

# Overview



Author: *Mitsuru Matsui\**

Encryption technology is widely utilized in IT systems and products as an indispensable means for protecting personal privacy and corporate confidentiality. We are living in an age where it would be difficult to go about our daily activities without using any encryption even though it may not be directly visible.

The algorithms that support encryption technology are classified according to their properties into various types including common key block encryption, hash functions, and public key encryption. Encryption algorithms are organically integrated to support the security of information communication while sharing their role in the system.

Since 1995, we have developed common key block encryption algorithms, typified by MISTY and Camellia, and released their specifications to the public, and we have also promoted activities for their standardization in and outside Japan. Consequently, the International Organization for Standardization (ISO) currently adopts these encryption algorithms as world standards.

In the meantime, cryptanalysis studies aimed at evaluating the security of encryption algorithms have also made remarkable progress. Recent concerns have surfaced about the future security of some encryption systems currently in wide use, such as hash functions. Therefore, the current encryption system is globally shifting to a new cryptography system.

In addition, the mathematical security of encryption as well as the security of its implementation in both software and hardware must be considered in actual systems. In this respect, the point of contact between encryption technology and physics has widened.

Against this backdrop, Mitsubishi Electric is developing encryption algorithms and information security systems that combine high security against cryptanalysis with high practicality such as compact size and high speed. This issue provides a sampling of our efforts