NEWS RELEASE

NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

July 20, 2005

Japan's First 128-bit Block Cipher "Camellia" Approved as a New Standard Encryption Algorithm in the Internet

Nippon Telegraph and Telephone Corporation (NTT) and Mitsubishi Electric Corporation (Mitsubishi) jointly developed in 2000 the 128-bit block cipher[*1] algorithm "Camellia." On this occasion, as the first Japanese encryption algorithm, Camellia was adopted as a new standard encryption algorithm (Standard Track RFC[*2]) in three major Internet secure protocols, SSL/TLS[*3], S/MIME[*4], and XML[*5]. Furthermore, the deliberations by the IETF[*6] have approved addition of Camellia into IPsec[*7] protocol, and Camellia will be adopted this fall.
As an encryption scheme with the world's highest level of excellent security and performance, Camellia was adopted as International standardization specification and recommended specification, the EU recommended cipher[*8], E-government recommended cipher[*9], ISO/IEC international standard cipher[*10], etc., and it was acknowledged as the standard that should be implemented in the Internet for the next generation encryption scheme.

Background and Significance of Standardization

Camellia is internationally recognized as the representative of Japanese ciphers and as the unique 128-bit block cipher that possesses the security level and processing capability equivalent to AES[*11]. Indeed, Camellia was selected as the EU recommended cipher and E-government recommended cipher in 2003 and was also adopted as the ISO/IEC international standard cipher recently.
Still, when using Web services such as online shopping and Internet banking, people generally take advantage of the SSL/TLS with which web browsers used on the Internet are standard-equipped. This also applies to the Web services in the E-government system.
The ciphers that are standard-equipped with the Web browsers are limited to those adopted by IETF as the SSL/TLS standard. This means that if Camellia were not adopted by the SSL/TLS standard, Camellia would not be able to be used with the Web services even in the E-government system, despite the fact that Camellia was already selected as the E-government recommended cipher.
In short, only in technical superiority of the algorithm and the adoption as de jure standard etc., it was insufficient as the environment that can be widely used for products and services.

In regard with the major encrypted communication protocols such as SSL/TLS and S/MIME, IETF adopted as standard Internet ciphers Triple DES, IDEA, RC2 and RC4 which were created prior to 1995 and hence available at the time of standardizing the protocols. Among these, Triple DES and RC4 are still currently used as standards. However, along with the recent progress in cipher research, anxiety has arisen regarding the security of these standard ciphers. To address this, the IETF has conducted additional investigations on the next generation encryption schemes, especially the 128-bit block ciphers that are recommended internationally as next generation ciphers and are secure than 64-bit block cipher Triple DES and RC4 to which weakness is pointed out.

Camellia was evaluated to have the world's highest level of excellent security and performance. It was also adopted into various standard/recommended specifications. As a result, Camellia was approved for adoption as a next generation Internet standard encryption specification for SSL/TLS and represents the first Japanese cipher algorithm to achieve this status. The IETF has also adopted or slated for adoption Camellia as IPsec, S/MIME, XML.

In regard to this, up until now aside from Camellia's adoption as the EU recommended cipher and E-government recommended cipher, in May of this year it was adopted as the ISO/IEC next generation international standard cipher. In light of this, Camellia should also be implemented as an Internet standard next generation encryption scheme. Accordingly, in the future, based on various systems such as the E-government system, Internet banking, and online shopping that use very convenient Internet communication methods, the Japanese encryption algorithm can be used for the first time as an Internet standard cipher.

The IETF has adopted or slated for adoption of only Camellia, AES, and SEED[*12], as the next generation Internet standard ciphers. These are corresponding to 128 bit block ciphers adopted for the ISO/IEC international standard cipher as the next generation standard.

Future Expansion

This time, in addition to adoption by the three main encryption evaluation/standardization projects supported by Japan (E-government cipher recommendation), the EU (EU cipher recommendation), and internationally (ISO/IEC international standard cipher), through the adoption of Camellia, we anticipate that Japanese encryption technology will be further broadly utilized as an international specification.

In order for Camellia to be more widely used, NTT continues on installing it into security products employing SSL/TLS. In addition to actively promoting the development of Camellia-equipped product and services, in order to contribute to achieving a truly secure information society, NTT will continue to actively pursue research and development in the future.

