NTT Press Releases

Nippon Telegraph and Telephone Corporation
Mitsubishi Electric Corporation

Camellia Encryption Algorithm Selected for New e-Government Recommended Ciphers List

- Japan's only 128-bit block cipher encryption algorithm to be adopted -

TOKYO, March 26, 2013 - Nippon Telegraph and Telephone Corporation (NYSE: NTT) and Mitsubishi Electric Corporation (TOKYO: 6503) announced today that Camellia, the 128-bit block cipher jointly developed by the two companies in 2000, has been selected for adoption in Japan's new e-Government Recommended Ciphers List as the only 128-bit block cipher encryption algorithm developed in Japan.

The selection is attributed to Camellia's high reputation for ease of procurement, and security and performance features comparable to those of the Advanced Encryption Standard (AES), the de facto standard 128-bit block Cipher adhering to U.S. government standards that was also selected for adoption in the new e-Government Recommended Ciphers List. As a leading technology strengthening the competitiveness of Japanese information security industries, Camellia is recognized as Japan's prime example of 128-bit block cipher algorithms, which are used widely in applications involving large-volume data, such as electronic communications, file encryption and mobile device authentication.

Background

The e-Government Recommended Ciphers List selected by the Cryptography Research and Evaluation Committees (CRYPTREC) consists of recommended cryptographic technologies that offer robust security and processing capabilities, for both software and hardware, and can be applied in system construction. The List, first released in February 2003, recently was updated for the first time in 10 years. Camellia, which also was selected for the original list, was reselected as the only Japanese encryption algorithm among 128-bit block ciphers.

Significance of the adoption

Safety and performance

An encryption algorithm is proven to be secure when it has resisted multiple deciphering attacks over a long period of time. Camellia's security has been continuously tested over a decade by the cryptography research community. Meanwhile, its ability to withstand newly-found attack techniques, including related-key, biclique-based meet-in-the-middle, and rebound attacks, was investigated, but no successful attack has been reported so far. Camellia's level of security therefore surpasses that of AES, which was subject to successful (but impractical) related-key attacks reported on its 192- and 256-bit versions.

Ease of procurement based on extensive applications

NTT and Mitsubishi Electric made essential patents for Camellia available at no cost in 2001, and its source codes were opened in 2006 with the aim of positioning Camellia to play a leading role in the realization of a safe, low-cost and advanced information distribution society. It was the first time in Japan that a well-recognized Japanese cipher source code was opened. Camellia's open-source codes have been provided to world famous open-source projects such as OpenSSL, Firefox, Linux kernel and FreeBSD. Camellia has been adopted by many international standards organizations, including the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and New European Schemes for Signatures, Integrity and Encryption (NESSIE), and Internet standards such as the SSL/TLS security protocol. Most importantly, it is the first time for a cipher developed in Japan to be adopted by Internet-related standards.

Future prospects

NTT and Mitsubishi Electric will continue to research and develop application services and products incorporating Camellia-equipped open-source software and security products to ensure the safety of public and private systems. The companies will thereby contribute to the development of a more secure and advanced information society, covering the management of information such as social security and tax number systems that is expected to be introduced in the future.

PRESS CONTACT

Nippon Telegraph and Telephone Corporation

Service Innovation Laboratory Group
Public Relations, Planning Division
TEL: +81-46-859-2032
E-mail: randd@lab.ntt.co.jp

Mitsubishi Electric Corporation

Public Relations Division
TEL: +81-3-3218-2346
E-mail: prd.gnews@nk.MitsubishiElectric.co.jp

About Nippon Telegraph and Telephone Corporation

NTT Group is the largest provider of wireline and wireless voice, data, leased circuit, telecommunications equipment, and system integration services in Japan, and operates one of the largest telephone networks in the world. Its predominant business is to provide nation-wide telecommunications services. NTT Group's business domain consists of five primary lines of business: regional communications business, long distance and international communications business, mobile communications business, data communications business, and other business. NTT Group reported consolidated revenues of 10.5 trillion yen (US$130billion) for the fiscal year ended March 31, 2012. Over 220,000 NTT Group people support customers in more than 100 countries. For more information, please see www.ntt.co.jp/index_e.html

About Mitsubishi Electric

With over 90 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. Embracing the spirit of its corporate statement, Changes for the Better, and its environmental statement, Eco Changes, Mitsubishi Electric endeavors to be a global, leading green company, enriching society with technology. The company recorded consolidated group sales of 3,639.4 billion yen (US$ 44.4 billion*) in the fiscal year ended March 31, 2012. For more information visit www.MitsubishiElectric.com

*At an exchange rate of 82 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2012

Information is current as of the date of issue of the individual press release.
Please be advised that information may be outdated after that point.

NTT Press Releases Index

NTT Press Releases

- Latest Press Releases
- Back Number
- Japanese is here

Search Among NTT Press Releases

January 1997 - November 2021

Search

▲ Page Top

▸Recent updates ▸Site Map ▸Copyright ▸Privacy Policy ▸Contact