FOR INFORMATION
March 10, 2000

Joint Development of Next-Generation Encryption Algorithm "Camellia" by NTT and Mitsubishi Electric

--- Symmetric Block Cipher Achieves High Security and World' Highest Efficiency ---

TOKYO, March 10, 2000-----Nippon Telegraph and Telephone Corporation (NTT) and Mitsubishi Electric Corporation (Mitsubishi) announced today their joint development of "Camellia," a next-generation symmetric-key encryption algorithm (*1).

Next-generation symmetric-key encryption algorithms with high security and efficiency on various platforms are indispensable for ensuring the secrecy of corporate and individual private information in the advanced information society.

The new next-generation encryption algorithm Camellia is a symmetric-key encryption algorithm with a block size (*2) of 128 bits. It was developed by NTT and Mitsubishi using NTT's cipher design technologies geared to high speed software implementation, Mitsubishi's cipher design technologies for compact and high-speed hardware implementation, and state-of-the-art security evaluation technologies of both companies.

Camellia was designed to ensure security in usage for more than 20 years and to provide high speed in software and hardware implementation as well as compactness of hardware chips. Camellia therefore provides world's highest level performance in terms of efficiency and practicality on various platforms.

Background

As the Internet has come into wide use, the protection of privacy has become an important issue. Cryptography is one of the keys that enable technology to solve this problem. To provide secure electronic commerce there is a particular need for next-generation encryption algorithms that can ensure both high security and efficiency on various platforms.

Encryption standards are being developed throughout the world. In the USA, the new federal Advanced Encryption Standard (AES)(*3) has been developed as a replacement for DES(*4). In Europe, a project to develop new schemes for signature, integrity and encryption algorithms has begun. In Japan there is a plan for "electronic government" scheduled to start in 2003, in which it is assumed next-generation encryption algorithms will be used.

NTT and Mitsubishi have world top-level researchers in this field, and have jointly developed the next-generation encryption algorithm, "Camellia," each contributing its own strong points. Camellia is characterized by its suitability for both software and

hardware implementation as well as its high level of security. Camellia supports 128-bit block size and 128-, 192-, and 256-bit key length(*5), which is the same interface as AES. From a practical viewpoint, it is designed to enable flexibility in software and hardware implementation including 32-bit processors widely used over the Internet and many applications, 8-bit processors used in smart cards, cryptographic hardware, and embedded systems.

Compared with the AES finalists(*6), the encryption speed is similar or possibly faster in software and hardware implementation. The distinguishing characteristic is the smallest 128-bit block cipher hardware in the world.

Technical Features

(1) Standard interface of next generation symmetric block ciphers(*7)
Most block ciphers in use now encrypt data in the block size of 64 bits. In the coming years block ciphers with a block size of 128 bits will be also be required to improve security. The block size of AES is 128 bits. The proposed encryption algorithm Camellia adopts has a block size of 128 bits and key sizes of 128, 192, and 256 bits.

(2) High level of security
Recently, cryptanalytic technology has been making remarkable progress. The quantitative evaluation of security against powerful cryptanalyses, e.g., differential cryptanalysis and linear cryptanalysis, is recognized to be important in designing a new block cipher.

NTT and Mitsubishi evaluated the security of Camellia through the concentrated application of a great deal of cryptanalytic skills. This evaluation has confirmed that Camellia cannot be broken by differential cryptanalysis and linear cryptanalysis. Moreover, Camellia's design takes into account security against other cryptanalytic techniques including related-key attacks, truncated differential cryptanalysis, and slide attacks.

(3) Suitability for multiple platforms
Since information security technology is widely applied, encryption algorithms which can be implemented efficiently in various environments are required. In addition to its high speed, Camellia was designed to provide efficient hardware and software implementation, including gate counts for hardware implementation and RAM requirements for software implementation.

For example, Camellia consists only of substitution tables and logical operations that can be efficiently implemented on a wide variety of platforms. Therefore, it can be implemented in software, including 8-bit processors used in smart cards, 32-bit processors widely used in PCs, and 64-bit processors. An optimized implementation of Camellia in assembly language encrypts on a Pentium III (800MHz) at a speed of 300 Mbits per second, which is more than twice the speed of DES.

Moreover, the substitution tables (s-boxes) are designed to be suitable for small hardware. The key schedule can share a part of data randomizing and the memory requirement for subkeys is reduced. As a result, Camellia encryption hardware achieves a size of approximately 10Kgates, which is in the smallest class in the world for 128-bit block ciphers.

Future Development

NTT and Mitsubishi will propose Camellia in response to calls for contributions from ISO/IEC JTC 1/SC 27 and are aiming at adoption as a international standard.

< Notes >

***1 Symmetric-key encryption algorithm**
An algorithm that uses the same key for both encryption and decryption. Widely used to quickly encrypt large quantities of data in messages or files.

***2 Block size**
The size of the bundle used in block ciphers. DES uses a block size of 64 bits. NIST has mandated a block size of 128 bits for a successor symmetric-key block cipher to improve security.

***3 AES**
Literally "Advanced Encryption Standard." NIST is seeking to establish a successor symmetric-key block cipher to DES by 2001.

***4 DES**
Literally "Data Encryption Standard." A symmetric-key encryption algorithm designated as the standard for encryption by the National Bureau of Standards (now NIST) in 1977. Still widely used for encrypting data sent between banks.

***5 Key length**
Determines the total number of available keys. For example, DES uses a 56-bit key, which means there are 256 possible keys. Longer keys result in encryption that is more resistant to brute force attacks.

***6 AES finalists**
Candidate algorithms for AES. NIST selected five finalists: MARS (U.S.A.), RC6 (U.S.A.), Rijndael (Belgium), Serpent (UK, Israel, Norway), and Twofish (U.S.A.).

***7 Block cipher**
There are two kinds of symmetric-key encryption algorithm: block ciphers and stream ciphers. Block ciphers bundle data into blocks of a certain length and encrypt each block. Stream ciphers encrypt data bit by bit.

***8 Differential cryptanalysis and linear cryptanalysis**
Currently, these techniques are the most effective methods of attacking block ciphers. Both rely on using plaintext-ciphertext pairs to find the key. Compared with brute-force attack, these can break certain block ciphers with fewer computing resources.

***9 ISO/JTC1/SC27**
ISO is the international organization for standardization. JTC1/SC27 is a committee of ISO for standardization of security techniques including encryption algorithms.

Attachment
-Fig1 : Encryption Process of Camellia (Sketch)

Fig2 : F-function and Sub Mixing Function of Camellia (Sketch)
Fig3 : Hardware of Camellia (Sketch)

For further information:

NTT
Kenya Nakatsuka
Press Relations
Tel: 03-5205-5550 Fax. 03-3510-9352
e-mail: info@ml.hco.ntt.co.jp

Mitsubishi Electric Corporation
Matthew Nicholson
PR Dept.
Tel: 03-3218-2346 Fax. 03-3218-2431
e-mail: Matthew.Nicholson@hq.melco.co.jp

NTT NEWS RELEASE