From the viewpoint of the early proliferation of Camellia as a world de facto standard, we will enrich the Camellia-equipped product line, and encourage other companies interested in Camellia to expand Camellia-equipped products through the royalty-free licensing of the essential patents.

<Reference>

RFC Numbers of Camellia

- RFC 3657 [Standard Track - Proposed Standard]:
Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)
- RFC 3713 [Non-standard Track - Informational]:
A Description of the Camellia Encryption Algorithm
- RFC 4051 [Standard Track - Proposed Standard]:
Additional XML Security Uniform Resource Identifiers (URIs)
- RFC 4132 [Standard Track - Proposed Standard]:
Addition of Camellia Cipher Suites to Transport Layer Security (TLS)
- RFC Ed Queue [Standard Track - Proposed Standard]:
The Camellia Cipher Algorithm and Its Use With IPsec

Features of Camellia

Camellia is a 128-bit block cipher (key lengths of 128, 192, and 256 bits) with the world's highest level of excellent security and performance. High-speed software implementation independent of the platform such as PC or IC cards, and the world's smallest hardware implementation that provides the highest level of processing efficiency can be achieved. In particular, Camellia differs from AES in terms of implementation. Since encryption processing and decryption processing are achieved using the same structure in Camellia, it exhibits superior performance particularly in IC cards that have a low capacity memory or compact hardware.

Furthermore, over several years, cryptographers around the world have conducted thorough evaluation of Camellia. The security of Camellia is very high, and the processing speed is several times or more as high-speed as that of 64 bit block cipher of the main current now, Triple DES etc.

Camellia is the only world's 128-bit block cipher which has the equivalent security and processing efficiency as AES. As Japan's representative, this cipher has gained international recognition. Actually, because Camellia has a different cipher structure[*13] compared to AES and since a sufficiently large security margin[*14] is adopted, from a security viewpoint, AES and Camellia are selected for many standardization/recommended specifications.

In order to fulfill a leadership role in establishing a secure high-level information society at a low cost through the spread and promotion of Camellia, the offering of non-exclusively royalty-free licenses of the essential patents for Camellia under reciprocal principles has been put into practice since 2001 to mainly enterprises and corporations that are willing to develop and commercialize products equipped with Camellia based on the disclosed specifications.

Camellia Homepage: http://info.isl.ntt.co.jp/crypt/camellia/index.html
Camellia News Releases:
http://www.ntt.co.jp/news/news00/0003/000310.html
http://www.mitsubishielectric.co.jp/news/2000/0310.htm

<Glossary>

*1 128-bit block cipher
The 128-bit block cipher is a symmetric key encryption that encrypts data in 128-bit long (the size of the data bundle) blocks. Symmetric key encryption is an encryption scheme that uses the same secret key to encrypt and decrypt data. Since it achieves high-speed encryption processing, it is used widely in various applications such as communication sessions that deal with large-volume data, file encryption, and mobile terminal authentication.

64-bit block ciphers (64-bit long blocks) such as Triple DES and MISTY1 were constructed by the mid 1990's and 128-bit block ciphers produced in and after the second half of the 1990's such as Camellia and AES.

*2 Standard Track RFC (Standard Track Request For Comments)
Standard Track RFC is an official draft document opened to the public as specifications for Internet Standard.

The number of RFC is given to all documents that IETF issues. They are classified into Standard Track RFC that IETF is a standard discussion, approves, and manages as the Internet standard, and Non-standard Track RFC opened to the public with aim at the dissemination.

*3 SSL/TLS (Secure Socket Layer /Transport Layer Security)
The Netscape Communications Corporation developed the SSL protocol, which encodes transmitted and received data for Internet communications and provides a secure communications mechanism. The "https:" that precedes Web contents indicates that SSL encrypted communications is utilized.
The Netscape Communications Corporation added a few improvements to the latest SSL version, SSL 3.0, changed the name, and released the protocol as TLS 1.0 instead of SSL 4.0. TLS 1.0 was standardized by the IETF.

*4 S/MIME (Secure/Multipurpose Internet Mail Extensions)
S/MIME is an E-mail encryption scheme proposed by RSA Security Inc. and standardized by the IETF. At the same time that the RSA public key encryption scheme is used to perform automatically functions such as certificate validation and session key encryption, symmetric key encryption based on the session key is used to encrypt and then send or receive messages.

