April 13, 2006

(Press release note)

Nippon Telegraph and Telephone Corporation

128-Bit Block Cipher "Camellia" Announced as Open Source
- Toward Wider and Easier Use of Internationally Standardized Next Generation Japanese Cipher -

On April 13, 2006, Nippon Telegraph and Telephone Corporation (NTT) begins to offer NTT's open source codes of the 128-bit block Cipher[*1] algorithm "Camellia", jointly developed with Mitsubishi Electric Corporation (Mitsubishi) in 2000, using the C and Java languages on the Camellia home page. This is based on the policy of expanding the international infrastructure technology to support a secure advanced information society as the first Japanese encryption algorithm.
The processing speed of the open source codes is approximately three times as fast as the reference code already published on the Camellia home page. NTT also schedules submission of the codes for contribution to various open source communities.

Camellia Home page: http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
Open source page: http://info.isl.ntt.co.jp/crypt/eng/camellia/source.html

BACKGROUND AND SIGNIFICANCE OF OPEN SOURCE ANNOUNCEMENT

Camellia has an international reputation for world's highest security level and processing capability. Indeed, Camellia was already adopted as international standardization specifications and recommended specifications of encryption algorithms, such as the ISO/IEC International standard Ciphers[*2], NESSIE[*3] (New European Schemes for Signatures, Integrity, and Encryption) and CRYPTREC[*4] (CRYPTography Research and Evaluation Committees). As the first Japanese encryption algorithm, Camellia was also accepted as a new standard encryption algorithm (IETF Standard Track RFC[*5]) in major Internet secure protocols, SSL/TLS, IPsec, S/MIME, and XML.
On this occasion, NTT decides to offer an environment of free use of Camellia without concluding royalty-free licensing agreement for essential patents, based on a policy of spreading further the use of Camellia as an international infrastructure technology to support securely advanced information society as the first Japanese encryption algorithm.
Today (April 13, 2006), NTT begins to publish NTT's open source codes of Camellia with free of charge by multiple open source software licenses, and expects that the burden of user's operation is drastically reduced when incorporating Camellia into product development and test applications. This is expected to spread and promote further the use of Camellia.

FEATURES OF CAMELLIA

Camellia is a 128-bit block Cipher (allowing key sizes of 128, 192, and 256 bits), which was jointly developed in 2000 by NTT and Mitsubishi. Camellia possesses the world's highest security level and high-speed software implementation independent of

the platform such as PC or smart cards. Also, the world's smallest level of hardware implementation is achieved which can provide the highest level of processing efficiency.
Furthermore, over several years, cryptographers around the world have conducted thorough evaluation of Camellia. This leads to an international reputation of Camellia, of which the security level is very high and the processing speed is four or five times faster than that of the currently mainstream 64-bit block Ciphers such as Triple DES.
As a result, Camellia is the world's only 128-bit block Cipher that possesses the equivalent security level and processing efficiency as AES[*6], and is internationally recognized as the representative of Japanese Ciphers.
From a security viewpoint, AES and Camellia were selected for many standardization/recommended specifications.

FUTURE PLANS

As an opportunity to publish the Camellia open source codes, NTT offers the codes to the open source communities such as OpenSSL and Linux, and works so that Camellia will become standard-equipped at an early date. In addition, NTT plans to establish a support system for industrial enterprises and corporations that develop products incorporating Camellia to enrich the Camellia-equipped product lines.
In order for Camellia to be more widely used, NTT advances actively the development of Camellia-equipped products and services, such as security products employing SSL/TLS. In addition, NTT continues to pursue research and development in order to contribute to achieving a securely advanced information society.

HANDLING OF ROYALTY-FREE LICENSING AGREEMENT FOR ESSENTIAL PATENTS

Up until now, NTT and Mitsubishi prepare the royalty-free licensing agreement for jointly owned Camellia essential patents mainly for industrial enterprises and corporations that develop products incorporating Camellia. Hereafter, however, in accordance with an agreement between NTT and Mitsubishi, Camellia essential patents can be used at no charge by any Camellia user without concluding such royalty-free licensing agreement hereafter.
Of course, if there is your request, patent execution consent from NTT and Mitsubishi based on the royalty-free licensing agreement for essential patents can be obtained in the same way as up to now.

HISTORY OF CAMELLIA

April 2006	Open source codes of Camellia are released (this release)
December 2005	Camellia is accepted as the IETF standard Cipher for IPsec [RFC4312]
July 2005	Camellia is accepted as the IETF standard Cipher for SSL/TLS Cipher suites [RFC4132]
May 2005	Camellia is adopted as the ISO/IEC standard Cipher [ISO/IEC18033-3]
April 2005	Camellia is accepted as the IETF standard Cipher for XML security URIs [RFC4051]
January 2004	Camellia is accepted as the IETF standard Cipher for S/MIME

	[RFC3657]
February 2003	Camellia is adopted as the DRM encryption by TV-Anytime Forum
February 2003	Camellia is selected as the European recommended Cipher by NESSIE
February 2003	Camellia is selected as the Japanese e-government recommended Cipher by CRYPTREC
April 2001	Camellia royalty-free licenses are prepared
March 2000	Camellia encryption algorithm is released by NTT and Mitsubishi

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.

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

*2 ISO/IEC International Standard Ciphers

The Ciphers are the first international standard encryption algorithms selected by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

In stead of the registration of encryption algorithms (ISO/IEC9979), ISO/IEC18033 was specified as the first international standard Ciphers, based on the investigation results on security and efficiency by third parties (NESSIE, CRYPTREC, etc.). The 128-bit block Ciphers, Camellia, AES, and SEED, are the only Ciphers adopted as next generation standards.

*3 NESSIE (New European Schemes for Signatures, Integrity, and Encryption)

NESSIE is a three-year project for making a portfolio of strong cryptographic primitives starting in 2000 within the Information Societies Technology (IST) Programme of the European Commission. NESSIE selected seventeen algorithms out of 44, including the 39 proposed encryption algorithms. Among the algorithms proposed by Japan, Camellia (a 128-bit block Cipher developed by NTT and Mitsubishi), MISTY1 (a 64-bit block Cipher developed by Mitsubishi) and PSEC-KEM (a public-key encryption algorithms developed by NTT) were adopted.

*4 CRYPTREC (CRYPTography Research and Evaluation Committees)

CRYPTREC was organized to investigate and evaluate cryptographic techniques suitable for the Japanese electronic government in terms of security, implementation, and other characteristics from the viewpoints of various objective specialists. Out of the total 66, including the 52 proposed encryption algorithms, 31 encryption algorithms were selected.

*5 Standard Track RFC (Standard Track Request For Comments)

Standard Track RFC is an official draft document opened to the public as an Internet standard specification (Internet Standard).

An RFC number is assigned to all documents that the IETF issues. These documents are classified into Standard Track RFC for which the IETF conducts standardization discussion, approval, and management as an Internet standard, and Non-standard Track RFC, which are opened to the public with the aim toward dissemination.

*6 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. AES is based on the "Rijndael" algorithms, proposed by J. Daemen and V. Rijmen, whose security and performance levels were considered to be the highest among the proposed algorithms in the AES project (from 1997 to 2000).

Reference
Fig. 1 Standardization of Block Ciphers