 modes of operation for AES and other FIPS-approved ciphers [\[SP800-38a\]](#): 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 cipher text from packets, which have identical data that spans the first block of the cipher algorithm's block size.

The CBC IV is XOR'd with the first plaintext block before it is encrypted. Then for successive blocks, the previous cipher text block is XOR'd with the current plain text, 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) block size. 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 block size guarantees that the ESP Pad Length and Next Header fields will be right aligned

Kato, Moriai, Kanda

[Page 3]

Internet-Draft

The Use of Camellia with IPsec

March 2005

within a 4-octet word). Additional padding MAY be included, as specified in [ESP], as long as the 16-octet block size 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

The ESP payload is made up of the IV followed by raw cipher-text. Thus the payload field, as defined in [ESP], is broken down according to the following diagram:

```
+-----+-----+-----+-----+
|                                             |
```


For Phase 1 negotiations, IANA has assigned an Encryption Algorithm ID of (TBD1) for CAMELLIA-CBC.

[4.2.](#) Phase 2 Identifier

For Phase 2 negotiations, IANA has assigned an ESP Transform Identifier of (TBD2) 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 affects 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.](#) IANA Considerations

IANA has assigned Encryption Algorithm ID (TBD1) to CAMELLIA-CBC. IANA has assigned ESP Transform Identifier (TBD2) to ESP_CAMELLIA.

[7.](#) Acknowledgments

Portions of this text were unabashedly borrowed from [[AES-IPSEC](#)].

This work was done when the first author worked for NTT.

[8.](#) References

[8.1.](#) Normative References

- [Camellia-Desc] Matsui, M., Nakajima, J., Moriai, S., "A Description of the Camellia Encryption Algorithm", [RFC3713](#), April 2004.
- [ESP] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [CBC] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms," [RFC 2451](#), November 1998.

8.2 Informative 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-CMS] Moriai, S. and Kato, A., "Use of the Camellia Encryption Algorithm in CMS", January 2004, [RFC3657](#).
- [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>.
- [IKE] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.
- [SP800-38a] Dworkin, M., "Recommendation for Block Cipher Modes of Operation – Methods and Techniques", NIST Special Publication 800-38A, December 2001.
- [NESSIE] The NESSIE project (New European Schemes for Signatures, Integrity and Encryption),
<http://www.cosic.esat.kuleuven.ac.be/nessie/>.
- [ROAD] Thayer, R., N. Doraswamy and R. Glenn, "IP Security Document Roadmap", [RFC 2411](#), November 1998.
- [RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC-2119](#), March 1997.

9. Authors' Addresses

Akihiro Kato
NTT Software Corporation
Phone: +81-45-212-7934
FAX: +81-45-212-7410

Email: akato@po.ntts.co.jp

Shiho Moriai
Sony Computer Entertainment Inc.

Kato, Moriai, Kanda

[Page 6]

Internet-Draft

The Use of Camellia with IPsec

March 2005

Phone: +81-3-6438-7523
FAX: +81-3-6438-8629
Email: camellia@isl.ntt.co.jp (Camellia team)
shiho "at" rd.scei.sony.co.jp (Shiho Moriai)

Masayuki Kanda
Nippon Telegraph and Telephone Corporation
Phone: +81-46-859-2437
FAX: +81-46-859-3365
Email: kanda@isl.ntt.co.jp

10. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

11. Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.