*5 XML (eXtensible Markup Language)
XML is a markup language that is used to describe the meaning and structures of document data. The specification of this language embeds into the structure of the original text specific text strings called "tags." Aside from its use for sending and receiving data between computers, it is supposed to enable the direct reading of the original data using a Web browser. XML is considered to be a future alternative specification to the current Web-page creation language html.

*6 IETF (Internet Engineering Task Force)
The IETF is an internationally open association that establishes Internet standard specifications and deals with generally Internet standards with the exception of issues related to the WWW. The IETF has established a diverse range of protocol specifications from TCP/IP to those for higher-level application layers. The IETF is not an international standardization body such as the International Organization for Standardization (ISO); however, the specifications established by the IETF are actual international standards for the Internet.

*7 IPsec (IP security protocol)
IPsec is a security technology that encrypts and authenticates IP packets, and conducts general-purpose encrypted communications over the Internet in a TCP/IP environment. This protocol is used as an option for IPv4, which is currently used over the Internet, and will be standard-equipped in the next generation IPv6 implementation.

*8 European Union (EU) Recommended Cipher
These are encryption technologies selected based on high-level security and processing efficiency by the New European Schemes for Signature, Integrity, and Encryption (NESSIE) project conducted by the European Union (EU) from 2000 to 2003. Out of the total 44 encryption technologies including 39 submissions, 17 encryption technologies were selected.
The Japanese ciphers Camellia (128-bit block cipher by NTT/Mitsubishi), MISTY1 (64-bit block cipher by Mitsubishi), and PSEC-KEM (Public key encryption by NTT) were selected.

*9 Electronic Government Recommended Cipher
Based on the evaluations and deliberations by the Cryptography Research & Evaluation Committees (CRYPTREC) from 2000 to 2003, encryption technologies were selected from the viewpoint of their possible contribution for use with the Electronic government system with a proper level of security. Out of the total 66

encryption technologies including 52 submissions, 31 encryption technologies were selected.

*10 ISO/IEC International Standard Cipher
This cipher is the first international standard cipher technology selected by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).
Previously the ISO/IEC focused on the standardization of authentication and signature schemes, and was only involved with the application of the encryption algorithm registration scheme (ISO/IEC9979). However, ISO/IEC9979 was replaced and as standardization target of the encryption scheme for 2000, ISO/IEC18033 was specified as the first international standard cipher based on the investigation results from third party evaluation (NESSIE, CRYPTREC, etc.). The 128-bit block ciphers, Camellia, AES, and SEED, are the only ciphers adopted as next generation standards.

*11 AES (Advanced Encryption Standard)
In 2001, the National Institute of Standards and Technology (NIST) established a US Government Standard 128-bit block cipher called the Advanced Encryption Standard. This was based on the Belgian Rijndael cipher, which is an AES winner in The AES project from 1997 to 2000, with the excellent security and processing efficiency characteristics.

*12 SEED
SEED is a 128 bit block cipher of Korea government standard enacted by KISA (Korea Information Security Agency) in 1998. This is different from Camellia and AES, and the length of the key is limited to 128 bits.

*13 Cipher Structure
The block cipher structure can be broadly divided into two types, the Feistel structure employed by ciphers such as DES, Triple DES, MISTY1, and Camellia and the substitution-permutation network (SPN) structure employed by AES. In the former structure, data are divided in half where each half is separately mixed, and in the latter structure, all the data are mixed at one time.
The Feistel structure is constructed such that encryption and decryption are the same processes, and basically the processing for both can be executed in one implementation. Since in the SPN structure encryption and decryption are executed separately, by improving the degree of parallel processing, high speed can be achieved overall.

*14 Security Margin
The security margin is an index that expresses the future expected security level of a block cipher. The index is computed as the ratio of the number of rounds based on the actual specification to the corresponding number of currently breakable rounds, and the larger this ratio is, the stronger we can expect that the resistance against future cryptanalysis methods will become. Furthermore, as new cryptanalytic methods are developed this value will gradually fall, and finally when it drops below one the cipher will be broken.
Incidentally, the security margin for AES is 1.25-1.4 and that for Camellia is 1.80-2.0.

- Fig. 1 Current status of the standardization of block ciphers
- Fig. 2 Description of cipher structure

Contact information

Chizuka, Sano, Ida
The Public Relations Section
The Planning Department
NTT Information Sharing Laboratory Group
Nippon Telegraph and Telephone Corporation
Phone: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp