Open Source Code Offered for the 128-bit Block Cipher Algorithm Camellia

NTT has decided to offer free use of the 128-bit block cipher algorithm Camellia [1]. This should drastically reduce the burden of incorporating Camellia into product development and test applications. Open source code can be downloaded from the Camellia Web site [2]. Previously, NTT and Mitsubishi Electric Corporation (hereafter Mitsubishi) required industrial enterprises and corporations developing products incorporating Camellia to sign royalty-free licensing agreements for their jointly owned Camellia essential patents. Now, since April 2006, in accordance with an agreement between NTT and Mitsubishi, Camellia essential patents can be used at no charge by any Camellia user without the need to conclude such a royalty-free licensing agreement [3].

NTT plans to offer the code to various open source communities such as OpenSSL and Linux. It also intends to establish a support system for industrial enterprises and corporations developing products incorporating Camellia and is promoting the development of Camellia-equipped products and services, such as security products employing SSL/TLS (secure sockets layer, transport layer security), in order to promote wider use of Camellia to achieve a secure, advanced information society.

As reported in NTT Technical Review earlier this year [4], Camellia is a 128-bit block cipher algorithm (allowing key sizes of 128, 192, and 256 bits) developed jointly between NTT and Mitsubishi in 2000. It possesses the world's highest security level as well as high-speed software implementation independent of the platform, such as personal computer or smart card. It is four or five times faster than current mainstream 64-bit block ciphers, such as Triple DES. It has also achieved the world's smallest level of hardware implementation for a 128-bit block cipher, which enables it to provide the highest level of processing efficiency. As the first Japanese encryption algorithm, Camellia has gained an international reputation because of its high security and processing efficiency. From a security viewpoint, Camellia has been adopted in international standardization specifications and recommended specifications of encryption algorithms. It has also been accepted as a new standard encryption algorithm in major Internet secure protocols.

References

[1] http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
[2] http://info.isl.ntt.co.jp/crypt/eng/camellia/source.html
[3] http://www.ntt.co.jp/news/news06e/0604/060413a.html
[4] M. Kanda, "Promoting the Use of Camellia," NTT Technical Review, Vol. 4, No. 2, pp. 49-53, 2006.

For further information, please contact:
PR, Planning Division
NTT Information Sharing Laboratory Group
T. Chizuka or T. Nakamura
Phone: +81-422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp